

Auditing



Michael Woolard

Risk and Compliance Manager

@wooly6bear | <https://wooly6bear.wordpress.com>



ATT&CK Matrix for Enterprise

layout: side ▾

show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques
Active Scanning ⁽³⁾	Acquire Infrastructure ⁽⁷⁾	Drive-by Compromise	Command and Scripting Interpreter ⁽⁸⁾	Account Manipulation ⁽⁵⁾	Abuse Elevation Control Mechanism ⁽⁴⁾	Abuse Elevation Control Mechanism ⁽⁴⁾	Adversary-in-the-Middle ⁽³⁾	Account Discovery ⁽⁴⁾	Exploitation of Remote Services	Adversary-in-the-Middle ⁽³⁾	Application Layer Protocol ⁽⁴⁾
Gather Victim Host Information ⁽⁴⁾	Compromise Accounts ⁽³⁾	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation ⁽⁵⁾	Access Token Manipulation ⁽⁵⁾	Brute Force ⁽⁴⁾	Application Window Discovery	Internal Spearphishing	Archive Collected Data ⁽³⁾	Communication Through Removable Media
Gather Victim Identity Information ⁽³⁾	Compromise Infrastructure ⁽⁷⁾	External Remote Services	Deploy Container	Boot or Logon Autostart Execution ⁽¹⁴⁾	Access Token Manipulation ⁽⁵⁾	BITS Jobs	Credentials from Password Stores ⁽⁵⁾	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	
Gather Victim Network Information ⁽⁶⁾	Develop Capabilities ⁽⁴⁾	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts ⁽⁵⁾	Boot or Logon Autostart Execution ⁽¹⁴⁾	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking ⁽²⁾	Automated Collection	Data Encoding ⁽²⁾
Gather Victim Org Information ⁽⁴⁾	Establish Accounts ⁽³⁾	Phishing ⁽³⁾	Inter-Process Communication ⁽³⁾	Browser Extensions	Boot or Logon Initialization Scripts ⁽⁵⁾	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services ⁽⁶⁾	Browser Session Hijacking	Data Obfuscation ⁽³⁾
Phishing for Information ⁽³⁾	Obtain Capabilities ⁽⁶⁾	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process ⁽⁴⁾	Deobfuscate/Decode Files or Information	Forge Web Credentials ⁽²⁾	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution ⁽³⁾
Search Closed Sources ⁽²⁾	Stage Capabilities ⁽⁶⁾	Supply Chain Compromise ⁽³⁾	Scheduled Task/Job ⁽⁵⁾	Create Account ⁽³⁾	Domain Policy Modification ⁽²⁾	Deploy Container	Input Capture ⁽⁴⁾	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel ⁽²⁾
Search Open Technical Databases ⁽⁵⁾		Trusted Relationship	Serverless Execution	Create or Modify System Process ⁽⁴⁾	Escape to Host	Direct Volume Access	Modify Authentication Process ⁽⁷⁾	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository ⁽²⁾	Fallback Channels
Search Open Websites/Domains ⁽³⁾		Valid Accounts ⁽⁴⁾	Shared Modules	Event Triggered Execution ⁽¹⁶⁾	Event Triggered Execution ⁽¹⁶⁾	Domain Policy Modification ⁽²⁾	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material ⁽⁴⁾	Data from Information Repositories ⁽³⁾	Ingress Tool Transfer
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails ⁽¹⁾	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Multi-Stage Channels
			System Services ⁽²⁾	Hijack Execution Flow ⁽¹²⁾	Hijack Execution Flow ⁽¹²⁾	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Application Layer Protocol
			User Execution ⁽³⁾	Implant Internal Image	Process Injection ⁽¹²⁾	File and Directory Permissions Modification ⁽²⁾	OS Credential Dumping ⁽⁸⁾	Group Policy Discovery		Data from Removable Media	Non-Standard Port
			Windows Management Instrumentation	Modify Authentication Process ⁽⁷⁾	Scheduled Task/Job ⁽⁵⁾	Hide Artifacts ⁽¹⁰⁾	Steal Application Access Token	Network Service Discovery		Data Staged ⁽²⁾	Proxy ⁽⁴⁾
				Hijack Execution Flow ⁽¹²⁾	Valid Accounts ⁽⁴⁾	Hijack Execution Flow ⁽¹²⁾	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection ⁽³⁾	Remote Access Software
						Impair Defenses ⁽⁹⁾		Permission Groups Discovery ⁽³⁾		Input Capture ⁽⁴⁾	Traffic Signaling ⁽²⁾
						Indicator Removal ⁽⁹⁾				Screen Capture	Web Service ⁽³⁾
						Indirect Command Execution					
						Masquerading ⁽⁷⁾					
						Modify Authentication Process ⁽⁷⁾					
						Modify Cloud Compute Infrastructure					



Execution Policy



Execution Policy



AllSigned

Bypass

Default

RemoteSigned

Restricted

Undefined

Unrestricted





Get-CimInstance



Get-CimInstance
-ClassName

Win32_BIOS
Win32_BootConfiguration
Win32_DiskDrive
Win32_GroupUser
Win32_LoggedOnSession
Win32_LogicalDisk
Win32_NetworkAdapterConfiguration
Win32_OperatingSystem
Win32_Process
Win32_Service
Win32_UserAccount
...

Get-CimInstance





Invoke-CimMethod





Get-ItemProperty





Get-WindowsFeature



Get-WindowsFeature

```
> Install-WindowsFeature ServerManager
```





Windows Defender



Windows Defender



Get-MpPreference

Set-MpPreference

Get-MpComputerStatus

Update-MpSignature

Start-MpScan

Remove-MpThreat





Summary



Summary

HoneyPots

- Tokens
- Creds
- Ports
- File
- Services

Maintain the Live Look

Plant Traps Along the Attack Pattern

Audit Your Systems





Web Application Penetration Testing Fundamentals

Getting Started with OWASP Zed Attack Proxy (ZAP)

Automate Web Application Scans with OWASP ZAP and Python

