



RED TEAM ESSENTIALS: A BEGINNER'S GUIDE TO MITRE ATT&CK FRAMEWORK



About CyberWarFare Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. Cyber Range Labs

2. Up-Skilling Platform



INFINITE LEARNING EXPERIENCE

John Sherchan

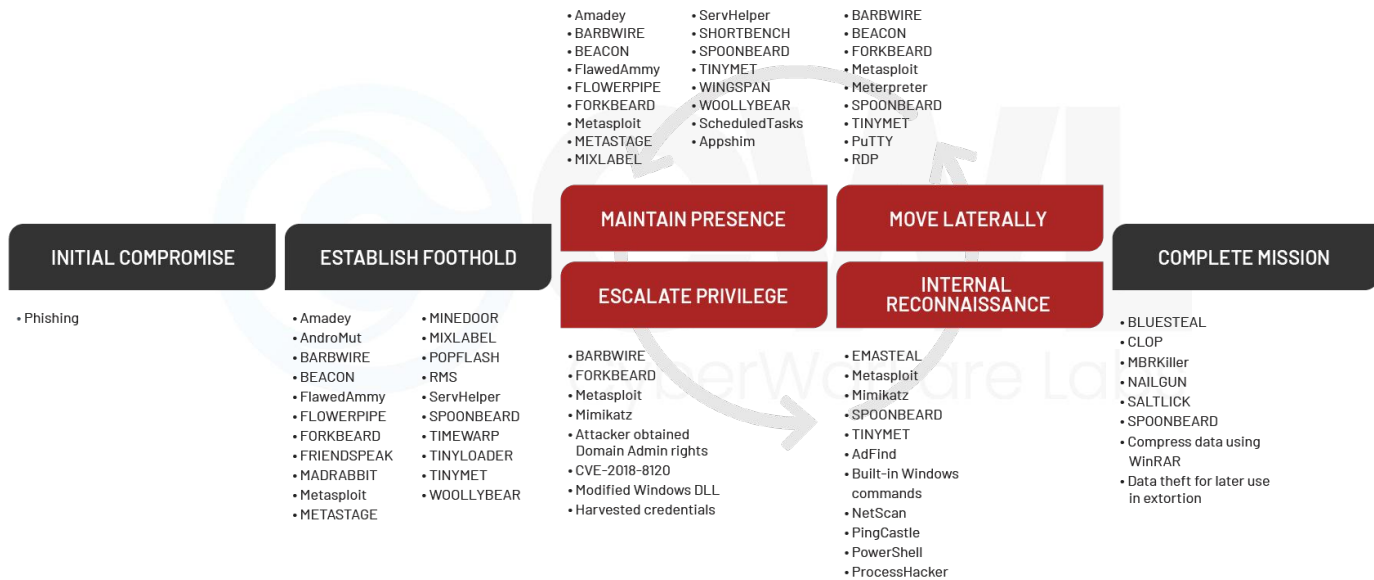
Red Team Security Researcher at CW Labs

He is a Red Team Security researcher, bringing over 5+ years of experience in Reverse Engineering, Malware Analysis/Development, and Source Code Reviewing, with a specialization in Windows Internals (User and Kernel Modes). Demonstrating an advanced understanding, he has successfully reversed multiple Antivirus (AV) and Endpoint Detection and Response (EDR) systems to comprehend its architecture. Committed to advancing cybersecurity, his additional interests include PWNing Active Directory, conducting Adversary emulation/simulation, writing rootkits, crafting exploits, and strategically overcoming challenges.

Red Teaming

- Methodology that organizations follow to reinforce their system's defenses.
- Simulates real-world threats akin to APT's attack or scenarios and tests them against the organization's system.
 - to evaluate the security, effectiveness, resilience of the system,
 - also, the defensive response to the attacks are evaluated

Cyber Attack Lifecycle



MITRE ATT&CK Framework

- Globally accessible framework that outlines adversary tactics & techniques
 - Based on real-world observations
- Aids organizations in comprehending & defending against real-world adversaries
 - foundation for creation of specific threat models and methodologies for:
 - Private sector,
 - government sector,
 - cybersecurity product & service community

MITRE ATT&CK Framework

- Tactics
 - goals the adversaries want to achieve
- Techniques
 - specific methods or ways adversaries use to achieve their goals within a tactic
- Procedures
 - Specific implementation or various techniques used by adversaries
 - vary widely depending on the threat actor

MITRE ATT&CK Framework

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	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	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	Build Image on Host	Credentials from Password Stores (8)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Scripts (5)	Boot or Logon Initialization	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (2)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Data from Cloud Storage	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Financial Theft
Search Open Technical Databases (3)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (3)	Domain or Tenant Policy Modification (2)	Execution Guardrails (1)	Modify Authentication Process (3)	Container and Resource Discovery	Data from Information Repository (2)	Data from Local System	Fallback Channels	Exfiltration Over Web Service (4)	Firmware Corruption
Search Open Websites/Domains (3)	Trusted Relationship	Valid Accounts (4)	Servless Execution	Event Triggered Execution (10)	Event Triggered Execution (10)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Data from Network Shared Drive	Data from Network Shared Media	Hide Infrastructure	Ingress Tool Transfer	Inhibit System Recovery
Search Victim-Owned Websites	Valid Accounts (4)	Software Deployment Tools	System Services (2)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery	Data from Removable Port	Data from Removable Media	Multi-Stage Channels	Non-Application Layer Protocol	Network Denial of Service (2)
	User Execution (3)	Windows Management Instrumentation	Implant Internal Image	Impair Defenses (11)	Impair Defenses (11)	Hide Artifacts (12)	Network Sniffing	Log Enumeration	Data Staged (2)	Email Collection (5)	Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop
	Modify Authentication Process (9)	Scheduled Task/Job (5)	Process Injection (12)	Indicator Removal (9)	Indicator Removal (9)	Hijack Execution Flow (13)	OS Credential Dumping (8)	Network Service Discovery	Input Capture (4)	Screen Capture	Proxy (4)	System Shutdown/Reboot	Resource Hijacking
	Office Application Startup (5)	Power Settings	Scheduled Task/Job (5)	Indirect Command Execution	Indirect Command Execution	Impair Defenses (11)	Stal Application Access Token	Network Share Discovery	Screen Capture	Video Capture	Remote Access Software	System Shutdown/Reboot	Service Stop
	Pre-OS Boot (5)	Scheduled Task/Job (5)	Server Software Component (5)	Massoperading (9)	Massoperading (9)	Impair Defenses (11)	Stal or Forge Kerberos Tickets (4)	Network Sniffing	Input Capture (4)	Video Capture	Traffic Signaling (2)	System Shutdown/Reboot	System Shutdown/Reboot
	Scheduled Task/Job (5)	Server Software Component (5)	Traffic Signaling (2)	Modify Authentication Process (9)	Modify Authentication Process (9)	Impair Defenses (11)	Stal Web Session Cookie	Password Policy Discovery	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Office Application Startup (5)	Office Application Startup (5)	Impair Defenses (11)	Unsecured Credentials (8)	Peripheral Device Discovery	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Power Settings	Power Settings	Impair Defenses (11)	Network Boundary Bridging (1)	Permission Groups Discovery (3)	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Pre-OS Boot (5)	Pre-OS Boot (5)	Impair Defenses (11)	Obfuscated Files or	Process Discovery	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Impair Defenses (11)	Obfuscated Files or	Query Registry	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Server Software Component (5)	Server Software Component (5)	Impair Defenses (11)	Obfuscated Files or	Remote System Discovery	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Traffic Signaling (2)	Traffic Signaling (2)	Impair Defenses (11)	Obfuscated Files or	Software Discovery (1)	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot
	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)	Impair Defenses (11)	Obfuscated Files or	System Information	Screen Capture	Video Capture	Web Service (3)	System Shutdown/Reboot	System Shutdown/Reboot

MITRE Att&CK x Red Teaming

- Provides a structured method for assessment through a comprehensive catalog of adversary tactics and techniques.
- Facilitates realistic threat simulations.
 - Assisting in identifying gaps in security controls by evaluating defenses against current threats.
- Supports the creation of effective training scenarios and skill development.
- Helps document tactics and generate clear, detailed reports.
- Promotes continuous improvement with the latest adversary tactics.

MITRE ATT&CK Navigator

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary in-the-Middle	DNS	Automated Exfiltration	Account Removal
Gather Victim Host Information	Botnet	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	File Transfer Protocols	Data Transfer	Data Destruction
Gather Victim Identity Information	DNS Server Domains	External Application	Container Administration Command	Root of Logon Autostart Execution	Account Taken	Account Taken	Credentials from Password Stores	Browser Information Discovery	Audio Capture	Remote Spearphishing Data	Mail Protocols	Data Streams	Data Encrypted for Impact
Gather Victim Network Information	Acquire Infrastructure	External Remote Services	Server Deployment Services	Boot of Logon Autostart Scripts	Account Manipulation	Account Manipulation	Token Password Stores	Cloud Infrastructure Discovery	Remote Service Hijacking	Cloud Service Dashboard	Web Protocols	Expiration Over Alternative Protocol	Data Manipulation
Gather Victim Org Information	Serverless	Hardware Additions	Virtual Private Server	Exploitation for Client Execution	Boot of Logon Autostart Execution	Boot of Logon Autostart Execution	Exploitation of Credential Access	Cloud Service Dashboard	Remote Session Hijacking	Cloud Service Dashboard	Content Injection	Expiration Over Alternative Protocol	Data Manipulation
Phishing for Information	Web Services	Spearphishing Attachment	Spearphishing Link	Component Object Model	Browser Extensions	Browser Extensions	Forceful Authentication	Cloud Infrastructure Discovery	Remote Session Hijacking	Cloud Service Dashboard	Data Encoding	Endpoint Denial of Service	Denial of Service
Search Closed Sources	Compromise Accounts	Phishing	Spearphishing via Service	Dynamic Data Exchange	Compromise Host Software Binary	Compromise Host Software Binary	Forged Authentication	Cloud Storage Object Discovery	Replication Through Removable Media	Cloud Storage Object Discovery	Data Offuscation	Exfiltration Over Network Channel	Financial Theft
Search Open Technical Databases	Compromise Infrastructure	Spearphishing via Service	Spearphishing via Service	KPI Services	Create Account	Create Account	Input Capture	Container and Resource Discovery	Software Deployment Tools	Container and Resource Discovery	Encrypted Data from Cloud Storage	Exfiltration Over Network Channel	Firmware Corruption
Search Open Websites/Domains	Develop Capabilities	Replication Through Removable Media	Native API	Create or Modify System Process	Create or Modify System Process	Create or Modify System Process	Input Capture	Debugger Evasion	Software Deployment Tools	Debugger Evasion	Dynamic Resuspension	Inhibit System Recovery	Inhibit System Recovery
Search Victim-Owned Websites	Establish Accounts	Schedule Task/Job	Schedule Task/Job	Scheduled Task	Domain or Tenant Policy Modification	Domain or Tenant Policy Modification	Modify Authentication Credentials	Device Driver Discovery	Taint Shared Content	Device Driver Discovery	Encrypted Data from Cloud Storage	Physical Medium	Network Denial of Service
	Artificial Intelligence	Trusted Relationship	Serverless Execution	External Remote Services	Escape to Host	Escape to Host	Multi-Factor Authentication Interception	File and Directory Discovery	Use Alternate Authentication Material	File and Directory Discovery	Hidden Data from Information Repositories	High Availability	Resource Hijacking
	Digital Certificates	Valid Accounts	Shared Modules	Think Execution Flow	Event Triggered Execution	Event Triggered Execution	Multi-Factor Authentication Interception	Hide Artifacts	Group Policy Discovery	File and Directory Discovery	Hidden Data from Information Repositories	High Availability	Service Stop
	Obtain Capabilities	Exploits	Shared Modules	System Services	Modify Authentication Process	Modify Authentication Process	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure
	Malware	Malware	Shared Modules	System Services	Malicious File	Malicious File	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure
	Vulnerabilities	Vulnerabilities	Shared Modules	System Services	Malicious Image	Malicious Image	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure
	Stage Capabilities	Stage Capabilities	Shared Modules	System Services	Malicious Link	Malicious Link	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure
	Upload Malware	Upload Malware	Shared Modules	System Services	Malicious Task	Malicious Task	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure
	Upload Tool	Upload Tool	Shared Modules	System Services	Malicious Task	Malicious Task	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure
			Shared Modules	System Services	Malicious Task	Malicious Task	Network Authentication Request Generation	Hide Artifacts	Log Enumeration	Multi-Factor Authentication Interception	Hidden Data from Information Repositories	High Availability	System Infrastructure



COURSE UNVEILING

CERTIFIED CYBER SECURITY ENGINEER (CCSE)



COURSE IS
NOW LIVE

USE COUPON CODE
"CCSE200FF"

ENROLL NOW

References

- <https://attack.mitre.org/>
- <https://mitre-attack.github.io/attack-navigator/>
- <https://www.mandiant.com/resources/insights/targeted-attack-lifecycle>



Thank You

**For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact**

info@cyberwarfare.live

To know more about our offerings, please visit:

<https://cyberwarfare.live>