CWL
CyberWarFare Labs

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

John Sherchan

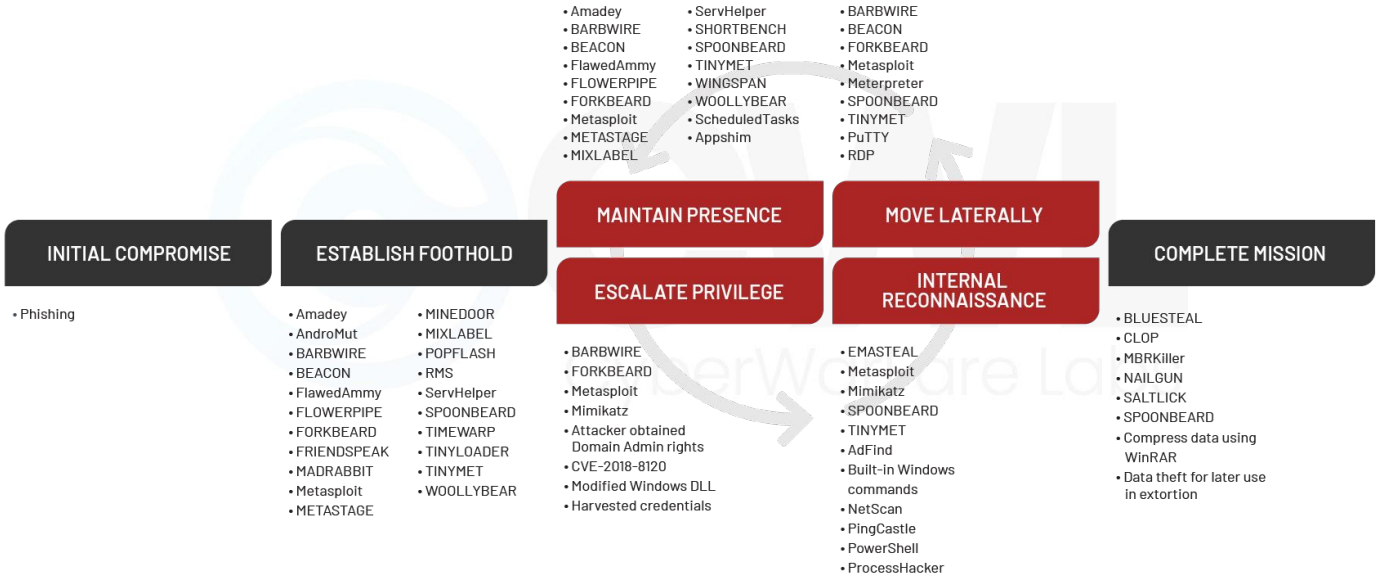
Red Team Security Researcher at CW Labs

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-word adversaries
  - foundation for creation of specific threat models and methodologies for:
    - Private sector,
    - government sector,
    - cybersecurity product & service community

MITRE ATT&CK Framework

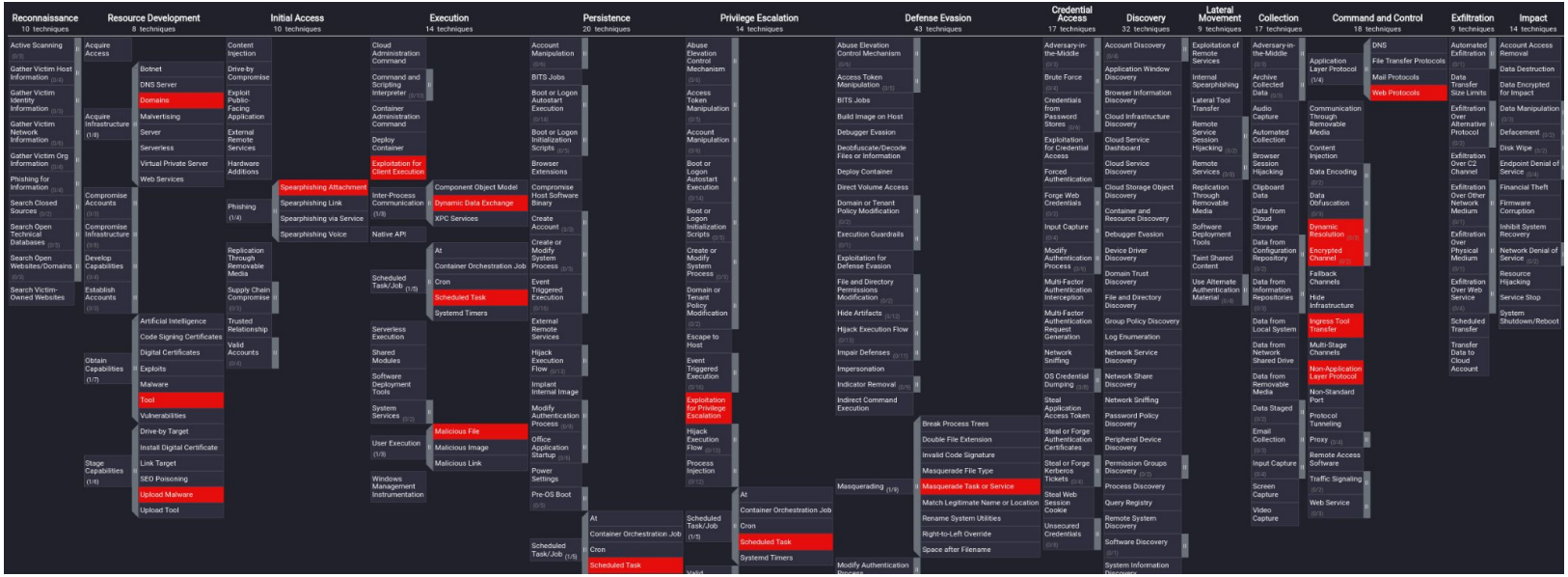
- Tactics
  - goals the adversaries want to achieve
- Techniques
  - specific methods or ways adversaries use to achieve their goals within a tactic
- Procedures
  - Specific implementation or various techniques used by adversaries
    - vary widely depending on the threat actor

MITRE ATT&CK Framework

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



CWL
CyberWarFare Labs

COURSE UNVEILING

CERTIFIED CYBER SECURITY ENGINEER (CCSE)

COURSE IS

NOW LIVE

USE COUPON CODE

"CCSE20OFF"

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