Penetration Testing

CSP010_W_EDUCON

PRESENTATION BY:
CHRISTOS GRIGORIADIS (FOCAL POINT)

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Red Teaming

01. What is Red Teaming
02. Red Teaming vs Pentesting
03. Attack Lifecycle
04. MITRE ATT&CK
05. Atomic Red Introduction

What is Red Teaming

Red Team Operations

- Purpose of Red Team Operations: Simulate full-scope attacks to test security across digital infrastructure, employees, applications, and physical security.
- Simulating Real Adversaries: Replicate techniques used by real-world adversaries to uncover vulnerabilities and assess the company's defensive capabilities.
- Full Attack Lifecycle: Operations span the entire lifecycle of an attack, providing a comprehensive evaluation of security readiness.
- Revealing Vulnerabilities: Identifies multiple attack vectors and weaknesses not typically found in standard penetration tests.

What is Red Teaming

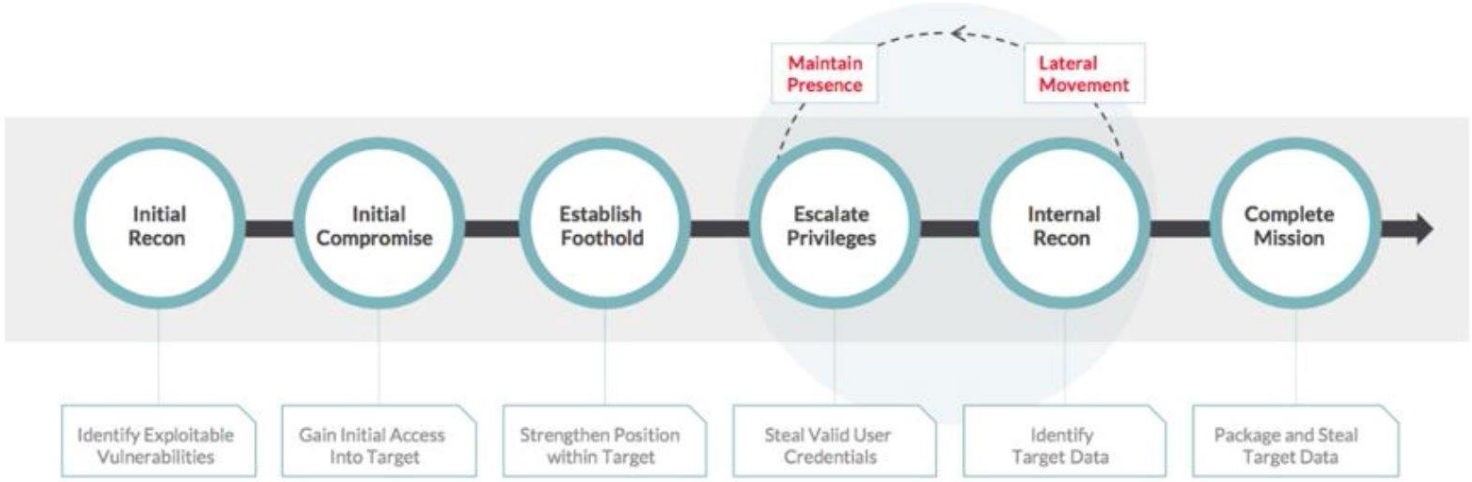
Impact and Integration with Blue Team

- Actionable Results: Red Team findings are used to improve security measures and prepare for potential threats.
- Blue Team Collaboration:
  - Role of Blue Team: Security professionals tasked with vulnerability identification, remediation, and effectiveness verification.
  - Utilizing Results: Develop signatures for malware, implement safeguards, and enhance infrastructure security.
- Training and Hardening:
  - Train employees to resist social engineering.
  - Patch vulnerabilities identified during operations.
  - APT Emulation: Red Teams emulate techniques of Advanced Persistent Threats to test long-term defense mechanisms.

Red Teaming vs Pentesting

Pentesting	Red Teaming
Defined scope	No defined scope
Used to identify and exploit vulnerabilities	Emulates adversary behavior
Provides a report of findings that are consequently used by companies to patch, harden and secure their infrastructure	Used to assess the resilience of an organization against adversaries attacks.
Preventative as opposed to detective. Penetration tests are useful at identifying vulnerabilities and threats, however, they do not provide actionable results that can be used for proactive detection of threats in the future.	Provides actionable results that can be used for detection.

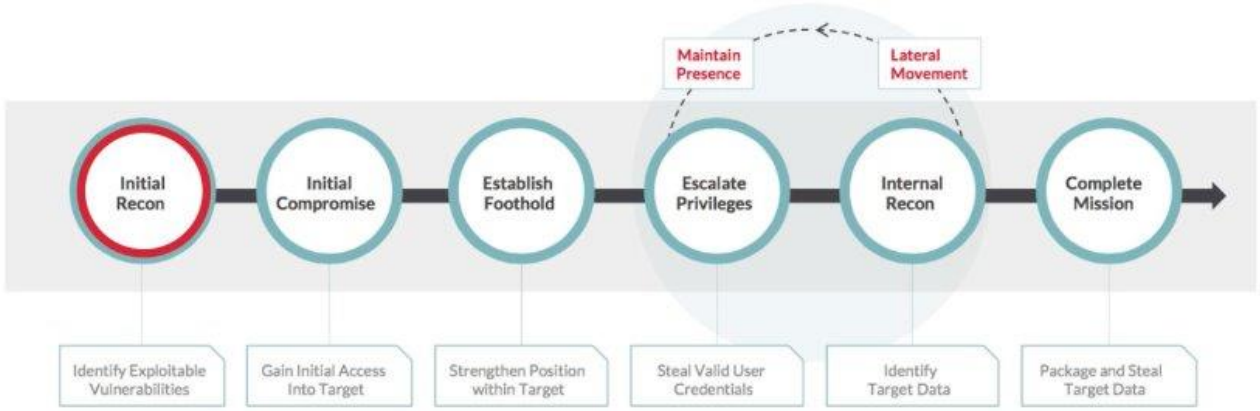
Attack Lifecycle



Attack Lifecycle

Attack Lifecycle – Initial Reconnaissance

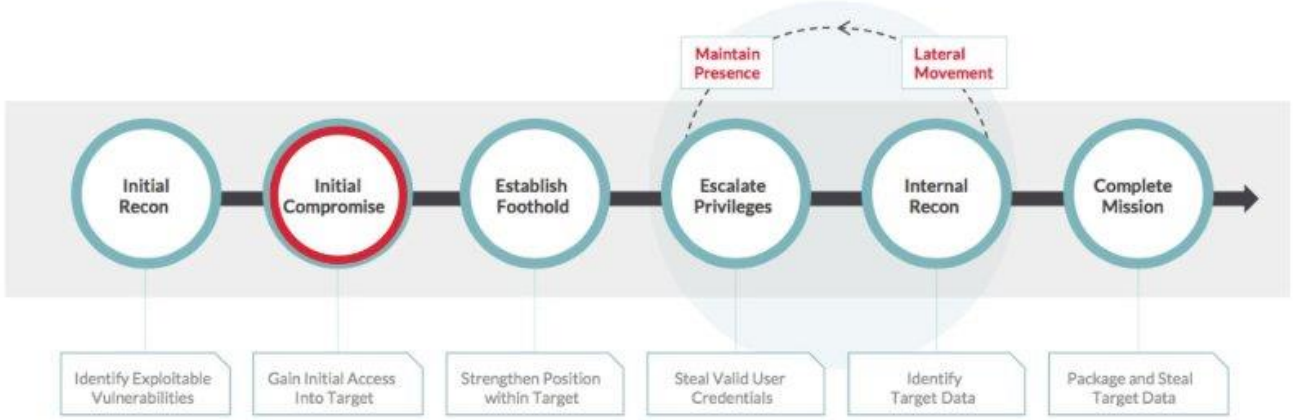
- Open source intelligence gathering
- Network and application reconnaissance
- Remote access identification



Attack Lifecycle

Attack Lifecycle – Initial Compromise

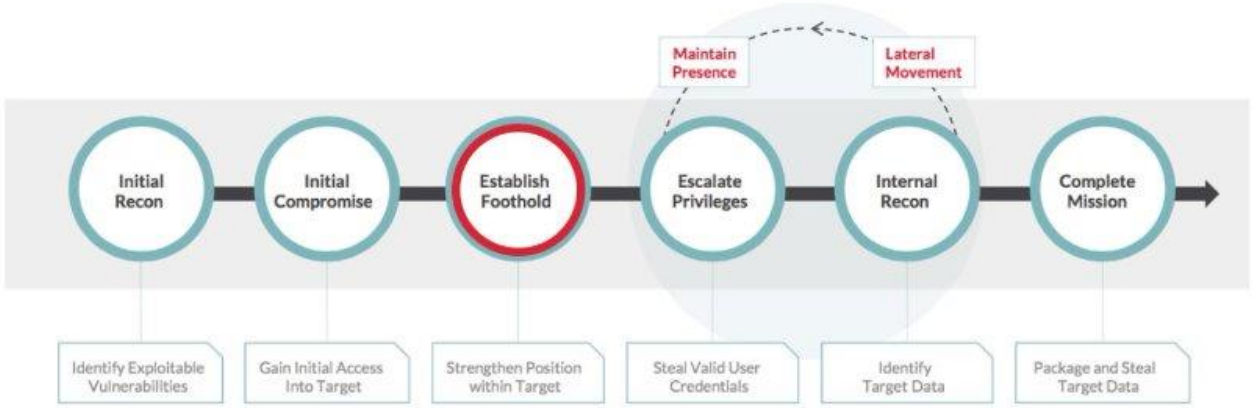
- Social engineering
- Internet-based attack
- Leverage service provider



Attack Lifecycle

Attack Lifecycle – Establish Foothold

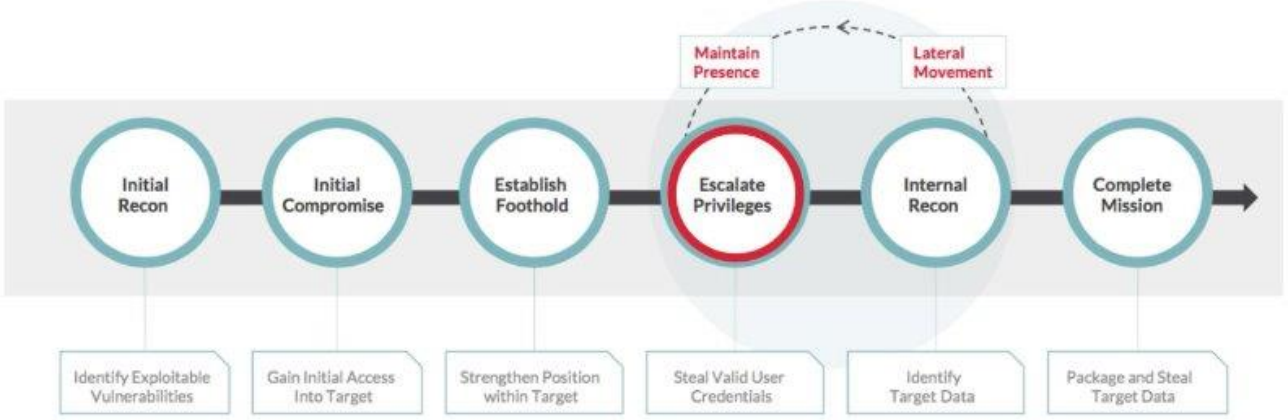
- Backdoors
- Remote access subversion



Attack Lifecycle

Attack Lifecycle – Escalate Privileges

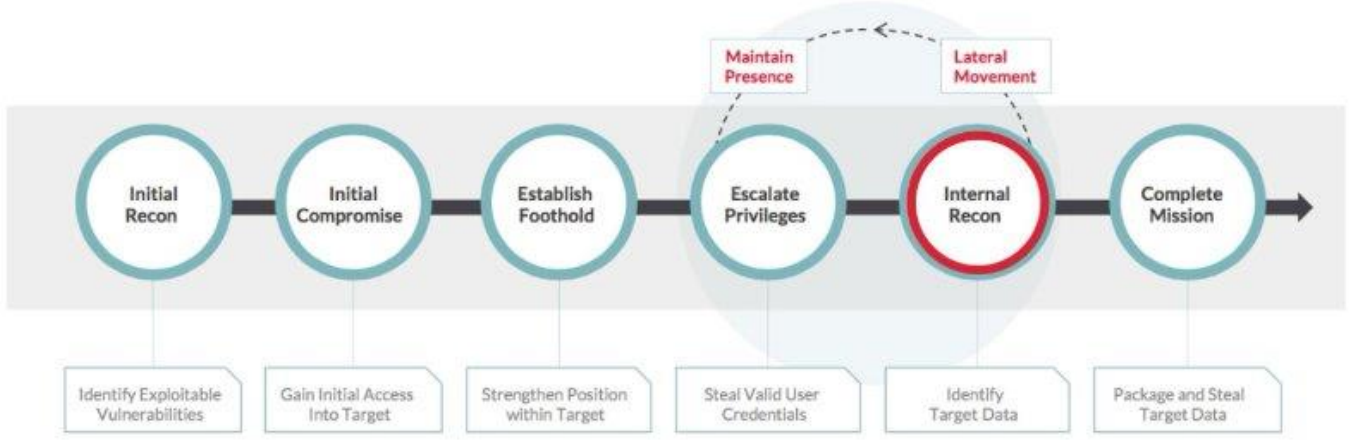
- Credential harvesting
- Password cracking
- Pass-the-Hash



Attack Lifecycle

Attack Lifecycle – Internal Reconnaissance

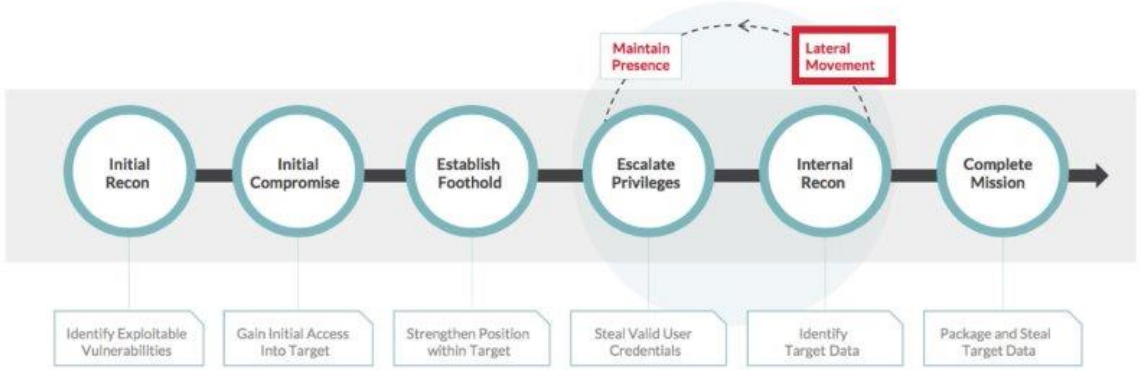
- Critical system identification
- System enumeration
- Account and password enumeration



Attack Lifecycle

Attack Lifecycle – Lateral Movement

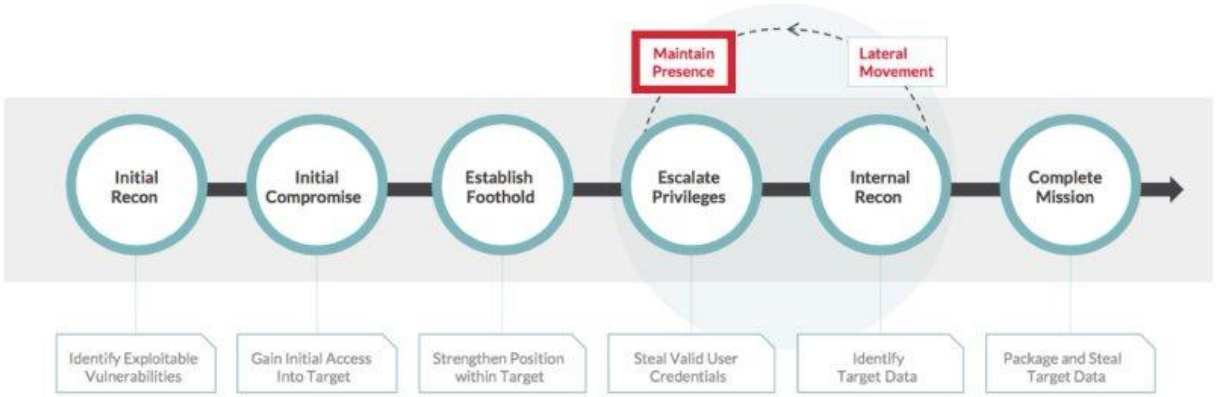
- Remote command execution
- Remote administration tools



Attack Lifecycle

Attack Lifecycle – Maintain Presence

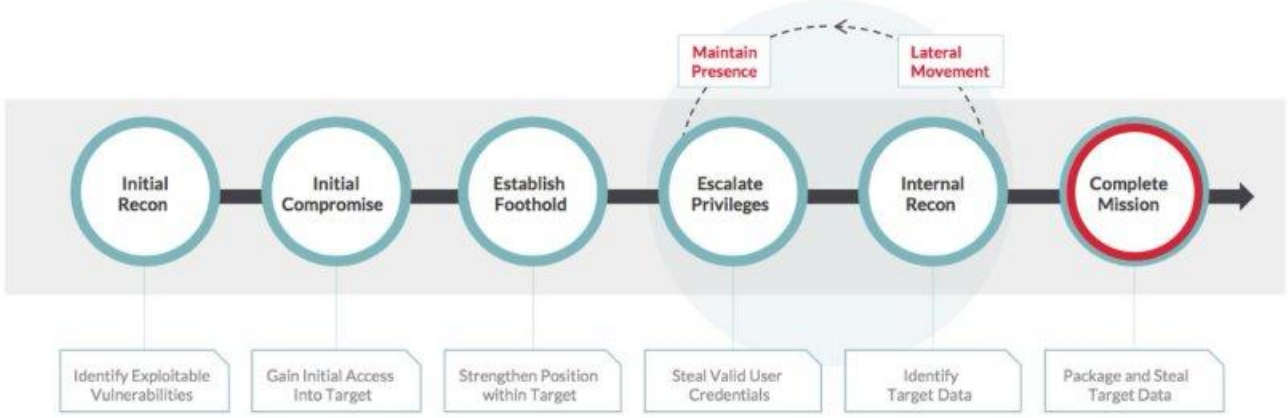
- Command and control
- Remote access subversion
- Account abuse



Attack Lifecycle

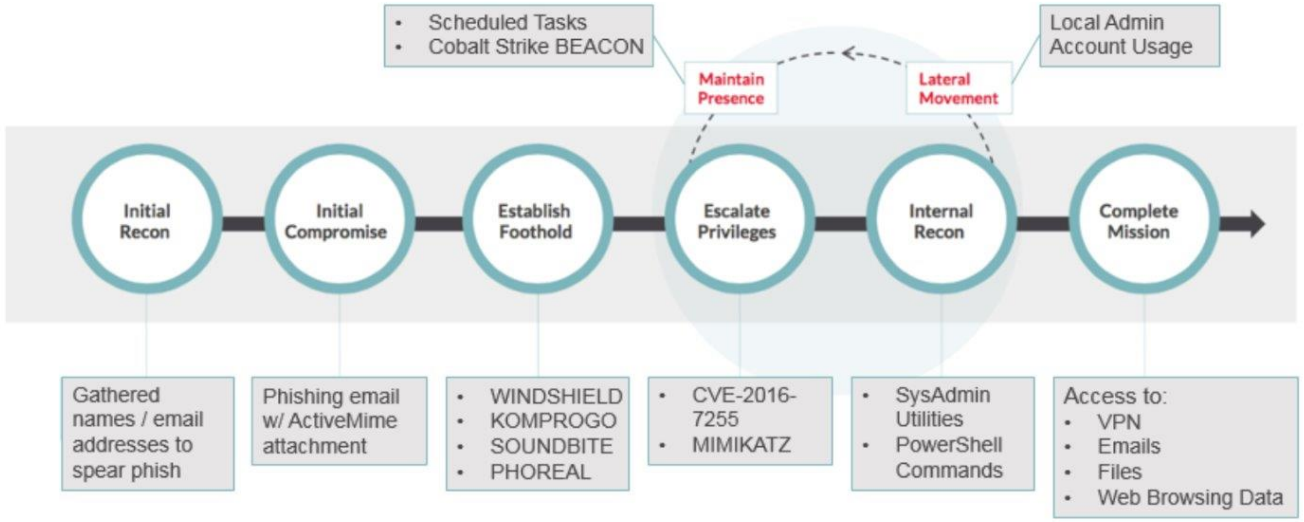
Attack Lifecycle – Complete Mission

- Data staging
- Data exfiltration
- Data modification
- Data destruction

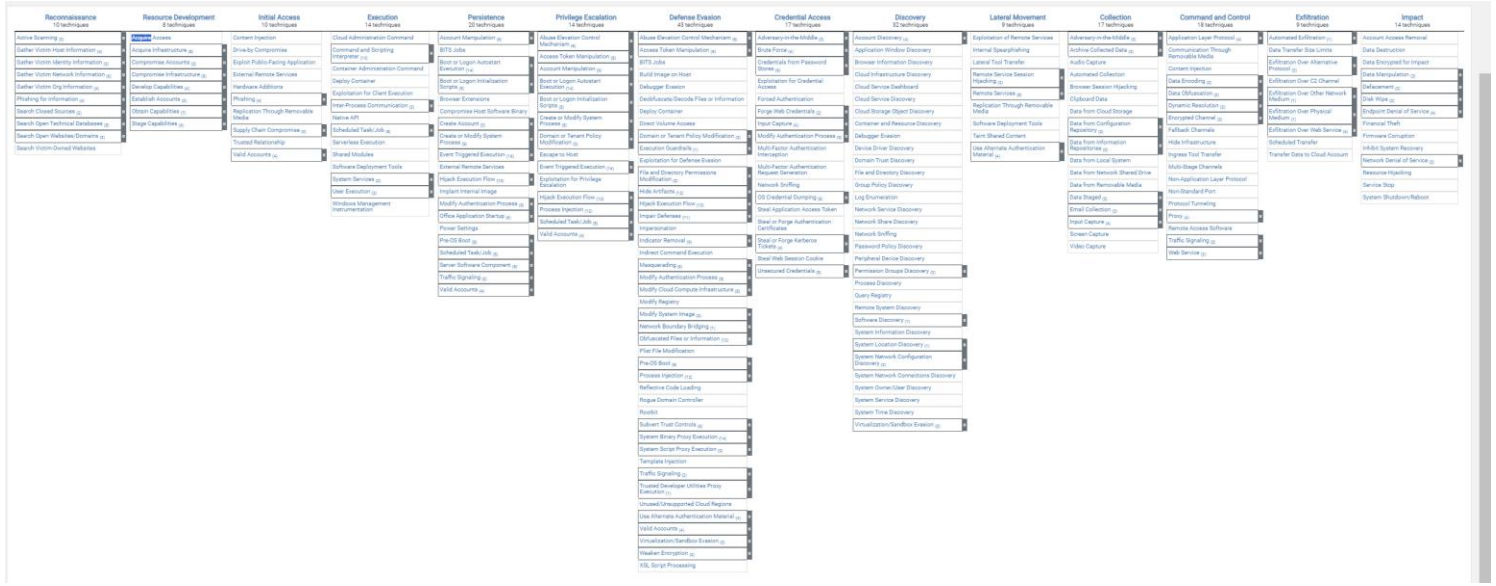


Attack Lifecycle

Attack Lifecycle – APT32



MITRE ATT&CK & Atomic Red Team Exploration



CyberSecPro

Thank you for your attention

Presentation by:

Christos Grigoriadis
(Focal Point)

CyberSecPro