OffSec

MITRE ATT&CK: Privilege Escalation Learning Path

(TA0004)

Enhance skills in privilege escalation, system enumeration, persistence mechanisms, and process injection techniques across Windows, Linux, and macOS environments. Train on eleven techniques covered in the privilege escalation tactic.

One of 12 MITRE ATT&CK Learning Paths from OffSec

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control

Learning Path Overview

Learners start with Windows and Linux privilege escalation techniques, understanding methods for escalating privileges and enumerating system details. They explore persistence mechanisms on Windows systems, including disk and registry-based persistence. Additionally, modules cover process injection techniques, enabling learners to detect and execute advanced injection methods.

Advanced topics include container escapes for interacting with the host system, modifying host configurations, and executing commands. Learners also gain insights into macOS-specific injection techniques like Dylib injection and DYLD hijacking.

Techniques covered

- T1548 - Abuse Elevation Control Mechanism
- T1134 - Access Token Manipulation
- T1543 - Create or Modify System Process
- T1068 - Exploitation for Privilege Escalation
- T1574 - Hijack Execution Flow
- T1053 - Scheduled Task/Job
- T1078 - Valid Accounts
- T1611 - Escape to Host
- T1547 - Boot or Logon Autostart Execution
- T1055 - Process Injection
- T1546 - Event Triggered Execution

Learning objectives

- Identify ways to escalate privileges by exploiting system weaknesses, misconfigurations, and vulnerabilities, such as services, file permissions, and scheduled tasks on both Windows and Linux Operating Systems.
- Recognize how to abuse insecure system components.
- Learn about escaping privileged container techniques.

Why complete the MITRE ATT&CK Privilege Escalation Learning Path from OffSec?

- **Corporate cybersecurity teams** learn to patch vulnerabilities that could be exploited for unauthorized access through hands-on demonstration. This empowers the organization to proactively defend against and mitigate potential threats, protecting sensitive information and maintaining the integrity of their systems.
- **Individual professionals** master advanced techniques in privilege escalation, system enumeration, and persistence across diverse platforms.

Earning an OffSec MITRE ATT&CK learning badge

Learners will be proficient in identifying and exploiting vulnerabilities in system security, enhancing their ability to assess and mitigate cybersecurity risks effectively.

FAQ

+ What's the syllabus?

- Windows Persistence
  - *Persistence on Disk*
  - *Persistence in Registry*
- Windows Privilege Escalation
  - *Enumerating Windows*
  - *Leveraging Windows Services*
  - *Abusing Other Windows Components*
- Linux Privilege Escalation
  - *Enumerating Linux*
  - *Exposed Confidential Information*
  - *Insecure File Permissions*
  - *Insecure System Components*
- Container Escapes - Interacting With The Host
  - *Modifying the Host*
  - *Executing Commands*
- Process Injection For Red Teamers
  - *Detecting Process Injection*
  - *Advanced Process Injection*
- Dylib Injection
  - *DYLD_INSERT_LIBRARIES Injection in macOS*
  - *DYLD Hijacking*

+ What skills are associated with this Learning Path?

- Windows Attacks
- Linux Attacks
- Cloud Attacks
- Monitoring
- Intrusion Detection and Analysis
- Exploit Development - macOS

+ What job roles are associated with this Learning Path?

- SOC Analyst
- Network Penetration Tester
- Security Researcher

+ Who is this Learning Path designed for?

This learning path is tailored for cybersecurity professionals. Honing skills in privilege escalation, persistence, and process injection across Windows, Linux, and macOS it's ideal for pen testers because it fortifies defenses against cyber threats.

+ Are there any prerequisites?

This learning path is considered an intermediate level learning path and learners should have completed Linux Basics 1 & 2, Windows Basics 1 & 2, Networking Fundamentals, and Containers for Cloud 1.

+ How long does the Learning Path take, and what's the format?

This self-paced path is designed for flexibility, typically taking 140 hours to complete. It includes text based content and 91 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com