OffSec

MITRE ATT&CK: PERSISTENCE Learning Path

(TA0003)

Learn about threat modeling, passive enumeration, client-side code execution, and phishing with Microsoft Office. Train on nine techniques covered in the persistence tactic.

MITRE | ATT&CK®

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

The MITRE ATT&CK - Persistence (TA0003) Learning Path equips cybersecurity learners, particularly penetration testers and security analysts, with skills vital for fortifying defenses and mitigating cyber threats. Modules cover Windows and Linux persistence techniques, privilege escalation methods, and attacking embedded systems. Topics include threat modeling, passive enumeration, client-side code execution, and phishing with Microsoft Office.

Learners delve into techniques for persistence on disk and in the registry, as well as methods for leveraging Windows services and abusing system components. Upon completion, learners will possess advanced skills in persistence, privilege escalation, and attacking embedded systems, enabling them to enhance organizational security posture and effectively defend against cyber threats.

Techniques covered

- T1547 - Boot or Logon Autostart Execution
- T1037 - Boot or Logon Initialization Scripts
- T1546 - Event Triggered Execution
- T1574 - Hijack Execution Flow
- T1053 - Scheduled Task/Job
- T1542 - Pre-OS Boot
- T1136 - Create Account
- T1543 - Create or Modify System Process
- T1137 - Office Application Startup

Learning objectives

- Identify the different methods adversaries use to maintain persistent access to a system, such as creating scheduled tasks and new accounts on Windows and Linux Operating Systems.
- Utilize ways to manipulate run keys and Winlogon helper objects in the registry.
- Abuse pre-OS boot mechanisms to establish persistence on a system.

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

- **Corporate cybersecurity teams** can bolster their security postures, mitigating potential breaches and minimizing financial and reputational damage. Ultimately, investing in this course empowers organizations to build a robust cybersecurity framework, safeguarding sensitive data and ensuring business continuity.
- **Individual professionals** gain insights into safeguarding critical assets, and enhancing organizational resilience against evolving cyber risks.

Earning an OffSec MITRE ATT&CK learning badge

By mastering persistence, privilege escalation, and attack techniques, learners safeguard critical assets, and enhance organizational resilience against evolving cyber risks.

FAQ

+ What’s the syllabus?

- Windows Persistence
  - *Persistence on Disk*
  - *Persistence in Registry*
- Introduction to Attacking Embedded Systems
  - *Threat Modeling*
  - *Passive Enumeration*
  - *Example: Reolink RLC-510A*
- 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*
- Client Side Code Execution With Office
  - *Will You Be My Dropper*
  - *Phishing with Microsoft Office*
  - *Keeping Up Appearances*
  - *Executing Shellcode in Word Memory*
  - *PowerShell Shellcode Runner*
  - *Keep That PowerShell in Memory*
  - *Talking To The Proxy*

+ What are the skills associated with this Learning Path?

- Monitoring
- Intrusion Detection and Analysis
- Windows Attacks
- Linux Attacks
- Client Side Attacks

+ What are the job roles associated with this Learning Path?

- SOC Analyst
- Network Penetration Tester
- Threat Hunter
- Incident Responder
- System Administrator

+ Who is this Learning Path designed for?

This learning path is tailored for cybersecurity professionals, especially those engaged in threat analysis and defense. It assists these professionals in understanding the tactics, techniques, and procedures (TTPs) needed to identify long-term, hidden threats.

+ Are there any prerequisites?

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

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

This self-paced path is designed for flexibility, typically taking 95 hours to complete. It includes text based content and 86 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com