OffSec

MITRE ATT&CK: EXECUTION Learning Path

(TA0002)

Learn techniques for lateral movement within Active Directory, leveraging persistence mechanisms, and executing XPC attacks on macOS systems. Train on four techniques covered in the execution 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 - Execution (TA0002) Learning Path equips learners with advanced cybersecurity skills, catering to roles such as penetration testers, security analysts, and ethical hackers. Modules cover diverse topics, including command injection, client-side attacks, cross-site scripting, and lateral movement in Active Directory and Linux environments. Learners delve into exploiting vulnerabilities in Microsoft Office, Windows Library Files, and XPC services on macOS.

This learning path is designed for cybersecurity professionals, including those involved in threat analysis and defense. It helps these professionals understand the tactics, techniques, and procedures (TTPs) involved in learning various execution techniques.

Techniques covered

- T1059 - Command and Scripting Interpreter
- T1203 - Exploitation for Client Execution
- T1053 - Scheduled Task/Job
- T1204 - User Execution

Learning objectives

- Understand the fundamental concepts and techniques of the execution phase of a cyber attack.
- Identify and mitigate vulnerabilities that could be exploited for malicious code execution across different platforms.
- Develop security policies and controls to prevent unauthorized execution of applications and scripts.

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

- **Corporate cybersecurity teams** benefit from enhanced security postures, risk reduction, and improved resilience against cyber threats. Practical modules on exploiting Microsoft Office and abusing Windows Library Files enhance learners' ability to understand and counter real-world threats. Exploration of XPC attacks on macOS systems offers insights into defending against platform-specific vulnerabilities.
- **Individual professionals** master techniques like command injection, client-side attacks, and lateral movement, learners become adept at identifying and mitigating security vulnerabilities.

Earning an OffSec MITRE ATT&CK learning badge

Demonstrate mastery of techniques like command injection, client-side attacks, and lateral movement to mitigate security vulnerabilities.

FAQ

What's the syllabus?

- Tools
  - *Shells*
- Command Injection
  - *Discovery of Command Injection*
  - *Enumeration and Exploitation*
- Client-side Attacks
  - *Target Reconnaissance*
  - *Exploiting Microsoft Office*
  - *Abusing Windows Library Files*
- Cross-Site Scripting Exploitation and Case Study
  - *Cross-Site Scripting - Exploitation*
  - *Case Study: Shopizer Reflected XSS*
- Lateral Movement in Active Directory
  - *Active Directory Lateral Movement Techniques*
  - *Active Directory Persistence*
- Linux Lateral Movement
  - *DevOps*
- XPC Attacks
  - *The Low Level C API: XPC Services*
  - *The Foundation Framework API*
  - *Attacking XPC Services*
  - *Apple's EvenBetterAuthorizationSample*
  - *CVE-2019-20057 - Proxyman Change Proxy Privileged Action Vulnerability*
  - *CVE-2020-0984 - Microsoft Auto Update Privilege Escalation Vulnerability*
  - *CVE-2019-8805 - Apple EndpointSecurity Framework Local Privilege Escalation*
  - *CVE-2020-9714 - Adobe Reader Update Local Privilege Escalation*

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 and Networking Fundamentals.

How long does the Learning Path take, and what's the format?
This self-paced path is designed for flexibility, typically taking 125 hours to complete. It includes text based content and 35 labs to reinforce training with hands-on experience.

What skills are associated with this Learning Path?

- Common Attack Techniques: SOC Analyst

What are the job roles associated with this Learning Path?

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

Who is this Learning Path designed for?
This learning path is designed for cybersecurity professionals, including those involved in threat analysis and defense. It helps these professionals understand the tactics, techniques, and procedures (TTPs) involved in learning various execution techniques.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com