OffSec

MITRE ATT&CK: Lateral Movement Learning Path

(TA0008)

Understand the techniques adversaries use to move through compromised networks. Train on four techniques covered in the lateral movement 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 - Lateral Movement (TA0008) Learning Path covers the techniques an adversary uses to move through a network to gain access and extend their reach within a compromised network. This involves strategies like using stolen credentials, exploiting system vulnerabilities, and manipulating protocols to navigate from one system to another without being detected. The attacker's goal is to reach high-value targets, expand their presence, and accomplish their objectives within the network.

This learning path is tailored for cybersecurity professionals, particularly those engaged in threat analysis and defense. It assists these professionals in understanding the tactics, techniques, and procedures (TTPs) necessary to practice the lateral movement techniques employed by an adversary.

Techniques covered

- T1021 - Remote Services
- T1550 - Use Alternate Authentication Material
- T1563 - Remote Service Session Hijacking
- T1072 - Software Deployment Tools

Learning objectives

- Learning how to use tools like PsExec, WinRM, or SMB, which adversaries use to move laterally.
- Understanding the importance of detecting and responding to unauthorized access and movements within the network.
- Using stolen password hashes and tickets to bypass normal access control systems within an environment.

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

- **Corporate cybersecurity teams** develop strategies that restrict an attacker's ability to move from one system to another within the network to reduces the likelihood of attackers accessing sensitive information and disseminating their influence throughout the organization's environment. Organizations can enhance the protection of their critical assets and uphold the integrity of their network security.
- **Individual professionals** gain skills to detect and neutralize vulnerabilities, ensuring robust protection of organizational assets and data.

Earning an OffSec MITRE ATT&CK learning badge

Highlight your enhanced cyber defense skills with advanced lateral movement and exploitation techniques.

FAQ

+ What's the syllabus?

- Lateral Movement in Active Directory
  - *Active Directory Lateral Movement Techniques*
  - *Active Directory Persistence*
- Windows Lateral Movement
  - *Remote Desktop Protocol*
  - *Fileless Lateral Movement*
- Linux Lateral Movement
  - *Lateral Movement with SSH*
  - *DevOps*
  - *Kerberos on Linux*
- Port Redirection and SSH Tunneling
  - *Why Port Redirection and Tunneling?*
  - *Port Forwarding with Linux Tools*
  - *SSH Tunneling*
  - *Port Forwarding with Windows Tools*
- Tunneling Through Deep Packet Inspection
  - *HTTP Tunneling Theory and Practice*
  - *DNS Tunneling Theory and Practice*

+ Who is this Learning Path designed for?

This learning path is tailored for cybersecurity professionals, particularly those engaged in threat analysis and defense. It assists these professionals in understanding the tactics, techniques, and procedures (TTPs) necessary to practice the lateral movement techniques employed by an adversary.

+ What are the associated skills for this Learning Path?

- Lateral Movement
- Common Attack Techniques: SOC Analyst

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

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

+ 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 65 hours to complete. It includes text based content and 36 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com