MITRE ATT&CK: DISCOVERY Learning Path

(TA0007)

Develop advanced skills in privilege escalation, cloud security, and reconnaissance techniques.Train on sixteen techniques covered in the reconnaissance tactic.

One of 12 MITRE ATT&CK Learning Paths from OffSec

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

Learning Path Overview

The MITRE ATT&CK - Discovery (TA0007) Learning Path covers the techniques adversaries use to gather sensitive information about a system and its environment once they have gained access. This includes identifying valuable data, system vulnerabilities, and understanding the network structure to further exploit it.

This Learning Path is tailored for cybersecurity professionals aiming to deepen their understanding of privilege escalation, cloud security, and reconnaissance techniques. Roles such as penetration testers, security analysts, and cloud security specialists would benefit most from this unit. Modules cover various topics, including Windows privilege escalation, AWS fundamentals, and reconnaissance methodologies.

Techniques covered

- T1083 - File and Directory Discovery
- T1654 - Log Enumeration
- T1069 - Permission Groups Discovery
- T1518 - Software Discovery
- T1082 - System Information Discovery
- T1016 - System Network Connections Discovery
- T1033 - System Owner/User Discovery
- T1007 - System Service Discovery
- T1087 - Account Discovery
- T1538 - Cloud Service Discovery
- T1619 - Cloud Storage Object Discovery
- T1046 - Network Service Discovery
- T1135 - Network Share Discovery
- T1580 - Cloud Infrastructure Discovery
- T1613 - Container and Resource Discovery
- T1652 - Device Driver Discovery

Learning objectives

- Recognize different methods an adversary uses for active and passive information gathering
- Understand ways to collect detailed data about targeted systems such as operating systems, open ports and running services
- Identify and assess vulnerabilities within organization networks, systems and applications by leveraging various tools

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

- **Corporate cybersecurity teams** understand how attackers search for information within systems after breaching them through hands-on demonstrations. This understanding helps organizations simulate and identify such activities, enhancing their ability to detect and respond to threats.
- **Individual professionals** gain expertise in identifying and addressing vulnerabilities in Windows systems and securing AWS environments. They acquire reconnaissance techniques to detect and remediate exposed Kubernetes and Docker dashboards, enhancing cloud security posture and protecting sensitive data.

Earning an OffSec MITRE ATT&CK learning badge

Badge earners possess advanced skills in privilege escalation, cloud security, and reconnaissance techniques. They are proficient in identifying and exploiting vulnerabilities in Windows systems, securing AWS environments, and conducting thorough cloud reconnaissance.

FAQ

What's the syllabus?

- Windows Privilege Escalation
- Introduction to AWS
- Information Gathering
- Public Cloud Reconnaissance - Post-Compromise Exploration - IAM
- Discovering Exposed Kubernetes Dashboards
- Discovering Exposed Docker Sockets
- Determining Chipsets and Drivers

Who is this Learning Path designed for?

This learning path is designed for cybersecurity professionals, especially those in threat analysis and defense. It helps these professionals understand the tactics, techniques, and procedures (TTPs) used by adversaries for discovery.

What are the associated skills for this Learning Path?

- Windows Attacks
- Enumeration
- Cloud Attacks

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, Windows Basics 1 &2, Networking fundamentals and Cloud Architecture Overview.

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

This self-paced path is designed for flexibility, typically taking 110 hours to complete. It includes text based content and 106 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise