MITRE ATT&CK: RECONNAISSANCE Learning Path

(TA0043)

Collect target information before launching operations to plan attack strategies effectively. Train on seven 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 - Reconnaissance (TA0043) Learning Path covers the techniques an adversary may use to collect information on their targets before launching their operations and attacks. This phase is key for an attacker to understand the environment they aim to compromise, identify vulnerabilities, and plan their attack strategies effectively.

This learning path is designed for any cybersecurity professionals including threat analysis and defense. It helps these professionals understand the tactics, techniques, and procedures (TTPs) used by an attacker, enhancing their ability to safeguard their organization from cyber threats.

Techniques covered

- T1595 - Active Scanning
- T1592 - Gather Victim Host Information
- T1589 - Gather Victim Identity Information
- T1590 - Gather Victim Network Information
- T1598 - Phishing for Information
- T1596 - Search Open Technical Databases
- T1593 - Search Open Websites/ Domains

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 Reconnaissance Learning Path from OffSec?

- **Corporate cybersecurity teams** can sharpen their penetration testing and incident-response skills by identifying network topology, system configurations, and potential vulnerabilities, enhancing their organization's defensive posture.
- **Individual professionals** can leverage it for skill advancement and to stay current in the ever-evolving field of cybersecurity.
- **Educational institutions** can integrate it into their programs to give students a hands-on understanding of real-world cyber attacks.

Earning an OffSec MITRE ATT&CK learning badge

Demonstrate hands-on readiness for initial stages of cyber attacks, allow for proactive defense and enhanced vulnerability management.

FAQ

What's the syllabus?

- Information Gathering
  - *The Penetration Testing Lifecycle*
  - *Passive Information Gathering*
  - *Active Information Gathering*
- Vulnerability Scanning
  - *Vulnerability Scanning Theory*
  - *Vulnerability Scanning with Nessus*
  - *Vulnerability Scanning with Nmap*
- Introduction to Attacking Embedded Systems
  - *Threat Modeling*
  - *Passive Enumeration*
  - *Example: Reolink RLC-510A*
- Container Escapes - Information Gathering
  - *Information Gathering*
  - *Discovering Sensitive Data*
- Attacker Methodology Introduction
  - *The Network as a Whole*
  - *The Lockheed-Martin Cyber Kill-Chain*
  - *MITRE ATT&CK Framework*

Who is this Learning Path designed for?

This learning path is designed for any cybersecurity professionals including threat analysis and defense. It helps these professionals understand the tactics, techniques, and procedures (TTPs) used by an attacker, enhancing their ability to safeguard their organization from cyber threats.

What are the associated skills for this Learning Path?

- Enumeration Vulnerability Detection
- Common Attack Techniques: SOC Analyst
- Cloud Attacks

What are the associated job roles for this Learning Path?

- Network Penetration Tester
- Security Researcher
- Incident Responder
- Threat Hunter
- System Administrator

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 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 91 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited | Learn Enterprise