MITRE ATT&CK: COLLECTION Learning Path

(TA0009)

Learn information gathering techniques, understanding the penetration testing lifecycle, delve into passive and active methods, crucial for reconnaissance and initial foothold establishment. Train on seven techniques covered in the reconnaissance tactic.

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 - Collection (TA0009) Learning Path explores the methods used by attackers to obtain sensitive information from various sources to achieve their goals. This phase involves recognizing and retrieving valuable data, such as documents, credentials, and emails, from compromised systems and networks. Techniques include data collection, taking screenshots, and monitoring network traffic to acquire the necessary information for subsequent actions within the attack lifecycle.

This learning path is tailored for cybersecurity professionals, including those engaged in threat analysis and defense. It equips these professionals with an understanding of the tactics, techniques, and procedures (TTPs) required to safeguard sensitive data and reduce the risk of data breaches.

Techniques covered

- T1602 - Data from Configuration Repository
- T1213 - Data from Information Repositories
- T1039 - Data from Network Shared Drive
- T1074 - Data Staged
- T1119 - Automated Collection
- T1056 - Input Capture
- T1123 - Audio Capture

Learning objectives

- Recognize the various collection techniques an adversary uses, including data from local system sources, network traffic interception, and data capture in transit;
- Understand the tools and methods used for data collection, enabling the identification and prevention of unauthorized data exfiltration;
- Develop strategies for protecting sensitive information, including data loss prevention (DLP), encryption, and access control systems.

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

- **Corporate cybersecurity teams** understand how to safeguard against data breaches and protect the confidentiality, integrity, and availability of their data through hands-on demonstration. This understanding enhances an organization's cybersecurity defenses by promoting a proactive approach to identifying and responding to threats.
- **Individual professionals** enhance their skills in penetration testing, Git security, Active Directory enumeration, cross-site scripting exploitation, secrets management, and bypassing privacy controls.

Earning an OffSec MITRE ATT&CK learning badge

Badge earners understand how to safeguard against data breaches and protect the confidentiality, integrity, and availability of their data through hands-on demonstration.

FAQ

+ What's the syllabus?

- Information Gathering
  - *The Penetration Testing Lifecycle*
  - *Passive Information Gathering*
  - *Active Information Gathering*
- Introduction to Git Security
  - *Git Secure: Examine Git from a Security Perspective*
- Active Directory Introduction and Enumeration
  - *Active Directory - Introduction*
  - *Active Directory - Manual Enumeration*
  - *Manual Enumeration - Expanding our Repertoire*
  - *Active Directory - Automated Enumeration*
- Cross-Site Scripting Exploitation and Case Study
  - *Cross-Site Scripting - Exploitation*
  - *Case Study: Shopizer Reflected XSS*
- Secrets Management - Removing Hard-coded Secrets
  - *Discovering and Fixing the Secrets in Code*
- Bypassing Transparency, Consent, and Control (Privacy)
  - *TCC Internals*
  - *CVE-2020-29621 - Full TCC Bypass via coreaudiod*
  - *Bypass TCC via Spotlight Importer Plugins*
  - *CVE-2020-24259 - Bypass TCC with Signal to Access Microphone*
  - *Gain Full Disk Access via Terminal*
  - *CVE-2021-1784 - TCC Bypass Via Mounting Over com.apple.TCC*
  - *CVE-2021-30782 - TCC Bypass Via AppTranslocation Service*
  - *CVE-2022-42859 - TCC Bypass using createmobileaccount*

+ Who is this Learning Path designed for?

This Learning Path is tailored for cybersecurity professionals keen on enhancing their skills in penetration testing, Git security, Active Directory enumeration, cross-site scripting exploitation, secrets management, and bypassing privacy controls. Roles best suited for this unit include penetration testers, security analysts, and ethical hackers.

+ 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 135 hours to complete. It includes text based content and 82 labs to reinforce training with hands-on experience.

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

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

+ What are the associated skills for this Learning Path?

- Common Attack Techniques: SOC Analyst

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com