OffSec

MITRE ATT&CK: INITIAL ACCESS Learning Path

(TA0001)

Explores how an adversary could obtain unauthorized access by exploiting weaknesses in a system or network. Train on five techniques covered in the initial access 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 - Initial Access (TA0001) Learning Path offers comprehensive training in web application security, covering input validation, cross-site scripting (XSS), SQL injection, SSRF, command injection, and more.

It's ideal for roles like penetration testers, security analysts, and developers. Learners will gain skills in identifying and exploiting vulnerabilities, such as XSS, SQLi, and SSRF, through hands-on modules and case studies. By completing this course, learners will be proficient in conducting security assessments, identifying attack vectors, and implementing effective security measures to safeguard organizational assets against opportunistic and targeted cyber attacks.

Techniques covered

- T1190 - Exploit Public-Facing Application
- T1189 - Drive-by Compromise
- T1133 - External Remote Services
- T1566 - Phishing
- T1078 - Valid Accounts

Learning objectives

- Recognize different methods for exploiting web application vulnerabilities, such as SQL injection, command injection, and server-side request forgery.
- Exploit a web application on a client endpoint by using the cross-site scripting (XSS) attack upon visiting a website.
- Identify ways to obtain and abuse credentials to gain initial access.

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

- **Corporate cybersecurity teams** enhance their cybersecurity posture by providing practical insights from case studies. Learners acquire vital skills in web app security, SQL injection, and more, enabling them to fortify defenses against cyber threats.
- **Individual professionals** can swiftly detect and mitigate vulnerabilities, minimizing the risk of data breaches and financial losses.

Earning an OffSec MITRE ATT&CK learning badge

Demonstrate proficiency in conducting security assessments, identifying attack vectors, and implementing effective security measures to safeguard organizational assets against opportunistic and targeted cyber attacks.

FAQ

+ What's the syllabus?

- Input Validation Fundamentals
- Cross-Site Scripting Introduction and Discovery
- Cross-Site Scripting Exploitation and Case Study
- SQL Injection
- Server Side Request Forgery
- Command Injection
- Discovering Exposed Kubernetes Dashboards
- Common Attack Techniques
- Port Redirection and SSH Tunneling
- Credential Attacks
- Attacking Active Directory Authentication

+ What skills are associated with this Learning Path?

- Handling User Input,
- Injection Attacks,
- Web Application Attacks
- SSRF Attacks
- Cloud Attacks
- Common Attack Techniques : Incident Responder
- Password Attacks
- Active Directory Penetration Testing
- Common Attack Techniques: SOC Analyst

+ Who is this Learning Path designed for?

This learning path is designed for any ccybersecurity professionals, including those engaged in threat analysis and defense. It aids these professionals in comprehending the tactics, techniques, and procedures (TTPs) involved in how an adversary may gain unauthorized entry into organization networks, systems, and applications.

+ What job roles are associated with this Learning Path?

- Software Developer
- Web Application Tester
- Network Penetration Tester
- Incident Responder
- SOC Analyst
- Threat Hunter

+ Are there any prerequisites?

This learning path is considered an intermediate level learning path and learners should have completed Linux Basics I, Windows Basics I, Web Applications, Introduction to Active Directory, Introduction to Kubernetes I

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

This self-paced path is designed for flexibility, typically taking 165 hours to complete. It includes text based content and 165 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com