MITRE ATT&CK: Credential Access Learning Path

(TA0006)

Explore the methods adversaries employ to acquire account names and passwords for system access, network traversal, data access, and malicious activities Train on nine 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 - Credential Access (TA0006) Learning Path is designed to bolster the skills of cybersecurity professionals in password attacks, credential exploitation, and Active Directory (AD) security. Modules cover various topics, including password cracking fundamentals, credential attacks, and attacks on AD authentication.

Learners start with password attacks, delving into techniques like password cracking and working with password hashes. They then explore credential attacks, including common design flaws and attacks on AD authentication. Additionally, modules on AD Certificate Services provide insights into cryptography, Windows certificates, and the attack taxonomy associated with certificate services.

Techniques covered

- T1557: Adversary-in-the-Middle
- T1110: Brute Force
- T1555: Credentials from Password Stores
- T1187: Forced Authentication
- T1040: Network Sniffing
- T1003: OS Credential Dumping
- T1552: Unsecured Credentials
- T1558: Steal or Forge Kerberos Tickets
- T1649: Steal or Forge Authentication Certificates

Learning objectives

- Enhance the understanding of tactics, techniques, and procedures (TTPs) to build skills in deterring unauthorized access.
- Explore the methods adversaries employ to acquire account names and passwords for system access, network traversal, data access, and malicious activities
- Identify and mitigate vulnerabilities related to password security and Active Directory authentication.

Why complete the MITRE ATT&CK Credential Access 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

Safeguard an organizations data, enhance their security strategies to protect sensitive information and prevent unauthorized access.

FAQ

What's the syllabus?

- Password Attacks
  - *Attacking Network Services Logins*
  - *Password Cracking Fundamentals*
  - *Working with Password Hashes*
- Credential Attacks
  - *Introduction to Credential Attacks*
  - *Common Credential Attacks and Design Flaws*
  - *Insecure CAPTCHAs*
  - *Running Credential Attacks*
- Attacking Active Directory Authentication
  - *Understanding Active Directory Authentication*
  - *Performing Attacks on Active Directory Authentication*
- Introduction to AD Certificate Services
  - *Cryptography Refresher*
  - *Understand Windows Certificates*
  - *Windows Certificate Templates*
  - *Understand the Attack Taxonomy*
  - *Log and Audit AD Certificate Services*
- Windows Credentials
  - *Local Windows Credentials*
  - *Access Tokens*
  - *Kerberos and Domain Credentials*
  - *Processing Credentials Offline*

Who is this Learning Path designed for?

Designed for cybersecurity professionals engaged in threat analysis and defense, this learning path enhances their understanding of tactics, techniques, and procedures (TTPs) to build skills in deterring unauthorized access.

What are the associated skills for this Learning Path?

- Password Attacks
- Common Attack Techniques: SOC Analyst
- Active Directory Penetration Testing
- Active Directory Administration
- Windows Attacks

What are the associated job roles for this Learning Path?

- Network Penetration Tester
- SOC Analyst
- 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 Introduction to Active Directory.

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

This self-paced path is designed for flexibility, typically taking 60 hours to complete. It includes text based content and 72 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise