MITRE ATT&CK: Command and Control Learning Path

(TA0011)

Master network security and evasion by covering topics like proxies, tunneling and intrusion detection. Train on seven techniques covered in the command and control 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 - Command and Control (TA0011) Learning Path helps learners master network security and evasion. Ideal for cybersecurity pros, admins, and testers. It covers basics like proxies to advanced topics including tunneling and intrusion detection. Learners gain skills to enhance security, mitigate risks, and defend against cyber threats.

Techniques covered

- T1090 - Proxy
- T1572 - Protocol Tunneling
- T1071 - Application Layer Protocol
- T1568 - Dynamic Resolution
- T1573 - Encrypted Channel
- T1219 - Remote Access Software

Learning objectives

- Master proxy technologies and network defense techniques.
- Gain expertise in network detections, intrusion detection systems (IDS), and intrusion prevention systems (IPS) sensors, enhancing their ability to detect and respond to threats effectively.
- Become proficient in utilizing proxies, detecting network intrusions, and implementing countermeasures against evasion techniques.

Why complete the MITRE ATT&CK Command and Control Learning Path from OffSec?

- **Corporate cybersecurity teams** streamline operations, reduce costs, and deliver software faster. With improved security practices and accelerated deployment, organizations benefit from enhanced productivity, reduced risks, and increased competitiveness in the market.
- **Individual professionals** gain skills in infrastructure automation, IAM, and CI/CD, and will master network security and evasion.

Earning an OffSec MITRE ATT&CK learning badge

Badge earners are proficient in utilizing proxies, detecting network intrusions, and implementing countermeasures against evasion techniques.

FAQ

What's the syllabus?

- Introduction to Proxies
  - *HTTP Proxy*
  - *HTTPS Proxy*
  - *SOCKS5 Proxy*
  - *Proxychains*
  - *Web Filtering*
- Port Redirection and SSH Tunneling
  - *Why Port Redirection and Tunneling?*
  - *Port Forwarding with Linux Tools*
  - *SSH Tunneling*
  - *Port Forwarding with Windows Tools*
- Tunneling Through Deep Packet Inspection
  - *HTTP Tunneling Theory and Practice*
  - *DNS Tunneling Theory and Practice*
- Network Detections
  - *Intrusion Detection Systems*
  - *Detecting Attacks*
  - *Detecting C2 Infrastructure*
- Bypassing Network Filters
  - *DNS Filters*
  - *Web Proxies*
  - *IDS and IPS Sensors*
  - *Full Packet Capture Devices*
  - *HTTPS Inspection*
  - *Domain Fronting*
  - *DNS Tunneling*

Who is this Learning Path designed for?

This Learning Path is essential for cybersecurity professionals interested in mastering proxy technologies and network defense techniques. Modules cover a range of topics, from proxy fundamentals to advanced intrusion detection and evasion methods. Roles best suited for this unit include security analysts, network administrators, and incident responders.

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 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 95 hours to complete. It includes text based content and 56 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?

- Monitoring
- Intrusion Detection and Analysis
- Lateral Movement

Available on:

Learn Unlimited

Learn Enterprise