OffSec

MITRE | ATT&CK®

MITRE ATT&CK: Resource Development Learning Path

(TA0042)

Hands-on experience Locating and exploiting public vulnerabilities, client-side attacks, the Metasploit framework, process injection, and ASLR bypass techniques. Train on five techniques covered in the resource development 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 - Resource Development (TA0042) Learning Path focuses on how adversaries gather, create, and use resources to support their malicious attacks. It empowers attackers to bypass security measures, exploit vulnerabilities, and maintain persistence in an organization's network, systems, and applications.

This learning path is tailored for cybersecurity professionals involved in threat analysis and defense. It aids these professionals in comprehending the tactics, techniques, and procedures (TTPs) employed by attackers to prepare, use, purchase, or compromise resources to bolster and improve their operations.

Techniques covered

- T1588 - Obtain Capabilities
- T1583 - Acquire Infrastructure
- T1586 - Compromise Accounts
- T1608 - Stage Capabilities
- T1587 - Develop Capabilities

Learning objectives

- Identify how to find public exploits to aid adversary operations.
- Use the Metasploit Framework and understand how it can assist attackers.
- Create custom payloads and exploits to circumvent defensive mechanisms specific to their targets.

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

- **Corporate cybersecurity teams** enhance an organization's cybersecurity posture. By mastering techniques like process injection and ASLR bypass, learners can effectively detect and mitigate vulnerabilities, safeguarding organizational assets against the most modern and advanced cyber threats.
- **Individual professionals** can conduct thorough security assessments, identify vulnerabilities, and implement effective security measures to safeguard organizational assets against cyber threats.

Earning an OffSec MITRE ATT&CK learning badge

Demonstrate hands-on readiness for effectively detecting and mitigating vulnerabilities. Safeguarding organizational assets against the most modern and advanced cyber threats.

FAQ

What's the syllabus?

- Locating Public Exploits
  - *Online Exploit Resources*
  - *Offline Exploit Resources*
  - *Exploiting a Target*
- Client-side Attacks
  - *Target Reconnaissance*
  - *Exploiting Microsoft Office*
  - *Abusing Windows Library Files*
- The Metasploit Framework
  - *Getting Familiar with Metasploit*
  - *Using Metasploit Payloads*
  - *Performing Post-Exploitation with Metasploit*
  - *Automating Metasploit*
- Process Injection and Migration
  - *Finding a Home for Our Shellcode*
  - *DLL Injection*
  - *Reflective DLL Injection*
  - *Process Hollowing*
- Creating Custom Shellcode
  - *Calling Conventions on x86*
  - *The System Call Problem*
  - *Finding kernel32.dll*
  - *Resolving Symbols*
  - *NULL-Free Position-Independent Shellcode (PIC)*
  - *Reverse Shell*
- Stack Overflows and ASLR Bypass
  - *ASL Introduction*
  - *Finding Hidden Gems*
  - *Expanding our Exploit (ASLR Bypass)*
  - *Bypassing DEP with WriteProcessMemory*

What are the skills associated with this Learning Path?

- Web Application Attacks
- Client Side Attacks
- Windows Attacks
- Common Attack Techniques: SOC Analyst
- Common Tools: Network Penetration Tester
- Exploit Development - Windows

What are the job roles associated with this Learning Path?

- Network Penetration Tester
- SOC Analyst
- Security Researcher

Are there any prerequisites?

- Linux Basics I
- Windows Basics I
- Windows Basics II
- Introduction to WinDbg, Part I

Who is this Learning Path designed for?

This learning path is tailored for cybersecurity professionals involved in threat analysis and defense. It aids these professionals in comprehending the tactics, techniques, and procedures (TTPs) employed by attackers to prepare, use, purchase, or compromise resources to bolster and improve their operations.

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

This self-paced path is designed for flexibility, typically taking 90 hours to complete. It includes text based content and 54 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com