MITRE ATT&CK: Defense Evasion Learning Path

(TA0005)

Delve into techniques to bypass antivirus software, understanding key components and operations, simulating target environments, and locating signatures in files. Train on fourteen techniques covered in the defense evasion 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

In the MITRE ATT&CK - Defense Evasion (TA0005) Learning Path, learners delve into techniques for bypassing antivirus software, understanding key components and operations, simulating target environments, and locating signatures in files. They explore methods for packing malware, detecting packed malware, and unpacking malware samples, enhancing their skills in malware analysis and evasion.

Additionally, modules cover advanced topics such as bypassing AMSI (Antimalware Scan Interface), automating event log tampering, and process injection techniques. Learners gain practical insights into bypassing application whitelisting using PowerShell, C#, and JScript, as well as bypassing Gatekeeper security on macOS systems.

Techniques covered

- T1574 - Hijack Execution Flow
- T1027 - Obfuscated Files or Information
- T1564 - Hide Artifacts
- T1036 - Masquerading
- T1221 - Template Injection
- T1497 - Virtualization/Sandbox Evasion
- T1562 - Impair Defenses
- T1070 - Indicator Removal
- T1140 - Deobfuscate/Decode Files
- T1202 - Indirect Command Execution
- T1218 - System Binary Proxy Execution
- T1127 - Trusted Developer Utilities Proxy Execution
- T1220 - XSL Script Processing
- T1553 - Subvert Trust Controls

Learning objectives

- Disable defensive mechanisms through log tampering and antivirus evasion techniques.
- Circumvent defensive measures by encrypting, encoding, and obfuscating content.
- Explore various methods to insert code into processes to avoid process-based defenses.

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

- **Corporate cybersecurity teams** invest in fortified cybersecurity defenses, proactive threat detection, and mitigation strategies, ensuring better protection of critical assets and data.
- **Individual professionals** learn advanced skills in evading antivirus, tampering with event logs, and bypassing security measures.

Earning an OffSec MITRE ATT&CK learning badge

Learners will be proficient in identifying and exploiting vulnerabilities in security mechanisms, enhancing their ability to assess and mitigate cybersecurity risks effectively.

FAQ

What's the syllabus?

- Antivirus Evasion
- Working with Packed Malware
- Introduction to Antivirus Evasion
- Advanced Antivirus Evasion
- Automating Event Log Tampering
- Windows Event Log Tampering Techniques
- Application Whitelisting
- Process Injection For Red Teamers
- Bypassing GateKeeper

What skills are associated with this Learning Path?

- Defense Evasion
- Malware Analysis
- Windows Attacks
- Exploit Development - macOS

What job roles are associated with this Learning Path?

- SOC Analyst
- Network Penetration Tester
- Security Researcher
- Incident Responder
- Threat Hunter
- System administrator

Who is this Learning Path designed for?

This learning path is tailored for roles like red teamers, penetration testers, and cybersecurity analysts, it equips learners with advanced skills in evading antivirus, tampering with event logs, and bypassing security measures.

Are there any prerequisites?

This learning path is considered an intermediate level learning path and learners should have completed EXP-100.

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

This self-paced path is designed for flexibility, typically taking 120 hours to complete. It includes text based content and 50 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise