Red Teaming with Post-Exploitation Techniques Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapidly evolving threat landscape mandates a shift from traditional vulnerability assessment to full-scope Adversary Emulation. Organizations with mature security postures require exercises that move beyond basic Penetration Testing to simulate the tactics, techniques, and procedures (TTPs) of sophisticated Advanced Persistent Threats (APTs). Red Teaming with Post-Exploitation Techniques Training Course instills the Adversary Mindset, teaching participants how to plan, execute, and report on covert, multi-staged Red Team Operations. The primary focus is on achieving defined objectives while maintaining Stealth and Evasion, forcing the Blue Team's detection and response capabilities to their absolute limit. Strong keywords: Adversary Emulation, Penetration Testing, Advanced Persistent Threats (APTs), Red Team Operations, Stealth and Evasion, Blue Team, TTPs, Adversary Mindset.

A successful initial breach is only the first step; the true measure of a red team's skill lies in its Post-Exploitation Tradecraft. This training dives deep into the complex world of maintaining Persistence, achieving Lateral Movement, performing Privilege Escalation in challenging environments like Active Directory, and establishing covert Command and Control (C2) infrastructure. Learners will master advanced techniques such as Living Off The Land (LOTL) binaries, Credential Access in memory, and Data Exfiltration via obscure channels. By mastering these Offensive Security techniques, participants will gain the essential knowledge to effectively test, measure, and enhance the defensive capabilities of modern enterprise environments. Strong keywords: Post-Exploitation Tradecraft, Persistence, Lateral Movement, Privilege Escalation, Active Directory, Command and Control (C2), Offensive Security, Living Off The Land (LOTL), Credential Access, Data Exfiltration.

Programme Curriculum

Red Teaming with Post-Exploitation Techniques Training Course

Introduction

The rapidly evolving threat landscape mandates a shift from traditional vulnerability assessment to full-scope Adversary Emulation. Organizations with mature security postures require exercises that move beyond basic Penetration Testing to simulate the tactics, techniques, and procedures (TTPs) of sophisticated Advanced Persistent Threats (APTs). Red Teaming with Post-Exploitation Techniques Training Course instills the Adversary Mindset, teaching participants how to plan, execute, and report on covert, multi-staged Red Team Operations. The primary focus is on achieving defined objectives while maintaining Stealth and Evasion, forcing the Blue Team's detection and response capabilities to their absolute limit. Strong keywords: Adversary Emulation, Penetration Testing, Advanced Persistent Threats (APTs), Red Team Operations, Stealth and Evasion, Blue Team, TTPs, Adversary Mindset.

A successful initial breach is only the first step; the true measure of a red team's skill lies in its Post-Exploitation Tradecraft. This training dives deep into the complex world of maintaining Persistence, achieving Lateral Movement, performing Privilege Escalation in challenging environments like Active Directory, and establishing covert Command and Control (C2) infrastructure. Learners will master advanced techniques such as Living Off The Land (LOTL) binaries, Credential Access in memory, and Data Exfiltration via obscure channels. By mastering these Offensive Security techniques, participants will gain the essential knowledge to effectively test, measure, and enhance the defensive capabilities of modern enterprise environments. Strong keywords: Post-Exploitation Tradecraft, Persistence, Lateral Movement, Privilege Escalation, Active Directory, Command and Control (C2), Offensive Security, Living Off The Land (LOTL), Credential Access, Data Exfiltration.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Formulate a covert Adversary Emulation Plan aligned with specific business objectives and the MITRE ATT&CK Framework.
2. Conduct advanced Open-Source Intelligence and Reconnaissance for target profiling and initial access vector identification.
3. Execute sophisticated Initial Access methods, including weaponized documents and client-side exploits.
4. Develop custom Malware and Payloads that successfully bypass modern Endpoint Detection and Response solutions.
5. Establish and manage resilient, stealthy Command and Control (C2) infrastructure using Domain Fronting and custom profiles.
6. Master Windows and Linux Persistence Techniques to maintain access across reboots and patching cycles.
7. Perform thorough Internal Reconnaissance and enumeration, with a focus on Active Directory Exploitation.
8. Execute complex Lateral Movement strategies, including Pass-the-Hash and WMI exploitation, without detection.
9. Achieve high-impact Privilege Escalation using advanced misconfiguration and kernel exploitation techniques.
10. Utilize Credential Access tools safely and effectively to harvest plaintext passwords and Kerberos tickets.

11. Demonstrate effective Defense Evasion techniques, including process injection, API unhooking, and Memory Hollowing.
12. Simulate critical Impact & Data Exfiltration scenarios via non-standard protocols.
13. Generate a comprehensive Red Team Report and participate in a formal Purple Teaming Debrief for maximum organizational value.

Target Audience

1. Experienced Penetration Testers.
2. Security Analysts/Engineers.
3. Threat Hunters.
4. Blue Team members and Incident Responders.
5. Security Consultants.
6. SOC Analysts
7. IT/System Administrators.
8. Cybersecurity Researchers.

Course Modules

Module 1: Red Teaming Fundamentals and Threat Modeling

- Define the Red Team lifecycle, Adversary Emulation, and ethical Rules of Engagement.
- In-depth analysis and mapping to the MITRE ATT&CK Framework.
- Master advanced OSINT techniques
- Case Study: The NotPetya Attack ?Çô Analyzing the initial access, rapid Lateral Movement, and final catastrophic impact to map TTPs.
- Develop a comprehensive, covert Adversary Emulation Plan for an enterprise target.

Module 2: Initial Access and Evasion

- Weaponization of documents and files for client-side execution.
- Crafting undetectable Phishing Campaigns using advanced techniques
- Exploiting common external vulnerabilities
- Case Study: Target Breach ?Çô Focus on the initial access via a third-party vendor's HVAC system and the pivot into the retail network.
- Introduction to Antivirus (AV) Evasion and basic Payload Obfuscation.

Module 3: Command and Control (C2) Infrastructure

- Setup and configuration of resilient C2 Frameworks
- Developing custom C2 Profiles for Defense Evasion and traffic mimicry.
- Implementing Domain Fronting and Cloud Egress for stealthy communication.
- Case Study: APT29 C2 Tradecraft ?Çô Analysis of their use of legitimate cloud services and custom C2 to bypass detection.
- Utilizing Covert Channels for low-and-slow communication.

Module 4: Windows Post-Exploitation and Credential Access

- Detailed Internal Reconnaissance on Windows systems and basic network enumeration.
- Mastering Credential Access via memory dumping
- Utilizing Pass-the-Hash, Pass-the-Ticket, and Token Impersonation.

- Case Study: SolarWinds/SUNBURST ?Çô Deep dive into how attackers used trusted access and credential abuse for widespread access.
- Working with PowerShell and Living Off The Land binaries for fileless execution.

Module 5: Active Directory and Lateral Movement

- Advanced Active Directory Enumeration using tools like BloodHound and SharpHound.
- Exploiting misconfigurations and vulnerabilities
- Executing sophisticated Lateral Movement techniques
- Case Study: WannaCry/EternalBlue ?Çô Analysis of how a single vulnerability and Lateral Movement via SMB spread rapidly through networks.
- Bypassing and manipulating Group Policy Objects for persistence.

Module 6: Privilege Escalation and Persistence

- Local Privilege Escalation techniques on Windows
- Linux Privilege Escalation
- Establishing Persistence Mechanisms in Windows
- Case Study: Palo Alto Networks Red Team ?Çô Focus on a specific AD misconfiguration exploitation that led to a Domain Admin compromise.
- Stealthy Persistence in Linux

Module 7: Advanced Defense Evasion and Tradecraft

- Advanced EDR Evasion techniques
- Executing Fileless Malware and in-memory attacks to avoid disk forensics.
- Advanced Obfuscation and custom tool Staging and deployment.
- Case Study: FIN7's Custom Evasion Tools ?Çô Exploring their highly customized malware and loaders designed to bypass specific enterprise security products.
- Operational Security best practices to prevent team compromise and maximize Stealth.

Module 8: Impact, Reporting, and Purple Teaming

- Simulating impact scenarios
- Techniques for staged Data Exfiltration using non-standard or trusted protocols.
- Developing a concise, high-impact Red Team Report for executive and technical audiences.
- Case Study: Mandiant FireEye Red Team Tool Theft ?Çô Analysis of the post-compromise response and how security vendors leverage such events for defensive improvement.
- Conducting a full Purple Teaming exercise: joint debriefing with the Blue Team for detection and prevention tuning.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.

- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com