Post-Exploitation and Lateral Movement 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

This intensive, hands-on training course dives deep into the Cyber Kill Chain's crucial phases of Post-Exploitation and Lateral Movement, equipping participants with the offensive security skills required to emulate real-world advanced persistent threats (APTs). Modern cyberattacks rarely end at the initial breach; sophisticated adversaries utilize a range of stealth techniques including credential harvesting, privilege escalation, and internal reconnaissance to maintain a persistent presence and navigate an organization's internal network. This course bridges the gap between initial system compromise and achieving the attacker's ultimate goal, be it data exfiltration or system sabotage. By mastering these advanced tactics, techniques, and procedures (TTPs), attendees will significantly enhance their capabilities as Penetration Testers and Red Team operators, or bolster their skills for Threat Hunting and Incident Response teams.

Post-Exploitation and Lateral Movement Training Course is meticulously designed around the MITRE ATT&CK Framework, focusing on practical, enterprise-level network penetration testing scenarios across both Windows and Linux environments. Participants will gain practical experience with industry-standard tools like Metasploit, Mimikatz, and Impacket, learning how to establish persistence, pivot through segmented networks, and evade modern Endpoint Detection and Response (EDR) solutions. Through comprehensive hands-on labs and real-world case studies, this training provides the indispensable knowledge for moving beyond simple exploitation to become a true network adversary, ultimately enabling organizations to build more resilient security architectures and implement effective defense-in-depth strategies.

Programme Curriculum

Post-Exploitation and Lateral Movement Training Course

Introduction

This intensive, hands-on training course dives deep into the Cyber Kill Chain's crucial phases of Post-Exploitation and Lateral Movement, equipping participants with the offensive security skills required to emulate real-world advanced persistent threats (APTs). Modern cyberattacks rarely end at the initial breach; sophisticated adversaries utilize a range of stealth techniques including credential harvesting, privilege escalation, and internal reconnaissance to maintain a persistent presence and navigate an organization's internal network. This course bridges the gap between initial system compromise and achieving the attacker's ultimate goal, be it data exfiltration or system sabotage. By mastering these advanced tactics, techniques, and procedures (TTPs), attendees will significantly enhance their capabilities as Penetration Testers and Red Team operators, or bolster their skills for Threat Hunting and Incident Response teams.

Post-Exploitation and Lateral Movement Training Course is meticulously designed around the MITRE ATT&CK Framework, focusing on practical, enterprise-level network penetration testing scenarios across both Windows and Linux environments. Participants will gain practical experience with industry-standard tools like Metasploit, Mimikatz, and Impacket, learning how to establish persistence, pivot through segmented networks, and evade modern Endpoint Detection and Response (EDR) solutions. Through comprehensive hands-on labs and real-world case studies, this training provides the indispensable knowledge for moving beyond simple exploitation to become a true network adversary, ultimately enabling organizations to build more resilient security architectures and implement effective defense-in-depth strategies.

Course Duration

5 days

Course Objectives with Strong Trending Keywords

1. Master Post-Exploitation fundamentals, including maintaining persistent access and foothold establishment.
2. Perform advanced Privilege Escalation on both Windows and Linux systems.
3. Execute effective Internal Network Reconnaissance and Network Mapping techniques post-compromise.
4. Utilize Credential Harvesting and Dumping methods, focusing on tools like Mimikatz and LSASS attack vectors.
5. Understand and perform Pass-the-Hash (PtH), Pass-the-Ticket (PtT), and Kerberoasting for Lateral Movement.
6. Articulate and practically apply MITRE ATT&CK techniques related to lateral movement and persistence.
7. Deploy and manage sophisticated Command and Control (C2) frameworks while employing Evasion Tactics.
8. Implement various Pivoting and Tunneling techniques to traverse segmented networks.
9. Exploit Active Directory misconfigurations for domain-wide compromise.
10. Conduct Data Staging and Exfiltration using covert channels and modern cloud vectors.
11. Develop Detection Evasion strategies against modern EDR/XDR solutions and security tooling.
12. Formulate Remediation Strategies and provide effective Security Architecture recommendations.
13. Apply professional Red Team Methodology for end-to-end network penetration testing engagements.

Target Audience

1. Penetration Testers.
2. Security Analysts looking to understand attacker TTPs for Threat Hunting.
3. Red Team Operators who want to master lateral movement and persistence.
4. Incident Responders needing deep insight into post-breach attacker actions.

5. Blue Team members focused on defensive architecture and monitoring.
6. Security Engineers responsible for implementing EDR and security controls.
7. Ethical Hackers preparing for advanced certifications.
8. Security Consultants focused on enterprise-level network assessments.

Course Modules

Module 1: The Post-Exploitation Imperative

- Initial Foothold and establishing Session Hijacking.
- In-depth study of TTPs and the Cyber Kill Chain post-exploitation phase.
- The essential use of Stagers and Payloads for initial access.
- Internal Reconnaissance methodologies: system and network enumeration.
- Case Study: Analyzing the initial backdoor and enumeration phase in the SolarWinds Attack.

Module 2: Persistence and Backdoors

- Techniques for creating Persistent Access on Windows
- Establishing Reverse Shells and Bind Shells for reliable connectivity.
- Using C2 Frameworks for session management.
- Deploying Backdoors and Rootkits to evade detection and maintain control.
- Case Study: Reviewing the persistence mechanisms used by the Emotet Malware across corporate networks.

Module 3: Privilege Escalation Techniques

- Local Privilege Escalation on Windows.
- Linux Privilege Escalation.
- Automating privilege checks with tools like PowerSploit and LinPEAS/WinPEAS.
- Exploiting Unquoted Service Paths and vulnerable registry permissions.
- Case Study: Demonstrating a vulnerable service exploitation that leads to SYSTEM level access.

Module 4: Credential Harvesting and Dumping

- Techniques for Credential Dumping from memory.
- Practical use of Mimikatz and its core functionalities
- Harvesting credentials from browsers, stored files, and configuration databases.
- Understanding the risks of Plaintext Passwords and effective hash cracking.
- Case Study: Simulating a successful Mimikatz execution to extract domain administrator hashes.

Module 5: Windows Lateral Movement and Active Directory Attacks

- Moving laterally using legitimate protocolsDeep dive into Active Directory attack paths and misconfigurations.
- Performing Pass-the-Hash and Over-Pass-the-Hash attacks.
- Executing Kerberos Attacks.
- Case Study: Tracing the lateral movement in the Colonial Pipeline incident via compromised VPN and RDP.

Module 6: Network Pivoting and Tunneling

- Introduction to network segmentation and the need for Pivoting.

- Setting up SOCKS Proxies and port forwarding using SSH, Metasploit, or Chisel.
- Creating Proxy Chains to obscure the attack path and bypass perimeter defenses.
- Utilizing DNS Tunneling and other covert channels for command and control.
- Case Study: A multi-segment network environment lab requiring chained SOCKS Proxy pivots to reach a target database.

Module 7: Evasion and Anti-Forensics

- Strategies for Evading EDR and modern defense mechanisms.
- Techniques for Anti-Virus Evasion and payload obfuscation.
- Anti-Forensics methods: clearing logs, modifying timestamps, and deleting evidence.
- Process Injection and Code Caves for stealthy execution.
- Case Study: Using memory-only payloads and custom injection to bypass a simulated Next-Gen Antivirus

Module 8: Data Exfiltration and Finalizing the Engagement

- Data Staging methods: gathering target data into a single, compressed location.
- Covert Data Exfiltration techniques.
- Post-engagement cleanup and maintaining the integrity of the target environment.
- Professional Reporting and translating technical findings into business risk.
- Case Study: Documenting the Target Data Breach kill chain, from HVAC compromise to massive Data Exfiltration.

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
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