Professional Penetration Testing and Exploit Development 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

Professional Penetration Testing and Exploit Development Training Course is designed to transform experienced security practitioners into elite Exploit Developers and Red Team operators. The modern threat landscape is dominated by sophisticated cyber threats and complex chained exploits targeting critical infrastructure like Cloud Configurations and vulnerable APIs. Traditional penetration testing is shifting from a yearly ritual to Continuous Pentesting integrated with CI/CD pipelines. This course provides a deep dive into Vulnerability Research, Advanced Exploit Writing, and Post-Exploitation techniques, moving beyond automated tooling to foster the critical, contextual thinking required to identify and leverage zero-day and complex, low-severity, but high-impact logical flaws. By mastering low-level programming, Reverse Engineering, and the art of bypassing contemporary security mitigations like DEP and ASLR, participants will be equipped with the offensive skills to perform the most demanding security assessments, ensuring they can anticipate, simulate, and ultimately help defend against the attacks of 2025 and beyond.

Our methodology is heavily focused on hands-on labs and real-world Adversary Emulation. We believe that defense is only as strong as the attacker's perspective, which is why we emphasize the cyber-attack lifecycle from reconnaissance to maintaining persistent access. Students will engage in practical exercises covering Windows User Mode exploitation, Linux Kernel vulnerability analysis, Web Application logic flaw exploitation, and advanced Social Engineering tactics. The course culminates in an intensive Red Team-style final challenge, requiring the chaining of multiple low-severity issues to achieve a business-critical compromise. Successful completion of this program certifies a mastery of the tools, techniques, and mindset required to excel as a top-tier security researcher and professional exploit writer, making participants indispensable assets in the fight against Advanced Persistent Threats (APTs).

Programme Curriculum

Professional Penetration Testing and Exploit Development Training Course

Introduction

Professional Penetration Testing and Exploit Development Training Course is designed to transform experienced security practitioners into elite Exploit Developers and Red Team operators. The modern threat landscape is dominated by sophisticated cyber threats and complex chained exploits targeting critical infrastructure like Cloud Configurations and vulnerable APIs. Traditional penetration testing is shifting from a yearly ritual to Continuous Pentesting integrated with CI/CD pipelines. This course provides a deep dive into Vulnerability Research, Advanced Exploit Writing, and Post-Exploitation techniques, moving beyond automated tooling to foster the critical, contextual thinking required to identify and leverage zero-day and complex, low-severity, but high-impact logical flaws. By mastering low-level programming, Reverse Engineering, and the art of bypassing contemporary security mitigations like DEP and ASLR, participants will be equipped with the offensive skills to perform the most demanding security assessments, ensuring they can anticipate, simulate, and ultimately help defend against the attacks of 2025 and beyond.

Our methodology is heavily focused on hands-on labs and real-world Adversary Emulation. We believe that defense is only as strong as the attacker's perspective, which is why we emphasize the cyber-attack lifecycle from reconnaissance to maintaining persistent access. Students will engage in practical exercises covering Windows User Mode exploitation, Linux Kernel vulnerability analysis, Web Application logic flaw exploitation, and advanced Social Engineering tactics. The course culminates in an intensive Red Team-style final challenge, requiring the chaining of multiple low-severity issues to achieve a business-critical compromise. Successful completion of this program certifies a mastery of the tools, techniques, and mindset required to excel as a top-tier security researcher and professional exploit writer, making participants indispensable assets in the fight against Advanced Persistent Threats (APTs).

Course Duration

5 days

Course Objectives

1. Master Advanced Exploit Writing techniques for both Windows and Linux, specifically targeting modern operating systems.
2. Perform in-depth Vulnerability Research and Root Cause Analysis on proprietary and open-source software to discover original flaws.
3. Develop custom Shellcode and payloads from scratch, overcoming size and platform constraints.
4. Bypass critical security mitigations including DEP, ASLR, Stack Canaries, and Control-Flow Integrity (CFI) using advanced techniques like ROP Chains and JOP.
5. Conduct professional-grade Reverse Engineering of binary applications and network protocols using tools like IDA Pro and Ghidra.
6. Understand and exploit the unique security challenges presented by Cloud Configurations and Serverless architectures.
7. Identify and exploit vulnerabilities in complex APIs, a rapidly growing, high-risk asset.
8. Execute Post-Exploitation strategies, including lateral movement, privilege escalation, and maintaining persistent access.
9. Integrate Python and PowerShell scripting for Security Automation of reconnaissance, scanning, and custom tool development.
10. Apply Active Directory (AD) and Kerberos exploitation techniques, including common attacks like Golden Ticket and Kerberoasting.
11. Simulate multi-stage, Adversary Emulation scenarios, practicing the Red Team methodology.

12. Analyze and report findings with Comprehensive Reporting that details technical vulnerabilities and provides business-contextualized remediation advice.
13. Leverage basic Generative AI and Machine Learning tools to assist in code review and vulnerability discovery, understanding both their offensive and defensive implications.

Target Audience

1. Intermediate-to-Advanced Penetration Testers.
2. Security Researchers.
3. Malware Analysts and Threat Intelligence professionals.
4. Software Engineers and Developers.
5. Blue Team members and Incident Responders.
6. Cybersecurity Consultants and Architects responsible for high-risk system security.
7. Individuals pursuing certifications like OSED, OSCE3, or GXPN.
8. Technical Leaders overseeing application and infrastructure security teams.

Course Modules

Module 1: Foundational Reverse Engineering & Binary Analysis

- Introduction to x86/x64 Assembly and Processor Architecture
- Mastering IDA Pro/Ghidra for static and dynamic analysis and patching.
- Advanced WinDbg/GDB debugging and memory manipulation techniques.
- Identifying and analyzing different file formats and section headers.
- Case Study: Analyzing a real-world, patched CVE to understand the root cause and initial exploitation vector.

Module 2: Classic Stack & Heap Buffer Overflows

- Detailed breakdown of Stack Buffer Overflow vulnerabilities and stack frame manipulation.
- Developing reliable exploit code against basic protections and non-executable stacks.
- Introduction to Heap Spraying and various Heap Exploitation techniques.
- Writing an Egghunter to overcome shellcode size restrictions and execute payloads reliably.
- Case Study: Exploiting an older, vulnerable network service to achieve remote code execution.

Module 3: Advanced Exploit Mitigation Bypass

- The science of Data Execution Prevention and its software/hardware implementations.
- Crafting Return-Oriented Programming chains on Windows and Linux to execute arbitrary functions.
- Bypassing Address Space Layout Randomization using techniques like Partial Overwrites and Information Leaks.
- Exploiting SEH Overflows and Structured Exception Handling for code redirection.
- Case Study: Developing a full-chain exploit to bypass DEP/ASLR on a recent version of Windows using a complex ROP chain.

Module 4: Custom Shellcode and Payload Development

- Writing Position-Independent Code and polymorphic shellcode from scratch.
- Advanced payload encoding, decoding, and encryption to evade anti-virus
- Developing Staged and Stageless payloads for various attack scenarios.
- Creating custom command-and-control communication channels and exfiltration methods.

- Case Study: Building a custom, encrypted C2 backdoor using Python/C++ that mimics legitimate network traffic to bypass IDS/IPS.

Module 5: Web Application Exploit Chaining & Logic Flaws

- Exploiting critical web vulnerabilities beyond the OWASP Top 10, focusing on API Vulnerabilities.
- In-depth look at exploiting Deserialization Vulnerabilities and prototype pollution.
- Identifying and chaining low-severity flaws into high-impact breaches.
- Advanced SQL Injection and Cross-Site Scripting payload crafting for post-exploitation.
- Case Study: Chaining an API-based IDOR with a low-severity file upload vulnerability for a full server compromise.

Module 6: Enterprise Infrastructure & Active Directory Exploitation

- Advanced Network Protocol Fuzzing for service discovery and vulnerability finding.
- In-depth Active Directory Enumeration and initial access vectors.
- Executing classic AD attacks: Kerberoasting, Pass-the-Hash/Ticket, and abusing misconfigurations.
- Techniques for Lateral Movement and Domain Privilege Escalation within an enterprise network.
- Case Study: Simulating a breach scenario by exploiting an AD misconfiguration to gain control of a Domain Controller.

Module 7: Cloud & Container Security Exploitation

- Understanding the Cloud Attack Surface in AWS, Azure, and GCP.
- Exploiting misconfigured IAM Policies and Cloud Storage Buckets.
- Attacking containerized environments through exposed APIs and insecure configurations.
- Serverless exploitation and Function-as-a-Service security.
- Case Study: Exploiting a vulnerable AWS S3 Bucket Policy or an overly permissive Azure/GCP service principal to pivot and steal sensitive data.

Module 8: Adversary Emulation & Professional Methodology

- Structuring a professional, goal-oriented Red Team Engagement using the MITRE ATT&CK Framework.
- Developing an effective Vulnerability Disclosure and Comprehensive Reporting plan.
- Hands-on experience with post-exploitation frameworks.
- Understanding ethical and legal boundaries, including the principle of "getting the flag and stopping."
- Case Study: An end-to-end APT Simulation requiring chained exploits, evasion, and stealth to compromise a mock critical system.

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