Exploit Development and Shellcoding 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 into the sophisticated world of Exploit Development and Shellcoding, focusing critically on the Data Security implications and the creation of Proactive Defenses. In today's landscape, where Advanced Persistent Threats and AI-Powered Cyberattacks are the norm, defense-only strategies are insufficient. Elite security professionals must master the attacker's mindset, a skill developed by learning to identify and weaponize vulnerabilities in modern software and complex architectures. This course is your path to becoming a top-tier expert, moving beyond simple Metasploit usage to custom-crafting zero-day exploits and writing position-independent shellcode for contemporary operating systems.

Exploit Development and Shellcoding Training Course is designed to arm students with a deep, low-level understanding of memory management, CPU architecture, and current security mitigations like ASLR, DEP, and CFG. You'll gain practical, real-world experience in Vulnerability Analysis, Reverse Engineering, and Heap Exploitation, skills critical for high-stakes roles in Red Teaming, Threat Intelligence, and Software Security Architecture. By learning to exploit, you learn to defend fortifying systems, validating security controls, and designing truly secure coding practices that stand up to the most challenging threats, thereby closing the dangerous attack surface of modern enterprise applications, especially those in Cloud and IoT environments.

Programme Curriculum

Exploit Development and Shellcoding Training Course

Introduction

This intensive, hands-on training course dives into the sophisticated world of Exploit Development and Shellcoding, focusing critically on the Data Security implications and the creation of Proactive Defenses. In

today's landscape, where Advanced Persistent Threats and AI-Powered Cyberattacks are the norm, defense-only strategies are insufficient. Elite security professionals must master the attacker's mindset, a skill developed by learning to identify and weaponize vulnerabilities in modern software and complex architectures. This course is your path to becoming a top-tier expert, moving beyond simple Metasploit usage to custom-crafting zero-day exploits and writing position-independent shellcode for contemporary operating systems.

Exploit Development and Shellcoding Training Course is designed to arm students with a deep, low-level understanding of memory management, CPU architecture, and current security mitigations like ASLR, DEP, and CFG. You'll gain practical, real-world experience in Vulnerability Analysis, Reverse Engineering, and Heap Exploitation, skills critical for high-stakes roles in Red Teaming, Threat Intelligence, and Software Security Architecture. By learning to exploit, you learn to defend fortifying systems, validating security controls, and designing truly secure coding practices that stand up to the most challenging threats, thereby closing the dangerous attack surface of modern enterprise applications, especially those in Cloud and IoT environments.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Master Vulnerability Analysis and Reverse Engineering of C/C++ binaries on Windows/Linux.
2. Develop reliable Stack-Based Buffer Overflow exploits against contemporary operating systems.
3. Write custom, NULL-free, position-independent shellcode for diverse architectures.
4. Bypass Data Execution Prevention (DEP) using Return-Oriented Programming (ROP) Chains.
5. Defeat Address Space Layout Randomization (ASLR) through effective Information Leakage and non-rebased module exploitation.
6. Understand and exploit advanced memory corruption techniques like Use-After-Free and Format String Vulnerabilities.
7. Analyze and manipulate the Windows/Linux Heap Manager for advanced Heap Exploitation.
8. Implement exploit strategies against modern browser and kernel vulnerabilities, including Sandbox Escape.
9. Integrate Defensive Coding Practices and principles of Secure by Design into the software development lifecycle.
10. Analyze the effectiveness of modern mitigations such as Control-Flow Guard (CFG) and Hardware-Assisted Enforcement.
11. Perform Fuzzing and Triage using industry-standard tools for Zero-Day Vulnerability discovery.
12. Design and deploy comprehensive Blue Team defenses and Threat Hunting mechanisms against custom shellcode.
13. Apply acquired knowledge in a final Capture the Flag Capstone exercise targeting a hardened environment.

Target Audience

1. Red Team Operators and Advanced Penetration Testers
2. Vulnerability Researchers and Bug Bounty Hunters
3. Malware Analysts and Reverse Engineers
4. Security Architects and Application Security Engineers
5. Blue Team and Threat Hunters seeking the attacker perspective
6. Software Developers focused on Secure Coding and Defense-in-Depth

7. Government/Military Cyber Warfare and Intelligence Analysts
8. Security consultants preparing for certifications like OffSec Exploit Developer

Course Modules

Module 1: Foundational Memory and x86/x64 Architecture

- Assembly Language Deep Dive.
- Stack, Heap, Data Segments, and Virtual Memory Management.
- Calling Conventions and Stack Frame Layouts on Windows and Linux.
- Tool Proficiency.
- Case Study: Dissecting the memory layout of a high-profile CVE to identify the vulnerable function and data flow.

Module 2: Classic Stack-Based Exploitation

- Introduction to Buffer Overflow vulnerabilities and control-flow hijacking.
- Overwriting the Saved Return Pointer to redirect execution flow.
- Exploiting Structured Exception Handlers on Windows.
- Dealing with Bad Characters and space constraints via Egghunting.
- Case Study: Developing a remote exploit for a retired Windows service that utilizes SEH to achieve code execution.

Module 3: Custom Shellcode Development

- Writing Position-Independent Code and NULL-Free Shellcode.
- Creating reverse shells, bind shells, and Stageless Shellcode payloads.
- Encoding techniques to bypass basic filters.
- Import Address Table and Export Address Table resolution.
- Case Study: Manually crafting a Linux x64 reverse shell payload that uses the syscall instruction without any call to external libraries.

Module 4: Bypassing Data Execution Prevention

- Understanding DEP and the move from Executable Stacks to NX Bit.
- Return-to-libc and Return-Oriented Programming theory.
- Building basic ROP Chains using ROP Gadgets and rop-chain builders.
- Practical implementation of a DEP bypass on a Windows application.
- Case Study: Developing a DEP-bypass exploit for a vulnerable application, chaining ROP gadgets to call VirtualAlloc.

Module 5: Defeating Address Space Layout Randomization (ASLR)

- ASLR fundamentals, Entropy, and the concept of Information Leakage.
- Exploiting non-rebased modules and the use of Partial Overwrites.
- Forcing an Info Leak to defeat randomization.
- Advanced techniques for full-ASLR bypass via JIT-Spray and other memory-shaping methods.
- Case Study: Creating a two-stage exploit for a Linux server that leaks a stack address to calculate a return address for full ASLR defeat.

Module 6: Advanced Memory Corruption

- In-depth analysis of Heap Corruption and the internal workings of the heap manager.
- Exploiting Use-After-Free and Double-Free vulnerabilities.
- Exploiting Format String Vulnerabilities to read/write arbitrary memory.
- Introduction to exploitation on hardened targets: Browsers and Kernels.
- Case Study: Exploiting a UAF bug in a simplified browser component to corrupt object pointers and gain arbitrary write primitive.

Module 7: Mitigations and Defense-in-Depth

- Analysis of modern mitigations.
- Advanced Fuzzing techniques for Zero-Day discovery and automated crash triage.
- Threat Modeling and integrating Data Security principles into exploit validation.
- DevSecOps and Secure Coding principles to prevent memory-related bugs.
- Case Study: Applying fuzzing to an existing network service to find a novel vulnerability, and then immediately documenting a secure code fix

Module 8: Real-World Scenarios and Capstone

- Exploiting Cloud-Native vulnerabilities and Container Escapes.
- Techniques for EDR/AV Evasion using custom shellcode execution methods.
- Creating and porting exploits into standardized frameworks
- Final CTF Challenge incorporating all learned exploit and mitigation bypass techniques.
- Case Study: Simulating a Red Team engagement: exploiting a COTS application, achieving persistence, and bypassing a simplified EDR/Blue Team monitor.

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.com 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
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now

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