Practical Malware 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

The modern cybersecurity landscape is defined by an ever-evolving arms race between defenders and sophisticated threat actors. To effectively implement proactive defenses and perform cutting-edge threat hunting, security professionals must intimately understand the mindset, methodologies, and tools of the adversary. Practical Malware Development Training Course is designed for the professional seeking to master the low-level offensive techniques that underpin contemporary Advanced Persistent Threats. By diving deep into the Windows Internals and utilizing languages like C/C++ and Assembly, students will learn to develop custom, highly evasive proof-of-concept malicious software. This practical knowledge is crucial not only for Red Team operations and Penetration Testing but also for Blue Team members dedicated to designing robust detection and Endpoint Detection and Response (EDR) bypass strategies, ensuring a truly comprehensive understanding of offensive security.

This specialized curriculum focuses heavily on anti-analysis techniques and low-level system programming, bridging the gap between theoretical knowledge and practical binary exploitation. Key areas covered include process injection, reflective DLL loading, API hooking, and various Command and Control (C2) communication methods. The course emphasizes a learn-by-doing approach within a controlled, safe environment, culminating in the development of a functional, custom malware implant. Graduates will possess the skills to create custom tooling that surpasses the capabilities of off-the-shelf exploit frameworks, making them invaluable assets in fields like Incident Response, Threat Intelligence, and Malware Analysis the most trending keywords in enterprise security today.

Programme Curriculum

Practical Malware Development Training Course

Introduction

The modern cybersecurity landscape is defined by an ever-evolving arms race between defenders and sophisticated threat actors. To effectively implement proactive defenses and perform cutting-edge threat hunting, security professionals must intimately understand the mindset, methodologies, and tools of the adversary. Practical Malware Development Training Course is designed for the professional seeking to master the low-level offensive techniques that underpin contemporary Advanced Persistent Threats. By diving deep into the Windows Internals and utilizing languages like C/C++ and Assembly, students will learn to develop custom, highly evasive proof-of-concept malicious software. This practical knowledge is crucial not only for Red Team operations and Penetration Testing but also for Blue Team members dedicated to designing robust detection and Endpoint Detection and Response (EDR) bypass strategies, ensuring a truly comprehensive understanding of offensive security.

This specialized curriculum focuses heavily on anti-analysis techniques and low-level system programming, bridging the gap between theoretical knowledge and practical binary exploitation. Key areas covered include process injection, reflective DLL loading, API hooking, and various Command and Control (C2) communication methods. The course emphasizes a learn-by-doing approach within a controlled, safe environment, culminating in the development of a functional, custom malware implant. Graduates will possess the skills to create custom tooling that surpasses the capabilities of off-the-shelf exploit frameworks, making them invaluable assets in fields like Incident Response, Threat Intelligence, and Malware Analysis the most trending keywords in enterprise security today.

Course Duration

5 days

Course Objectives

1. Gain an expert-level understanding of Windows OS Internals.
2. Master C/C++ and the WinAPI for developing native, high-performance malicious software.
3. Develop custom Position-Independent Code and advanced Shellcode for payload delivery.
4. Implement various Process Injection methods like APC Queue, Classic DLL Injection, and Process Hollowing for stealth.
5. Identify, understand, and develop techniques to bypass modern EDR and Antivirus (AV) solutions
6. Implement robust and hidden Persistence techniques in target systems.
7. Design and implement Command and Control (C2) channels using covert protocols
8. Apply String Obfuscation, API Hashing, and Anti-Debugging/VM checks to hinder reverse engineering.
9. Develop and utilize Reflective DLL Loading techniques to execute code entirely in memory.
10. Build a multi-stage, modular Malware Implant from scratch, demonstrating full attack lifecycle capabilities.
11. Integrate Lateral Movement techniques into custom payloads.
12. Translate offensive skills into defensive strategies for Threat Intelligence and YARA Rule creation.
13. Create practical Red Team tools and proof-of-concepts for authorized offensive security assessments.

Target Audience

1. Red Team Operators/Penetration Testers.
2. Malware Analysts/Reverse Engineers.
3. Security Software Developers.
4. Threat Hunters
5. Incident Responders.
6. Security Researchers.

7. Cybersecurity Architects
8. Senior Security Engineers.

Course Modules

Module 1: Foundations of Offensive Programming

- Deep Dive into Windows Internals.
- C/C++ and WinAPI Refresher.
- PE File Format Exploration.
- Introduction to Assembly
- Lab Setup and Tooling
- Case Study: Analyzing the PE header of Petya or NotPetya to understand how it modified the boot sector/MFT.

Module 2: Shellcode & Basic Execution

- Custom Shellcode Development.
- Encoding and Decoding Payloads.
- Basic Code Injection.
- Staged Payloads.
- Direct System Calls.
- Case Study: Developing a custom Metasploit-style reverse-shell payload and analyzing the system calls it generates.

Module 3: Advanced Process Injection & Evasion

- Process Hollowing and Doppelg?ñnging.
- APC Queue Injection.
- Reflective DLL Loading.
- Manual Mapping of Executables
- Hiding Threads and Processes.
- Case Study: Implementing a basic RDLL to mimic the loading process seen in the Cobalt Strike Beacon.

Module 4: EDR/AV Anti-Analysis Techniques

- Anti-Debugging & Anti-VM Checks.
- API Hashing and Dynamic Resolution.
- String and Data Obfuscation.
- Un-Hooking EDR/AV Hooks
- Memory Evasion.
- Case Study: Modifying a simple dropper to implement Anti-VM checks, preventing execution on automated sandboxes like Any.Run.

Module 5: Persistence and Privilege Escalation

- Common Persistence Methods.
- Service and Driver Persistence.
- WMI and COM Hijacking.
- Token Impersonation and Manipulation.
- UAC Bypass Techniques.

- Case Study: Developing a persistence mechanism using a WMI Event Consumer (as seen in some state-sponsored attacks) and detecting it with Windows Event Logs.

Module 6: Command and Control (C2)

- Basic TCP/HTTP C2.
- Covert C2 using DNS
- Named Pipes and Mailslots
- Jitter and Sleep Masking.
- Developing a Simple C2 Server.
- Case Study: Building a basic DNS C2 channel and analyzing its network traffic in Wireshark to demonstrate low signature network activity.

Module 7: Weaponization and Delivery

- Document-Based Payload Delivery.
- Sideloading and Hijacking.
- Binary Packing and Protectors.
- Post-Exploitation Modules
- Supply Chain Attack Vectors.
- Case Study: Developing a DLL Sideloading payload for a common, signed application to demonstrate execution via a trusted process.

Module 8: Defensive Countermeasures & Ethics

- Malware Analysis & Triage.
- YARA Rule Development.
- Blue Team Detection Strategies.
- Ethics and Legal Frameworks.
- Capstone Project.
- Case Study: Writing YARA rules for the custom implant built in this module and testing their effectiveness against it.

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