Training Course on Advanced Malware Reverse Engineering

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s cybersecurity landscape, malware analysis and reverse engineering are crucial skills for understanding sophisticated threats and defending modern digital infrastructures. Training Course on Advanced Malware Reverse Engineering is designed to equip cybersecurity professionals with in-depth technical knowledge to dissect complex malware targeting Windows architectures, analyze advanced obfuscation techniques, and trace execution through assembly-level debugging. This course leverages real-world malware samples, sandboxing, and dynamic/static analysis strategies to ensure learners gain practical, hands-on experience in identifying and neutralizing malicious code.

This course bridges the gap between theory and practice, diving deep into x86 and x64 assembly instructions, anti-reverse engineering tactics, packer/unpacker technologies, code injection, and kernel-level rootkits. Learners will emerge with the skills to perform binary dissection, identify command-and-control (C2) mechanisms, and craft custom tools for reverse engineering and behavioral analysis. Whether you’re aiming for a career in threat intelligence, digital forensics, or incident response, this course provides cutting-edge content aligned with today’s advanced persistent threat (APT) landscape.

Programme Curriculum

Training Course on Advanced Malware Reverse Engineering

Introduction

In today’s cybersecurity landscape, malware analysis and reverse engineering are crucial skills for understanding sophisticated threats and defending modern digital infrastructures. Training Course on Advanced Malware Reverse Engineering is designed to equip cybersecurity professionals with in-depth technical knowledge to dissect complex malware targeting Windows architectures, analyze advanced obfuscation techniques, and trace execution through assembly-level debugging. This course leverages real-world malware samples, sandboxing, and dynamic/static analysis

strategies to ensure learners gain practical, hands-on experience in identifying and neutralizing malicious code.

This course bridges the gap between theory and practice, diving deep into x86 and x64 assembly instructions, anti-reverse engineering tactics, packer/unpacker technologies, code injection, and kernel-level rootkits. Learners will emerge with the skills to perform binary dissection, identify command-and-control (C2) mechanisms, and craft custom tools for reverse engineering and behavioral analysis. Whether you're aiming for a career in threat intelligence, digital forensics, or incident response, this course provides cutting-edge content aligned with today's advanced persistent threat (APT) landscape.

Course Objectives

1. Understand x86/x64 architecture and assembly language for malware analysis
2. Perform static and dynamic malware analysis using IDA Pro, Ghidra, and x64dbg
3. Unpack and decrypt obfuscated and packed malware
4. Analyze real-world APT samples and zero-day malware
5. Apply anti-debugging and anti-VM detection techniques
6. Build custom scripts and plugins for automation using Python
7. Identify and analyze C2 protocols and persistence mechanisms
8. Reverse engineer kernel-mode drivers and rootkits
9. Use API hooking and memory forensics for deep analysis
10. Map malware behavior to MITRE ATT&CK framework
11. Perform behavioral analysis in a secure sandbox environment
12. Craft YARA rules for malware classification and detection
13. Document and report malware capabilities for threat intelligence

Target Audience

1. Malware Analysts
2. Threat Intelligence Researchers
3. Cybersecurity Engineers
4. Reverse Engineers
5. Incident Responders
6. Penetration Testers
7. Digital Forensics Experts
8. Advanced Computer Science Students

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Reverse Engineering

- Overview of malware reverse engineering
- Importance of static and dynamic analysis
- Basic x86/x64 architecture
- Tools of the trade: IDA, Ghidra, x64dbg
- Lab setup and best practices
- **Case Study: Dissecting a simple backdoor Trojan**

Module 2: Mastering x86/x64 Assembly Language

- Registers, instructions, and calling conventions
- Control flow structures (loops, branches, conditions)
- Stack management and memory layout
- Function prologues and epilogues
- Common malware patterns in assembly

- **Case Study: Analyzing a ransomware dropper**

Module 3: Static Analysis Techniques

- Disassembly using IDA Pro and Ghidra
- Control flow graph (CFG) and function analysis
- String analysis and imports/exports
- Embedded resource and metadata analysis
- Limitations of static techniques
- **Case Study: Static analysis of a phishing Trojan**

Module 4: Dynamic Analysis and Debugging

- Debugging tools and techniques (x64dbg, OllyDbg)
- Setting breakpoints and tracing execution
- Memory inspection and manipulation
- Analyzing runtime behavior and IOCs
- Anti-debugging detection and bypassing
- **Case Study: Dynamic analysis of a RAT (Remote Access Trojan)**

Module 5: Understanding Packing and Obfuscation

- Types of packers and obfuscators
- Manual and automated unpacking
- XOR, Base64, and custom encryption methods
- Code virtualization and opaque predicates
- Using PEiD, UPX, and Scylla tools
- **Case Study: Unpacking a polymorphic virus**

Module 6: Malware Persistence and Evasion

- Registry persistence and scheduled tasks
- DLL injection and process hollowing
- API hooking and function redirection
- Evasion techniques (sandbox, AV, EDR)
- Detecting stealth behaviors
- **Case Study: Analyzing malware with advanced evasion logic**

Module 7: Network Behavior and C2 Analysis

- Identifying network indicators
- Reverse engineering C2 protocols
- Traffic analysis using Wireshark and Fiddler
- DNS tunneling and covert channels
- C2 infrastructure mapping
- **Case Study: Tracking an active malware C2 infrastructure**

Module 8: Kernel-Level Rootkit Analysis

- Introduction to Windows kernel architecture
- Rootkit techniques and hooks
- Ring 0 vs Ring 3 malware
- Analyzing drivers with WinDbg
- Detection and removal techniques
- **Case Study: Reverse engineering a stealthy kernel-mode rootkit**

Module 9: Memory Forensics in Reverse Engineering

- Memory dump acquisition and tools (Volatility, Rekall)
- Extracting malicious artifacts
- Identifying code injection and API hooks
- Process hollowing and DLL sideloading
- Timeline and process tree reconstruction
- **Case Study: Memory analysis of fileless malware**

Module 10: Python for Malware Automation

- Python scripting for reverse engineering
- Automating unpacking and decoding
- Ghidra and IDA scripting
- Parsing logs and extracting IOCs
- Creating automation pipelines
- **Case Study: Automating analysis of a malware family**

Module 11: Threat Attribution and TTP Mapping

- Mapping TTPs to MITRE ATT&CK
- APT group profiling and indicators
- Linking malware samples to threat actors
- Threat intelligence reporting standards
- Intelligence correlation and pivoting
- **Case Study: Attribution of an APT campaign using reverse engineering**

Module 12: YARA Rules and Signature Creation

- Writing effective YARA rules
- Rule testing and tuning
- Binary pattern matching
- Integration into SIEMs and antivirus
- Rule obfuscation avoidance
- **Case Study: Creating YARA rules for a malware campaign**

Module 13: Reverse Engineering Android/IoT Malware

- ARM vs x86 architecture differences
- Tools: Apktool, Radare2, Ghidra for ARM
- Firmware unpacking and binwalk
- Memory analysis for mobile devices
- IoT malware communication
- **Case Study: Reverse engineering Mirai botnet variant**

Module 14: Exploit and Shellcode Analysis

- Common exploitation techniques
- Shellcode decoding and emulation
- Buffer overflows and ROP chains
- Analyzing exploits in malware payloads
- Exploit kit behaviors
- **Case Study: Deconstructing a shellcode-based dropper**

Module 15: Final Malware Lab Challenge & Report

- Complex malware dissection capstone
- Static and dynamic analysis summary

- Threat classification and documentation
- IOC extraction and YARA creation
- Presenting findings in a threat report
- **Case Study: Final analysis of nation-state malware sample**

Training Methodology

- Instructor-led virtual or in-person sessions
- Hands-on labs with real-world malware samples
- Scenario-based exercises and simulations
- Collaborative group projects and knowledge sharing
- Assessments and lab certifications after each module

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
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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