Training Course on Disassembly and Debugging for Malware Analysts

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s cyber-threat landscape, disassembly and debugging have become essential skills for cybersecurity professionals, particularly malware analysts. As malware authors continually evolve their tactics, understanding the inner workings of binaries through reverse engineering techniques is critical. Training Course on Disassembly and Debugging for Malware Analysts provides deep technical knowledge in reverse engineering, assembly language, and dynamic code analysis using advanced debugging tools such as IDA Pro, x64dbg, Ghidra, and WinDbg. Participants will learn how to dissect malicious software, uncover obfuscation techniques, and extract Indicators of Compromise (IOCs).

With increasing ransomware, spyware, and rootkit attacks globally, this course empowers analysts to proactively respond by gaining practical, in-depth skills in static and dynamic analysis. Covering everything from PE file structure to unpacking packed malware and interpreting assembly instructions, this course transforms participants into competent reverse engineers capable of making critical cybersecurity decisions. This training aligns with threat intelligence, vulnerability research, incident response, and national cybersecurity defense strategies.

Programme Curriculum

Training Course on Disassembly and Debugging for Malware Analysts

Introduction

In today’s cyber-threat landscape, disassembly and debugging have become essential skills for cybersecurity professionals, particularly malware analysts. As malware authors continually evolve their tactics, understanding the inner workings of binaries through reverse engineering techniques is critical. Training Course on Disassembly and Debugging for Malware Analysts provides deep technical knowledge in reverse engineering, assembly language, and dynamic code analysis using advanced debugging tools such as IDA Pro, x64dbg, Ghidra, and WinDbg. Participants will learn how to dissect malicious software, uncover obfuscation techniques, and extract Indicators of Compromise (IOCs).

With increasing ransomware, spyware, and rootkit attacks globally, this course empowers analysts to proactively respond by gaining practical, in-depth skills in static and dynamic analysis. Covering everything from PE file structure to unpacking packed malware and interpreting assembly instructions, this course transforms participants into competent reverse engineers capable of making critical cybersecurity decisions. This training aligns with threat intelligence, vulnerability research, incident response, and national cybersecurity defense strategies.

Course Objectives

1. Understand the fundamentals of malware analysis and reverse engineering.
2. Gain in-depth knowledge of x86/x64 assembly language and control flow analysis.
3. Analyze PE file structures and recognize malware signatures.
4. Use IDA Pro and Ghidra for disassembly and static analysis.
5. Employ x64dbg and WinDbg for dynamic malware debugging.
6. Unpack and deobfuscate packed or encrypted malware samples.
7. Identify and extract IOCs for threat intelligence and incident response.
8. Recognize anti-debugging and anti-disassembly techniques used by malware.
9. Develop custom scripts and plugins to automate analysis workflows.
10. Apply sandboxing and emulation for safe behavioral malware testing.
11. Integrate malware analysis into real-world SOC workflows.
12. Reverse engineer real malware samples from APT campaigns.
13. Generate actionable reports for security operations and leadership.

Target Audience

1. Malware Analysts
2. Cybersecurity Engineers
3. SOC Analysts
4. Incident Responders
5. Threat Intelligence Professionals
6. Digital Forensics Experts
7. Security Researchers
8. Penetration Testers & Ethical Hackers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Malware Analysis & Assembly

- Overview of malware types and classification
- Introduction to x86/x64 architecture and registers
- Understanding memory models and addressing
- Common malware behaviors and attack vectors
- Hands-on: Inspecting simple malware in a lab
- **Case Study: Analyzing the ILOVEYOU worm (static)**

Module 2: Working with Disassembly Tools

- Overview of IDA Pro and Ghidra interfaces
- Understanding control flow graphs (CFG)
- Symbolic and hexadecimal representation
- Creating function comments and annotations
- Static unpacking of basic binaries
- **Case Study: Disassembling a downloader Trojan**

Module 3: Debugging with x64dbg and WinDbg

- Setting up a safe analysis environment (VMs, snapshots)
- Breakpoints, stack analysis, and memory inspection
- Analyzing loops, jumps, and conditional logic
- Identifying malware behavior at runtime
- Anti-debugging tricks and how to bypass them
- **Case Study: Debugging a ransomware dropper**

Module 4: PE File Structure and Obfuscation Techniques

- Understanding sections: .text, .data, .rsrc, etc.
- Import Address Table (IAT) and Export Table analysis
- Recognizing packing and obfuscation patterns
- Manual unpacking and memory dumping
- Rebuilding PE headers and fixing IATs
- **Case Study: Unpacking a UPX-packed infostealer**

Module 5: Malware Evasion and Decryption Methods

- Evasion techniques: polymorphism, metamorphism
- Encryption algorithms used in malware (XOR, AES)
- Finding keys and decryption routines in code
- Handling encrypted strings and payloads
- Using emulation to analyze obfuscated code
- **Case Study: Reverse engineering a Crypter**

Module 6: Behavior Analysis and Threat Attribution

- API hooking and behavior monitoring
- Using sandboxing and dynamic behavioral tools
- Extracting IOCs for threat feeds
- Pivoting malware analysis for threat attribution
- Using YARA rules and signature generation
- **Case Study: Attribution of Lazarus group malware**

Module 7: Automating Malware Analysis

- Scripting in IDAPython and Ghidra's scripting console
- Batch unpacking and automated decryption
- Integrating tools into CI/CD or SIEM pipelines
- Custom plugin development basics
- Reporting automation and documentation tips
- **Case Study: Automating string decryption in a malware family**

Module 8: Advanced Real-World Malware Case Studies

- Walkthroughs of APT campaigns (e.g., FIN7, Sandworm)
- Analysis of kernel-mode malware/rootkits
- Fileless malware debugging approaches
- Nation-state malware vs. cybercriminal malware
- Final hands-on lab with a blended malware sample
- **Case Study: Deconstructing Stuxnet components**

Training Methodology

- Hands-on labs with real malware samples in isolated VMs

- Step-by-step tool walkthroughs with instructor guidance
- Interactive whiteboard explanation of assembly logic
- Practical exercises with quiz-based knowledge checks
- End-of-module case study discussions
- Final capstone project with certificate of completion

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	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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