Malware Analysis and Reverse Engineering Training Course

Professional Development Training Course Outline

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

Course Introduction

Malware Analysis and Reverse Engineering is a critical skill set in the modern cybersecurity landscape, enabling organizations to detect, dissect, and defend against complex cyber threats. Malware Analysis and Reverse Engineering Training Course provides an in-depth exploration of malicious software behavior, attack vectors, and advanced reverse engineering techniques, emphasizing hands-on practical skills and strategic threat intelligence. Participants will gain expertise in static and dynamic malware analysis, debugging, unpacking obfuscated code, and understanding advanced persistent threats (APTs). The course combines theoretical frameworks with real-world scenarios, ensuring learners can accurately identify malware characteristics, assess risks, and develop effective mitigation strategies.

As cyber threats become increasingly sophisticated, security professionals must understand both the technical and analytical aspects of malware. This course equips participants with practical tools, scripting skills, forensic techniques, and knowledge of malware lifecycles to proactively safeguard networks, endpoints, and critical information assets. Learners will acquire the capability to analyze suspicious binaries, trace execution flows, interpret system changes, and contribute to threat intelligence reporting. By integrating reverse engineering practices into cybersecurity operations, organizations can enhance incident response, reduce damage, and maintain robust digital defenses.

Programme Curriculum

Malware Analysis and Reverse Engineering Training Course

Introduction

Malware Analysis and Reverse Engineering is a critical skill set in the modern cybersecurity landscape, enabling organizations to detect, dissect, and defend against complex cyber threats. Malware Analysis and Reverse Engineering Training Course provides an in-depth exploration of malicious software behavior, attack

vectors, and advanced reverse engineering techniques, emphasizing hands-on practical skills and strategic threat intelligence. Participants will gain expertise in static and dynamic malware analysis, debugging, unpacking obfuscated code, and understanding advanced persistent threats (APTs). The course combines theoretical frameworks with real-world scenarios, ensuring learners can accurately identify malware characteristics, assess risks, and develop effective mitigation strategies.

As cyber threats become increasingly sophisticated, security professionals must understand both the technical and analytical aspects of malware. This course equips participants with practical tools, scripting skills, forensic techniques, and knowledge of malware lifecycles to proactively safeguard networks, endpoints, and critical information assets. Learners will acquire the capability to analyze suspicious binaries, trace execution flows, interpret system changes, and contribute to threat intelligence reporting. By integrating reverse engineering practices into cybersecurity operations, organizations can enhance incident response, reduce damage, and maintain robust digital defenses.

Course Objectives

1. Understand the fundamentals of malware types, behaviors, and attack vectors.
2. Apply static analysis techniques to dissect and understand malicious code.
3. Conduct dynamic analysis using sandbox environments and debuggers.
4. Utilize reverse engineering tools to decompile, unpack, and examine binaries.
5. Identify obfuscation and packing methods used by advanced malware.
6. Analyze network traffic and system artifacts to detect malware activity.
7. Develop scripts and automation to enhance malware analysis efficiency.
8. Conduct forensic investigations and incident response using malware insights.
9. Understand Advanced Persistent Threats (APT) and their attack methodologies.
10. Apply memory analysis techniques to extract hidden malware behavior.
11. Integrate malware analysis findings into threat intelligence reports.
12. Develop mitigation strategies and preventive controls for malware attacks.
13. Enhance overall cybersecurity posture through advanced reverse engineering.

Organizational Benefits

- Strengthened cybersecurity defense and threat detection capabilities
- Improved incident response and forensic investigation efficiency
- Enhanced ability to analyze and mitigate malware outbreaks
- Reduced operational risk from cyber-attacks and data breaches
- Increased staff expertise in malware analysis and reverse engineering
- Better integration of threat intelligence into security operations
- Enhanced organizational resilience against advanced persistent threats
- Improved network and endpoint monitoring practices
- Increased ROI on security investments through proactive threat mitigation
- Reinforced regulatory compliance and security governance

Target Audiences

- Cybersecurity analysts and engineers
- Incident response teams and SOC staff
- Malware researchers and threat intelligence professionals
- IT auditors and compliance officers
- Digital forensics investigators

- Security consultants and penetration testers
- IT operations managers responsible for network security
- Students and researchers in cybersecurity and digital forensics

Course Duration: 5 days

Course Modules

Module 1: Introduction to Malware and Threat Landscape

- Overview of malware types, families, and characteristics
- Evolution of malware and emerging threats
- Understanding attack vectors and infection mechanisms
- Malware lifecycle and propagation techniques
- Basics of threat intelligence in malware detection
- Case Study: Analysis of a recent ransomware outbreak

Module 2: Static Malware Analysis Techniques

- Examining file headers, strings, and metadata
- Understanding disassembly and reverse engineering basics
- Identifying obfuscation and packing techniques
- Analyzing code without execution to determine behavior
- Tools for static analysis (IDA Pro, Ghidra, Binary Ninja)
- Case Study: Static analysis of a trojan binary

Module 3: Dynamic Malware Analysis

- Setting up secure sandbox environments for testing
- Monitoring system changes, registry, and file modifications
- Debugging and tracing malware execution
- Capturing network communications and indicators of compromise
- Automating dynamic analysis using scripts and tools
- Case Study: Behavioral analysis of a spyware sample

Module 4: Reverse Engineering Fundamentals

- Introduction to assembly language and instruction sets
- Understanding executable formats (PE, ELF, Mach-O)
- Decompilation and binary dissection techniques
- Identifying control flows and function calls
- Reverse engineering packed and obfuscated malware
- Case Study: Reverse engineering a packed malware sample

Module 5: Memory and Code Analysis

- Memory forensics and volatile data analysis
- Extracting hidden malware behavior from memory dumps
- Understanding code injection and process hollowing techniques
- Using memory analysis tools (Volatility, Rekall)
- Tracing runtime anomalies for malware detection
- Case Study: Memory analysis of a ransomware in execution

Module 6: Network and Communication Analysis

- Capturing and analyzing network traffic of malware
- Detecting command-and-control communication
- Extracting indicators of compromise from network data
- Using packet analyzers and network monitoring tools
- Identifying stealthy malware communication patterns
- Case Study: Analyzing botnet network behavior

Module 7: Malware Mitigation and Defensive Strategies

- Applying insights from malware analysis to incident response
- Designing preventive security controls
- Patch management, endpoint security, and threat hunting
- Creating signatures and rules for malware detection
- Integrating malware analysis into SOC operations
- Case Study: Preventive measures against ransomware spread

Module 8: Threat Intelligence and Reporting

- Documenting malware behavior and attack indicators
- Sharing findings with internal teams and external partners
- Producing actionable threat intelligence reports
- Correlating malware activity with threat actor campaigns
- Continuous improvement through intelligence-driven defense
- Case Study: Intelligence report creation for a nation-state malware attack

Training Methodology

- Instructor-led presentations and guided discussions
- Hands-on labs for static, dynamic, and memory analysis
- Practical exercises using real malware samples in secure environments
- Group analysis, collaborative reverse engineering tasks
- Case study reviews and peer-to-peer knowledge sharing
- Development of threat intelligence reports and mitigation plans

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
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