Reverse Engineering Malware (REM) Techniques Training Course

Professional Development Training Course Outline

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

Course Introduction

Reverse Engineering Malware (REM) Techniques is an advanced cybersecurity course that provides professionals with the analytical skills and technical expertise to dissect, understand, and mitigate malicious software threats. With the increasing sophistication of cyberattacks, organizations are facing persistent threats from ransomware, trojans, worms, spyware, and advanced persistent threats (APTs). Reverse Engineering Malware (REM) Techniques Training Course equips participants with the knowledge of malware lifecycles, attack vectors, obfuscation techniques, and anti-analysis mechanisms, enabling them to proactively analyze malware behavior, uncover hidden functionalities, and develop effective mitigation strategies. Participants will gain practical experience using state-of-the-art tools, debugging techniques, and static and dynamic analysis approaches for comprehensive malware investigation.

The course also emphasizes actionable threat intelligence, secure coding practices, memory analysis, and vulnerability research, providing participants with the ability to anticipate and respond to evolving cyber threats. By integrating real-world case studies, hands-on labs, and interactive simulations, learners will enhance their capability to reverse engineer malware, extract Indicators of Compromise (IOCs), and strengthen enterprise cybersecurity posture. This REM training fosters critical thinking, technical problem-solving, and the application of best practices in malware analysis to secure organizational systems against emerging and sophisticated cyber threats.

Programme Curriculum

Reverse Engineering Malware (REM) Techniques Training Course

Introduction

Reverse Engineering Malware (REM) Techniques is an advanced cybersecurity course that provides professionals with the analytical skills and technical expertise to dissect, understand, and mitigate malicious

software threats. With the increasing sophistication of cyberattacks, organizations are facing persistent threats from ransomware, trojans, worms, spyware, and advanced persistent threats (APTs). Reverse Engineering Malware (REM) Techniques Training Course equips participants with the knowledge of malware lifecycles, attack vectors, obfuscation techniques, and anti-analysis mechanisms, enabling them to proactively analyze malware behavior, uncover hidden functionalities, and develop effective mitigation strategies. Participants will gain practical experience using state-of-the-art tools, debugging techniques, and static and dynamic analysis approaches for comprehensive malware investigation.

The course also emphasizes actionable threat intelligence, secure coding practices, memory analysis, and vulnerability research, providing participants with the ability to anticipate and respond to evolving cyber threats. By integrating real-world case studies, hands-on labs, and interactive simulations, learners will enhance their capability to reverse engineer malware, extract Indicators of Compromise (IOCs), and strengthen enterprise cybersecurity posture. This REM training fosters critical thinking, technical problem-solving, and the application of best practices in malware analysis to secure organizational systems against emerging and sophisticated cyber threats.

Course Objectives

1. Understand malware types, behaviors, and lifecycle techniques.
2. Apply static analysis methods for disassembling and decompiling malware.
3. Conduct dynamic malware analysis using sandboxing and monitoring tools.
4. Detect obfuscation, encryption, and anti-debugging mechanisms.
5. Utilize debugging and disassembly tools for effective malware reverse engineering.
6. Analyze memory dumps and extract malicious code execution paths.
7. Identify Indicators of Compromise (IOCs) and develop threat intelligence reports.
8. Understand exploit techniques and advanced persistent threats (APTs).
9. Examine malware communication channels and network-based behaviors.
10. Develop remediation strategies and incident response plans.
11. Integrate malware analysis into proactive cybersecurity defense frameworks.
12. Apply safe lab practices and containment procedures during malware analysis.
13. Use reverse engineering techniques to support vulnerability research and security assessments.

Organizational Benefits

- Strengthened cybersecurity posture through proactive malware detection
- Enhanced incident response and mitigation capabilities
- Improved threat intelligence and reporting efficiency
- Reduced downtime and financial losses from malware attacks
- Advanced skill development for IT security and SOC teams
- Improved vulnerability research and penetration testing effectiveness
- Increased resilience against ransomware and APTs
- Standardized processes for malware analysis and documentation
- Reduced risk of data breaches and system compromise
- Competitive advantage through advanced cybersecurity expertise

Target Audiences

- Cybersecurity analysts and threat hunters
- Incident response teams and SOC operators
- Malware researchers and reverse engineering specialists

- Network and system security engineers
- Digital forensics investigators
- Penetration testers and ethical hackers
- IT security managers and directors
- Security consultants and auditors

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Analysis

- Overview of malware types and behaviors
- Malware lifecycle and propagation techniques
- Common malware attack vectors
- Introduction to malware analysis tools
- Security lab setup for safe analysis
- Case Study: Dissecting a ransomware attack

Module 2: Static Malware Analysis

- Understanding binary structures and file formats
- Disassembly and decompilation techniques
- Analyzing code without executing malware
- Signature-based detection methods
- Extracting IOCs from static artifacts
- Case Study: Reverse engineering a trojan executable

Module 3: Dynamic Malware Analysis

- Setting up sandbox environments
- Monitoring runtime behavior of malware
- Capturing system changes and registry modifications
- Analyzing process and network activity
- Detecting anti-analysis and evasion techniques
- Case Study: Analyzing a worm’s propagation mechanism

Module 4: Debugging Techniques

- Using debuggers for malware inspection
- Breakpoint setting and step execution
- Analyzing memory and CPU registers
- Understanding malware control flow
- Detecting runtime anti-debugging techniques
- Case Study: Debugging an advanced spyware sample

Module 5: Disassembly and Decompilation

- Disassembler tools and techniques
- Extracting assembly instructions from binaries
- Mapping code flow and logic structures
- Identifying malicious routines

- Integrating disassembly into analysis reports
- Case Study: Decompiling a packed malware sample

Module 6: Obfuscation and Encryption Techniques

- Identifying code obfuscation methods
- Understanding packing and encryption in malware
- Deobfuscating strings and code segments
- Analyzing custom encryption routines
- Techniques for automated unpacking
- Case Study: Breaking obfuscation in a ransomware sample

Module 7: Memory and Process Analysis

- Analyzing memory dumps for malware artifacts
- Identifying malicious processes and threads
- Examining injected code and reflective DLLs
- Live memory analysis techniques
- Extracting payloads from running malware
- Case Study: Memory forensics on an APT sample

Module 8: Network and Communication Analysis

- Capturing network traffic from malware
- Understanding C2 channels and protocols
- Detecting exfiltration and lateral movement
- Analyzing encrypted communications
- Tools for network behavior monitoring
- Case Study: Investigating malware beaconing to C2 server

Module 9: Indicators of Compromise (IOCs)

- Identifying file, registry, and network IOCs
- Using IOCs for threat detection and alerts
- Creating signatures for detection tools
- Correlating IOCs with threat intelligence feeds
- Documenting findings for SOC teams
- Case Study: Generating actionable IOCs from a ransomware attack

Module 10: Advanced Persistent Threat (APT) Analysis

- Understanding APT attack lifecycle
- Malware techniques used in APT campaigns
- Behavioral analysis for stealthy malware
- Threat actor TTP mapping
- Integration with threat intelligence platforms
- Case Study: Reverse engineering malware used in APT intrusion

Module 11: Malware Remediation and Incident Response

- Developing remediation strategies
- Containment and eradication techniques

- Integrating malware analysis into IR workflows
- Post-incident monitoring and reporting
- Best practices for secure system restoration
- Case Study: Responding to a corporate network ransomware incident

Module 12: Safe Lab Practices

- Segregated environments for malware handling
- Virtualization and snapshot techniques
- Preventing accidental spread of malware
- Tool and software hygiene in labs
- Compliance and regulatory considerations for analysis labs
- Case Study: Setting up a safe malware research lab

Module 13: Malware Analytics and Threat Intelligence

- Extracting actionable intelligence from malware
- Integrating analysis results into SOC dashboards
- Threat hunting using malware indicators
- Reporting techniques for stakeholders
- Correlating multiple malware events
- Case Study: Intelligence-driven malware mitigation

Module 14: Automated Malware Analysis

- Automated analysis frameworks and sandbox tools
- Advantages and limitations of automation
- Combining manual and automated analysis techniques
- Parsing results from analysis platforms
- Reducing time-to-detection through automation
- Case Study: Automated malware triage in enterprise environment

Module 15: Emerging Malware Trends and Research

- IoT, mobile, and cloud-based malware analysis
- Machine learning applications in malware detection
- Tracking evolution of malware families
- Researching zero-day malware threats
- Preparing for future threats in cybersecurity
- Case Study: Reverse engineering a novel zero-day exploit

Training Methodology

- Instructor-led lectures and interactive presentations
- Hands-on labs and guided malware analysis exercises
- Case study evaluations and peer learning discussions
- Practical exercises using debuggers, disassemblers, and sandbox tools
- Simulated attack scenarios and incident response drills
- Action-plan development for integrating REM techniques into organizational security

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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