Training Course on Static Malware Analysis Techniques (Advanced)

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, understanding static malware analysis techniques is crucial for preventing and mitigating advanced persistent threats (APTs). Training Course on Static Malware Analysis Techniques (Advanced) equips cybersecurity professionals, forensic analysts, and malware researchers with the skills to dissect and interpret malicious binaries without executing them. With increasing incidents of nation-state cyberattacks, ransomware variants, and polymorphic malware, this course offers cutting-edge knowledge using SEO-optimized keywords such as reverse engineering, binary dissection, signature detection, and code obfuscation to enhance visibility and relevance.

This course dives deep into advanced topics like analyzing PE files, disassembling obfuscated malware, and interpreting encoded payloads using static analysis tools and techniques. Designed with trending cybersecurity needs in mind, learners will engage with hands-on labs, case studies, and in-depth walkthroughs. Whether you're in incident response or threat intelligence, this course will enhance your capabilities to uncover embedded threats, detect vulnerabilities, and build proactive defense mechanisms.

Programme Curriculum

Training Course on Static Malware Analysis Techniques (Advanced)

Introduction

In today's cybersecurity landscape, understanding static malware analysis techniques is crucial for preventing and mitigating advanced persistent threats (APTs). Training Course on Static Malware Analysis Techniques (Advanced) equips cybersecurity professionals, forensic analysts, and malware researchers with the skills to dissect and interpret malicious binaries without executing them. With increasing incidents of nation-state cyberattacks, ransomware variants, and polymorphic malware, this course offers cutting-edge knowledge using SEO-optimized keywords such as reverse engineering, binary dissection, signature detection, and code obfuscation to enhance visibility and relevance.

This course dives deep into advanced topics like analyzing PE files, disassembling obfuscated malware, and interpreting encoded payloads using static analysis tools and techniques. Designed with trending cybersecurity needs in mind, learners will engage with hands-on labs, case studies, and in-depth walkthroughs. Whether you're in incident response or threat intelligence, this course will enhance your capabilities to uncover embedded threats, detect vulnerabilities, and build proactive defense mechanisms.

Course Objectives

1. Analyze malicious binaries using advanced static malware techniques
2. Perform deep inspection of Portable Executable (PE) files
3. Identify obfuscation and packing techniques used in malware
4. Reverse engineer shellcode and malicious scripts
5. Extract and interpret embedded resources in binary files
6. Apply string analysis for detecting hardcoded IOCs
7. Use disassemblers like Ghidra and IDA Pro for advanced analysis
8. Detect encryption and encoding in malware payloads
9. Understand API call patterns for malicious behavior mapping
10. Automate static malware analysis workflows using Python
11. Correlate findings with threat intelligence reports
12. Build YARA rules for malware family detection
13. Create static analysis reports with actionable insights

Target Audiences

1. Malware Analysts
2. Cybersecurity Professionals
3. Threat Intelligence Analysts
4. Incident Responders
5. Security Researchers
6. Reverse Engineers
7. Digital Forensic Experts
8. SOC (Security Operations Center) Teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to Static Malware Analysis

- Definitions and concepts
- Difference between static and dynamic analysis
- Advantages and limitations
- Malware analysis process flow
- Common static analysis tools
- *Case Study: Dissecting a basic keylogger using only static tools*

Module 2: PE File Format Deep Dive

- PE headers and sections
- Analyzing import/export tables
- Detecting anomalies in PE structure
- Tools for PE analysis (PEview, CFF Explorer)
- Static detection of malware behavior
- *Case Study: Analyzing PE header tampering in a trojan sample*

Module 3: Disassemblers and Decompilers

- IDA Pro and Ghidra overview
- Basic disassembly techniques
- Understanding assembly code
- Code flow reconstruction
- Function-level analysis
- *Case Study: Reverse engineering a ransomware loader*

Module 4: String and Metadata Analysis

- Extracting readable strings
- Identifying hardcoded IOCs
- Unicode, ASCII, and encoded strings
- Using tools like FLOSS and Strings
- Metadata inspection tools
- *Case Study: IOC extraction from a phishing malware sample*

Module 5: Identifying Packing and Obfuscation

- Common packing techniques
- How to detect packed files
- Static unpacking tips
- Anti-reversing methods used in malware
- Tools: PEiD, DIE, UPX
- *Case Study: Analyzing a UPX-packed dropper*

Module 6: Shellcode and Encoding Techniques

- What is shellcode?
- Shellcode identification via hex inspection
- Encoding schemes (Base64, XOR, etc.)
- Decoding obfuscated payloads
- Shellcode extraction tools
- *Case Study: Extracting shellcode from an obfuscated Word macro*

Module 7: API Call and Function Analysis

- Understanding common Windows APIs in malware
- Static tracing of API usage
- Suspicious API call patterns
- Tools for API inspection
- Detection of indirect API resolution
- *Case Study: Static detection of DLL injection techniques*

Module 8: Resource Section Analysis

- Embedded files, icons, strings
- Analyzing .rsrc section
- Tools: Resource Hacker, BinText
- Extracting malicious DLLs
- Decryption of resource content
- *Case Study: Extracting and analyzing payload from a malicious PDF*

Module 9: Control Flow and Code Obfuscation

- What is control flow obfuscation

- Recognizing jump-based obfuscation
- Flattened code structure analysis
- Simplifying control flow
- Tools for control flow graphing
- *Case Study: Analyzing an obfuscated stealer malware*

Module 10: Static Analysis with Ghidra

- Ghidra installation and interface
- Creating and analyzing projects
- Decompilation overview
- Scripting with Ghidra
- Advanced reverse engineering features
- *Case Study: Ghidra-based dissection of a spyware sample*

Module 11: YARA Rule Development

- Introduction to YARA
- Writing basic and advanced rules
- Testing and refining signatures
- Integration with analysis workflows
- Rule repositories
- *Case Study: Creating YARA rules for a known malware family*

Module 12: Automating Analysis with Python

- Parsing PE files with pefile
- Extracting strings and hashes
- Automating YARA scanning
- Custom script development
- Building CLI tools
- *Case Study: Automating the detection of credential harvesters*

Module 13: Threat Intelligence Integration

- Mapping analysis results to MITRE ATT&CK
- Linking indicators with threat feeds
- Enrichment of static data
- Building threat profiles
- Creating threat intelligence reports
- *Case Study: Correlating malware analysis with APT38 behaviors*

Module 14: Reporting and Documentation

- Standard malware report templates
- Visualizing analysis data
- Providing actionable insights
- Communication with stakeholders
- Sharing reports responsibly
- *Case Study: Writing a professional report for a law enforcement case*

Module 15: Capstone Project and Assessment

- Apply techniques from all modules
- Analyze a complex malware sample
- Write full static analysis report

- Develop YARA rule
- Present findings to panel
- *Case Study: Full static analysis lifecycle of a nation-state malware*

Training Methodology

- Interactive instructor-led sessions
- Hands-on labs and exercises
- Group-based case study analysis
- Tool walkthroughs and demos
- Pre/post assessments for progress tracking

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
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
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