Training Course on Analyzing Malicious Documents

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 rapidly evolving cyber threat landscape, malicious documents—particularly Microsoft Office files and PDFs—are frequently used as vectors for malware, ransomware, and phishing campaigns. Cybercriminals exploit vulnerabilities in macros, embedded scripts, and document metadata to compromise systems. Training Course on Analyzing Malicious Documents equips cybersecurity professionals, digital forensic analysts, and incident responders with cutting-edge skills and tools for dissecting and neutralizing malicious document-based threats. With the rise of remote work and document-sharing platforms, securing digital communication channels has never been more critical.

The Training Course on Analyzing Malicious Documents (Office, PDF) offers a hands-on, real-world-driven experience. Participants will explore document exploit techniques, reverse engineering embedded code, sandbox evasion strategies, and threat actor behavior patterns. Through interactive labs and real-world case studies, this course enhances your capability to identify, analyze, and mitigate document-based attacks. Leverage trending cybersecurity tools, malware analysis frameworks, and document sanitization methodologies to elevate your professional defense strategy.

Programme Curriculum

Training Course on Analyzing Malicious Documents

Introduction

In today's rapidly evolving cyber threat landscape, malicious documents—particularly Microsoft Office files and PDFs—are frequently used as vectors for malware, ransomware, and phishing campaigns. Cybercriminals exploit vulnerabilities in macros, embedded scripts, and document metadata to compromise systems. Training Course on Analyzing Malicious Documents equips cybersecurity professionals, digital forensic analysts, and incident responders with cutting-edge skills and tools for dissecting and neutralizing malicious document-based threats. With the rise of remote work and document-sharing platforms, securing digital communication channels has never been more critical.

The Training Course on Analyzing Malicious Documents (Office, PDF) offers a hands-on, real-world-driven experience. Participants will explore document exploit techniques, reverse engineering embedded code, sandbox evasion strategies, and threat actor behavior patterns. Through interactive labs and real-world case studies, this course enhances your capability to identify, analyze, and mitigate document-based attacks. Leverage trending cybersecurity tools, malware analysis frameworks, and document sanitization methodologies to elevate your professional defense strategy.

Course Objectives

1. Understand malicious Office document attack vectors and macro exploitation.
2. Detect and analyze embedded malware in PDF and Office formats.
3. Perform static and dynamic analysis of suspicious document files.
4. Utilize YARA rules and IOC extraction techniques for threat hunting.
5. Apply reverse engineering on document-based payloads.
6. Understand sandbox evasion and obfuscation techniques in documents.
7. Use advanced tools (e.g., olevba, pdfid, oledump) for forensic inspection.
8. Conduct memory analysis of malware executed via documents.
9. Automate document analysis workflows using Python scripting.
10. Map malicious documents to MITRE ATT&CK techniques.
11. Implement secure document handling and sanitization practices.
12. Identify and respond to zero-day exploits in documents.
13. Generate actionable reports for SOCs and threat intelligence platforms.

Target Audiences

1. Cybersecurity Analysts
2. Malware Reverse Engineers
3. Incident Response Teams
4. Threat Intelligence Analysts
5. Digital Forensic Experts
6. SOC Team Members
7. Red Team Operators
8. IT Security Managers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malicious Document Threats

- Overview of Office and PDF-based malware
- Common exploitation techniques
- Types of payloads delivered
- File format vulnerabilities
- Recent attack trends
- **Case Study: Emotet document-based infection campaign**

Module 2: Office Macros and VBA Exploits

- Anatomy of macro-enabled files
- Extracting and decoding macros
- Behavioral patterns of malicious VBA
- Tools: olevba, olevba3
- Anti-analysis tricks
- **Case Study: Dridex banking trojan via macro documents**

Module 3: PDF Threat Landscape

- PDF structure and vulnerability points
- JavaScript in PDF-based attacks
- Embedded objects and shellcode
- Tools: pdfid, pdf-parser
- Document sanitization overview
- **Case Study: CVE-2010-0188 exploited via malicious PDFs**

Module 4: Static Analysis Techniques

- File signature and entropy inspection
- Metadata extraction and analysis
- Hex-level inspection
- Detection using YARA
- IOC identification methods
- **Case Study: Static detection of LokiBot-infected DOCX**

Module 5: Dynamic Analysis of Document Malware

- Setting up a sandbox (Cuckoo, Any.Run)
- Safe document execution methods
- API and process behavior tracking
- Network traffic monitoring
- Identifying dropped files and persistence
- **Case Study: Sandboxing a malicious RTF loader**

Module 6: Obfuscation & Evasion Techniques

- Encoding techniques (Base64, XOR, GZIP)
- Shellcode obfuscation in macros
- Use of living-off-the-land binaries (LOLBins)
- Anti-VM and anti-sandbox logic
- Detection bypass strategies
- **Case Study: Excel 4.0 macro evasion in APT attacks**

Module 7: Deep Dive into OLE and RTF Formats

- Structure of OLE2 and RTF documents
- Exploitable components
- OLE object parsing
- Tools: oledump.py, rtfobj
- Common attack signatures
- **Case Study: CVE-2017-0199 exploitation through RTF**

Module 8: Python Automation in Document Analysis

- Using Python for parsing documents
- Creating custom scanners
- Scripted IOC extraction
- Report automation
- Batch analysis pipeline
- **Case Study: Automating macro analysis across 100+ samples**

Module 9: Memory and Payload Analysis

- Capturing memory dumps post-execution

- Analyzing injected payloads
- Identifying malicious DLLs and EXEs
- Use of volatility plugins
- Correlating memory IOCs to document behavior
- **Case Study: PowerShell payload injected via DOC file**

Module 10: Exploit Kits and Delivery Mechanisms

- Exploit delivery via phishing attachments
- Use of malicious templates
- Watering hole campaigns
- Embedded Flash/ActiveX objects
- Detection and prevention strategies
- **Case Study: RIG exploit kit targeting Office vulnerabilities**

Module 11: APT Document Campaigns

- Tactics, techniques, and procedures (TTPs)
- MITRE ATT&CK mapping
- Document fingerprinting
- Timeline reconstruction
- Attribution basics
- **Case Study: Operation Transparent Tribe**

Module 12: Threat Intelligence Integration

- Extracting and sharing IOCs
- STIX/TAXII for threat data
- Cross-tool intelligence correlation
- Enrichment using VirusTotal, Hybrid Analysis
- Reporting for CTI platforms
- **Case Study: Integrating document IOCs into MISP**

Module 13: Defensive Countermeasures

- Endpoint hardening techniques
- Blocking macros and embedded scripts
- Email gateway policies
- Office Protected View settings
- User awareness and training
- **Case Study: Organizational macro-blocking policy implementation**

Module 14: Legal and Ethical Considerations

- Handling PII and sensitive data
- Document forensics in legal cases
- Chain of custody practices
- Compliance with GDPR and HIPAA
- Digital evidence preservation
- **Case Study: Court-admissible PDF malware analysis**

Module 15: Capstone Project and Certification Prep

- Simulated document attack scenarios
- Hands-on malware dissection
- Full-chain analysis and reporting

- Final assessment and feedback
- Course review and certification prep
- **Case Study: End-to-end investigation of spear-phishing PDF**

Training Methodology

- Instructor-led live sessions with demonstrations
- Interactive hands-on labs and sandbox environments
- Case-based learning with real-world malware campaigns
- Group discussions and knowledge sharing forums
- Access to downloadable toolkits and scripts
- Post-training assessments and certification exam

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	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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