Training Course on Scripting for Malware Analysis

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 the evolving landscape of cybersecurity threats, malware analysis remains a critical skill for security professionals and digital forensics experts. Training Course on Scripting for Malware Analysis is designed to equip learners with cutting-edge scripting techniques to identify, dissect, and neutralize modern malware threats. With Python and PowerShell at the core, this hands-on course dives deep into reverse engineering, automated behavioral analysis, sandboxing, and memory forensics — empowering participants to automate complex tasks, improve detection rates, and understand advanced persistent threats (APTs).

This intensive and highly practical course is ideal for professionals aiming to enhance their incident response capabilities or transition into cybersecurity roles. Through real-world use cases, case studies, and lab-based learning, participants will gain proficiency in writing defensive and offensive scripts, constructing automation pipelines for malware classification, and utilizing forensic tools for post-breach analysis. By mastering scripting for malware analysis, learners will strengthen both their blue and red team skillsets in today’s threat-centric environments.

Programme Curriculum

Training Course on Scripting for Malware Analysis

Introduction

In the evolving landscape of cybersecurity threats, malware analysis remains a critical skill for security professionals and digital forensics experts. Training Course on Scripting for Malware Analysis is designed to equip learners with cutting-edge scripting techniques to identify, dissect, and neutralize modern malware threats. With Python and PowerShell at the core, this hands-on course dives deep into reverse engineering, automated behavioral analysis, sandboxing, and memory forensics — empowering participants to automate complex tasks, improve detection rates, and understand advanced persistent threats (APTs).

This intensive and highly practical course is ideal for professionals aiming to enhance their incident response capabilities or transition into cybersecurity roles. Through real-world use cases, case studies, and lab-based learning, participants will

gain proficiency in writing defensive and offensive scripts, constructing automation pipelines for malware classification, and utilizing forensic tools for post-breach analysis. By mastering scripting for malware analysis, learners will strengthen both their blue and red team skillsets in today's threat-centric environments.

Course Objectives

1. Understand the fundamentals of malware types, behavior, and infection vectors.
2. Learn to use Python scripting for static and dynamic malware analysis.
3. Develop PowerShell scripts to automate reverse engineering tasks.
4. Build custom tools for malware detection and memory forensics.
5. Automate sandboxing environments for malware behavior analysis.
6. Gain insights into obfuscation, packing, and anti-analysis techniques.
7. Analyze ransomware, trojans, and fileless malware using scripting.
8. Integrate YARA rules and threat intelligence with scripts.
9. Build automation workflows for malware triage and classification.
10. Apply Python and PowerShell for forensic data extraction.
11. Develop scripts for IOC (Indicators of Compromise) detection.
12. Use scripting to support SIEM threat correlation and log analysis.
13. Understand ethical hacking and red teaming perspectives through scripting.

Target Audience

1. Cybersecurity Analysts
2. Digital Forensics Investigators
3. Ethical Hackers and Penetration Testers
4. Malware Reverse Engineers
5. Security Operation Center (SOC) Personnel
6. IT Security Professionals
7. Incident Response Teams
8. Computer Science and Cybersecurity Students

Course Duration: 5 days

Course Modules

Module 1: Introduction to Malware Analysis and Scripting

- Fundamentals of malware and its classification
- Introduction to scripting languages (Python and PowerShell)
- Setting up malware analysis environments
- Basic static analysis techniques
- Introduction to analysis tools (IDA Pro, PEStudio)
- **Case Study: Static analysis of a trojan using Python script**

Module 2: Python for Static Malware Analysis

- Automating unpacking and deobfuscation
- Reading and extracting metadata from PE files
- Hashing and signature-based detection using Python
- Automating YARA rule scanning
- Integrating Python with VirusTotal API
- **Case Study: Building a static malware scanner using Python**

Module 3: Dynamic Analysis using Python Scripts

- Emulating malware behavior in sandbox environments

- Automating file system and registry monitoring
- Network traffic logging and packet inspection
- API call tracing with scripting
- Visualizing malware behavior
- **Case Study: Python-based dynamic analysis of a ransomware sample**

Module 4: PowerShell Scripting for Malware Analysis

- PowerShell for memory analysis and dump extraction
- Registry and event log parsing
- Building detection rules using PowerShell
- Script obfuscation and detection techniques
- PowerShell and Windows Defender bypass methods
- **Case Study: Analyzing fileless malware using PowerShell**

Module 5: Scripting for Memory Forensics

- Memory acquisition with Volatility and Rekall
- Automating Volatility plugins with Python
- Identifying injected code and DLLs
- Timeline reconstruction from memory
- Extracting credentials and artifacts
- **Case Study: Automating credential theft detection from memory dump**

Module 6: Automating Threat Hunting and IOC Detection

- Automating IOC scanning with Python
- Parsing logs from SIEM and EDR tools
- Threat intelligence integration
- Building IOC extraction and alerting pipelines
- Continuous monitoring and alerting via scripts
- **Case Study: IOC detection and alerting with Python**

Module 7: Advanced Malware Techniques and Countermeasures

- Anti-debugging and anti-VM detection
- Script-based detection of obfuscated malware
- Automating detection of C2 communication
- Detecting rootkits and stealthy implants
- Implementing anomaly detection scripts
- **Case Study: Python-based detection of an advanced rootkit**

Module 8: Red Team Automation and Ethical Scripting

- Offensive scripting fundamentals
- Emulating adversary techniques with scripts
- Payload generation using Python and PowerShell
- Integrating with Cobalt Strike and Metasploit
- Scripting for post-exploitation forensics
- **Case Study: Red team script to simulate APT behavior**

Training Methodology

- Hands-on scripting labs with real malware samples
- Live demonstrations of analysis techniques
- Virtual machine-based simulation exercises

- Weekly scripting assignments and feedback
- Case-based learning using real-world attack scenarios
- Access to malware sandbox environments and threat intel tools

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

Start Date	End Date	Location	Price
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