Training Course on Detecting Fileless Malware and Living-Off-The-Land Binaries

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the ever-evolving cyber threat landscape, fileless malware and Living-Off-The-Land Binaries (LOLBins) have become sophisticated tools used by adversaries to bypass traditional defenses. Unlike conventional malware, fileless attacks operate in-memory and utilize trusted system tools, making them highly evasive and extremely difficult to detect using standard endpoint protection systems. Organizations require advanced detection and forensic capabilities to proactively identify, neutralize, and respond to these covert threats in real time.

Training Course on Detecting Fileless Malware and Living-Off-The-Land Binaries

is designed for cybersecurity professionals, SOC analysts, incident responders, and threat hunters who are looking to enhance their advanced threat detection skill set. The program delivers real-world case studies, hands-on lab simulations, and AI-driven detection strategies to ensure participants can defend against stealthy attacks leveraging PowerShell, WMI, MSHTA, Rundll32, and other legitimate tools for malicious purposes. Upon completion, participants will be equipped to identify, analyze, and mitigate these stealthy adversarial tactics using modern behavior-based detection techniques.

Programme Curriculum

Training Course on Detecting Fileless Malware and Living-Off-The-Land Binaries

Introduction

In the ever-evolving cyber threat landscape, fileless malware and Living-Off-The-Land Binaries (LOLBins) have become sophisticated tools used by adversaries to bypass traditional defenses. Unlike conventional malware, fileless attacks operate in-memory and utilize trusted system tools, making them highly evasive and extremely difficult to detect using standard endpoint protection systems. Organizations require advanced detection and forensic capabilities to proactively identify, neutralize, and respond to these covert threats in real time.

Training Course on Detecting Fileless Malware and Living-Off-The-Land Binaries

is designed for cybersecurity professionals, SOC analysts, incident responders, and threat hunters who are looking to enhance their advanced threat detection skill set. The program delivers real-world case studies, hands-on lab simulations, and AI-driven detection strategies to ensure participants can defend against stealthy attacks leveraging PowerShell, WMI, MSHTA, Rundll32, and other legitimate tools for malicious purposes. Upon completion, participants will be equipped to identify, analyze, and mitigate these stealthy adversarial tactics using modern behavior-based detection techniques.

Course Objectives

1. Understand the anatomy of fileless malware and LOLBins.
2. Identify common attack vectors for fileless threats.
3. Analyze the use of PowerShell and WMI in memory-resident attacks.
4. Implement endpoint detection and response (EDR) strategies.
5. Examine Windows Sysinternals tools for memory forensics.
6. Detect suspicious activity using behavioral analytics.
7. Conduct real-time memory analysis for threat detection.
8. Utilize AI and machine learning for anomaly detection.
9. Investigate privilege escalation and lateral movement via LOLBins.
10. Develop custom YARA rules and Sigma rules for detection.
11. Create an incident response playbook specific to fileless threats.
12. Integrate MITRE ATT&CK framework into detection pipelines.
13. Simulate red team vs blue team exercises to build resilience.

Target Audiences

1. SOC Analysts
2. Threat Hunters
3. Malware Analysts
4. Penetration Testers
5. Incident Responders
6. Security Engineers
7. Forensic Investigators
8. Cybersecurity Students

Course Duration: 10 days

Course Modules

Module 1: Introduction to Fileless Malware

- Definition and evolution of fileless attacks
- Fileless vs traditional malware
- Use of native OS tools
- Case Study: PowerShell-based fileless ransomware
- Fileless attack kill chain overview
- Threat landscape analysis

Module 2: LOLBins Exploitation Techniques

- What are Living-Off-The-Land Binaries (LOLBins)?
- Common LOLBins: Rundll32, Regsvr32, Certutil
- Detection challenges with LOLBins
- Red Team TTPs using LOLBins
- Case Study: LOLBins in APT campaigns

- Mapping to MITRE ATT&CK

Module 3: PowerShell Abuse in Fileless Attacks

- Fileless payload delivery via PowerShell
- Obfuscation techniques
- Logging and telemetry for PowerShell
- Use of AMSI and logging bypass
- Case Study: Kovter malware
- Hardening PowerShell environments

Module 4: WMI and Scheduled Task Exploitation

- WMI as a persistence and execution mechanism
- Detecting WMI event consumers
- Task Scheduler-based execution
- Analyzing Windows logs
- Case Study: Fileless backdoor via WMI
- SIEM correlation rules for WMI

Module 5: In-Memory Threat Detection

- Memory injection techniques
- Reflective DLL injection
- Analysis using Volatility and Rekall
- Indicators of memory compromise
- Case Study: Metasploit meterpreter injection
- EDR solutions comparison

Module 6: Windows Sysinternals for Investigation

- Core Sysinternals tools: Autoruns, Process Explorer
- Live system inspection
- Registry and memory dumps
- Malware behavior correlation
- Case Study: LOLBins detection with Autoruns
- Threat hunting cheat sheets

Module 7: AI and ML in Threat Detection

- Introduction to AI for malware detection
- Supervised vs unsupervised learning models
- Feature engineering from system telemetry
- Model training using malicious behaviors
- Case Study: Detecting polymorphic fileless malware
- Open-source ML tools for analysts

Module 8: MITRE ATT&CK Mapping

- Overview of the ATT&CK framework
- Mapping techniques to tactics and techniques
- Custom detection logic
- Building threat profiles
- Case Study: Mapping a Lazarus Group attack

- Integrating ATT&CK with SIEM

Module 9: Behavioral Analytics and SIEM Integration

- What is behavioral threat detection?
- Setting baselines and thresholds
- SIEM log sources and parsing
- Alert fatigue and false positive handling
- Case Study: Detecting lateral movement using SIEM
- SIEM playbook development

Module 10: Red Team Simulation

- Simulating a fileless intrusion
- Building a lab for red teaming
- Customizing C2 frameworks
- Blue team monitoring and detection
- Case Study: Red team emulation using Empire
- Feedback and debrief analysis

Module 11: Incident Response Planning

- Incident triage and containment
- Response to in-memory threats
- Communication protocols
- Eradication and recovery
- Case Study: IR during fileless ransomware outbreak
- IR policy templates

Module 12: Threat Intelligence and IOC Sharing

- Threat feeds and fileless malware
- IOC formats: STIX, TAXII
- Enrichment techniques
- IOC lifecycle management
- Case Study: Sharing IOCs post-APT attack
- Threat intel platforms comparison

Module 13: Advanced Forensics for Fileless Threats

- Memory forensics methodology
- Registry and event log parsing
- Reconstructing attack timelines
- Chain of custody handling
- Case Study: Memory dump analysis using Volatility
- Forensic report writing

Module 14: Detection Rules with YARA and Sigma

- YARA rule creation and testing
- Sigma rules for SIEM integration
- Use cases in malware detection
- Sharing and standardization of rules
- Case Study: YARA rule for reflective loader detection
- Rule repositories and contribution

Module 15: Future Trends in Fileless Malware

- Emerging threat vectors
- Cloud-native fileless attacks
- LOLBins in macOS/Linux environments
- Quantum computing and malware
- Case Study: Fileless crypto-jacking in cloud workloads
- Defensive roadmap for the future

Training Methodology

- Hands-on Labs: Virtual labs simulating fileless malware environments
- Live Demonstrations: Real-time analysis of LOLBins and PowerShell misuse
- Case-Based Learning: Detailed case studies per module
- Interactive Discussions: Collaborative threat modeling and response drills
- Assessment & Certification: Practical tests and final evaluation
- Access to Tools & Templates: Sigma rules, detection scripts, IOC templates

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
03 Aug 2026	14 Aug 2026	Online	$2,200
10 Aug 2026	21 Aug 2026	Online	$2,200

Start Date	End Date	Location	Price
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200

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

Register Online Now

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