Training Course on Hunting for Fileless Malware and Living Off the Land Attacks

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 today's dynamic threat landscape, traditional signature-based security solutions are increasingly ineffective against sophisticated **cyber adversaries**. This training course delves into the insidious world of **fileless malware** and **Living Off the Land (LOTL) attacks**, highly stealthy techniques that leverage legitimate system tools and processes to evade detection. Participants will gain critical **threat hunting** skills to proactively identify, analyze, and mitigate these advanced **persistent threats (APTs)**, which leave minimal forensic artifacts, making them exceptionally challenging for incident responders.

Training Course on Hunting for Fileless Malware and Living Off the Land Attacks focuses on **behavioral analytics**, **memory forensics**, and **endpoint detection and response (EDR)** strategies to uncover hidden malicious activity. Through practical, hands-on labs and real-world **case studies**, attendees will learn to recognize subtle indicators of compromise (IOCs) and indicators of attack (IOAs) associated with these **evasive techniques**. By mastering the art of **proactive defense** and understanding adversary tactics, techniques, and procedures (TTPs), organizations can significantly enhance their **cyber resilience** and protect critical assets from the most advanced forms of **cyber espionage** and **data exfiltration**.

Programme Curriculum

Training Course on Hunting for Fileless Malware and Living Off the Land Attacks

Introduction

In today's dynamic threat landscape, traditional signature-based security solutions are increasingly ineffective against sophisticated **cyber adversaries**. This training course delves into the insidious world of **fileless malware** and **Living Off the Land (LOTL) attacks**, highly stealthy techniques that leverage legitimate system tools and processes to evade detection. Participants will gain critical

threat hunting skills to proactively identify, analyze, and mitigate these advanced **persistent threats (APTs)**, which leave minimal forensic artifacts, making them exceptionally challenging for incident responders.

Training Course on Hunting for Fileless Malware and Living Off the Land Attacks focuses on **behavioral analytics**, **memory forensics**, and **endpoint detection and response (EDR)** strategies to uncover hidden malicious activity. Through practical, hands-on labs and real-world **case studies**, attendees will learn to recognize subtle indicators of compromise (IOCs) and indicators of attack (IOAs) associated with these **evasive techniques**. By mastering the art of **proactive defense** and understanding adversary tactics, techniques, and procedures (TTPs), organizations can significantly enhance their **cyber resilience** and protect critical assets from the most advanced forms of **cyber espionage** and **data exfiltration**.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Define and differentiate various types of fileless malware, including PowerShell, WMI, and in-memory resident threats.
2. Identify and categorize common Living Off the Land (LOTL) attack vectors, such as **DLL hijacking**, **registry manipulation**, and abuse of native Windows tools (e.g., PsExec, Certutil).
3. Utilize advanced memory analysis tools and techniques to extract and analyze volatile data for **hidden malware artifacts** and malicious process injection.
4. Apply **User and Entity Behavior Analytics (UEBA)** principles to detect anomalous activities indicative of fileless and LOTL attacks.
5. Effectively utilize **Endpoint Detection and Response (EDR)** platforms for real-time monitoring, **threat visualization**, and automated response to sophisticated attacks.
6. Develop and execute structured **threat hunting methodologies** to proactively search for unknown or undetected threats within an enterprise network.
7. Understand the lifecycle of APTs and how fileless and LOTL techniques are integrated into sophisticated multi-stage attacks.
8. Identify suspicious network communications, command and control (C2) channels, and data exfiltration attempts associated with stealthy attacks.
9. Conduct comprehensive **incident response** procedures tailored for fileless and LOTL compromises, including containment, eradication, and recovery.
10. Create custom detection rules (e.g., YARA, Sigma) and alerts for novel fileless and LOTL attack patterns.
11. Recognize how fileless and LOTL attacks manifest in **cloud environments** and implement appropriate **cloud security posture management (CSPM)**.
12. Identify and address supply chain vulnerabilities that can be exploited by attackers employing fileless and LOTL methods.
13. Propose and implement robust security controls, including **zero-trust architecture**, **application whitelisting**, and enhanced **security awareness training**, to counter evolving threats.

Organizational Benefits

- Improved ability to detect and respond to advanced, stealthy cyberattacks that bypass traditional security solutions.
- Faster identification and containment of breaches, minimizing potential damage and data loss.
- Transition from a reactive to a proactive defense strategy through effective threat hunting capabilities.
- Development of in-house expertise in cutting-edge **malware analysis** and **incident response** techniques.
- Strengthened adherence to regulatory requirements by demonstrating advanced threat mitigation capabilities.
- Reduced financial impact of security incidents by preventing successful attacks and minimizing recovery efforts.
- Safeguarding sensitive data and critical infrastructure from high-impact cyber incidents.
- Leveraging **threat intelligence** and behavioral insights for more effective security strategies.

Target Audience

1. Security Analysts.
2. Incident Responders.
3. Threat Hunters.
4. Forensic Investigators.
5. Red Team / Blue Team Members.
6. Security Architects.
7. Penetration Testers.
8. Cybersecurity Consultants.

Course Outline

Module 1: Foundations of Fileless and LOTL Attacks

- Understanding the Evolution of Malware and Evasion Techniques.
- Defining Fileless Malware: In-Memory, Registry-Resident, and Script-Based.
- Introduction to Living Off the Land (LOTL) Principles and Attack Chains.
- Common Native Tools Abused by Attackers (e.g., PowerShell, WMI, Bitsadmin, Certutil).
- Case Study: Analyzing a recent fileless ransomware attack (e.g., Ryuk, Maze) and its initial infection vector.

Module 2: Advanced PowerShell and Scripting Obfuscation

- Deep Dive into PowerShell Remoting and Malicious Script Execution.
- Techniques for Obfuscating PowerShell and VBScript Code.
- Detecting Deobfuscation and Script Block Logging Evasion.
- Leveraging Sysmon and Event Logs for PowerShell Activity Monitoring.
- Case Study: Unpacking an obfuscated PowerShell script used in a state-sponsored attack.

Module 3: Memory Forensics for Fileless Malware

- Introduction to Volatile Memory Acquisition and Analysis.
- Tools for Memory Forensics (e.g., Volatility Framework, Rekall).
- Identifying Malicious Process Injections and Hooking Techniques.
- Extracting Network Connections, Handles, and Command Line Arguments from Memory.
- Case Study: Reconstructing a multi-stage attack by analyzing memory dumps from compromised endpoints.

Module 4: Windows Management Instrumentation (WMI) and COM Hijacking

- Understanding WMI Internals and its Legitimate Uses.
- Exploiting WMI for Persistence, Lateral Movement, and Data Exfiltration.
- Detecting WMI Event Subscription Backdoors and Permanent Event Consumers.
- COM Hijacking and its Role in Fileless Persistence.
- Case Study: Tracing an attack that used WMI for lateral movement within an Active Directory environment.

Module 5: Behavioral Analytics and Anomaly Detection

- Establishing Baselines for Normal User and System Behavior.
- Implementing User and Entity Behavior Analytics (UEBA) for Threat Detection.
- Identifying Anomalous Process Relationships and Executions.
- Leveraging Machine Learning for Anomaly Scoring and Alerting.
- Case Study: Utilizing a UEBA platform to detect insider threat activity employing legitimate tools.

Module 6: Endpoint Detection and Response (EDR) Deep Dive

- Core Capabilities of EDR Solutions in Detecting Fileless Attacks.
- Configuring EDR for Optimal Visibility and Alerting on LOTL Techniques.
- Leveraging EDR Telemetry for Threat Hunting and Investigation.
- Automated Response and Containment Strategies within EDR.
- Case Study: Using a leading EDR solution to investigate and remediate a live fileless malware infection.

Module 7: Proactive Threat Hunting Methodologies

- Developing Threat Hunting Hypotheses based on Threat Intelligence and Adversary TTPs (MITRE ATT&CK Framework).
- Data Sources for Threat Hunting (Endpoint, Network, Log Data).
- Structured Threat Hunting Loops and Iterative Analysis.
- Building Custom Detection Rules (YARA, Sigma) for Emerging Threats.
- Case Study: Conducting a hypothesis-driven threat hunt for specific LOTL attack patterns.

Module 8: Incident Response and Mitigation Strategies

- Tailoring Incident Response Plans for Fileless and LOTL Attacks.
- Containment, Eradication, and Recovery Best Practices for Stealthy Threats.
- Hardening Systems Against Fileless Persistence and Execution.
- Advanced Application Whitelisting and Software Restriction Policies.
- Case Study: Simulating an incident response scenario involving a persistent fileless compromise, from detection to full recovery.

Training Methodology

This course employs a highly interactive and practical training methodology, combining:

- **Instructor-Led Sessions:** Expert-led lectures with real-world examples and in-depth explanations.
- **Hands-on Labs:** Extensive practical exercises using virtualized environments to simulate attack scenarios and apply detection techniques.

- **Real-World Case Studies:** Analysis of notable fileless and LOTL attacks to understand their impact and effective response strategies.
- **Tool Demonstrations:** Live demonstrations of industry-leading cybersecurity tools and open-source utilities.
- **Group Discussions:** Collaborative problem-solving and sharing of best practices among participants.
- **Challenge Scenarios:** Capstone exercises to test comprehensive understanding and practical application of learned skills.

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

Start Date	End Date	Location	Price
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
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