Training Course on Hunting for Persistence Mechanisms

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 ever-evolving landscape of **cybersecurity threats**, **Advanced Persistent Threats (APTs)** and sophisticated **malware** leverage diverse techniques to maintain a foothold within compromised systems. **Persistence mechanisms** are critical to these attacks, enabling adversaries to re-establish access, exfiltrate data, and continue their malicious activities even after reboots or security interventions. Training Course on Hunting for Persistence Mechanisms is meticulously designed for **cyber defense professionals** seeking to **master threat hunting** for these elusive mechanisms across various operating systems, thereby significantly enhancing an organization's **resilience against advanced attacks** and **reducing dwell time**.

This program delves deep into the **tactics, techniques, and procedures (TTPs)** employed by threat actors for **persistent access**, providing **hands-on experience** with **forensic tools** and **detection methodologies**. Participants will gain actionable knowledge to **identify, analyze, and remediate** common and stealthy persistence artifacts, empowering them to proactively defend their networks. The focus on practical application, **real-world case studies**, and **cutting-edge intelligence** ensures that attendees are equipped with the skills necessary to become proficient **persistence hunters** and contribute to a robust **security posture**.

Programme Curriculum

Training Course on Hunting for Persistence Mechanisms

Introduction

In the ever-evolving landscape of **cybersecurity threats**, **Advanced Persistent Threats (APTs)** and sophisticated **malware** leverage diverse techniques to maintain a foothold within compromised systems. **Persistence mechanisms** are critical to these attacks, enabling adversaries to re-establish access, exfiltrate data, and continue their malicious activities even after reboots or security

interventions. Training Course on Hunting for Persistence Mechanisms is meticulously designed for **cyber defense professionals** seeking to **master threat hunting** for these elusive mechanisms across various operating systems, thereby significantly enhancing an organization's **resilience against advanced attacks** and **reducing dwell time**.

This program delves deep into the **tactics, techniques, and procedures (TTPs)** employed by threat actors for **persistent access**, providing **hands-on experience** with **forensic tools** and **detection methodologies**. Participants will gain actionable knowledge to **identify, analyze, and remediate** common and stealthy persistence artifacts, empowering them to proactively defend their networks. The focus on practical application, **real-world case studies**, and **cutting-edge intelligence** ensures that attendees are equipped with the skills necessary to become proficient **persistence hunters** and contribute to a robust **security posture**.

Course Duration

5 days

Course Objectives

1. Understand the MITRE ATT&CK Framework as it relates to persistence techniques (T1547).
2. Identify and enumerate common Windows persistence mechanisms, including Registry Run keys, Scheduled Tasks, and Service hijackings.
3. Detect and analyze Linux persistence methods, such as Cron jobs, SSH keys, and Systemd services.
4. Explore macOS persistence techniques, including LaunchAgents, LaunchDaemons, and Login Items.
5. Leverage endpoint detection and response (EDR) solutions for persistence artifact collection and analysis.
6. Implement threat hunting methodologies to proactively search for unknown or evasive persistence.
7. Utilize forensic tools and scripting (PowerShell, Bash, Python) for automated persistence detection.
8. Analyze system logs and event data for indicators of compromise (IOCs) related to persistence.
9. Differentiate between legitimate system behavior and malicious persistence attempts.
10. Develop effective response strategies for eradicating detected persistence mechanisms.
11. Apply proactive defense strategies to prevent initial persistence establishment.
12. Understand the role of threat intelligence in informing persistence hunting efforts.
13. Conduct post-compromise analysis to uncover hidden persistence layers.

Organizational Benefits

- Proactively identifying and eliminating persistence mechanisms significantly shortens the time attackers remain undetected in a network, minimizing potential damage.
- A deeper understanding of attacker persistence techniques strengthens overall cybersecurity defenses and resilience against sophisticated attacks.
- Equips security teams with the knowledge and tools to more effectively investigate and remediate breaches involving persistence.
- Shifts security operations from reactive to proactive, enabling the identification of threats before they escalate into major incidents.
- Helps organizations meet regulatory compliance requirements related to data security and reduces the risk of costly data breaches.

- Maximizes the effectiveness of existing EDR, SIEM, and other security tools by providing the expertise to leverage them for persistence hunting.
- Builds a highly skilled and specialized team capable of tackling advanced cyber threats.
- Safeguards sensitive data, intellectual property, and critical infrastructure from long-term compromise.

Target Audience

1. Security Analysts
2. Threat Hunters
3. Incident Responders
4. Digital Forensics Professionals
5. SOC Analysts
6. Red Teamers / Penetration Testers (for understanding defensive mechanisms)
7. System Administrators with security responsibilities
8. IT Security Managers overseeing defensive operations

Course Outline

Module 1: Introduction to Persistence and Threat Hunting Fundamentals

- Defining Persistence Mechanisms in the Cyber Kill Chain.
- Overview of the MITRE ATT&CK Framework with a focus on T1547 (Boot or Logon Autostart Execution).
- The Threat Hunting Loop and hypothesis generation for persistence.
- Key forensic artifacts and log sources for persistence analysis.
- Case Study: Analyzing a recent APT campaign where initial persistence was achieved through a compromised startup entry.

Module 2: Windows Persistence: System-Level Techniques

- In-depth analysis of Registry Run keys (Run, RunOnce, Load) and their abuse.
- Hunting for malicious Windows Services and Service DLL hijacking.
- Detecting Scheduled Tasks and WMI Event Subscriptions for persistence.
- Investigating Image File Execution Options (IFEO) and Accessibility Features for backdoor access.
- **Case Study:** Dissecting a ransomware attack that utilized WMI persistence to maintain control after system reboots.

Module 3: Windows Persistence: User-Level & Advanced Techniques

- Analyzing Startup Folders and Shell Folders for malicious executables.
- Exploring COM Hijacking, DLL Sideloading, and AppInit_DLLs as persistence vectors.
- Hunting for Browser Helper Objects (BHOs) and IE Toolbars.
- Understanding User Logon Scripts and Group Policy Objects (GPOs) for persistence.
- **Case Study:** Uncovering a sophisticated phishing campaign that established persistence via a hidden browser extension and a modified user logon script.

Module 4: Linux Persistence: Core System & User Methods

- Examining Cron Jobs (crontab, /etc/cron.d/) for scheduled execution.
- Detecting SSH authorized_keys compromise and SSH client configuration.
- Analyzing Systemd service units and SysV Init scripts for malicious startup.

- Investigating user profile modifications (.bashrc, .profile, .zshrc).
- Case Study: Tracing the persistence mechanism of a Linux-based cryptocurrency miner utilizing a root-level cron job.

Module 5: Linux Persistence: Advanced & Kernel-Level Techniques

- Hunting for SUID/SGID binaries and shared library preloading (LD_PRELOAD).
- Exploring Kernel Modules (Loadable Kernel Modules - LKMs) and rootkit detection.
- Analyzing rc.local and other system startup scripts.
- Detecting backdoored applications and package manager hooks.
- Case Study: Identifying a stealthy Linux rootkit establishing persistence via a custom LKM.

Module 6: macOS Persistence: Common & Advanced Techniques

- Investigating LaunchAgents and LaunchDaemons (.plist files).
- Analyzing Login Items and Startup Items for user-level persistence.
- Detecting Browser Extensions and Safari/Chrome policies.
- Exploring Kernel Extensions (kexts) and System Extensions.
- Case Study: Forensic analysis of malware that persisted on macOS using a hidden LaunchAgent and a deceptive login item.

Module 7: Cross-Platform Persistence Hunting Tools & Methodologies

- Utilizing Sysinternals Suite (Autoruns, Process Monitor) for Windows.
- Leveraging OSquery for cross-platform endpoint visibility and persistence hunting.
- Applying YARA rules for signature-based detection of known persistence artifacts.
- Automating persistence analysis with PowerShell scripts and Python tools.
- Case Study: Implementing a multi-OS persistence hunt using a combination of EDR data, OSquery, and custom YARA rules.

Module 8: Remediation, Prevention, and Future Trends in Persistence

- Developing effective remediation strategies for various persistence types.
- Best practices for hardening systems against common persistence techniques.
- The role of Application Whitelisting, Least Privilege, and MFA in prevention.
- Emerging trends in cloud persistence, container persistence, and firmware persistence.
- Case Study: Designing and implementing a robust defense strategy for an enterprise network, focusing on preventing and detecting new persistence vectors.

Training Methodology

This course employs a dynamic and interactive training methodology designed for maximum knowledge retention and skill development.

- **Hands-on Labs:** Extensive practical exercises using virtualized environments (Windows, Linux, macOS) to simulate real-world scenarios.
- **Instructor-Led Sessions:** Expert-led lectures with interactive discussions and Q&A sessions.
- **Live Demonstrations:** Real-time demonstrations of persistence techniques and their detection.
- **Case Studies:** In-depth analysis of actual cyber incidents and the persistence mechanisms involved.
- **Group Activities & Discussions:** Collaborative problem-solving and sharing of experiences.
- **CTF-style Challenges:** Optional capture-the-flag exercises to test acquired skills.

- **Tool-Based Training:** Practical application of industry-standard and open-source forensic and threat hunting tools.
- **Scenario-Based Learning:** Participants work through realistic scenarios, from initial compromise to persistence eradication.

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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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