Training Course on Advanced Operating System (OS) Artifact Analysis for APTs

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

Advanced Persistent Threats (APTs) represent the pinnacle of cyber warfare, characterized by their stealth, persistence, and sophisticated use of custom malware and living-off-the-land techniques. Traditional forensic methods often fall short against these elusive adversaries, necessitating a deeper, more granular understanding of operating system (OS) artifacts. Training Course on Advanced Operating System (OS) Artifact Analysis for APTs provides an unparalleled deep dive into advanced OS artifact analysis, specifically tailored to equip digital forensic investigators, incident responders, and threat hunters with the cutting-edge skills required to uncover the subtle digital footprints left by APTs. Participants will learn to navigate the intricate layers of Windows, Linux, and macOS operating systems, extracting and interpreting high-value evidence that reveals the full scope of a sophisticated breach, transforming seemingly innocuous data into decisive actionable intelligence.

This intensive program goes far beyond surface-level log analysis, focusing on the nuances of malware persistence mechanisms, sophisticated lateral movement techniques, data exfiltration methodologies, and anti-forensic measures employed by APT actors. Through extensive hands-on labs, real-world APT case studies, and the application of advanced forensic tooling, attendees will master techniques for analyzing volatile memory, registry hive data, file system journaling, hidden process activity, and obscure system logs. By the end of this course, you will possess the expertise to dissect complex APT campaigns, attribute attack methodologies, and build robust, legally defensible cases crucial for defending against the most formidable cyber adversaries.

Programme Curriculum

Training Course on Advanced Operating System (OS) Artifact Analysis for APTs

Introduction

Advanced Persistent Threats (APTs) represent the pinnacle of cyber warfare, characterized by their stealth, persistence, and sophisticated use of custom malware and living-off-the-land techniques. Traditional forensic methods often fall short against these elusive adversaries, necessitating a deeper, more granular understanding of operating system (OS) artifacts. Training Course on Advanced Operating System (OS) Artifact Analysis for APTs provides an unparalleled deep dive into advanced OS artifact analysis, specifically tailored to equip digital forensic investigators, incident responders, and threat hunters with the cutting-edge skills required to uncover the subtle digital footprints left by APTs. Participants will learn to navigate the intricate layers of Windows, Linux, and macOS operating systems, extracting and interpreting high-value evidence that reveals the full scope of a sophisticated breach, transforming seemingly innocuous data into decisive actionable intelligence.

This intensive program goes far beyond surface-level log analysis, focusing on the nuances of malware persistence mechanisms, sophisticated lateral movement techniques, data exfiltration methodologies, and anti-forensic measures employed by APT actors. Through extensive hands-on labs, real-world APT case studies, and the application of advanced forensic tooling, attendees will master techniques for analyzing volatile memory, registry hive data, file system journaling, hidden process activity, and obscure system logs. By the end of this course, you will possess the expertise to dissect complex APT campaigns, attribute attack methodologies, and build robust, legally defensible cases crucial for defending against the most formidable cyber adversaries.

Course Duration

10 Days

Course Objectives

1. Understand APT Attack Lifecycle: Comprehend the typical phases of an APT campaign and corresponding OS artifacts at each stage.
2. Master Advanced Windows Artifacts: Deeply analyze Registry hives, Event Logs (including advanced custom logs), Prefetch, Superfetch, SRUM, and AppCompatCache for APT activity.
3. Perform Comprehensive Linux Artifact Analysis: Investigate system logs (/var/log), auditd, bash history, cron jobs, network configurations, and kernel modules for signs of compromise.

4. Conduct In-depth macOS Artifact Analysis: Examine Unified Logs, fseventsd, .DS_Store, plists, and kernel extensions for APT persistence and activity.
5. Analyze Volatile Memory for APT Indicators: Extract and interpret memory dumps to uncover injected code, hidden processes, network connections, and credential theft.
6. Detect & Analyze Persistence Mechanisms: Identify sophisticated APT persistence across all major OS platforms (e.g., WMI, Scheduled Tasks, LaunchAgents/Daemons, Systemd).
7. Trace Lateral Movement Techniques: Uncover evidence of credential reuse, remote execution (PsExec, WinRM, SSH), and network tunneling used by APTs.
8. Investigate Data Staging & Exfiltration Artifacts: Identify evidence of data compression, encryption, staging areas, and various exfiltration methods.
9. Identify Anti-Forensic & Evasion Techniques: Detect and counter APT methods for log clearing, file wiping, timestomping, and rootkit deployment.
10. Correlate Disparate OS Artifacts: Integrate findings from various OS sources to build a comprehensive, high-fidelity timeline of APT activities.
11. Leverage Advanced Forensic Tooling: Proficiency in using cutting-edge commercial and open-source tools specifically designed for APT artifact analysis.
12. Develop APT Hunt Methodologies: Formulate proactive threat hunting strategies based on OS artifact analysis patterns.
13. Generate Actionable Forensic Reports: Produce detailed, technical, and defensible reports outlining complex APT investigation findings.

Organizational Benefits

1. Superior APT Detection & Response: Rapidly identify, contain, and eradicate the most advanced cyber threats.
2. Minimized Breach Impact: Reduce downtime and data loss from sophisticated, persistent attacks.
3. Enhanced Threat Intelligence: Extract invaluable intelligence on APT methodologies, tools, and targets.
4. Proactive Threat Hunting Capability: Empower security teams to proactively search for hidden APT presence.
5. Stronger Root Cause Analysis: Pinpoint the exact entry points, vulnerabilities exploited, and full attack chains of APTs.
6. Reduced Litigation & Reputational Risk: Provide irrefutable evidence for legal proceedings and public reporting of breaches.
7. Optimized Security Investments: Maximize the effectiveness of existing EDR, SIEM, and security controls.
8. Upskilled Internal Workforce: Develop elite-level forensic talent capable of handling nation-state level threats.
9. Improved Compliance Posture: Meet stringent regulatory requirements for advanced threat detection and reporting.

10. Fortified Digital Defenses: Lessons learned from APT investigations directly inform and harden organizational security architecture.

Target Participants

- Digital Forensic Investigators
- Incident Response Team Leads
- Threat Hunters
- Malware Analysts
- Security Operations Center (SOC) Analysts (Tier 3+)
- Cybersecurity Engineers
- Red Team/Blue Team Members
- Reverse Engineers
- Security Architects
- Advanced Penetration Testers

Course Outline

Module 1: APT Fundamentals & OS Forensic Readiness

- **Understanding APTs:** Characteristics, motivations, and common attack lifecycle phases.
- **Targeting OS Artifacts:** Why OS-level data is critical for APT detection.
- **Forensic Readiness:** Logging, auditing, and data retention best practices for APT investigations.
- **Advanced Acquisition Techniques:** Live vs. dead, full disk, memory, targeted artifacts.
- **Case Study:** The NotPetya Ransomware: Beyond the Surface Infection.

Module 2: Advanced Windows Registry Forensics for APTs

- **Registry Hive Deep Dive:** SYSTEM, SOFTWARE, SAM, NTUSER.DAT hives.
- **Persistence via Registry:** Run keys, services, BITS jobs, userinit, Winlogon.
- **USB Device & ShellBag Analysis:** Tracing device connections and user folder access.
- **UserAssist & AppCompatCache:** Reconstructing program execution and user activity.
- **Case Study:** Uncovering Registry-based APT Persistence.

Module 3: Windows Event Logs: Beyond the Basics

- **Advanced Event Log Channels:** PowerShell, WMI, AppLocker, Sysmon logs.
- **Custom Event Log Creation & Analysis:** Detecting specific APT behaviors.
- **Log Tampering & Evasion:** Identifying cleared logs, log manipulation.
- **Correlating Event IDs:** Building attack narratives from disparate log entries.
- **Case Study:** Tracing Lateral Movement via Remote Event Log Analysis.

Module 4: Windows Execution & Activity Artifacts

- **Prefetch & Superfetch Analysis:** Identifying executed programs and their launch counts.
- **SRUM (System Resource Usage Monitor) Forensics:** Analyzing network usage by applications.
- **Jump Lists & Recent Documents:** Identifying recently accessed files and programs.
- **PowerShell History & Transcripts:** Uncovering command-line activity.

- **Case Study:** Reconstructing a PowerShell Empire Post-Exploitation Activity.

Module 5: Windows Process & Memory Forensics

- **Memory Acquisition from Servers/Endpoints:** Tools and best practices.
- **Volatility Framework Deep Dive:** Plugin architecture, advanced usage for APTs.
- **Process Injection & Hollowing Detection:** Identifying stealthy malware techniques.
- **Credential Dumping Forensics:** Analyzing LSASS for stolen credentials.
- **Case Study:** Unmasking In-Memory Malware Persistence.

Module 6: Linux Forensics for APT Detection

- **Linux File System Internals:** ext4, XFS, inode analysis.
- **System Logs & Journald:** /var/log files, journalctl for activity.
- **Auditd Configuration & Analysis:** Tracing system calls, file access, command execution.
- **Cron Jobs & Systemd Units:** Identifying persistence mechanisms.
- **Case Study:** Investigating a Linux Server Compromise via SSH Log Analysis.

Module 7: macOS Forensics for APT Detection

- **macOS File System (APFS):** Snapshotting, hidden volumes.
- **Unified Logging System:** Interpreting complex macOS log data.
- **LaunchAgents & LaunchDaemons:** Analyzing persistence mechanisms.
- **Kernel Extensions (Kexts) & Frameworks:** Detecting suspicious loaded modules.
- **Case Study:** Uncovering Persistent Malware on a macOS Endpoint.

Module 8: File System Timestamps & Anti-Forensics

- **MACE Timestamps (Modified, Accessed, Created, Entry Modified):** Their significance.
- **NTFS Timestomping & Artifact Manipulation:** Detecting alteration attempts.
- **Metadata Analysis for File History:** Beyond MACE (e.g., $LogFile, $UsnJrnl).
- **Recovering Deleted Files & File Fragments:** Advanced carving techniques.
- **Case Study:** Detecting APT Attempts to Cover Their Tracks.

Module 9: Malware Persistence & Evasion Techniques

- **Common Persistence Methods:** Beyond registry (DLL Hijacking, COM Hijacking).
- **Rootkits & Bootkits:** Detecting low-level stealth.
- **Code Obfuscation & Packing:** Static analysis challenges.
- **Defense Evasion Strategies:** AMSI bypass, UAC bypass, antivirus evasion.
- **Case Study:** Unpacking a Multi-Stage APT Malware Dropper.

Module 10: Lateral Movement & Pivoting Forensics

- **Credential Access Indicators:** Pass-the-Hash/Ticket, Mimikatz artifacts.
- **Remote Execution Artifacts:** PsExec, WinRM, WMI, SSH logs.
- **Network Share Access:** SMB logs, RDP session artifacts.
- **Service & Scheduled Task Creation:** Detecting remote creation of malicious tasks.
- **Case Study:** Tracing an APT's Movement Across Multiple Internal Systems.

Module 11: Data Staging & Exfiltration Forensics

- **Staging Area Identification:** Temporary files, encrypted archives.
- **Compression & Encryption Artifacts:** Identifying use of 7-Zip, WinRAR, custom encryption.

- **Exfiltration Channels:** C2 communication, cloud storage, email, DNS tunneling.
- **Network Flow Data & Packet Capture Analysis:** Detecting large or unusual data transfers.
- **Case Study:** Investigating Data Exfiltration to a Cloud Storage Service.

Module 12: Advanced OS Forensic Tooling

- **Enterprise EDR/Forensic Platforms:** Deep dive into advanced features (e.g., Mandiant HX, Carbon Black, CrowdStrike Falcon).
- **Open-Source Powerhouses:** Velociraptor, KAPE, OSQuery, Sysmon, Autoruns, Process Monitor.
- **Custom Scripting for Automation:** PowerShell, Python for artifact parsing and correlation.
- **Big Data Forensics (ELK Stack, Splunk):** Ingesting and analyzing large volumes of OS logs.
- **Case Study:** Building an Automated APT Artifact Collection & Analysis Pipeline.

Module 13: Threat Hunting with OS Artifacts

- **Defining Threat Hunting:** Proactive search for unseen threats.
- **Hypothesis-Driven Hunting:** Developing hypotheses based on APT TTPs.
- **Hunting for Persistence, Lateral Movement, and Exfiltration:** Specific OS artifacts.
- **Automation for Hunting:** Using OSQuery and similar tools for continuous monitoring.
- **Case Study:** A Hunt for a Specific APT's Known TTPs in Enterprise Endpoints.

Module 14: APT Case Studies & Post-Mortem Analysis

- **Analyzing Real-World APT Attacks:** Deep dive into specific campaigns (e.g., SolarWinds, NotPetya).
- **Mapping to MITRE ATT&CK Framework:** Categorizing TTPs based on discovered artifacts.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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