800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Endpoint Live Forensics Training

Applied Technology Academy

While there is undoubtedly a need for deep forensic analysis in the investigation of malware and operating system intrusions, an investigator has to know that there has been an intrusion before that activity can begin. Many organizations rely on technology to perform this task, but there is still no substitute for a well-trained analyst, when it comes to identifying and investigating abnormal behavior on a system.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**3 years: Windows Systems**	**$152,773**	**Yes**

Course Overview

By the end of the course, you should be able to meet the following objectives:

Identify the core components of the operating system and ascertain their current state using built-in or other trusted tools

Analyze a running system and detect abnormal behavior relating to operating system objects such as processes, handles, network connections, etc.

- Use event log analysis to verify and correlate the artifacts of anomalous behavior, and determine the scope of an intrusion
- Use PowerShell to interact with the operating system and build scripts to automate repetitive analytic tasks
- Create and use a system baseline to identify unexpected items such as rogue accounts or configuration changes

Course Outline

- **Lesson 1: Windows Core Components - OS Overview**
  - OS Definition
  - Architecture Overview
  - OS Structure
  - OS Motivation
  - Kernel Mode vs. User Mode
  - Windows Structure
  - Windows Boot Process
  - Lab
  - OS Familiarization

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- **Lesson 2: Windows Core Components - The Registry**
  - Registry Overview
  - Signs of File Execution
  - Registry Persistence Mechanisms
  - Baselining the Registry
  - Lab
  - Navigate Regedit.exe and reg.exe
  - Add and remove keys and values
  - Investigate the registry for
  - potentially malicious behavior
- **Lesson 3: Windows Core Components - Processes**
  - What is a Process?
  - Process Tree
  - Single vs. Multiple Instances
  - Threads
  - Process Objects
  - Process Tools
  - Normal Windows Processes
  - Suspicious Processes
  - Lab
  - Examine system information related to networking, sockets, and active connections with TCPView
  - Execute a piece of malware and document the findings
- **Lesson 4: Windows Core Components - Dynamic Linked Libraries (DLLS)**
  - Libraries
  - Program Linking
  - What are DLLs?
  - Imports and Exports
  - DLL Search Order
  - Code and DLL Injection
  - Known Windows DLLs
- **Lesson 5: Windows Core Components - Memory Management and Injection**
  - Memory Management
  - Page Protections
  - Code and DLL Injection
  - Reflective DLL Injection
  - Hollow Process Injection

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Lab
  - Identify process injection using the
  - discussed tools
- **Lesson 6: Windows Core Components - Services**
  - What is a Service?
  - The Services Registry
  - Common Service Control Programs
  - Analyzing Services
  - Lab
  - Examine and interact with services using multiple tools
  - Differentiate information types and sources
- **Lesson 7: Windows Core Components - Logs and Timelines**
  - Logs Overview
  - Event Logs
  - Scheduled Task Logs
  - Antivirus Logs
  - PowerShell Logs
  - Timelining
  - Anti-analysis
  - Lab
  - Analyze malicious behavior with EventViewer
- **Lesson 8: Powershell**
  - What Is PowerShell?
  - Cmdlets and Providers
  - Getting Help
  - Objects, Piping, and Selection
  - I/O and Formatting
  - Lab
  - Discover language features and cmdlets, using the PowerShell help system
  - Use object members to obtain more functionality from cmdlets and sort the output
  - Create variables and use static members
- **Lesson 9: Powershill - Querying the Operating System**
  - Processes
  - Services
  - User Accounts
  - Event Logs
  - File System

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Registry
  - Network Connections
  - Lab
  - Demonstrate the use of PowerShell to access and display Process and Service attributes
  - Query Registry Keys using PowerShell
  - Access and display Registry and File System attributes with PowerShell
- **Lesson 10: Powershell - Scripting with Powershell**
  - What Is a Script?
  - Branching
  - Repetition
  - Functions
  - Script I/O
  - Execution Policy
  - Lab
  - Modify a script using PowerShell
- **Lesson 11: Powershell - Baselining with PowerShell**
  - What Is Baselining?
  - Baselining Elements
  - Differencing Tools
  - Lab
  - Compose a Baseline Script with PowerShell
  - PowerShell Baseline Scenario
- **Lesson 12: Powershell - Baselining Linux**
  - File System
  - File Structure
  - Virtual File System
  - Links
  - Permissions
  - Accounts
  - Lab
  - Summarize the Linux File System permissions and file integrity
  - Demonstrate how Linux determines a user's shell
- **Lesson 13: Powershell - Privilege Escalation**
  - Suid
  - Sudo
  - Wildcard Attacks
- **Lesson 14: Powershell - Linux Internals**

- Processes
- Scheduled Tasks
- Networking
- Services
- Logs
- Lab
- Monitor and interact with services
- Investigate processes and /proc filesystem
- Investigate concepts regarding two systems

Intended Audience

- Incident Responders who need to quickly identify a security breach
- Forensic Investigators needing to analyze the state of a running system
- Malware Analysts requiring a thorough understanding of operating system intrusions

Prerequisites

- Familiarity with the use of desktop operating systems, including command-line experience in Windows and/or Linux
- Working knowledge of TCP/IP networking

Follow-On Courses

- Computer Hacking Forensic Investigator
- EC-Council Certified Ethical Hacker (CEH)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.