800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Network Forensics and Investigation II Training

Applied Technology Academy

Learn how to use advanced features, apply threat intelligence, and identify and investigate more complex or hard-to-detect intrusions. There are a tremendous number of network-based attacks occurring every day, and that number is increasing rapidly. To defend against these attacks, they must be understood at the packet level. This course teaches you how to analyze, detect, and understand the network-based attacks that have become pervasive on today's Internet.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**2 years: CompTIA Net+ or CompTIA Sec+**	**$106,570**	**Yes**

Course Overview

- Identify and analyze events at all stages of the attack lifecycle
- Apply threat intelligence feeds to focus monitoring, investigation, and hunt activities

Detect and investigate tunneling, botnet command and control traffic, and other forms of covert communications being employed in a network

Use fingerprinting techniques to detect the use of encrypted traffic flows by malware or an active intruder

Accurately correlate and reconstruct multiple stages of malicious activity in order to build a complete picture of the scope and impact of complex network intrusions

Course Outline

- OVERVIEW AND LIFECYCLE
- Trends in Malicious Traffic
- Network Attack Lifecycle
- Targeted vs. Large-Scale Attack
- Network Intrusion Analysis Process
- Analytic Tools of the Trade
- Wireshark Exercises 1 and 2
- Analyze a Packet Capture Lab
- ANALYZING RECONNAISSANCE
- Beginning Phase of Attacks – Recon
- Host Discovery
- Port Scans

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- OS & Service Discovery
- Vulnerability Discovery
- HairSalon.com Lab
- BlendTec 1 Lab
- BlendTec 2 Lab
- Big Bad Recon Scan Lab
- Global Consulting - 1 Lab
- Transport Layer Attacks Demo
- Global Consulting 2 Lab
- Input Validation Attacks Demo
- Holophone 1 Lab
- Holophone 2 Lab
- Blendtec 3 Lab
- HoloPhone 3 Lab
- Analyzing XSS Javascript
- HoloPhone 4 Lab
- ATTACKER METHODOLOGY
- Social Engineering-Enabled Exploitation
- Physical Layer Attacks
- Data-Link Layer Attacks
- Network Layer Attacks
- Transport Layer Attacks
- Session Layer Attacks
- Presentation Layer Attacks
- Application Layer Attacks
- Global Consulting 1 Lab
- Global Consulting 2 Lab
- HoloPhone 1 Lab
- HoloPhone 2 Lab
- BlendTec 3 Lab
- HoloPhone 3 Lab
- HoloPhone 4 Lab
- BOTNETS
- Analysis Techniques
- History and Evolution
- Architecture and Design

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Malicious Uses
- Communications
- Examples
- Botnet Lab
- Global Consulting 3 Lab
- Data Mining Lab
- ADVANCED COMMUNICATIONS
- Transport Layer Security (TLS)
- Advanced Communication Methods
- Network Layer Tunneling
- Transport Layer Tunneling
- Application Layer Tunneling
- Traffic Cloaking
- Transport Layer Security Lab
- Johnson Trucking Lab
- STUDENT PRACTICAL DEMONSTRATION
- Using the tools, skills, and methodologies taught in Days 1 through 4 of the class students will uncover a
- multi-part network intrusion. In the intrusion capture files there will be multiple application-layer attacks,
- multiple advanced communications methods, and a hacker toolkit to discover. Students will have to prepare
- a report detailing the attack from start to finish as well as document what things the hacker did as well as what
- information was leaked if any.

Intended Audience

- Threat operation analysts seeking a better understanding of network-based malware and attacks
- Incident responders who need to quickly address a system security breach
- Forensic investigators who need to identify malicious network attacks
- Individuals who want to learn what malicious network activity looks like and how to identify it

Prerequisites

- Successful completion of the Network Forensics and Investigation I course is highly recommended
- Thorough knowledge of TCP/IP networking is required
- Skills and experience with Wireshark display filtering is required

- CompTIA's Network+ and Security+ certifications would be beneficial, but are not required

Follow-On Courses

Behavioral Malware Analysis

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.