SEC503: Network Monitoring and Threat Detection - In-Depth

GIAC CERTIFIED GCIA INTRUSION ANALYST

Course Overview

SEC503 is the most important course that you will take in your information security career – past students describe it as the most difficult but most rewarding course they've ever taken. If you want to be able to perform effective threat hunting to find zero-day activities on your network before public disclosure, this is definitely the course for you. SEC503 is not for people looking to understand alerts generated by an out-of-the-box network monitoring tool; rather, it is for those who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about.

What sets SEC503 apart from any other course in this space is that we take a bottom-up approach to teaching network monitoring and network forensics, which leads naturally to effective threat hunting. Rather than starting with a tool and teaching you how to use it in different situations, this course teaches you how and why TCP/IP protocols work the way they do. The first two sections present what we call "Packets as a Second Language," then we move to presenting common application protocols and a general approach to researching and understanding new protocols. Throughout the discussion, direct application of this knowledge is made to identify both zero-day and known threats.

With this deep understanding of how network protocols work, we turn our attention to the most important and widely used automated threat detection and mitigation tools in the industry. You will you learn how to develop efficient detection capabilities with these tools, and you'll come to understand what existing rules are doing and identify whether they are useful. The result is that you will leave this course with a clear understanding of how to instrument your network and perform detailed threat hunting, incident analysis, network forensics, and reconstruction.

Job Roles

- Practitioners Responsible For Intrusion Detection
- System Analysts
- Security Analysts
- Network Engineers
- Network Administrators
- Hands-On Security Managers

Intended Audience

- **Intrusion detection (all levels), system, and security analysts**
  - Analysts will be introduced to or become more proficient in the use of traffic analysis tools for signs of intrusions.
- **Network engineers/administrators**
  - Network engineers/ administrators will understand the importance of optimal placement of IDS sensors and how the use of network forensics such as log data and network flow data can enhance the capability to identify intrusions.
- **Hands-on security managers**
  - Hands-on security managers will understand the complexities of intrusion detection and assist analysts by providing them with the resources necessary for success.

Duration

6 Days

Certifications

GIAC Certified Intrusion Analyst (GCIA)

Contact Us

☎ 800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

SEC503: Network Monitoring and Threat Detection - In-Depth

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Network Monitoring and Analysis: Part I

TOPICS: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

SECTION 2: Network Monitoring and Analysis: Part II

TOPICS: Wireshark Display Filters; Writing BPF Filters; TCP; UDP; ICMP; IP6; Real-World Analysis – Researching a network

SECTION 3: Signature-Based Threat Detection and Response

TOPICS: Scapy; Advanced Wireshark; Introduction to Snort/Suricata; Effective Snort/Suricata; DNS; Microsoft Protocols; Modern HTTP; How to Research a Protocol; Real-world Application: Identifying Traffic of Interest

SECTION 4: Building Zero-Day Threat Detection Systems

TOPICS: Network Architecture; Introduction to Network Monitoring at Scale; Zeek; IDS/IPS Evasion Theory

SECTION 5: Large-Scale Threat Detection, Forensics, and Analytics

TOPICS: Using Network Flow Records; Threat Hunting and Visualization; Introduction to Network Forensic Analysis

SECTION 6: Advanced Network Monitoring and Threat Detection Capstone

TOPICS: The course culminates with a hands-on server-based Network Monitoring and Threat Detection capstone that is both fun and challenging. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the course.

Course Objectives

- Configure and run Snort and Suricata
- Create and write effective and efficient Snort, Suricata and FirePOWER rules
- Configure and run open-source Zeek to provide a hybrid traffic analysis framework
- Create automated threat hunting correlation scripts in Zeek
- Understand TCP/IP component layers to identify normal and abnormal traffic for threat identification
- Use traffic analysis tools to identify signs of a compromise or active threat
- Perform network forensics to investigate traffic to identify TTPs and find active threats
- Carve out files and other types of content from network traffic to reconstruct events
- Create BPF filters to selectively examine a particular traffic trait at scale
- Craft packets with Scapy
- Use NetFlow/IPFIX tools to find network behavior anomalies and potential threats
- Use your knowledge of network architecture and hardware to customize placement of network monitoring sensors and sniff traffic off the wire

GIAC Certified Intrusion Analyst (GCIA)

The GIAC Intrusion Analyst certification validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. GCIA certification holders have the skills needed to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files.

- Fundamentals of Traffic Analysis and Application Protocols
- Open-Source IDS: Snort and Bro
- Network Traffic Forensics and Monitoring