SEC503: **Intrusion Detection In-Depth**

GCIA
Intrusion Analyst
giac.org/gcia

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

SEC503 is one of the most important courses that you will take in your information security career. While past students describe it as the most difficult class they have ever taken, they also tell us it was the most rewarding. This course isn't for people who are simply looking to understand alerts generated by an out-of-the-box Intrusion Detection System (IDS). It's for people 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. If you want to be able to find zero-day activities on your network before disclosure, this is definitely the class for you.

What sets this course apart from any other training is that we take a bottom-up approach to teaching network intrusion detection and network forensics. Rather than starting with a tool and teaching you how to use that tool in different situations, this course teaches you how and why TCP/IP protocols work the way they do. After spending the first two days examining what we call "Packets as a Second Language," we add in common application protocols and a general approach to researching and understanding new protocols. With this deep understanding of how network protocols work, we turn our attention to the most widely used tools in the industry to apply this deep knowledge. The result is that you will leave this class with a clear understanding of how to instrument your network and the ability to perform detailed incident analysis and reconstruction.

These benefits alone make this training completely worthwhile. What makes the course as important as we believe it is (and students tell us it is), is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic, and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

> **"The course has equipped me with super powers. I can see everything! I don't know how I was able to do my job without this knowledge. This course is a must for any cyber defense analyst."**
>
> — Joe Morrissey, **Nationwide**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Fundamentals of Traffic Analysis – Part 1

Section 1 begins our bottom-up coverage of the TCP/IP protocol stack, providing a refresher or introduction, depending on your background, to TCP/IP. This is the first step in what we think of as a "Packets as a Second Language" course. Students begin to be introduced to the importance of collecting the actual packets involved in attacks and are immediately immersed in low-level packet analysis. We will cover the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, and the meaning and expected behavior of every field in the IP header. Students are introduced to the use of open-source Wireshark and tcpdump tools for traffic analysis.

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

SECTION 2: Fundamentals of Traffic Analysis – Part 2

Section 2 continues where the first section ended. Students will gain a deep understanding of the primary transport layer protocols used in the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using advanced features to give you the skills to analyze your own traffic. The focus of these tools is to filter large-scale data down to traffic of interest using Wireshark display filters and tcpdump Berkeley Packet Filters. These are used in the context of our exploration of the TCP/IP transport layers covering TCP, UDP, and ICMP. Once again, we discuss the meaning and expected function of every header field, covering a number of modern innovations that have very serious implications for modern network monitoring, and we analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

TOPICS: Wireshark Display Filters; Writing tcpdump Filters; TCP; UDP; ICMP; Real-World Analysis – Command Line Tools

SECTION 3: Application Protocols and Traffic Analysis

Section 3 builds on the foundation of the first two sections of the course, moving into the world of application layer protocols. Students are introduced to the versatile packet crafting tool Scapy. This is a very powerful Python-based tool that allows for the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. Various practical scenarios and uses for Scapy are provided throughout this section.

TOPICS: Scapy; Advanced Wireshark; Detection Methods for Application Protocols; DNS; Microsoft Protocols; HTTP(2)/TLS; SMTP; IDS/IPS Evasion Theory; Identifying Traffic of Interest

SECTION 4: Network Monitoring: Signatures vs. Behaviors

The fundamental knowledge gained from the first three sections provides the foundation for deep discussions of modern network intrusion detection systems during section 4. Everything that students have learned so far is now synthesized and applied to designing optimized detection rules for Snort/Firepower, and this is extended even further with behavioral detection using Zeek. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a discussion about options and requirements for devices that can sniff and capture the traffic for inspection. This section provides an overview of deployment options and considerations, and allows students to explore specific deployment considerations that might apply to their respective organizations.

TOPICS: Network Architecture; Introduction to IDS/IPS Analysis; Snort; Zeek

SECTION 5: Network Traffic Forensics

Section 5 continues the trend of less formal instruction and more practical application using hands-on exercises. It consists of three major topics, beginning with practical network forensics and an exploration of data-driven monitoring vs. alert-driven monitoring, followed by a hands-on scenario that requires students to use all of the skills developed so far. The second topic continues the theme of data-driven analysis by introducing large-scale analysis and collection using NetFlow and IPFIX data.

TOPICS: Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

SECTION 6: Advanced IDS Capstone Event

The course culminates with a fun, hands-on, score-server-based IDS challenge. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the first five sections. The challenge presented is based on hours of live-fire, real-world data in the context of a time-sensitive incident investigation. The challenge is designed as a "ride-along" event, where students are answering questions based on the analysis that a team of professional analysts performed of these same data.

Who Should Attend

- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

> **"I got a deeper understanding of key topics from SEC503. This training will help me get more data out of my investigations."**
>
> — Alphonse Wichrowski, **Allegiant Air**

Course Preview
available at: **sans.org/demo**