SANS EMEA

Hands On | Six Days | Laptop Required | 36 CPEs

SEC 503

# INTRUSION DETECTION IN-DEPTH

**Reports of prominent organisations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?**

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence.

**#SANSDubai**

## Take SEC503 at SANS Dubai 2016

Dubai 9 - 14 Jan, 2016
Register online at **www.sans.org/event/dubai-2016**

**Ned Baltagi,** Director Middle East, SANS Institute. UAE +971 55 336 1943

## Who should attend

- 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
- Hands-on Security Managers

## Hands-on training

The hands-on training in SEC503 is intended to be both approachable and challenging for beginners and seasoned veterans. There are two different approaches for each exercise. The first contains guidance and hints for those with less experience, and the second contains no guidance and is directed toward those with more experience. In addition, an optional "Extra Credit" question is available for each exercise for advanced students who want a particularly challenging brain teaser.

## You will receive

- Course book with each day's material
- Workbook with hands-on exercises and questions
- DVD with the Packetrix Linux VMware image
- TCP/IP pamphlet cheat sheet
- MP3 audio files of the complete course lecture

For more information see our course catalogue or visit **www.sans.org/emea**

WORLD-CLASS INFORMATION SECURITY TRAINING

# Course Syllabus

## 503.1 Fundamentals of Traffic Analysis: Part I

Day 1 covers the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, an introduction to Wireshark, the IP layer, and both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyse traffic not just in theory and function, but from the perspective of an attacker and defender.

**Topics:** Concepts of TCP/IP, Introduction to Wireshark, Network Access/Link Layer: Layer 2, IP Layer: Layer 3

## 503.2 Fundamentals of Traffic Analysis: Part II

Two essential tools - Wireshark and tcpdump - are explored to give you the skills to analyse your own traffic. The focus of these tools on Day 2 is filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP.

**Topics:** Wireshark Display Filters, Writing tcpdump Filters, TCP, UDP, ICMP

## 503.3 Application Protocols and Traffic Analysis

Day 3 culminates the examination of TCP/IP with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols: HTTP, SMTP, DNS, and Microsoft communications.

**Topics:** Advanced Wireshark, Detection Methods for Application Protocols, Microsoft Protocols, HTTP, SMTP, DNS, IDS/IPS Evasion Theory, Real-World Traffic Analysis

## 503.4 Open-Source IDS: Snort and Bro

The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days SEC503. Snort and Bro are widely deployed open-source IDS/IPS solutions that have been industry standards for over a decade. We take a unique approach of teaching both open-source IDS solutions by presenting them in their operational life-cycle phases from planning to updating. This will offer you a broader view of what is entailed for the production operation of each of the tools.

**Topics:** Operational Lifecycle of Open-Source IDS, Introduction, Snort, Bro, Comparing Snort and Bro to Analyse Same Traffic

## 503.5 Network Traffic Forensics and Monitoring

On the penultimate day, you'll become familiar with other tools in the "analyst toolkit" to enhance your analytical skills and give you alternative perspectives of traffic.

**Topics:** Analyst Toolkit, SiLK, Packet Crafting, Network Forensics, Network Architecture for Monitoring, Correlation of Indicators.

## 503.6 IDS Challenge

The week culminates with a fun hands-on challenge where you find and analyse traffic to a vulnerable honeynet host using many of the same tools you mastered during the week. Students can work alone or in groups with or without workbook guidance. This is a great way to end the week because it reinforces what you've learned by challenging you to think analytically, gives you a sense of accomplishment, and strengthens your confidence to employ what you've learned in a real-world environment.

**#SANSDubai**

## Take SEC503 at SANS Dubai 2016

Dubai 9 - 14 Jan, 2016
Register online at:
**www.sans.org/event/dubai-2016**

**Ned Baltagi,** Director Middle East, SANS Institute.
UAE +971 55 336 1943

## 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
- Synthesize disparate log files to widen and augment analysis
- 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

SANS EMEA

**www.sans.org/emea**

**Email:** emea@sans.org • **Tel:** +44 20 3384 3470
**Address:** SANS EMEA,
PO Box 124, Swansea, SA3 9BB, UK