Sophisticated attackers frequently go undetected in a victim network for an extended period of time. Attackers know how to blend their traffic with legitimate traffic and only the skilled network traffic analyst will know how to find them. Network traffic analysis is a critical skill set for any organization. MANDIANT’s intense three-day MANDIANT Network Traffic Analysis course prepares students to face the challenge of identifying malicious network activity. The course provides students an overview of network protocols, network architecture, intrusion detection systems, network traffic capture and traffic analysis. The course consists of lecture and multiple hands-on labs to reinforce technical concepts.

**Duration**

3 days

**Who Should Attend**

Information technology and security staff, corporate investigators, or other staff requiring an understanding of networks, network traffic, network traffic analysis and network intrusion investigations.

**Prerequisites**

Students should have a basic understanding of TCP/IP and be familiar with Windows and UNIX platforms. A familiarity with computer security terminology and concepts is helpful.

**Students Will Learn**

- Common network protocols
- Network monitoring and the Incident Response process
- Why network monitoring is important in today’s networks
- The different types of network monitoring
- Pros and cons of Statistical, Connection, Full Content and Event Monitoring and tools to perform each type of monitoring
- The tools commonly used to analyze captured network traffic
- What Botnets are and how to investigate them
- Honeypots and honeynets and how they are used in Network Monitoring
- How to perform event-based monitoring using Snort
- Snort rule structure and custom rule creation for network traffic minimization and the Sguil front-end for reviewing Snort alerts

**Exercise Overview**

- Value of Network Monitoring
- Network Protocol Analysis
- Network Monitor Placement
- Full Content Monitoring
- Investigating Botnets
- Wireshark Filters
- Traffic Analysis Tools
- Honeypot Data Analysis
- Event Monitoring with Snort and Sguil

**Course Materials**

- Student manual
- Class handouts
- MANDIANT gear
- USB thumb drive containing course tools and scripts

**Suggested Next Courses**

- MANDIANT Enterprise Incident Response
- MANDIANT Introduction to Malware Analysis

**Contact**

1.800.647.7020

education@mandiant.com

www.mandiant.com/education.htm
Case Studies

Students are presented a case study coupled with a lab to reinforce critical concepts.

Network Protocol Review

Instructors will provide a quick overview of the TCP/IP protocol stack to ensure students understand the foundational elements of network traffic. Students will also learn the various daemons and services that support network communications.

Incident Response Process

Students will explore the Incident Response process and how network monitoring supports a network intrusion investigation.

Network Monitor Hardware & Placement

Explore various hardware and software configurations and the techniques used to collect network traffic. Students will also learn to identify the proper placement of network traffic monitoring devices for wired and wireless networks.

Statistical Monitoring

Students learn how network traffic statistical analysis can point to signs of a network intrusion. Students will also explore open source tools commonly used to perform network traffic statistical analysis.

Event-based Monitoring

Event-Based Monitoring introduces students to the various technologies designed to alert security personnel of a network intrusion. The section covers: Discuss Network Intrusion Detection Systems (NIDS), Introduction to Snort NIDS, Snort rule structure and custom rule creation and Sguil as a graphical interface for Snort alert review.

Traffic Analysis: Protocols

Wireshark is the tool of choice for traffic analysis. This section introduces the student to Wireshark and how it is used to dissect various network protocols and identify and extract suspect payloads.

Traffic Analysis: Tools

Discuss and use various tools that aid an analyst during the course of a network intrusion investigation.

Honeypots: Real-World Attacks

This section sheds light on honeypots and their role in discovering attacker tactics and techniques. Students will learn about the Honeynet Project and use tools from the project to analyze data harvested from a successful attack.

Investigating Botnets

Discuss what Botnets are and how they work. Tools and methods used to analyze and investigate Botnets.

Final Exercise

Students put their knowledge to the test during the final exercise. During the final exercise, students are provided data from a network intrusion and are challenged to determine the attack methods used and the origin of the attack.