

NETWORK TRAFFIC ANALYSIS

Performing network traffic analysis is a critical skill set for any organization that wants to monitor incoming traffic (intrusion detection) as well as monitor outgoing traffic (extrusion detection). During this intense three-day course, experienced Mandiant instructors cover the processes and technology that allow an organization to successfully implement network traffic monitoring. We discuss how to place network sensors, how to eliminate white noise and isolate traffic of interest, and how to interpret the data.

Duration

3 days

Who Should Attend

Information technology staff, information security staff, corporate investigators, or other staff that require an understanding of how networks work, how to capture network traffic, how to investigate network use, how to identify and escalate suspected computer security incidents, and how to safeguard corporate assets via network defense will greatly benefit from this course.

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 protocols involved in a majority of investigations
- Where Network Monitoring fits in to the Incident Response process
- Why Network Monitoring is important in today's networks
- The different types of Network Monitoring
- The 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 the data that is captured while performing the different types of Network Monitoring
- What Botnets are and how to investigate them
- Overview of honeypots and honeynets and how they can be used for Network Monitoring
- Use of open source honeypot software and analysis tools from the HoneyNet Project
- How event based monitoring is deployed using Snort
- Snort rule structure and custom rule creation for network traffic minimization and the Sguil front end for reviewing Snort alerts

Exercises

- Importance 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
- Free Tools CD with course tools and scripts

Suggested Next Courses

- Incident Response
- Linux for Security Professionals
- Malware Analysis

Contact

1.800.647.7020

education@mandiant.com

www.mandiant.com/education.htm

Case Studies

- Real world current case study discussed in detail

Network Protocol Review

- A quick overview of the TCP/IP protocol stack
- Discuss daemons and services and how they open listening network ports
- Review of the common types of network hardware and the pros and cons of each

Incident Response Process

- Examine the Incident Response process
- See where Live Response factors into the IR Process
- Address how Network Monitoring fits into the Live Response portion of the Incident Response Process

Network Monitor Hardware and Placement

- Analyze different hardware, software and techniques to collect network traffic
- Identify the proper location for network traffic monitoring devices for wired and wireless networks

Statistical Monitoring

- Learn how statistical analysis of network data can point to signs of a system compromise
- Discuss open source tools that can be used to perform statistical analysis

Connection Monitoring

- Discuss what connection monitoring is, what we are looking for and potential legal repercussions of monitoring
- Learn how to perform connection monitoring using open source tools and how to analyze the data

Full Content Monitoring

- Discuss how full content monitoring differs from other types of Network Monitoring
- Analyze the data collected during full network capture
- Discuss the pros and cons of full content monitoring
- Multiple tools for full content data collection, minimization of collected data, and analysis of packet captures

Event Based Monitoring

- Discuss Network Intrusion Detection Systems (NIDS)
- Introduction to Snort NIDS
- Snort rule structure and custom rule creation
- Sguil as a graphical interface for Snort alert review

Traffic Analysis - Protocols

- Become very familiar with the Wireshark interface for deeper inspection of multiple protocols
- Analyze some of the more common protocols an analyst is likely to encounter during the course of an investigation

Traffic Analysis- Tools

- Discuss and use free and commercial tools that will aid an analyst during the course of an investigation

Honeypots – Real World Attacks

- Discuss what honeypots are and how they work
- Overview of the HoneyNet Project
- Use tools from the HoneyNet Project to analyze a successful Linux attack

Investigating Botnets

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

Final Exercise

- Analyze Statistical, Connection and Full-Content network data from a network based intrusion
- Discover what attack methods were used and what locations the attacks originated from
- Produce an Investigative Report of the intrusion