FireEye Cyber Defense Summit 2017

Network Traffic Analysis (2 days)

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. FireEye's intense three-day 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.

What You 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
- 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 captured network traffic
- What Botnets are and how to investigate them
- What Honeypots and honeynets are 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

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.

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.