네트워크 트래픽 분석 (3일 과정)

수준 높은 공격자들은 종종 피해자 네트워크에서 오랜 시간 동안 탐지되지 않습니다.
공격자들은 공격 트래픽을 정상적인 트래픽과 혼합하는 방법을 알고 있으며, 숙련된 네트워크 트래픽 분석가만이 공격 트래픽을 찾을 수 있습니다.
모든 조직에 있어서 네트워크 트래픽 분석은 중요한 기술입니다.
참가자들은 맨디언트의 집중적인 3일간의 네트워크 트래픽 분석 과정을 통해 악의적인 네트워크 활동을 식별하는 것을 배우게 됩니다.
이 과정은 참가자들에게 네트워크 프로토콜, 네트워크 아키텍처, 침입 탐지 시스템, 네트워크 트래픽 캡처 및 트래픽 분석의 개요를 제공하며, 기술 개념을 강화하기 위하여 여러 개의 실습 랩으로 구성되어 있습니다.

(1) 교육 내용
》일반적인 네트워크 프로토콜
》네트워크 모니터링 및 침해 대응 프로세스
》오늘날의 네트워크에서 네트워크 모니터링이 중요한 이유
》다양한 유형의 네트워크 모니터링
》통계, 커넥션, 전체 컨텐츠의 장단점과 이벤트 모니터링, 각 타입의 모니터링을 하는 프로그램들
》캡처 된 네트워크 트래픽을 분석하는데 일반적으로 사용되는 프로그램들
》Botnet과 조사하는 방법
》Honypot 및 Honeynet과 네트워크 모니터링에서 사용 방법
》Snort를 사용하여 이벤트 기반의 모니터링을 수행하는 방법
》Snort Alert을 검토하기 위한 Sguil front-end와 네트워크 트래픽 최소화를 위한 Snort 룰 구조와 사용자 정의 규칙 생성

(2) 참석 대상
》IT 및 보안 종사자, 기업 보안 조사관 또는 네트워크, 네트워크 트래픽, 네트워크 트래픽 분석 및 네트워크 침입 조사에 대한 이해가 필요한 사람

(3) 과정 전제조건
》참가자들은 TCP/IP에 대한 기본적인 지식과 Windows와 UNIX 플랫폼에 익숙해야 합니다. 컴퓨터 보안 용어 및 개념에 익숙하면 과정에 도움이 됩니다.

<원문>
Network Traffic Analysis
Description of Services

Network Traffic Analysis (3 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. Mandiant'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.

(a) Students 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.

(b) 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.

(c) Course Pre-requisites

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.