Course Outline

Introduction to Security Analysis

Course Summary

Description

Most IT professionals are aware of the importance their jobs play in securing an organization, but many are not adequately trained in this important function and may not know where to begin. This hands-on course gives a jumpstart into the analysis of network intrusions, compromised hosts, and malware. Students will learn what common attacks look like, how to track and analyze malicious activity, and what mitigation steps should be taken.

Topics

- Profile/baseline the hosts, services and activity in a computer network
- Perform user-level attribution of unwanted activity in a network
- Compare observed network traffic to expected topology
- Identify and observe the core components of an operating system
- Conduct basic behavioral analysis of malware on a running Windows system

Audience

This course is designed for IT Professionals wanting to learn the analysis of network intrusions, compromised hosts, and malware.

Prerequisites

- A background in information technology
- Basic understanding of networking and security concepts
- Light experience with the Windows Sysinternals Suite

Duration

Two days