Network Forensics Advanced

Index: CF202

40 Hours
Network Forensics Advanced

Description

Network Forensics - Advanced takes forensics specialists another step forward to help them master the tasks of capturing, recording and analyzing network events to discover the source of security incidents. Network investigators need to have advanced capabilities of accessing the deepest, most hidden places on the network and understanding how to extract data from there. The course is a drill-down to network protocols, intrusion detection on the network and advanced capabilities of log forensics.

Objectives

During this course and upon completion, participants will be able to:

- Understand networks on a deep level – how they function and how information is stored on them.
- Monitor and analyze user and system activities on the network in order to recognize patterns of typical attacks.
- Analyze abnormal activity patterns to detect signs of an intrusion.
- Use advanced tools for intrusion detection.
- Analyze log files and log data using available tools, and create their own tools for more advanced uses.

Target Audience

The course is intended for participants with former background in network forensics, and preferably some experience in the field, who wish to advance and deepen their knowledge and capabilities. The primary target audience is:

- Law enforcement officers & intelligence corps
- Incident responders
- Computer investigators
- IT/network administrators
- Cyber Forensics analysts

Prerequisites

- Background knowledge in network forensics.
- CF201 provides a solid foundation of preliminary knowledge required for this course.
Course Outline

**01 Deep Dive into Networks**

The first module will take participants deeper into the world of networking to gain a better understanding of every layer in the OSI model, so they can perform more advanced and “deep” inspections of the network as part of the investigation process. The most recent IPv6 will also be covered.

- OSI application layer
- OSI presentation layer
- OSI session layer
- OSI transport layer
- OSI network layer
- OSI datalink layer
- OSI physical layer
- Advanced subnetting
  - Networks
  - Hosts
  - VLSM
- IPv6
  - Basic protocols
  - IPv6 structure
  - Transition mechanism
  - Routing basics
  - Security

**02 Intrusion Detection**

During this module, participants will further explore the study of data packets on a deeper level, learn to identify network anomalies, and understand system alerts. Students will master the use of well-known command-line-interface (CLI) and graphic-user-interface (GUI) tools to further specialize in the field.

- Case study: a recent and well-known network attack incident will be analyzed among participants guided by the instructor. Students will be required to formulate how they would approach the investigation of the incident and raise it up in an open discussion, gaining more insight into network attacks from the investigator’s point of view.

- Basic intrusion detection tools and methods:
  - Sysmon
  - Hashes
  - Events
  - Filtering
  - Network events
- Advanced Wireshark
  - Streams analysis
  - Wireshark display filters
  - Exporting web objects
  - Advanced incident investigation
  - TShark: Wireshark CLI tool
- Using Scapy module
  - Crafting and analyzing packets
  - Working with PCAP files
  - Replaying packets for investigating
- IDS/IPS analysis

**03 Log Forensics**

Log files are used to maintain a record of activities of the system and its applications. Through the analysis of logs, investigators can inspect the system during an attack and after it, and build tools that will help in future identification. During this module, participants will learn how to work with various defense mechanisms on the workstation and servers, and build some of their own tools for later use.

- Analyzing firewall logs
  - Using different analyzers
  - Manually analyzing data
  - Analyzing suspicious behavior of the firewall
  - Working with advanced tools
- Analyzing Apache/IIS logs
  - Investigating web logs
  - Filtering and analyzing log files
  - Log parser automation
- Python
  - Learning to write scripts with Python
- Logs with Python
  - Extracting data from logs
  - Automation with Python
  - Using Python scripts for the analysis
- Building an agent that creates logs, analyses them and sends out alerts
  - Alerts
  - Network anomalies
  - MiTM attacks
  - Trojans
- Lab: network under attack -- students will identify the source of the attack and handle the incident.

**04 Decrypting SSL**

SSL is a standard for transmitting secure data over the internet. During this module, students will learn how to decrypt SSL using available tools and tools they will build by themselves.

- Downgrading SSL with MiTM
- Extracting the certificate
  - With physical access
  - Remotely
- Lab: building automated tools for decrypting SSL.