FOR400 Fundamentals of Network Forensics

Course Overview

FOR400 - Fundamentals of Network Forensics expands on acquired networking knowledge and extends into the computer forensic mindset. Students will learn about common devices used in computer networks and where useful data may reside. Students will also learn how to collect that data for analysis using hacker methodology.

Additionally, the course covers information related to common exploits involved in Windows server systems and common virus exploits. Students will learn how to recognize exploit traffic, and the difference between attacks and poor network configuration.

Objectives

- Provide an understanding of devices used to set up computer networks, where useful data may reside within the network, and how the data is stored and retrieved to acquire analysis

Target Audience

- Professionals looking to either broaden their cyber skills or begin developing a skill set within the network defense community

Estimated Course Length: 24 hours

Day 1

Students will learn to understand and demonstrate the use of a standard methodology for exploitation, the concepts of various software threats and the techniques expected of a professional hacker.

Topics List

- Hacker mindset and steps of an attack
- Hacker techniques
- Tools used for exploitation
- Packet capturing and analysis
- Tools used for network analysis

Day 2

Students will identify protocols helpful when performing network forensics. Students will gain an understanding of filters and how they can help identify specific packets of interest. Students will setup Ethernet ports for capturing data and analyze traffic using Snort to identify malicious activity.

Topics List

- Filtering traffic and protocol analysis
- Comparing file hashes to identify malicious files
- Parsing network traffic to identify malicious files and attacker activity
- Network devices, packet capturing in a switched environment
- Configuring Ethernet ports on an IDS
- Advantages of internal and external IDS placement
- Running Snort
- Examining Snort rules and using Snort to analyze packet capture files

Day 3

Students will learn how to edit Snort configuration files to use local rules, edit rules files and write custom rules to detect malicious activity, command shells and malware. Students analyze traffic using Snort as an intrusion detection system. Students will learn to recognize anomalous activity in web, FTP authentication and access logs in Linux and Windows.

Topics List

- Editing Snort configuration files
- Editing Snort rules files
- Writing custom Snort rules to detect malicious activity
- Analyzing traffic using Snort as an IDS
- Recognizing anomalous activity in Linux and Windows logs

Day 4

Students will learn how to recognize anomalous activity in Linux and Windows. Student will understand how to detect evidence of an attack using incident response toolkits as well as native tools to view process lists, established connections, scheduled jobs, and account activity.

Topics List

- Analyzing Windows incident response data
- Analyzing Linux incident response data
- Using visualization tools to recognize anomalous communications
- Correlating data from established connections processes and traffic
- Using Sawmill to analyze Snort logs
- Recognizing internal and external threats

Day 5

Students will demonstrate the ability to identify attacker IP addresses, exfiltrated data, malware, method of compromise, accounts used, and document observed activity in an executive summary and timeline of events.

Capstone Exercise

Students will be required to assign attribution to an attack and final exercise.

About CYBRScore®

Comtech Mission-Critical Technologies (Comtech MCT) provides cybersecurity solutions and services tailored to training and workforce development. The CYBRScore® product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech MCT CYBRScore® offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

CYBRScore®
Comtech Mission-Critical Technologies
275 West Street, Annapolis, MD 21401

www.cybrscore.io
ComtechMCT-CYBRScore@comtechtel.com