Training overview

DFIR370-Host Intrusion Methodology and Investigation

Day 1

After a course introduction and an orientation of the virtual workspace used throughout the week, day one instruction dives right into material on reconnaissance and browser exploits.

Students will learn about various types of reconnaissance and the use of honey networks. Next, students will examine the structure of a cyberattack, then create and launch their own web browser exploit.

Instruction follows with an explanation of best practices in the development and implementation of a triage plan. After that, instruction focuses on creating and maintaining a thorough methodology for analysis.

The main areas covered on day one include:

- Introduction to host intrusion investigations
- Working with a virtual workspace
- Understanding reconnaissance methods and utilizing them against the victim computers
- Using honey networks to aid in the identification of attackers
- Developing a comprehensive methodology for analyzing an intrusion
- Understanding and learning how to respond to browser exploits
- The lifecycle of a cyber attack
- Setting up and weaponizing a browser exploit
- Conducting a dynamic analysis
- Infecting a machine and establishing persistence

Day 2

Instruction on day two begins with a continuation and reinforcement of the host intrusion analysis methodology. Then the course moves on to a lesson on various techniques used to hide data.

Next, students will learn phishing techniques, one of the oldest and most successful types of attacks on the internet. Students will participate in practical exercises throughout the day, reinforcing the day's activities.

The main areas covered on day two include:

- How to triage a live host while referencing multiple strategy models and the host intrusion methodology
- Understanding tactical readiness and determining risk tolerance and the operational impact of an incident response
- Establishing a triage protocol
- Understanding and using common volatile and disk-based artifacts used during investigations to the best advantage
- Using the methods of hiding data, as well as locating and identifying various hidden data
- Understanding phishing techniques, including methods of luring, stealing login credentials, sending malicious attachments and how to manually send phishing emails through terminal commands

Day 3

Day three begins with a review of the instruction thus far. The course will demonstrate OpenText™ EnCase™ Portable as a backup method to collect volatile data, network data and live registry items. Next, students will learn about malware infections involving a malicious remote administration tool.

Students will participate in the investigation triad, which consists of memory and packet capture analysis, as well as log file review. Practical exercises of the malware infection will also be conducted.

The main areas covered on day three include:

- Setting up and using EnCase Portable to collect and store volatile data from a live machine
- Conducting a malware infection and discussing packet capture and log file collection techniques
- Analyzing memory artifacts affected by intrusions
- Analyzing packet capture network artifacts and event logs to determine the extent of intrusions

Day 4

A review will begin day four, which is followed by a lesson on analyzing malware. A practical exercise will challenge students to analyze captured volatile data to determine the story behind a compromised system. The course ends with a lesson on the various methods used to enhance a hacker's status on a computer or network.

The main areas covered on day four include:

- Analyzing log files created during a malware infection
- Using various programs to parse and investigate event logs
- Conducting basic analysis of malware and volatile data related to successful intrusions
- Escalating a hacker's privilege on a system and analyzing the compromise

opentext.com/contact