skillsoft global knowledge™

FOCAL POINT - NETWORK FORENSICS AND INVESTIGATION II

Course Code: 100218

Learn how to use advanced features, apply threat intelligence, and identify and investigate more complex or hard-to-detect intrusions.

There are a tremendous number of network-based attacks occurring every day, and that number is increasing rapidly. To defend against these attacks, they must be understood at the packet level. This course teaches you how to analyze, detect, and understand the network-based attacks that have become pervasive on today’s Internet.

Building on the skills developed in the Network Forensics and Investigation course, students will learn how to use advanced features in tools such as Elastic, Wireshark, Zeek and Suricata, how to apply threat intelligence to enrich analysis and direct response actions, and how to identify and investigate more complex or hard-to-detect intrusions. This course covers malicious actions from across the attacker lifecycle, from initial reconnaissance and access through to activities such as data exfiltration and command-and-control traffic attributed to botnets or APTs.

What You'll Learn

- Identify and analyze events at all stages of the attack lifecycle
- Apply threat intelligence feeds to focus monitoring, investigation, and hunt activities
- Detect and investigate tunneling, botnet command and control traffic, and other forms of covert communications being employed in a network
- Use fingerprinting techniques to detect the use of encrypted traffic flows by malware or an active intruder

Accurately correlate and reconstruct multiple stages of malicious activity in order to build a complete picture of the scope and impact of complex network intrusions

Who Needs to Attend

- Threat operation analysts seeking a better understanding of network-based malware and attacks
- Incident responders who need to quickly address a system security breach
- Forensic investigators who need to identify malicious network attacks
- Individuals who want to learn what malicious network activity looks like and

how to identify it

Prerequisites

- Successful completion of the Network Forensics and Investigation I course is highly recommended
- Thorough knowledge of TCP/IP networking is required
- Skills and experience with Wireshark display filtering is required
- CompTIA’s Network+ and Security+ certifications would be beneficial, but are not required

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/11/2025 12:18:30 AM