

FOCAL POINT - NETWORK FORENSICS AND INVESTIGATION I

Course Code: 100216

Learn how to differentiate between normal and abnormal network traffic, track the flow of packets through a network, and attribute conversations and actions taken over a network segment to specific hosts or users.

Focal Point - Network Traffic Analysis will teach you to differentiate between normal and abnormal network traffic, track the flow of packets through a network, and attribute conversations and actions taken over a network segment to specific hosts or users. This course focuses on research, filtering, and comparative analysis to identify and attribute the different types of activity on a network. You will learn how to follow conversations across a wide range of protocols and through redirection, as well as how to develop custom filters for non-dissected protocols. On Day 5 of the course, you will participate in a team-based capture-the-flag exercise to test your new skills.

Learn more about this topic. View the recorded webinar [From Analyst to Threat Hunter](#).

What You'll Learn

- Create a baseline of the protocols, hosts and interactions in a network environment
- Identify anomalous network traffic using a combination of in-depth packet analysis and high-level statistical analysis
- Reconstruct event timelines and accurately correlate, or distinguish between, event threads
- Identify and extract network artifacts for further forensic analysis
- Compare observed network traffic to expected topology
- Research and analyze unknown (non-dissected) protocols
- Track web activity at the user or session level via HTTP header analytics

Student Practical:

Using the tools, skills, and methodologies taught in Days 1 - 4, on day 5 of the course students will participate in a competitive capture-the-flag exercise that includes various categories, including a simulated SCADA attack scenario. Designed to challenge the participants, each correctly completed milestone will unlock a

successively more difficult challenge.

Course Outline:

1. Building Blocks
2. OSI & TCP/IP Review
3. Wireshark Tutorial
4. Day in the Life (Common Protocols)
5. Extracting Objects
6. TCP - A Deeper Look
7. Analytic Approach
8. Internet Research
9. Isolating Traffic
10. Routing Principles
11. Traceroute Analysis
12. Standards and Protocol Analysis
13. Start-to-Finish Protocol
14. Analysis (Email Example)
15. Analysis Beyond Wireshark
16. Secure Protocols
17. HTTP Header Analytics
18. Big Capture
19. More Tools and Tricks

Labs:

1. Wireshark Filtering (Part 1, Part 2)
2. A Day in the Life (Common Protocols)
3. Exporting Objects
4. TCP/IP Analysis
5. Internet Research
6. Isolate Event #1
7. Isolate Event #2
8. Isolate Event #3
9. Isolate Event #4
10. Isolate Event #5
11. RFC Research
12. Meta-data Analysis
13. Non-Dissected Protocol Analysis
14. Encrypted Traffic Analysis Referer
15. User-Agents
16. Web Request Tracking
17. Large Capture Investigation

Who Needs to Attend

- Network analysts seeking to develop security-related skills
- Incident responders needing to quickly address system security breaches
- Penetration testers looking to reduce their detectability

- Threat operations analysts seeking a better understanding of network intrusions
- All network administrators needing a better understanding of network security

Prerequisites

- A broad understanding of TCP/IP and associated protocols
- Knowledge of network hardware and segment types
- Previous exposure to Wireshark or other protocol analysis software is also recommended

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

Date created: 5/9/2025 4:46:54 AM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.