Sharkfest EU 2021 - Next Generation Protocols & Advanced Network Analysis

(v3.4.3)

Format: 1-day Instruction
Start/End Times – 0800-1700
Audience: Intermediate

Target Audience:

This course is for Networking, Engineering, and Security personnel who want to advance their packet investigation techniques by studying the Next Generation Networking Protocols using Wireshark. Successful completion of this course will provide these individuals with a path-way into the field of both Network and Forensics Analysis.

Recommended Prerequisites:

This course is at an intermediate level, and given the fast pace, students should, at a minimum, be proficient with creating Wireshark profiles, columns, color rules, capture and display filtering, and the basics of the IPV4-based TCP/IP protocol stack.

Description:

Time is money when troubleshooting and optimizing network performance issues. Practical network analysis encompasses capturing data and discerning the critical patterns hidden within network traffic streams to identify the problem. Additional complexity due to the increasing adoption of the Nest Generation Protocol stacks, including the IPV6-based family, threatens to make this job even more challenging.

This course provides the student with an introduction to investigating and analysis techniques focusing on the use of vendor-neutral, Open-Source Tools such as Wireshark to provide insight into the following areas:

- Recognition, analysis, and threat recognition for many of the next generation user protocol issues, including IPv4/v6/v10, DHCPv4/v6, SCTP, ICMP (v4 /v6), Internet-based User Protocols (HTTP, HTTP 2, HTTP 3, SPDY, and QUIC)

- Specialized Analysis techniques including suspicious data traffic reconstruction and viewing

Real-World examples will be utilized throughout the course in conjunction with multiple hands-on exercises to provide field-proven, practical analysis skills. Attendees will receive a student guide, including various reference files and a library of essential reference documents.

Course Details:

I. Introduction to Advanced Network Analysis and the Next Generation Protocols

II. Advanced Network Analysis Methodology

1. Sample Advanced Network Analysis Methodology -Answering the key questions
    a. What's Normal vs. Abnormal – The Role of Baseline Files and Where Do I go to Find Samples?
    b. Diagraming Conversations – A Picture is worth 1024 Words

III. Analysis of Network Applications and User Traffic

1. New Protocols and New Functions
    a. Configuration Protocols – Structure and Analysis of DHCPv4 / DHCPv6

    b. The Network Layer - IPv4 / IPv6 / IPv10
        i. Structure and Analysis of IPv4 vs. IPv6 vs. IPv10
        ii. IP Options – What's the Big Deal?
        iii. Common IP Exploits and Examples of Intrusion Signatures

    c. Utility and Troubleshooting Protocols - Internet Control Message Protocol (ICMPv4 / ICMPv6)
        i. Structure and Analysis of ICMPv4 vs. ICMPv6
        ii. Network Analysis Using the ICMP Analysis – Types and Codes
        iii. Common ICMP Exploits and Examples of Intrusion Signatures

    d. The Transport Layer - Moving the Data – TCP / UDP / SCTP
        i. Recap - Structure and Advanced Analysis of TCP / UDP
        ii. Structure and Analysis of STCP
        iii. Common Transport Layer Exploits and Examples of Intrusion Signatures

        iv. The Application Layer – Web-Based Applications Using HTTP / HTTP 2 / HTTP 3
            1. Structure and Analysis of HTTP, HTTP2, and HTTP 3
            2. Response Codes – The answer to analyzing HTTP,
            3. Reassembling and Exporting of Objects
            4. Google Transport Protocols SPDY / QUIC

IV. Where do we go from here?

a. Wireshark 0 – TCP/IP Networking Fundamentals Using Wireshark
b. Wireshark 1 - TCP/ IP Network Analysis
c. Wireshark 2 – Advanced Network and Security Analysis
d. Wireshark 3 – Network Forensics Analysis
e. Wireshark 4 – Mobile Device Forensics Analysis
f. Wireshark 5 - Cloud and Internet of Things (IoT) Advanced Network Analysis
g. Wireshark 6 - VoIP & Multimedia Advanced Network Analysis
h. Wireshark 7 - WiFi Advanced Network Analysis
i. Wireshark 8 – SCADA and ICS Advanced Network Analysis
k. Wireshark 9 – Wireshark Command Line Tools