Next Generation Protocols & Advanced Network Analysis (v2.6.6)

Format: 2 days Classroom Instruction
Audience: Intermediate

Target Audience:
This course is designed for Networking, Government and Security personnel that need to develop a set of packet investigation techniques through study of the Next Generation Networking Protocols using Wireshark and other Open-Source Analysis tools. Successful completion of this course will provide these individuals with a path-way into the field of both Network and Forensics Analysis.

Recommended Prerequisites:
Network analysis experience using Wireshark.

Description:
Advanced Network encompasses the skills of not only capturing data, but also the ability to discern unusual patterns hidden within seemingly normal network traffic. This course will provide attendees with a set of investigate and analysis techniques focusing on Wireshark and the use of other vendor-neutral, Open-Source Tools to provide insight into the following areas:

- Specialized and advanced packet capture techniques

- Recognition, analysis and threat recognition for many of the next generation user protocol issues including IPv4/v6/v10, DHCPv4/v6, SCTP, DNS/DNSSec/MDNS, ICMP (v4 /v6), Email Protocols (POP / SMTP / IMAP), File Transfer Protocols (FTP/TFTP/FIX/File Sharing), and common Internet based User Protocols (HTTP / HTTP 2.0)

- Specialized analysis techniques including suspicious data traffic reconstruction and viewing

Real-World examples will be utilized throughout the course in conjunction with hands-on exercises to transfer field proven, practical analysis skills. Attendees will receive a student guide that includes numerous reference files, networking and forensics tools, and a library of reference documents.

Course Details:

Day 1 –

I. Introduction to Advanced Network Analysis

1. Network analysis challenges – Nomenclature, Terminology and the Next Generation Protocols

II. Recap - Collecting the Data

a. Configuring Wireshark
   i. New features to enhance capture
   ii. Using capture filters to capture specific suspect traffic
b. Stealth / Silent Collection of Data – Tips & Techniques
c. Location – How Network Infrastructure Devices Affect Network Analysis
   i. Hubs, Switches, Bridges, Routers, Firewalls and CSU / DSU

III. Advanced Network Analysis Methodology

1. **Analyzing Conversations and Activities**
   a. Analyzing conversations and activities using expert systems to determine unusual activity
      i. Determining which conversations are suspect - analyzing latency and throughput to recognize and analyze suspicious user traffic
2. **A Sample Advanced Network Analysis Methodology**
   a. 6 Steps for practical network analysis of suspicious traffic
      i. Answering the key questions –
      ii. A sample network analysis methodology
3. **Diagraming Conversations – A Picture is worth 1024 Words**

IV. Analysis of Network Applications and User Traffic

1. The Networking Protocols
   a. What's normal vs. abnormal – The role of baseline files
   b. Building a Baseline Library - Where to go to find samples
   c. Forensics Analysis of an Intrusion
      i. Scouting out the target – network reconnaissance and scanning tools
      ii. Recognizing scanning signatures – NMAP / Retina / Nessus, etc.

Day 2 –

2. **Before and after IPv6 – New Protocols and New Functions**
    a. **Configuration Protocols –**
        i. Structure and analysis of DHCPv4 / DHCPv6
        ii. Common DHCP exploits, attacks and examples of intrusion signatures

    b. **Resolving Addresses – DNS / DNSSec / MDNS / LMNR**
        i. Structure and analysis of DNS / DNSSec / MDNS / LMNR
        ii. Common DNS exploits, attacks and examples of intrusion signatures

    c. **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

    d. **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

    e. **The Transport Layer - Moving the Data – TCP / UDP / SCTP / QUIC / SPDY**
        i. Structure and advanced analysis of TCP
        ii. TCP options – What's the big deal?
        iii. Advanced TCP analysis using expert systems
        iv. Structure and advanced analysis of UDP
        v. Structure and analysis of the new STCP
        vi. Google transport protocols SPDY / QUIC
        vii. Common transport layer exploits and examples of intrusion signatures

    f. **The Application Layer – Analyzing Common User Protocols**
        i. **Email Applications Using POP / SMTP / IMAP**
            a. Structure and analysis of the email cloud
            b. Assembling and evaluating email traffic

        ii. **Web-Based Applications Using HTTP / HTTP2**
            1. Structure and analysis of HTTP / HTTPS - decrypting SSL
            2. Response codes – The answer to analyzing HTTP and the new HTTP2
            3. Reassembling and exporting of objects