TCP/IP Analysis and Troubleshooting with Wireshark Training

Course Outline

I. **Introduction to Network Analysis**

1. Network analysis challenges – Nomenclature and Terminology for Wireshark 3.0

II. **Collecting the Data**

a. **Configuring Wireshark**

ii. Building and optimizing configuration Profiles for data capture

1. Importing and Exporting Porfiles

iii. Using capture filters to capture specific suspect traffic

iv. Fine-Tuning Wireshark 3.0 – Advanced Wireshark Profile Optimization

v. Remote Capture Using Wireshark 3.0

2. **Location – How Network Infrastructure Devices Effect Ethernet Network Analysis**

i. Hubs, Switches, Bridges, Routers, Firewalls and CSU / DSU

III. **Analyzing the Data – A Sample Network Analysis Methodology**

1. **Effectively Navigating Wireshark 3.0 and Interpreting Color Rules**

.6 Steps for practical Network Analysis of suspicious traffic

i. Answering the key questions – A Sample Network Analysis Methodology

a. Understanding and Using Shortcuts

b. Constructing, Using and Interpreting Color Rues in Wireshark 3.0

2. **My Network is Slow! – Using Wireshark 3.0 to Effectively Trouble Shoot Latency Issues**

.The Importance of Effectively Using Time Values in Troubleshooting

.How Location affects Time Values

a. Default vs. Specialized Time Values

.Cumulative Time Value

i. Delta Time Value

ii.Conversational Time Values

3. **Expert Analysis – Introduction to Statistical Analysis and Graphing**

.Wireshark 3.0 Updated Expert Systems

a.Analyzing Conversations and Activities Using Expert Systems to Determine Unusual Activity

.The 6 Key Statistical Displays to Master

1. What's Normal vs. Abnormal – The Role of Baseline Files
2. Building a Baseline Library – Where Do I go to Find Samples?

i.Statistical Displays vs. Graphing

1. Types of Graphs

a. I/O vs. Flow vs. TCP

4. **Show me the Money! – Display Filters and Regular Expressions**

.Using Wireshark 3.0 Standard Display Filtering

.Creating and Using Filter Buttons

a.Advanced Display Filters

b.Extending the Power of Wireshark 3.0 – Regular Expressions

IV. **Analysis of Network Applications and User Traffic**

1. **The Networking Protocols**

. What's Normal vs. Abnormal – The Role of Baseline Files

a.Building a Baseline Library – Where Do I go to Find Samples?

2. **The Key Networking Protocols and Functions**

. Configuration Protocols – DHCPv4

. Structure and Analysis of DHCPv4

a.Resolving Addresses – DNS / DNSSec

.Structure and Analysis of DNS

i. Fixing the Problem – DNSSec structure and Analysis

b.The Network Layer – IPv4

. Structure and Analysis of IPv4

i. IP Options – What's the Big Deal?

c. Utility and Troubleshooting Protocols – Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMPv4)

.Structure and Analysis of ARP

i. Structure and Analysis of ICMPv4

ii. Network Analysis Using the ICMP Analysis – Types and Codes

d. The Transport Layer – Moving the Data – TCP / UDP

.Structure and Analysis of TCP

i. TCP Options – What's the Big Deal?

ii. TCP Analysis Using Expert Systems

iii. Structure and Advanced Analysis of UDP

e. The Application Layer – Analyzing Common User Protocols

.Web-Based Applications Using HTTP / HTTP 2.0

1. Structure and Analysis of HTTP
2. Response Codes – The answer to analyzing HTTP
3. Reassembling and Exporting of HTTP Objects
4. New and Improved – HTTP 2.0 – a. Structure and Analysis of HTTP 2.0

i. The Forgotten Part of the Internet – Usenet and NNTP

1. Structure and Analysis of NNTP
2. Response Codes – The answer to analyzing NNTP
3. Reassembling and Exporting of NNTP Objects

f. Securing the Data – SSL / TLS

.Secure Socket Layer

1. Structure and Analysis of SSL
2. Response Codes – The answer to analyzing SSL
3. Decrypting and Reassembling of SSL Objects

i.Transport Layer Security

1. Structure and Analysis of TLS

3. **Recap – Effective Troubleshooting Techniques**

V. **Supplemental Resources**

3. Appendix “A” – Useful Stuff
4. Appendix “B” – Book List: Recommended Reading
5. Appendix “C” – Wireshark Command Line Program User Guides
6. Appendix “D” – Wireshark USB Capture Guide

VI. **Where do I go From Here? – Continuing Your Wireshark Education**

. Wireshark 0 – TCP/IP Networking Fundamentals Using Wireshark

a. Wireshark 1 – TCP/IP Troubleshooting & Network Optimization Using Wireshark 3.0

b. Wireshark 2 – Advanced Network and Security Analysis

c. Wireshark 3 – Network Forensics Analysis

d. Wireshark 4 – Mobile Device Forensics Analysis

e. Wireshark 5 – Cloud and Internet of Things (IoT) Advanced Network Analysis

f. Wireshark 6 – VoIP Advanced Network Analysis

g. Wireshark 7 – WiFi Advanced Network Analysis

h. Wireshark 8 – SCADA and ICS Advanced Network Analysis