TEC016: Wireshark Certified Network Analyst

COURSE DESCRIPTION :
This class focuses on the key areas covered in the most current version of the Wireshark Certified Network Analyst.

AUDIENCE PROFILE :
This course is designed for network professionals interested in obtaining the Wireshark Certified Network Analyst designation.

PREREQUISITES :
Students should have a strong working knowledge of interconnecting device functionality (switch, router, NAT, for example) and be comfortable with the elements of the TCP/IP protocol suite (ARP, TCP, UDP, IP, DHCP, ICMP, for example). In addition, students should already be familiar with the Wireshark interface and basic methods used to capture and filter traffic.

COURSE OUTLINE :
Section 1: Network Analysis Overview
- Define the Purpose of Network Analysis
- List Troubleshooting Tasks for the Network Analyst
- List Security Tasks for the Network Analyst
- List Optimization Tasks for the Network Analyst
- List Application Analysis Tasks for the Network Analyst
- Define Legal Issues of Listening to Network Traffic
- Overcome the "Needle in the Haystack " Issue
- Understand General Network Traffic Flows
- Review a Checklist of Analysis Tasks

Section 2: Introduction to Wireshark
- Describe Wireshark's Purpose
- Know How to Obtain the Latest Version of Wireshark
- Compare Wireshark Release and Development Versions
- Report a Wireshark Bug or Submit an Enhancement
- Capture Packets on Wired or Wireless Networks
- Open Various Trace File Types
- Describe How Wireshark Processes Packets
- Define the Elements of the Start Page
- Identify the Nine GUI Elements
- Navigate Wireshark’s Main Menu
- Use the Main Toolbar for Efficiency
- Focus Faster with the Filter Toolbar
- Make the Wireless Toolbar Visible
- Access Options through Right-Click Functionality
- Define the Functions of the Menus and Toolbars

Section 3: Capture Traffic
- Know Where to Tap into the Network
- Know When to Run Wireshark Locally
- Capture Traffic on Switched Networks
- Use a Test Access Port (TAP) on Full-Duplex Networks
- Define When to Set up Port Spanning/Port Mirroring on a Switch
- Analyze Routed Networks ‧ Analyze Wireless Networks
- Define Options for Capturing at Two Locations Simultaneously (Dual Captures)
- Identify the Most Appropriate Capture Interface

- Capture on Multiple Adapters Simultaneously
- Capture Traffic Remotely
- Automatically Save Packets to One or More Files
- Optimize Wireshark to Avoid Dropping Packets
- Conserve Memory with Command-Line Capture

Section 4: Create and Apply Capture Filters

- Describe the Purpose of Capture Filters
- Build and Apply a Capture Filter to an Interface
- Filter by a Protocol
- Create MAC/IP Address or Host Name Capture Filters
- Capture One Application's Traffic Only
- Use Operators to Combine Capture Filters
- Create Capture Filters to Look for Byte Values
- Manually Edit the Capture Filters File
- Share Capture Filters with Others

Section 5: Define Global and Personal Preferences

- Find Your Configuration Folders
- Set Global and Personal Configurations
- Customize Your User Interface Settings
- Define Your Capture Preferences
- Define How Wireshark Automatically Resolves IP and MAC Names
- Plot IP Addresses on a World Map with GeoIP
- Resolve Port Numbers (Transport Name Resolution)
- Resolve SNMP Information
- Configure Filter Expressions
- Configure Statistics Settings
- Define ARP, TCP, HTTP/HTTPS and Other Protocol Settings
- Configure Protocol Settings with Right-Click

Section 6: Colorize Traffic

- Use Colors to Differentiate Traffic
- Disable One or More Coloring Rules
- Share and Manage Coloring Rules
- Identify Why a Packet is a Certain Color
- Create a "Butt Ugly" Coloring Rule for HTTP Errors
- Color Conversations to Distinguish Them
- Temporarily Mark Packets of Interest

Section 7: Define Time Values and Interpret Summaries

- Use Time to Identify Network Problems
- Understand How Wireshark Measures Packet Time
- Choose the Ideal Time Display Format
- Identify Delays with Time Values
- Create Additional Time Columns
- Measure Packet Arrival Times with a Time Reference
- Identify Client, Server and Path Delays
- Calculate End-to-End Path Delays
- Locate Slow Server Responses
- Spot Overloaded Clients
- View a Summary of Traffic Rates, Packet Sizes and Overall Bytes Transferred

Section 8: Interpret Basic Trace File Statistics

- Launch Wireshark Statistics
- Identify Network Protocols and Applications
- Identify the Most Active Conversations
- List Endpoints and Map Them on the Earth
- Spot Suspicious Targets with GeoIP
- List Conversations or Endpoints for Specific Traffic Types
- Evaluate Packet Lengths
- List All IPv4/IPv6 Addresses in the Traffic
- List All Destinations in the Traffic
- List UDP and TCP Usage
- Analyze UDP Multicast Streams
- Graph the Flow of Traffic
- Gather Your HTTP Statistics
- Examine All WLAN Statistics

Section 9: Create and Apply Display Filters

- Understand the Purpose of Display Filters
- Create Display Filters Using Auto-Complete
- Apply Saved Display Filters
- Use Expressions for Filter Assistance
- Make Display Filters Quickly Using Right-Click Filtering
- Filter on Conversations and Endpoints
- Understand Display Filter Syntax
- Combine Display Filters with Comparison Operators
- Alter Display Filter Meaning with Parentheses
- Filter on the Existence of a Field
- Filter on Specific Bytes in a Packet
- Find Key Words in Upper or Lower Case
- Use Display Filter Macros for Complex Filtering
- Avoid Common Display Filter Mistakes
- Manually Edit the dfilters File

Section 10: Follow Streams and Reassemble Data

- Follow and Reassemble UDP Conversations
- Follow and Reassemble TCP Conversations
- Follow and Reassemble SSL Conversations
- Identify Common File Types

Section 11: Customize Wireshark Profiles

- Customize Wireshark with Profiles
- Create a New Profile
- Share Profiles
- Create a Troubleshooting Profile
- Create a Corporate Profile
- Create a WLAN Profile
- Create a VoIP Profile
- Create a Security Profile

Section 12: Annotate, Save, Export and Print Packets

- Annotate a Packet or an Entire Trace File
- Save Filtered, Marked and Ranges of Packets
- Export Packet Contents for Use in Other Programs
- Export SSL Keys
- Save Conversations, Endpoints, I/O Graphs and Flow Graph Information
- Export Packet Bytes

Section 13: Use Wireshark's Expert System
- Launch Expert Info Quickly
- Colorize Expert Info Elements
- Filter on TCP Expert Information Elements
- Define TCP Expert Information

Section 14: TCP/IP Analysis Overview
- Define Basic TCP/IP Functionality
- Follow the Multistep Resolution Process
- Define Port Number Resolution
- Define Network Name Resolution
- Define Route Resolution for a Local Target
- Define Local MAC Address Resolution for a Target
- Define Route Resolution for a Remote Target
- Define Local MAC Address Resolution for a Gateway

Section 15: Analyze Domain Name System (DNS) Traffic
- Define the Purpose of DNS
- Analyze Normal DNS Queries/Responses
- Analyze DNS Problems
- Dissect the DNS Packet Structure
- Filter on the DNS/MDNS Traffic

Section 16: Analyze Address Resolution Protocol (ARP) Traffic
- Define the Purpose of ARP Traffic
- Analyze Normal ARP Requests/Responses
- Analyze Gratuitous ARP
- Analyze ARP Problems
- Dissect the ARP Packet Structure
- Filter on ARP Traffic

Section 17: Analyze Internet Protocol (IPv4/IPv6) Traffic
- Define the Purpose of IP
- Analyze Normal IPv4 Traffic
- Analyze IPv4 Problems
- Dissect the IPv4 Packet Structure
- Filter on IPv4/IPv6 Traffic
- Sanitize IPv4 Addresses in a Trace File
- Set Your IP Protocol Preferences

Section 18: Analyze Internet Control Message Protocol (ICMPv4/ICMPv6) Traffic
- Define the Purpose of ICMP
- Analyze Normal ICMP Traffic
- Analyze ICMP Problems
- Dissect the ICMP Packet Structure
- Filter on ICMP and ICMPv6 Traffic

Section 19: Analyze User Datagram Protocol (UDP) Traffic
- Define the Purpose of UDP
- Analyze Normal UDP Traffic
- Analyze UDP Problems
- Dissect the UDP Packet Structure
- Filter on UDP Traffic

Section 20: Analyze Transmission Control Protocol (TCP) Traffic

- Define the Purpose of TCP
- Analyze Normal TCP Communications
- Define the Establishment of TCP Connections
- Define How TCP-based Services Are Refused
- Define How TCP Connections are Terminated
- Track TCP Packet Sequencing
- Define How TCP Recovers from Packet Loss
- Improve Packet Loss Recovery with Selective Acknowledgments
- Define TCP Flow Control
- Analyze TCP Problems
- Dissect the TCP Packet Structure
- Filter on TCP Traffic
- Set TCP Protocol Parameters

Section 21: Graph IO Rates and TCP Trends

- Use Graphs to View Trends
- Generate Basic I/O Graphs
- Filter I/O Graphs
- Generate Advanced I/O Graphs
- Compare Traffic Trends in I/O Graphs
- Graph Round Trip Time
- Graph Throughput Rates
- Graph TCP Sequence Numbers over Time
- Interpret TCP Window Size Issues
- Interpret Packet Loss, Duplicate ACKs and Retransmissions

Section 22: Analyze Dynamic Host Configuration Protocol (DHCPv4/DHCPv6) Traffic

- Define the Purpose of DHCP
- Analyze Normal DHCP Traffic
- Analyze DHCP Problems
- Dissect the DHCP Packet Structure
- Filter on DHCPv4/DHCPv6 Traffic
- Display BOOTP-DHCP Statistics

Section 23: Analyze Hypertext Transfer Protocol (HTTP) Traffic

- Define the Purpose of HTTP
- Analyze Normal HTTP Communications
- Analyze HTTP Problems
- Dissect HTTP Packet Structures
- Filter on HTTP or HTTPS Traffic
- Export HTTP Objects
- Display HTTP Statistics
- Graph HTTP Traffic Flows
- Set HTTP Preferences
- Analyze HTTPS Communications
- Analyze SSL/TLS Handshake
- Analyze TLS Encrypted Alerts
- Decrypt HTTPS Traffic
- Export SSL Keys

Section 24: Analyze File Transfer Protocol (FTP) Traffic

- Define the Purpose of FTP
- Analyze Normal FTP Communications
- Analyze Passive Mode Connections
- Analyze Active Mode Connections
- Analyze FTP Problems
- Dissect the FTP Packet Structure
- Filter on FTP Traffic
- Reassemble FTP Traffic

Section 25: Analyze Email Traffic

- Analyze Normal POP Communications
- Analyze POP Problems
- Dissect the POP Packet Structure
- Filter on POP Traffic
- Analyze Normal SMTP Communication
- Analyze SMTP Problems
- Dissect the SMTP Packet Structure
- Filter on SMTP Traffic

Section 26: Introduction to 802.11 (WLAN) Analysis

- Analyze Signal Strength and Interference
- Capture WLAN Traffic
- Compare Monitor Mode and Promiscuous Mode
- Set up WLAN Decryption
- Prepend a Radiotap or PPI Header
- Compare Signal Strength and Signal-to-Noise Ratios
- Describe 802.11 Traffic Basics
- Analyzed Normal 802.11 Communications
- Dissect Basic 802.11 Frame Elements
- Filter on WLAN Traffic
- Analyze Frame Control Types and Subtypes
- Customize Wireshark for WLAN Analysis

Section 27: Voice over IP (VoIP) Analysis Fundamentals

- Define VoIP Traffic Flows
- Analyze Session Bandwidth and RTP Port Definition
- Analyze VoIP Problems
- Examine SIP Traffic
- Examine RTP Traffic
- Play Back VoIP Conversations
- Decipher RTP Player Marker Definitions
- Create a VoIP Profile
- Filter on VoIP Traffic

Section 28: Baseline "Normal" Traffic Patterns

- Define the Importance of Baselining
- Baseline Broadcast and Multicast Types and Rates
- Baseline Protocols and Applications
- Baseline Boot up Sequences
- Baseline Login/Logout Sequences
- Baseline Traffic during Idle Time
- Baseline Application Launch Sequences and Key Tasks
- Baseline Web Browsing Sessions
- Baseline Name Resolution Sessions

- Baseline Throughput Tests
- Baseline Wireless Connectivity
- Baseline VoIP Communications

Section 29: Find the Top Causes of Performance Problems

- Troubleshoot Performance Problems
- Identify High Latency Times
- Point to Slow Processing Times
- Find the Location of Packet Loss
- Watch Signs of Misconfigurations
- Analyze Traffic Redirections
- Watch for Small Payload Sizes
- Look for Congestion
- Identify Application Faults
- Note Any Name Resolution Faults

Section 30: Network Forensics Overview

- Compare Host to Network Forensics
- Gather Evidence
- Avoid Detection
- Handle Evidence Properly
- Recognize Unusual Traffic Patterns
- Color Unusual Traffic Patterns

Section 31: Detect Scanning and Discovery Processes

- Define the Purpose of Discovery and Reconnaissance
- Detect ARP Scans (aka ARP Sweeps)
- Detect ICMP Ping Sweeps
- Detect Various Types of TCP Port Scans
- Detect UDP Port Scans
- Detect IP Protocol Scans
- Define Idle Scans
- Know Your ICMP Types and Codes
- Analyze Traceroute Path Discovery
- Detect Dynamic Router Discovery
- Define Application Mapping Processes
- Use Wireshark for Passive OS Fingerprinting
- Detect Active OS Fingerprinting
- Identify Spoofed Addresses and Scans

Section 32: Analyze Suspect Traffic

- Identify Vulnerabilities in the TCP/IP Resolution Processes
- Find Maliciously Malformed Packets
- Identify Invalid or Dark Destination Addresses
- Differentiate between Flooding or Standard Denial of Service Traffic
- Find Clear Text Passwords and Data
- Identify Phone Home Behavior
- Catch Unusual Protocols and Applications
- Locate Route Redirection Using ICMP
- Catch ARP Poisoning
- Catch IP Fragmentation and Overwriting
- Spot TCP Splicing
- Watch Other Unusual TCP Traffic
- Identify Password Cracking Attempts
- Build Filters and Coloring Rules from IDS Rules

Section 33: Effective Use of Command-Line Tools

- Define the Purpose of Command-Line Tools
- Use Wireshark.exe (Command-Line Launch)
- Capture Traffic with Tshark
- List Trace File Details with Capinfos
- Edit Trace Files with Editcap
- Merge Trace Files with Mergecap
- Convert Text with Text2pcap
- Capture Traffic with Dumpcap
- Define Rawshark

วิทยากร :

อาจารย์เอกฤทธิ์ ธรรมสถิต

- Microsoft Certified professional (MCP)
- Microsoft Certified Systems Administrator (MSCA)
- Microsoft Certified Systems Engineer (MSCE)
- Cisco Certified Network Associate (CCNA)
- Certificate of CompTIA Security+
- Certified Ethical Hacker
- Certified Wireless Network Administrator
- Certified Wireless Security Professional

จำนวนชั่วโมงในการฝึกอบรม : 5 วัน (30 ชั่วโมง)

ช่วงเวลาฝึกอบรม : 9.00 - 16.00 น.

สถานที่ฝึกอบรม :

สถาบันวิทยาการ สวทช.
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง :

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.NSTDAacademy.com
E-mail: training@nstda.or.th