

Wireshark Application

Analysis and optimization of typical TCP/IP applications

In addition to good TCP/IP knowledge and experience in using Wireshark, a solid understanding of how the applications used in the network work is a prerequisite for successful analysis. This course covers the functionality of typical TCP/IP applications and their protocols in theory and practice. The focus is on analysis with Wireshark to quickly identify, isolate and rectify errors.

Course Contents

- Wireshark at a glance
- TCP/IP analysis with Wireshark - The most important points
- Analyzing applications with Wireshark
- Application performance and performance parameters
- Evaluate and assess response times
- Analyzing HTTP
- Analyzing secure protocols - SSL/TLS, SSH and more
- Analyze DNS and DNS server processes
- Analysis of FTP and TFTP
- Analysis of Citrix and RDP
- Analysis of multi-tier database applications

E-Book You will receive the comprehensive documentation package from ExperTeach – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

Target Group

This workshop is suitable for network administrators and all technical staff who are responsible for the planning, implementation and error-free operation of networks and who want to familiarize themselves specifically with Wireshark analysis of TCP/IP applications.

Prerequisites

Participants should have solid knowledge and practical experience in using Wireshark as well as knowledge of TCP/IP and IP addressing. Prior attendance of the course Wireshark Protocol Analysis - Practical Use in the Network is highly recommended.

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.expertech-training.com/go/WISA

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	3 Days	€ 2,195
Online Training	3 Days	€ 2,195
Date/course venue	Course language German 	
11/09-13/09/24 	11/09-13/09/24	

Status 03/08/2024



Table of Contents

Wireshark Application – Analysis and optimization of typical TCP/IP applications

1	Anwendungen mit Wireshark analysieren	3.2.3	HTTP Responses	6.2.1	Das ICA-Protokoll
1.1	Wireshark im Kurzüberblick	3.3	Analyse von HTTP/1.1 mit Wireshark	6.2.2	Session Reliability
1.1.1	Installation und Betrieb des Npcap-Treibers	3.3.1	HTTP-Fehler in Wireshark	6.3	Remote Desktop Protocol
1.1.2	Messen in Ethernet Netzwerken	3.3.2	HTTP-Antwortzeiten	6.3.1	Verbindungsaufbau von RDP verschlüsselt
1.1.3	Aufzeichnen mit Wireshark	3.3.3	Browsertypen	6.3.2	RDP über UDP
1.1.4	Mitschnittfilter – Capture Filter	3.3.4	HTTP Connection Persistence		
1.1.5	Einstellungen - Preferences	3.3.5	Caching im Client	A	Lab-Übungen und Lösungen
1.1.6	Voreinstellungen und Profile	3.3.6	HTTP Cookies	A.1	Lab Übungen – Kapitel 1
1.1.7	Display Filter – Anzeigefilter	3.4	HTTP/1.1 über Proxys	A.1.1	Optionale Lab Übung: Anzeigefilter
1.1.8	Vergleichsoperatoren	3.4.1	Explizite Proxys	A.2	Lab Übungen – Kapitel 2
1.1.9	Logische Operatoren	3.4.2	Transparente Proxys	A.2.1	Lab Übung: TLS in Wireshark analysieren
1.1.10	Speichern von Anzeigefiltern	3.4.3	Reverse Proxys	A.2.2	Lab Übung: TLS Decrypt
1.2	Anwendungstypen und Performancefaktoren	3.4.4	Aufgaben von Web Proxys	A.2.3	Lab Übung: SSH
1.2.1	Durchsatzorientierte Anwendungen	3.4.5	Authentisierung mit Proxys	A.3	Lab Übungen – Kapitel 3
1.2.2	Transaktionsorientierte Anwendungen	3.5	HTTP Version 2	A.3.1	Lab Übung: HTTP/2-Grundfunktionen und Decrypt
1.2.3	Echtzeitanwendungen – Voice und Streaming	3.5.1	HTTP/2-Versionen	A.3.2	Lab Übung: HTTP/2 und QUIC im Überblick
1.3	Netzwerkprobleme und Anwendungsprobleme	3.5.2	HTTP over TCP (H2C)	A.3.3	Lab Übung: Untersuchung von QUIC
1.3.1	Typische Netzwerkprobleme	3.5.3	HTTP over TLS (H2)	A.4	Lab Übungen – Kapitel 4
1.3.2	Typische Anwendungsprobleme	3.5.4	HTTP/2-Datenaustausch	A.4.1	Lab Übung: DNS-Probleme 1
1.4	Vorgehen bei der Analyse (Analysetechniken)	3.5.5	HTTP/2 - Verbindungsabbau	A.4.2	Lab Übung: DNS-Probleme-2
1.4.1	Netzwerkprobleme erkennen und ausschließen	3.5.6	Flusssteuerung mit HTTP/2-WINDOW	A.4.3	Lab Übung: DNS-Probleme-3
1.4.2	Potentielle Probleme an Servern	3.5.7	HTTP/2 PRIORITY	A.5	Lab Übungen – Kapitel 5
1.4.3	Der Einfluss von SAN oder NAS	3.6	Google QUIC, IETF-QUIC und HTTP/3	A.5.1	Lab Übung: Datenbankabfrage für Bibliothekensoftware
1.4.4	Client-Server-Architektur überprüfen	3.6.1	Verbindungsaufbau von Google-QUIC	A.5.2	Lab Übung: Langsame Datenbankabfrage für Vertriebssoftware
1.4.5	Probleme in Anwendungen finden	3.6.2	IETF-QUIC	A.5.3	Lab Übung: Datenbankabfragen im Produktionsumfeld
2	Analyse von Secure Protocols – TLS und SSH	3.6.3	HTTP/3 in Wireshark	A.6	Lab Übungen – Kapitel 6
2.1	Security Grundlagen	4	Analyse von DNS	A.7	Lab Übungen – Anhang B
2.1.1	Symmetrische Verschlüsselung	4.1	DNS – Das Adressbuch	A.7.1	Lab Übung: FTP-Basisfunktionen
2.1.2	Asymmetrische Verschlüsselung	4.1.1	Funktionsweise und Abfragen	A.7.2	Lab Übung: FTP-Probleme 1
2.1.3	Hybride Verfahren	4.2	DNS-Analyse mit Wireshark	A.7.3	Lab Übung: FTP-Probleme 2
2.1.4	Authentisierung	4.2.1	Wichtige DNS-Typen	A.7.4	Lab Übung: TFTP-Basisfunktionen
2.1.5	Sichere Applikationen	4.2.2	DNS Kompression	A.7.5	Lab Übung: FTP vs. TFTP - Wer ist schneller?
2.2	Sicherheit mit TLS	4.2.3	DNS Fehler im Wireshark	A.7.6	Lab Übung: Sichere File Transfers
2.2.1	SSL und TLS	4.2.4	DNS-Antwortzeiten in Wireshark	A.8	Lösungen der Lab Übungen
2.2.2	Der TLS Protokollstapel	4.2.5	Typische DNS Probleme und Hintergründe	A.8.1	Lösungen der Lab Übungen – Kapitel 1
2.2.3	Aufgaben von TLS	4.3	Primary and Secondary Name Server	A.8.2	Lösungen der Lab Übungen – Kapitel 2
2.2.4	Aufbau einer TLS-Verbindung für HTTPS	4.3.1	DNS-Zonentransfer	A.8.3	Lösungen der Lab Übungen – Kapitel 3
2.2.5	TLS-Fehlersuche	4.4	Dynamisches DNS	A.8.4	Lösungen der Lab Übungen – Kapitel 4
2.2.6	TLS-Decrypt über RSA-Keys – Beispiel HTTPS	4.5	DNS over TLS (DoT) und DNS over HTTPS (DoH)	A.8.5	Lösungen der Lab Übungen – Kapitel 5
2.2.7	TLS-Decrypt über Logfiles			A.8.6	Lösungen der Lab Übungen – Anhang B
2.3	Analyse von SSH	5	Analyse von Datenbankanwendungen	B	Analyse von File Transfers
2.3.1	SSH Transport Protocol	5.1	Prinzipien und Komponenten	B.1	Analyse von FTP
2.3.2	SSH Authentication Protocol	5.2	Einfache Systeme	B.1.1	Active FTP
2.3.3	SSH Connection Protocol	5.3	Multi Tier - Umgebungen	B.1.2	Passive FTP
3	Analyse von HTTP, HTTP/2, QUIC und HTTP/3	5.3.1	Kommunikationsmuster für Multi-Tier-Umgebungen	B.1.3	FTP-Fehler und Antwortcodes
3.1	HTTP und World Wide Web	5.3.2	Auswertung der Prozessdaten	B.2	Analyse von TFTP
3.1.1	HTTP-Versionen	5.4	Auswerten der Antwortzeiten mit Wireshark	B.2.1	TFTP Basisfunktionen
3.1.2	Kommunikationsverhalten von HTTP/1.0	5.4.1	Antwortzeiten Back-End	B.2.2	TFTP-Probleme und Fehlermeldungen
3.1.3	Kommunikationsverhalten von HTTP/1.1	5.4.2	Auswertetechnik Wireshark	B.2.3	TFTP Optionen
3.1.4	Kommunikationsverhalten von HTTP/2	6	Analyse von Citrix und RDP	B.3	FTP und TFTP im Vergleich
3.2	HTTP Version 1.1	6.1	Terminal Services	B.4	Sichere File Transfers
3.2.1	Requests und Responses	6.1.1	Analyse von TS-Sitzungen	B.4.1	Secure Copy – Verschlüsselte Übertragung
3.2.2	HTTP Request Header	6.2	Analyse von Citrix		

