Wireshark Protokollanalyse

Praktischer Einsatz im Netzwerk

Die aus dem Ethereal-Projekt hervorgegangene Analysesoftware Wireshark ist ein mächtiges Werkzeug für Netzwerk- und Systemadministratoren. Dieser Kurs bildet eine solide Basis mit einer systematischen Einführung in die grundlegenden Funktionen und die Bedienung von Wireshark sowie Methoden und Techniken zu Monitoring, Analyse und Fehlersuche von Netzwerken auf Paketebene und die Abgrenzung von Netzwerk- und Applikationsproblemen. Darauf aufbauend erlernen die Teilnehmer die Analyse und Fehlersuche typischer Netzwerktechnologien wie Switched Ethernet und TCP/IP mit dem Wireshark im Detail. Besonders das Transportprotokoll TCP wird dabei genau unter die Lupe genommen. Der Kurs hat einen hohen Praxisanteil und versetzt die Teilnehmer in die Lage, selbstständig komplexe Analysen mit Wireshark durchzuführen. Kursinhalte und Übungen basieren auf der jeweils aktuellen Wireshark Version.

Kursinhalt

- Arbeitsweise des Wireshark Analyzer
- Live Capture und Live Capture Einstellungen
- Anzeigeoptionen und Auswertungsmöglichkeiten
- Display-Filter und Capture Filter
- Erweiterte Funktionen: Voreinstellungen, Benutzerprofile und Namensauflösung
- Methoden und Techniken der Paketanalyse
- Wireshark Statistiken und Baselining
- Fehlersuche: Eingrenzung von Netzwerk- und Anwendungsproblemen
- Analyse von Switched Ethernet: Duplex und Speed, Spanning Tree und VLAN-Analyse
- TCP/IP-Analyse der Netzwerkschicht für IPv4 und IPv6
- TCP/IP-Analyse der Transportschicht

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Dieser Workshop eignet sich für Netzwerker, die lernen möchten, mit Hilfe des Wireshark komplexe Analysen und Fehlersuche von Netzwerk und Anwendungen durchzuführen.

Voraussetzungen

Die Teilnehmer sollten sattelfest im Ethernet- und TCP/IP-Umfeld sein. Der vorherige Besuch eines der beiden Kurse TCP/IP oder Ethernet, Routing & Switching - Technologiegrundlagen für Unternehmensnetzwerke ist sehr zu empfehlen.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**WISH**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Deutschland	**5 Tage**	**CHF 3.295,-**
Termine in Österreich	**5 Tage**	**CHF 3.295,-**
Termine in der Schweiz	**5 Tage**	**CHF 3.990,-**
Online Training	**5 Tage**	**CHF 3.295,-**

Termin/Kursort — Kurssprache Deutsch

13.05.-17.05.24	HY München	16.09.-20.09.24	HY Online
13.05.-17.05.24	HY Online	16.09.-20.09.24	Zürich
03.06.-07.06.24	Berlin	07.10.-11.10.24	Berlin
03.06.-07.06.24	HY Hamburg	07.10.-11.10.24	HY Hamburg
03.06.-07.06.24	HY Online	07.10.-11.10.24	HY Online
24.06.-28.06.24	HY Online	04.11.-08.11.24	HY Online
24.06.-28.06.24	HY Wien	04.11.-08.11.24	HY Wien
22.07.-26.07.24	HY Frankfurt	25.11.-29.11.24	HY Frankfurt
22.07.-26.07.24	HY Online	25.11.-29.11.24	HY Online
19.08.-23.08.24	HY Düsseldorf	16.12.-20.12.24	HY Düsseldorf
19.08.-23.08.24	HY Online	16.12.-20.12.24	HY Online
16.09.-20.09.24	HY München		

Stand 23.04.2024

Wireshark Protokollanalyse

Inhaltsverzeichnis

Wireshark Protokollanalyse – Praktischer Einsatz im Netzwerk

1 Einführung in die Analyse mit Wireshark
1.1 Was ist Wireshark?
1.1.1 Was sieht Wireshark?
1.1.2 Wireshark Architektur
1.1.3 Installation und Betrieb des Npcap-Treibers
1.2 Messen in Ethernet Netzwerken
1.2.1 Ethernet-Daten auswerten
1.3 Messen in Wireless LAN Netzwerken
1.3.1 Capture ohne Monitor Mode
1.3.2 Capture in Monitor Mode – Linux
1.4 Erste Schritte mit Wireshark
1.4.1 Aufzeichnungsoptionen – Capture Options
1.4.2 Display Filter während der Aufzeichnung
1.4.3 Speichern einer Aufzeichnung
1.4.4 Einstellung der Sprache

2 Mit Wireshark arbeiten
2.1 Anzeigeoptionen und Navigation
2.1.1 Einstellungen – Preferences
2.1.2 Ändern der Ansicht – Layout
2.1.3 Einstellen von Schriftart und Farben
2.1.4 Anpassen der Spalten – Columns
2.1.5 Zeitoptionen
2.1.6 Speichern der Einstellungen
2.1.7 Gehe zu Paket – Goto Packet
2.1.8 Paket finden – Find Packet
2.2 Voreinstellungen und Profile
2.2.1 Benutzerprofile – Configuration Profiles
2.3 Anzeigefilter – Display Filter
2.3.1 Eingabe und Syntax
2.3.2 Das Filterergebnis
2.3.3 Grundlegende Anzeigefilter
2.3.4 Vergleichsoperatoren
2.3.5 Layer Operator – mehrfache Felder
2.3.6 Logische Operatoren
2.3.7 Speichern von Anzeigefiltern
2.3.8 „This"-Filter
2.3.9 Kontext-Filter – Als Filter anwenden
2.3.10 Kontext-Filter – Verbindungsfilter
2.3.11 Filter aus Statistiken – Endpunkte
2.3.12 Filter aus Statistiken – Verbindungen
2.3.13 Follow TCP Stream
2.3.14 Anzeigefilter – Tipps aus der Praxis
2.4 Mitschnittoptionen und Mitschnittfilter
2.4.1 Voreinstellungen für den Mitschnitt
2.4.2 Optionen der Aufzeichnung – Eingabe
2.4.3 Optionen der Aufzeichnung – Ausgabe
2.4.4 Optionen der Aufzeichnung – Optionen
2.4.5 Mitschnittfilter – Capture Filter
2.4.6 Aufzeichnen von Dateisätzen – File Sets
2.4.7 Mehrere Interfaces
2.5 Ein- und Ausgabe

3 Erweiterte Funktionen des Wireshark Analyzers
3.1 Namensauflösung – Name Resolution
3.1.1 Namensauflösung – Physikalische Adressen
3.1.2 Namensauflösung – Transportadressen
3.1.3 Namensauflösung – Netzwerkadressen
3.2 Was ist Protocol Reassembly?
3.2.1 Packet Reassembly am Beispiel von TCP
3.2.2 Packet Reassembly im Detail
3.3 Farben im Decode
3.3.1 Einfärbungsregeln – Coloring Rules
3.3.2 Verbindung einfärben – Colorize Conversation
3.3.3 Mit Filter einfärben – Colorize with Filter
3.4 Kommandozeile – Command Line Tools
3.4.1 Command Line – capinfos
3.4.2 Command Line – tshark
3.4.3 Command Line – mergecap
3.4.4 Command Line – editcap

4 Wireshark Statistiken
4.1 Statistiken – Eigenschaften
4.2 Protokollhierarchie
4.3 Statistiken – Endpunkte
4.4 Statistiken – Verbindungen
4.5 Statistiken – IO-Graph
4.6 Grenzen der Wireshark-Statistiken

5 Performanceanalyse und Fehlersuche
5.1 Paketanalyse erklärt
5.1.1 Netzwerkdokumentation
5.1.2 Baselining
5.2 Fehler systematisch eingrenzen
5.2.1 Troubleshooting-Methoden
5.2.2 Bottom Up – Fehlersuche mit dem OSI-Modell
5.3 Fehlersuche im Netz ohne Wireshark
5.3.1 Duplex Mismatch im Ethernet
5.3.2 Überlastung im Router oder am WAN
5.3.3 Paketfilter und Firewalls
5.4 Messtechnik mit Wireshark
5.4.1 Messpunkte wählen
5.4.2 Port Monitoring – SPAN
5.4.3 Test Access Point – TAP
5.4.4 Wireshark auf dem Endgerät
5.4.5 Doppelte Pakete bei VLAN-Spiegelung
5.4.6 Auswerten von VLAN und VLAN Tags
5.5 Netzwerkperformance mit Wireshark
5.5.1 Round Trip Time – Initial RTT
5.5.2 Round Trip Time – während einer Verbindung
5.5.3 Service Response Time – SRT
5.5.4 Durchsatz und Overhead
5.6 Auswerten von Laufzeitproblemen
5.6.1 Hohe Round-Trip-Zeiten
5.6.2 Hohe Service-Response-Zeiten
5.7 Netzwerkprobleme und Anwendungsprobleme
5.8 Applikationstypen und Performancefaktoren
5.8.1 Durchsatzorientierte Anwendungen
5.8.2 Transaktionsorientierte Anwendungen
5.8.3 Echtzeitanwendungen – Voice und Streaming

6 TCP/IP-Analyse der Transportschicht
6.1 Transport über UDP und TCP
6.1.1 Adressierung einer Applikation
6.1.2 UDP – Einfach und ungesichert
6.1.3 TCP – Verbindungsorientiert und gesichert
6.2 TCP-Funktionen in Wireshark
6.2.1 TCP-Verbindungsaufbau
6.2.2 Sequenzierung von Daten
6.2.3 Verbindungsabbau
6.2.4 TCP-Reset
6.2.5 Sequenzierung in Wireshark
6.3 TCP-Window und Performance
6.3.1 Sliding Window Mechanismus
6.3.2 Window Size im Wireshark
6.3.3 Window Mechanismus und Performance
6.3.4 TCP Window Scaling Option
6.3.5 Bytes in flight und Window Size
6.4 Paketverluste, Retransmissions und Timing
6.4.1 Wiederholung bei Paketverlust
6.4.2 Retransmissions in Wireshark
6.4.3 Eingrenzen von Retransmissions
6.4.4 Selective Acknowledgements (SACK)
6.4.5 Retransmission – Timing
6.5 TCP-Probleme mit Wireshark auswerten
6.5.1 RTT und RTO in Wireshark
6.5.2 Experteninformationen für TCP
6.6 Weitere TCP-Funktionen
6.6.1 Delayed Acknowledgements
6.6.2 TCP-Push
6.7 Tipps zur Fehlersuche

7 TCP/IP-Analyse der Netzwerkschicht
7.1 Das Internet Protokoll im Überblick
7.1.1 Das Netzwerkprotokoll und seine Adressierung
7.1.2 Adressierung und ARP
7.1.3 Doppelte IP-Adressen
7.2 Dynamic Host Configuration Protocol
7.2.1 DHCP Standardfunktionen: DORA
7.2.2 Weitere DHCP-Funktionen
7.2.3 DHCP-Relay
7.2.4 DHCP-Statistiken
7.3 MTU, PMTU, Fragmentierung
7.3.1 MTU
7.3.2 IP-Fragmentierung
7.3.3 PMTU und PMTU-Discovery
7.3.4 Anpassung der MSS
7.4 Internet Control Message Protocol
7.4.1 ICMP Echo und ICMP Echo Reply
7.4.2 ICMP – Destination Unreachable
7.4.3 ICMP Time Exceeded
7.5 Analyse von DNS
7.5.1 Funktionsweise und Abfragen
7.5.2 DNS in Wireshark
7.5.3 Wichtige DNS-Typen
7.5.4 DNS Fehler im Wireshark
7.5.5 DNS-Antwortzeiten in Wireshark
7.5.6 Typische DNS Probleme und Hintergründe

A Lab-Übungen und Lösungen
A.1 Lab Übungen – Kapitel 1
A.1.1 Lab Übung – Internetdaten aufzeichnen
A.2 Lab Übungen – Kapitel 2
A.2.1 Lab Übung – Spalten anlegen
A.2.2 Lab Übung – Profile (Configuration Profiles)
A.2.3 Opt. Lab Übung – Paket finden (Find Packet)
A.2.4 Lab Übung – Anzeigefilter (Display Filter)
A.3 Lab Übungen – Kapitel 3
A.3.1 Lab Übung – Erweiterte Profileinstellungen
A.3.2 Lab Übung – Kommandozeilentools - Teil 1
A.3.3 Lab Übung – Kommandozeilentools - Teil 2
A.3.4 Lab Übung – Kommandozeilentools - Teil 3
A.3.5 Lab Übung – Kommandozeilentools - Teil 4
A.4 Lab Übungen – Kapitel 4
A.4.1 Lab Übung – Durchsatz und zeitlicher Verlauf
A.5 Lab Übungen – Kapitel 5
A.5.1 Lab Übung – Durchsatz
A.5.2 Lab Übung – Overhead
A.5.3 Lab Übung – Effizienz und Fehlanpassung
A.5.4 Opt. Lab Übung – VLAN Messung – Inline
A.5.5 Opt. Lab Übung – VLAN-Messung - Span Port 1
A.5.6 Opt. Lab Übung – VLAN-Messung - Span Port 2
A.6 Lab Übungen – Kapitel 6
A.6.1 Lab Übung – TCP-Verbindungsaufbau
A.6.2 Lab Übung – TCP-Verbindungsabbau
A.6.3 Lab Übung – TCP Zero Window
A.6.4 Lab Übung – TCP Retransmissions – 1
A.6.5 Lab Übung – TCP Retransmissions – 2
A.6.6 Optionale Lab Übung – Des Kunden Pein
A.7 Lab Übungen – Kapitel 7
A.7.1 Lab Übung – DHCP mit Windows 7
A.7.2 Lab Übung – DHCP decline
A.7.3 Lab Übung – Fragmentierung
A.7.4 Lab Übung – PMTU Discovery
A.7.5 Lab Übung – Black Hole
A.7.6 Lab Übung – ICMP
A.7.7 Lab Übung – DNS Probleme
A.8 Lösungen der Lab Übungen
A.8.1 Lösungen der Lab Übungen – Kapitel 1
A.8.2 Lösungen der Lab Übungen – Kapitel 2
A.8.3 Lösungen der Lab Übungen – Kapitel 3
A.8.4 Lösungen der Lab Übungen – Kapitel 4
A.8.5 Lösungen der Lab Übungen – Kapitel 5
A.8.6 Lösungen der Lab Übungen – Kapitel 6
A.8.7 Lösungen der Lab Übungen – Kapitel 7

B Referenzen
B.1 Links zu Tools und Zusatzinfos
B.2 Weitergehende Anzeigefilter
B.2.1 Filtern auf Bitebene
B.2.2 Reguläre Ausdrücke – Regex
B.2.3 Beispiele für Display Filter
B.3 Windows Registry Einstellungen für TCP/IP

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch