Wireshark I

Grundkurs mit Übungen zu dem wichtigsten Werkzeug der Netzanalyse

Kursbeschreibung

Welche Protokolle kursieren im Netz, welche sind für mich relevant und wie kann ich diese gezielt aus der Datenflut herausfiltern?

Die freie Software Wireshark ist das bekannteste und beliebteste Werkzeug zur Netzwerk-Protokollanalyse. Wireshark ist ein sehr mächtiges Tool mit einem Funktionsumfang, der beeindruckt. Alle gängigen Protokolle sind implementiert, neue kommen laufend dazu. Doch bei diesem gewaltigen Funktionsumfang ist es wichtig, diejenigen Funktionen und Menüpunkte zu kennen, die zum gewünschten Ziel führen. Dazu gehört auch das gekonnte Filtern nach speziellen Inhalten und Protokollen. Die Teilnehmer lernen in diesem Grundkurs, mit Wireshark umzugehen, die wichtigen Analysemöglichkeiten und Statistiken zu nutzen und gezielt Daten zu filtern.

Die Wissensvermittlung erfolgt anhand von Erklärungen, Demonstrationen und praktischen Übungen. Die Teilnehmer nutzen für die Übungen ihr vorinstalliertes Wireshark auf ihren Rechnern und analysieren Netzwerkdaten (Traces, Packet Captures), die für den Schulungszweck der Einführung erstellt wurden.

Trainer

Dipl.-Ing. Bernhard Hauser

Dauer

1 Tag

Format

Live Online-Schulung

Max. Teilnehmer

12 Personen

Kontakt

Frau Julia Noglik
noglik@vaf.de / 02103 700-253

Zielgruppe

- Techniker in den Bereichen Systemintegration, Service (Fehlersuche/-klärung), Inbetriebnahme von IT-Systemen, Netzwerkadministration

Lernziele

- Übersicht über den Funktionsumfang von Wireshark und Kenntnis der wichtigsten Funktionen
- eigenständige Anwendung von Wireshark
- Verständnis für den Einsatz von Filtern, das Verfolgen von Datenflüssen und das Extrahieren von Daten

Know-how-Voraussetzungen

- Grundlagenwissen zu LAN und TCP/IP

Technisches Equipment

- Eigener Rechner + Audio + Video
- Internetzugang mit ausreichend Bandbreite
- Wireshark-Installation auf dem eigenen Rechner (für Übungen)

Agenda / Inhalte

Was ist Wireshark?

- Anwendungsgebiet der Paketanalyse
- Paketanalyse in geswitchten und virtuellen Netzen
- SPAN/Mirror-Port, die Vor- und Nachteile
- Inline-Netzwerkmessung mittels TAPs: Breakout-, Aggregation- und Filter-TAPs
- Darstellung der Paketverschachtelung in Wireshark mit Bezug auf das ISO/OSI-Modell
- Anpassen von Wireshark an die aktuellen Bedürfnisse

Protokolle und Wireshark

- Bedeutung der Header für die Analyse mit Wireshark
- Aufbau wichtiger Header:
    - Media Access Control (MAC)
    - Address Resolution Protocol (ARP)
    - Internet Protocol (IP)
    - Transmission Control Protocol (TCP)
    - User Datagram Protocol (UDP)

Pakete mit Wireshark aufzeichnen

- Wichtige Optionen für die Datenaufzeichnung
- Aufzeichnungsfilter einrichten
- Datenaufzeichnung mit mehr als einer Netzwerkkarte
- Langzeitnetzwerkanalyse mit Wireshark, Ringpuffer
- Datenaufzeichnung mit Wireshark in hochperformanten Netzen

Display Filter für die Fehlersuche effektiv nutzen

- Grundlagen der Filterdefinitionen:
- Möglichkeiten, um Filter zu definieren
- Expert Filtereinstellungen
- Text on Wire Filter
- Filter exportieren
- Was ist bei der Filterdefinition zu beachten
- Typische Fehler in der Filtererstellung

Wireshark Statistiken für die Analyse und Fehlersuche einsetzen

- Statistiken zu Verbindungen und Endpunkten
- Das Zeitwertediagramm IO-Stats
- Flowdiagramme und Ermitteln von Antwortzeiten
- Erweiterte Statistiken

Netzwerkprobleme vs. Applikationsprobleme

- Ursachen von schlechter Performance
- Typische Netzwerkprobleme
- Paketverluste verstehen
- Interpretation der Paketverluste im Wireshark
- Hinweise zu Paketverlusten richtig verstehen
- Ermitteln von Laufzeiten
- Durchsatz vs. Laufzeit

Zum Trainer

Dipl.-Ing. Bernhard Hauser

Bernhard Hauser ist Experte für Netzwerktechnik und für Netzanalysen sowie Autor einschlägiger Lehr- und Fachbücher, u. a. „Netzwerkanalyse mit Wireshark" (2. Auflage 2018). Nach Fernmeldelehre und Studium der Elektrotechnik war er als Entwicklungsleiter und als Netzadministrator tätig. Später wechselte er in das Lehramt, unterrichtete an einer Berufsschule und lehrt heute als Dozent an der Fachhochschule Esslingen im Bereich der Netze.