Netzwerkprotokollanalyse mit Wireshark

KURZBESCHREIBUNG

Wireshark ist ein freies Netzwerkanalyse-Tool ("Packet Sniffer") und kann Informationen aus verkapselten Netzwerkprotokollen auslesen und für den Administrator für die Auswertung aufbereiten. Es stellt ein wichtiges Werkzeug dar, um Datenverkehr zu analysieren, zu verstehen und um mögliche Performance- sowie Sicherheitslücken zu entdecken. Daher ist Wireshark bei zahlreichen privaten Firmen und öffentlichen Organisationen täglich im Einsatz. In diesem Kurs wird Ihnen das nötige Hintergrundwissen vermitteln, um mit Wireshark schnell aber effizient Ihre Analyse durchzuführen – so, wie es Ihrem jeweiligen Einsatzzweck entspricht.

IHR NUTZEN

- Entwickeln Sie ein Verständis für die unzähligen Funktionen von Wireshark
- Lernen Sie in wenigen Schritten Informationen aus Ihrem Netzwerk effektiv herauszufiltern

und zu analysieren
- Führen Sie manuell Deep Packet Inspection von Hunderten von Protokollen durch und

verstehen Sie, welche Daten in Ihrem Netzwerk transportiert werden.

ZIELGRUPPE

Mitarbeiter*innen aus den Bereichen Systemservice, IT und Support von TCP/IP-Netzwerken

THEMEN

- Einführung in Netzwerk-Analyse-Tools, technische Informationen zur Wireshark und zur

pcap API (libpcap, Npcap)
- Cross-Plattform-Installationen auf Windows, Linux, macOS, Solaris und FreeBSD
- Einrichten von Display Layout, Coloring Rules, Name Resolution, Profiles und Capture

Options
- Syntax von Capture-Filtern und von Display-Filtern
- Durchführung von Live-Aufzeichnungen und Offline-Analyse
- Packetanalyse in geswitchten Umgebungen (Port Mirroring, SPAN, RSPAN, ERSPAN)
- Packetanalyse mit Network TAPs (Test Access Point)
- Messung von QoS-Parametern (Quality of Service), wie Bandwidth, Delay, Jitter und Packet

Loss
- Analyse von Ethernet (IEEE 802.3, IEEE 802.1Q, IEEE 802.1p)
- Analyse von IPv4 (IHL, Type of Service, Total Length, Identification, Flags, Fragment

Offset, TTL, Protocol, Header Checksum)
- Analyse von IPv6 (Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit)

LEHRMETHODEN

Lehrvortrag und Handhabungstraining am PC-Netzwerk

SEMINARAUSSTATTUNG

Seminarraum mit PC-Netzwerk

VORAUSSETZUNGEN

Die Teilnehmenden sollten mit den Begriffen wie OSI-Referenzmodell, TCP/IP Internet protocol suite, Encapsulation/De-Encapsulation und Protokoll-Headern (Ethernet, IPv4, IPv6, TCP, UDP) bereits vertraut sein.

TERMINE

22.02.2022 (09:00 Uhr) bis
24.02.2022 (16:00 Uhr)
Präsenz | Nürnberg
ARD.ZDF medienakademie (BR-Gelände)
Preis: 2.130,– € p.P.
Seminarleitung: Thomas Frank

18.10.2022 (09:00 Uhr) bis
20.10.2022 (16:00 Uhr)
Präsenz | Nürnberg
ARD.ZDF medienakademie (BR-Gelände)
Preis: 2.130,– € p.P.
Seminarleitung: Thomas Frank

INHALTLICH VERANTWORTLICH

Martin Kaiser
E-Mail: m.kaiser@ard-zdf-medienakademie.de
Telefon: +49 911 9619-484

KUNDENSERVICE

Anette Barth
E-Mail: kundenservice@ard-zdf-medienakademie.de
Telefon: +49 911 9619-251

SEMINARNUMMER

39 826