

Technische Trainings

Workshop-Reihe: IPv4, Wireshark und SIP ganz praktisch

Inhalt

Wireshark-Analysen Teil 1: IPv4 Grundlagen.....	2
Wireshark-Analysen Teil 2: TCP-Protokolle und Einstieg in Wireshark.....	3
Wireshark-Analysen Teil 3: Das SIP-Protokoll verstehen und analysieren	4
Kontakt	5

Wireshark-Analysen Teil 1: IPv4 Grundlagen

Die Workshop Reihe „**Wireshark-Analysen und SIP ganz praktisch**“ besteht aus drei Teilen und zeichnet sich durch ihren sehr hohen Praxisanteil aus. Alle Themen werden anschaulich in praxisnahen Übungen erarbeitet.

Die Teilnahme an einem Workshop Teil ist NICHT Voraussetzung für die folgenden Teile, die Teilnehmer sollten sich aber mit jeweils behandelten Themen gut auskennen.

Der Inhalt dieses Workshops „**IPv4 Grundlagen**“ ist wichtig für die nachfolgenden Workshops. Techniker, die sich mit dem Inhalt dieses Workshops sicher fühlen, können selbstverständlich direkt im nächsten Teil einsteigen. Bei Unsicherheiten mit den hier behandelten Themen wird eine Teilnahme empfohlen, auch wenn es nur zur Auffrischung dient.

Kursdauer: 1 Tag

Kursart: Präsenzworkshop

Kursinhalte:

In diesem Workshop wird ein grundsätzliches Verständnis dafür vermittelt, wie IP-basierte Netzwerke funktionieren. Dieses Verständnis ist die Grundlage für die nachfolgenden Workshops.

In bereitgestellten Netzwerken probieren die Teilnehmer selbst aus, wie IP-Adressen funktionieren, wie man Subnetze bestimmt, und warum ein Gerät nur ein einziges Default-Gateway haben kann. Es werden eigene Netzwerke mit und ohne VLANs eingerichtet. Durch das Erzeugen verschiedener Routen ins Internet erarbeiten sich die Teilnehmer selbst ein grundlegendes Verständnis dafür, wie IP-Adressen und Netzwerke funktionieren.

- IP-Adressen und Netzwerkmasken verstehen und berechnen
- Eigene Netzbereiche einrichten
- Mehrere Netzwerke auf einem Gerät
- Default Routing und statische Routen verstehen und einrichten
- Private Netzwerke vs. öffentliche Netzwerke
- VLAN Tagging einrichten und nutzen
- Gleiche VLANS für unterschiedliche Subnetze
- DNS-Server Funktionsweise und Nutzen
- Netzwerk Scans
- NAT-Router Besonderheiten
- Das Wichtigste zu MAC-Adressen und ARP-Tabellen

Voraussetzungen:

Ein eigener PC mit Microsoft Windows, WLAN und Ethernet Port. Adminrechte zum Installieren von Software und zum Ändern von Netzwerk- und Firewall- Einstellungen.

Wireshark-Analysen Teil 2: TCP-Protokolle und Einstieg in Wireshark

Die Workshop Reihe „**Wireshark-Analysen und SIP ganz praktisch**“ besteht aus drei Teilen und zeichnet sich durch ihren sehr hohen Praxisanteil aus. Alle Themen werden anschaulich in praxisnahen Übungen erarbeitet.

Die Teilnahme an einem Workshop Teil ist NICHT Voraussetzung für die folgenden Teile, die Teilnehmer sollten sich aber mit jeweils behandelten Themen gut auskennen.

Der Inhalt dieses Workshops „**TCP-Protokolle und Einstieg in Wireshark**“ ist wichtig für die nachfolgenden Workshops. Techniker, die sich mit dem Inhalt dieses Workshops sicher fühlen, können selbstverständlich direkt im nächsten Teil einsteigen. Bei Unsicherheiten mit den hier behandelten Themen wird eine Teilnahme empfohlen, auch wenn es nur zur Auffrischung dient.

Kursdauer: 1 Tag

Kursart: Online Workshop

Kursinhalte:

Dieser Workshop bietet einen einfachen Einstieg in die Netzwerk- und Protokoll-Analyse mit Wireshark. Anhand einfacher TCP-Protokolle entsteht schnell ein Verständnis dafür, wie Protokolle funktionieren und in Wireshark dargestellt werden. Dieses Verständnis ist die Grundlage für den nachfolgenden Workshop.

Wireshark wird installiert und die wichtigsten Funktionen, Einstellungen und Besonderheiten erklärt. Es werden einfache TCP-Protokolle selbst ausgetestet, um deren Funktionsweise zu erarbeiten. Diese werden anschließend im Wireshark nachvollzogen. Danach erfolgt ein Reverse Engineering, die Information aus einem Wireshark-Trace werden genutzt um spezifische Daten von Webseiten über die Kommandozeile abzufragen. In diesem Workshop werden Tipps und Tricks zum einfachen Umgang mit Wireshark vermittelt.

- Kennenlernen von TCP-Protokollen und der Funktionsweise von TCP
- Installation von Wireshark und grundsätzliche Funktionen
- Das SMTP-Protokoll: E-Mails über Telnet Befehle senden
- TCP-Sessions und SMTP-Befehle in Wireshark nachvollziehen
- Analyse von HTTP und LDAP-Verbindungen in Wireshark
- Nutzen der Traces zum manuellen senden von HTTP-Befehlen
- Wichtige Wireshark Einstellungen
- Tipps und Tricks zum einfachen Umgang mit Wireshark
- Interessante IP- und TCP-Header Informationen

Voraussetzungen:

Teilnahme am Workshop „**IPv4 Grundlagen**“ oder gleichwertiges Wissen.

Ein eigener PC mit Microsoft Windows und Adminrechten zum Installieren von Software.

Wireshark-Analysen Teil 3: Das SIP-Protokoll verstehen und analysieren

Die Workshop Reihe „**Wireshark-Analysen und SIP ganz praktisch**“ besteht aus drei Teilen und zeichnet sich durch ihren sehr hohen Praxisanteil aus. Alle Themen werden anschaulich in praxisnahen Übungen erarbeitet.

Der Inhalt dieses Workshops „**Das SIP-Protokoll verstehen und analysieren**“ ist der Abschluss dieser Workshop-Reihe aber noch nicht das Ende beim Troubleshooten von SIP-Anschlüssen.

Kursdauer: 1 Tag

Kursart: Präsenzworkshop

Kursinhalte:

Dieser Workshop behandelt die häufigsten Praxisfälle und hilft dabei, die gängigsten Fehler bei einem SIP-Anschluss zu analysieren und zu beheben. Er bildet die Grundlage dafür, eigene Erfahrungen mit Wireshark und dem Tracen von SIP in der Praxis zu sammeln.

Zuerst kümmern wir uns in diesem Workshop darum, wie man an die notwendigen Datenpakete kommt, denn meistens läuft der SIP-Trunk auf einem eigenen SBC. Anschließend werden verschiedenen Verbindungsarten Schritt für Schritt mit Hilfe von Wireshark in Betrieb genommen und so lange angepasst, bis der SIP-Anschluss vollständig funktioniert. Dabei werden ganz automatisch alle relevanten Parameter eines SIP-Trunks erarbeitet.

- Trace-Möglichkeiten von SIP
 - Mirror/SPAN Port, Network TAP, Remote Capture, Recording, tcpdump
 - Herstellerspezifische Trace Optionen
- Einrichten eines eigenen TAP mit Hilfe eines kleinen Switches
- SIP-Register vs. registrierungslose Verbindungen
- Einrichten von SIP-Verbindungen mit einem Beispiel Hersteller
- Ablauf von SIP-Verbindung und Aufbau von SIP-Messages
- VoIP-Features in Wireshark
- Die wichtigsten SIP-Header Informationen
- Rufnummernformatierung im From-, To- und Identity-Header
- Reverse Engineering zum eigenständigen Erarbeiten der SIP-Trunk Einstellungen
- Der SDP-Part im Detail
 - Endpunkt Informationen (IP-Adressen und Ports)
 - Codec Informationen und Verschlüsselung
 - Der Latching Mode von SIP-Providern
- SIP-DTMF
- Fax T.38 vs. G.711

Voraussetzungen:

Teilnahme am Workshop „**TCP-Protokolle verstehen und Einstieg in Wireshark**“ oder gleichwertiges Wissen.

Ein eigener PC mit Microsoft Windows, WLAN und Ethernet Port. Funktionierende Wireshark Installation und Adminrechte.

Kontakt

Sie haben Fragen zu den Inhalten, Interesse an meinem Service oder sonstige Anliegen?

Ich freue mich auf Ihre Nachricht!

Tobias Rust

IT-Coaching & Consulting

www.t-rust.net

tobias.rust@t-rust.net