Technical Trainings

Workshop series: IPv4, Wireshark and SIP very practical

Content

www.t-rust.net

Wireshark Analyzes Part 1: IPv4 Basics

The workshop series “**Wireshark analyzes and SIP very practically**” consists of three parts and is characterized by its very high practical content. All topics are clearly developed in practical exercises.

Participation in a workshop part is NOT a prerequisite for the following parts, but participants should be well versed in the topics covered.

The content of this workshop “**IPv4 Basics**” is important for the subsequent workshops. Technicians who feel confident with the content of this workshop can of course jump straight into the next part. If you are unsure about the topics covered here, participation is recommended, even if it is just a refresher.

Course duration: 1 Day

Training type: face-to-face workshop

Course content:

This workshop provides a basic understanding of how IP-based networks work. This understanding is the basis for the subsequent workshops.

In deployed networks, participants try out for themselves how IP addresses work, how subnets are determined, and why a device can only have a single default gateway. Separate networks are set up with and without VLANs. By creating different routes to the Internet, participants gain a basic understanding of how IP addresses and networks work.

- Understand and calculate IP addresses and network masks
- Set up your own network areas
- Multiple networks on one device
- Understand and set up default routing and static routes
- Private networks vs. public networks
- Set up and use VLAN tagging
- Same VLANS for different subnets
- DNS server functionality and benefits
- Network scans
- NAT router special features
- The most important thing about MAC addresses and ARP tables

Requirements:

Your own PC with Microsoft Windows, Wi-Fi and Ethernet port. Admin rights to install software and change network and firewall settings.

Wireshark Analyzes Part 2: TCP Protocols and Getting Started with Wireshark

The workshop series “**Wireshark analyzes and SIP very practically**” consists of three parts and is characterized by its very high practical content. All topics are clearly developed in practical exercises.

Participation in a workshop part is NOT a prerequisite for the following parts, but participants should be well versed in the topics covered.

The content of this workshop “**TCP protocols and getting started with Wireshark**” is important for the subsequent workshops. Technicians who feel confident with the content of this workshop can of course jump straight into the next part. If you are unsure about the topics covered here, participation is recommended, even if it is just a refresher.

Course duration: 1 Day

Training type: Online workshop

Course content:

This workshop offers an easy introduction to network and protocol analysis with Wireshark. Using simple TCP protocols, you can quickly gain an understanding of how protocols work and are represented in Wireshark. This understanding is the basis for the following workshop.

Wireshark is installed and the most important functions, settings and special features are explained. Simple TCP protocols are tested in order to work out how they work. These are then tracked in Wireshark. Reverse engineering then takes place; the information from a Wireshark trace is used to query specific data from websites via the command line. This workshop teaches tips and tricks for easy use of Wireshark.

- Learn about TCP protocols and how TCP works
- Installation of Wireshark and basic functions
- The SMTP protocol: Send emails via Telnet commands
- Trace TCP sessions and SMTP commands in Wireshark
- Analysis of HTTP and LDAP connections in Wireshark
- Using traces to send HTTP commands manually
- Important Wireshark settings
- Tips and tricks for easy use of Wireshark
- Interesting IP and TCP header information

Requirements:

Participation in the “IPv4 Basics” workshop or equivalent knowledge.

A personal PC with Microsoft Windows and admin rights to install software.

Wireshark Analytics Part 3: Understanding and Analyzing the SIP Protocol

The workshop series "**Wireshark analyzes and SIP very practically**" consists of three parts and is characterized by its very high practical content. All topics are clearly developed in practical exercises.

The content of this workshop "**Understanding and analyzing the SIP protocol**" is the conclusion of this workshop series but is not the end of troubleshooting SIP connections.

Course duration: 1 Day

Training type: face-to-face workshop

Course content:

This workshop covers the most common practical cases and helps to analyze and resolve the most common errors with a SIP connection. It forms the basis for gaining your own experience with Wireshark and tracing SIP in practice.

In this workshop we will first look at how to get the necessary data packets, because the SIP trunk usually runs on its own SBC. Various types of connection are then put into operation step by step using Wireshark and adjusted until the SIP connection is fully functional. All relevant parameters of a SIP trunk are developed automatically.

- SIP trace capabilities
    - Mirror/SPAN Port, Network TAP, Remote Capture, Recording, tcpdump
    - Manufacturer-specific trace options
- Setting up your own TAP using a small switch
- SIP registers vs. registrationless connections
- Setting up SIP connections with an example manufacturer
- Process of SIP connection and establishment of SIP messages
- VoIP features in Wireshark
- The most important SIP header information
- Phone number formatting in the From, To and Identity headers
- Reverse engineering for independently developing the SIP trunk settings
- The SDP part in detail
    - Endpoint information (IP addresses and ports)
    - • Codec information and encryption
    - • The latching mode of SIP providers
- SIP-DTMF
- Fax T.38 vs. G.711

Requirements:

Participation in the workshop "Understanding TCP protocols and getting started with Wireshark" or equivalent knowledge.

Your own PC with Microsoft Windows, Wi-Fi and Ethernet port. Working Wireshark installation and admin rights.

Contact

Do you have any questions about the content, interest in my service or any other concerns?

I look forward to your message!

Tobias Rust
IT-Coaching & Consulting
www.t-rust.net
tobias.rust@t-rust.net