Agenda TCP/IP Netzwerkanalyse mit Wireshark

1. TAG

08:30 - 09.00

- Eintreffen der Teilnehmer im Gebäude 4 (Mensa) **mit eigenem Notebook & entsprechenden Administratorenrechten**
- Begrüssung bei Kaffee und Gipfeli

09:00 - 10:30

- Kurze Einführung und Hintergrund von Wireshark
- Technische Informationen zu Wireshark und WinPcap
- Installation der Wireshark Software und des WinPcap Drivers (Praxis)
- Einrichten von Display Layout, Coloring Rules, Name Resolution, Profile (Praxis)
- Konfiguration der Capture Options (Praxis)

Pause

10:50 - 12:30

- Limiten und Leistungsoptimierung von Wireshark
- Vermeiden von Wireshark Falschmeldungen wie IP/UDP/TCP Checksum Errors (Praxis)
- Erklärung und Analyse VLAN 802.1Q Tagging (Praxis)
- Einrichten eines VLAN Profils (Praxis)

Mittagessen

13:30 - 14:30

- Capture/Display Filtering mit Wireshark (Praxis)
- Unterschiede zwischen Capture und Display Filter
- Einrichten von Quick Filter Buttons (Praxis)
- Datenaufzeichnung im Umfeld von Switches und Routern
- TAPs, Span Ports, Monitoring Switches
- Systematisches Vorgehen zur Fehlereingrenzung

Pause

14:45 - 15:45

- Erklärung und Analyse Unicast, Multicast, Broadcast auf Layer 1 & 2 (Praxis)
- Erklärung und Analyse der Protokolle STP, CDP, LLDP, Cisco LOOP, HSRP (Praxis)

Pause

16:00 - 17:00

- Überblick TCP/IP Protokolle
- Erklärung und Analyse Address Resolution Protocol (ARP) (Praxis)

ins INSTITUTE FOR NETWORKED SOLUTIONS

Agenda TCP/IP Netzwerkanalyse mit Wireshark

2. TAG

09:00 - 10:30	• Erklärung und Analyse DHCP im KMU- und Enterprise-Model (Praxis) • Erklärung und Analyse der wichtigsten IP Felder wie zum Beispiel ID, TTL, Fragmentation, TOS/DiffServ (Praxis)
Pause	
10:50 - 12:30	• Einrichten von IP Kolonnen (Praxis) • Erklärung und Analyse Microsoft Network Load Balancing Protokoll (MS-NLB) (Praxis)
Mittagessen	
13:30 - 14:30	• Überblick der TCP Funktionen • Erklärung und Analyse der TCP Phasen Sessionaufbau, Datentransfer, Sessionabbau (Praxis) • Erklärung und Analyse der TCP Sequenz-, Acknowledge-Nummern und Window-Size (Praxis)
Pause	
14:45 - 15:45	• Erklärung und Analyse der TCP Funktionen Flow Control, Sliding Window, Error Correction (Praxis) • Erklärung und Analyse der TCP Funktionen Slow Start, Duplicate Acknowledges, Fast Retransmission
Pause	
16:00 - 17:00	• Erklärung und Analyse der TCP Funktionen Window-Full, Window-Zero, Congestion Avoiding (Praxis) • Erklärung und Analyse der TCP Flags Push, Urgent • Graphische TCP Session Analyse mit Wireshark TCP-Stream-Graph (Praxis)

ins INSTITUTE FOR NETWORKED SOLUTIONS

Agenda TCP/IP Netzwerkanalyse mit Wireshark

3. TAG

09:00 - 10:30

- Nutzung des Wireshark Expert-Systems für die Fehlereingrenzung (Praxis)
- Erklärung und Analyse der Wireshark Expert Meldungen (Praxis)
- Erklärung und Analyse von TCP Real-Problem Situationen (Praxis)
- Analyse von Application Layer Protokollen HTTP, SMB (Praxis)

Pause

10:50 - 12:30

- TCP Erweiterungen für hohe Geschwindigkeiten
- Erklärung und Analyse der TCP Optionen Selective Ack, Window Scaling, Time Stamp (Praxis)
- TCP Analyse mit zwei Interfaces (Praxis)
- Erklärung und Analyse von MTU Problemen bei Path MTU Black-Hole-Router (Praxis)

Mittagessen

13:30 - 14:30

- Erklärung und Analyse TCP Chimney und Bulk Offloading
- Auto-Tuning TCP-Parameter ab Windows 7, Server 2008/R2
- Erklärung und Analyse UDP basierender Protokolle DNS, SNMP, VoIP (Praxis)
- Erklärung und Analyse des ICMP Protokolls (Praxis)

Pause

14:45 - 15:45

- Capturing in VMware® Environment (Slides in English)
- Capturing packets with Wireshark on a VM (Slides in English)
- Remote capturing packets with WinPcap (Slides in English)
- Capturing packets with pktcap-uw (Slides in English)
- Kurs Feedback

Kursende

16:00

- Ende des dreitägigen Kurses TCP/IP Netzwerkanalyse mit Wireshark

Anmerkung

- Der Kurs umfasst Theorie und zahlreiche Hands-On markiert mit (Praxis). Dazu werden den Teilnehmern von Leutert NetServices dutzende Trace Files zur Verfügung gestellt.
- Folgende Betriebssysteme werden von Wireshark unterstützt: https://www.wireshark.org/docs/wsdg_html_chunked/ChIntroPlatforms.html

ins INSTITUTE FOR NETWORKED SOLUTIONS

MYLEARNING.
WHERE SCIENCE MEETS BUSINESS

HSR Hochschule für Technik • INS Institute for networked solutions
Oberseestrasse 10 • CH-8640 Rapperswil • +41 55 222 18 38 • info@mylearning.ch • mylearning.ch