>> Wireshark

Analyse von Netzwerken

EGOS! the education company

Wireshark ist das führende Netzwerk-Protokoll Analyse Werkzeug. Es ist der De-Facto-Standard der IT- und Netzwerk-Industrie.

Ihr Nutzen

Nach dem Seminar sind Sie in der Lage Netzwerkpakete mit Wireshark zu untersuchen und die entsprechenden Werkzeuge zu nutzen. Im Seminar analysieren Sie Netzwerkpaketströme und erstellen Filter sowie Auswertungen der gescannten Netzwerkpakete.

Voraussetzungen

Networking Technologies~6231

oder dem entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 2850,- exklusive der gesetzlichen MwSt.

Seminardauer

5 Tag(e)/Day(s)

Hinweise

Besprochene Protokolle: DNS, ARP, IPv4, ICMP, UDP, TCP, DHCP, HTTP, Telnet, FTP, POP, SMTP

Version: 101

Seminarinhalte

1. Tag
* Einführung in die Analyse mit Wireshark
- Was ist Wireshark?
- Erste Aufzeichnung mit Wireshark

* Mit Wireshark arbeiten
- Navigation und Anzeigeoptionen
- Display-Filter – Anzeigefilter
- Capture Optionen und Capture Filter
- Ein- und Ausgabe

2. Tag
* Erweiterte Funktionen des Wireshark Analyzers
- Voreinstellungen und Profile
- Namensauflösung
- Was ist Protocol Reassembly?
- TCP Checksum Errors
- Experteninformationen
- Farbige Pakete
- Capture und Packet Comments
- Command Line Tools

3. Tag
* Wireshark Statistiken
- Generelle Statistiken
- TCP/IP-Statistiken
- Grenzen der Wireshark-Statistiken

* Performanceanalyse und Fehlersuche
- Paketanalyse erklärt
- Messen im Switched Ethernet
- Messen in Wireless Netzwerken
- Fehler systematisch eingrenzen
- Auswerten von Laufzeitproblemen
- Netzwerkprobleme und Anwendungsprobleme
- Applikationstypen und Performancefaktoren

4. Tag
* TCP/IP-Analyse der Transportschicht
- Transport über UDP und TCP
- TCP-Funktionen in Wireshark
- TCP-Window und Performance
- TCP-Timing und Retransmissions
- TCP-Optionen
- Weitere TCP-Funktionen
- Tipps zur Fehlersuche

5. Tag
* TCP/IP-Analyse der Netzwerkschicht
- Das Internet Protokoll im Überblick
- MTU, PMTU, Fragmentierung
- Internet Control Message Protocol
- Dynamic Host Configuration Protocol
- Analyse von DNS

* Analyse von Switched Ethernet
- Ethernet Duplex und Speed
- Analyse von Spanning Tree
- Analyse von Virtuellen LANs