NT150 Netzwerkverkehrsanalyse mit Wireshark

Kurzbeschreibung:

Das Training **NT150 Netzwerkverkehrsanalyse mit Wireshark** ist ein intensiver Kurs zur Paketanalyse. Es richtet sich an Administratoren, Netzwerkspezialisten, Troubleshooter und Allround-Admins. Das Motto des Kurses lautet: "Lerne die cleveren Tricks der Netzwerkanalysten, um zu beweisen, dass das Netzwerk nicht schuld ist."

Zielgruppe:

Der Workshop **NT150 Netzwerkverkehrsanalyse mit Wireshark** ist ideal geeignet für:

- Netzwerkadministratoren
- Netzwerktechniker
- Systemadministratoren
- Troubleshooter
- Muss-Alles-Können-Admins

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo des Worskhops **NT150 Netzwerkverkehrsanalyse mit Wireshark** gut folgen zu können, sind grundlegende IT-Kenntnisse und Netzwerkkenntnisse nötig.

Alternativ empfehlen wir vorab folgende Kurse zu besuchen:

- LI100 Linux Basics
- NT101 Netzwerk Administration Advanced

Sonstiges:

Dauer: 5 Tage

Preis: 3150 Euro plus Mwst.

Ziele:

Im Training **NT150 Netzwerkverkehrsanalyse mit Wireshark** bringen wir im 5-tägigen Workshop Ihre Wireshark-Fähigkeiten auf Expertenniveau.
Sie erlangen praktisches Wissen im Bereich der Netzwerkanalyse und im speziellen mit Wireshark.
Wir vermitteln Ihnen praxisrelevante Erfahrungen an Hand verschiedener Fallstudien und vertiefen diese durch eine Vielzahl an Basis,- Fortgeschrittenen- und Sicherheitsübungen aus echten Kundenproblemen.
Der Kurs Netzwerkverkehrsanalyse mit Wireshark ist ein intensives Hands-On Training, welches genug Zeit lässt, auch mitgebrachte Tracefiles von Teilnehmern gemeinsam zu analysieren.

Inhalte/Agenda:

- ♦ **Hands-On Training**
- ♦ **Wireshark Grundlagen**
- ♦
  - ◊ Grundfunktionen
  - ◊ Benutzeroberflache und Navigation
  - ◊ Konfiguration
  - ◊ Display Filter
  - ◊ Capture Dialog
  - ◊ Capture Filter
  - ◊ Dateioperationen

- ♦ **Funktionen und Statistiken**
- ♦
  - ◊ Endpoints, Verbindungen und Protokolle
  - ◊ Wireshark Graphen
  - ◊ Service Response Time
  - ◊ Wireshark Experte und FlowGraph
  - ◊ Performance Faktoren
  - ◊ Durchsatz, Antwortzeit und Overhead

- ♦ **Erweiterte Konfiguration und Tools**
- ♦
  - ◊ Namensauflosung
  - ◊ Farbregeln und Kommentare
  - ◊ Protocol Reassembly
  - ◊ Wireshark Merkwürdigkeiten
  - ◊ Konfigurationsprofile
  - ◊ Kommandozeilen Tools

- ♦ **Grundlagen der Netzwerkanalyse**
- ♦
  - ◊ Problemanalyse und Fehlersuche
  - ◊ Grundlagen der Aufzeichnung
  - ◊ Planen der Aufzeichnung Umgang mit großen Tracefiles
  - ◊ Typische Netzwerkprobleme
  - ◊ Ist das Netzwerk oder die Anwendung schuld?

- ♦ **Protokolle I**
- ♦
  - ◊ Ethernet
  - ◊ 802.1q VLANs
  - ◊ ARP Protokoll

- ♦ **Protokolle II**
- ♦
  - ◊ IPv4/IPv6 fur Netzwerkanalysten
  - ◊ Analyse von ICMP Meldungen
  - ◊ DHCP

- ♦ **Protokolle III**
- ♦
  - ◊ TCP Grundlagen
  - ◊ TCP flow control packet loss, retransmissions Strategien
  - ◊ TCP extensions, SACK, window scaling, Nagle etc.
  - ◊ Moderne TCP Stacks
  - ◊ TCP Performanceanalyse und Tuning
  - ◊ Erkennen von Flaschenhälsen (Bandbreite, Latenz, Anwendung, OS)

- ♦ **Multipoint Analyse**
- ♦
  - ◊ Capture Strategie
  - ◊ Bestimmung von Netzwerklatenzen
  - ◊ Analyse über mehrere Messpunkte hinweg (Proxy, Reverse Proxy, NAT, TCP termination)
  - ◊ Analyse mit Wireshark und Tshark

- ♦ **Fallstudien**
- ♦
  - ◊ Analyse der Tracefiles der Teilnehmer
  - ◊ FTP, HTTP/1.1, HTTP/2, QUIC, DNS, SMB, SQL
  - ◊ Analyse und Entschlüsselung von TLS/SSL Verkehr
  - ◊

◊ Rekonstruktion von Dekodierungsfehlern TLS Verbindungen

◊