

## WIRESHARK SICHERHEIT

*Wireshark, der "Nachfolger von Ethereal" ist ein überaus beliebtes, weil hochleistungsfähiges und zudem kostenfreies Tool zur Netzwerkanalyse. Es dient im wesentlichen dazu, diverse Fehler in Netzwerken aufzuspüren und wird deshalb vor allem von Kommunikationsexperten, Netzwerkadministratoren, Sicherheitsverantwortlichen, aber auch von Softwareentwicklern eingesetzt.*

*Ziel ist es meist, einzelne Pakete in Netzwerken nach diversen Kriterien für Analysezwecke auszufiltern, um anschließend gezielte Maßnahmen durchführen zu können. So sollten z. B. Administratoren neue Sicherheitsmaßnahmen erwägen, wenn alle Passwörter im Klartext übertragen werden.*

*Auch zur Performanceanalyse ist es häufig hilfreich, lassen sich defekte Netzwerkgeräte oder mutwillige Störungen mit Wireshark das notwendige Wissen vorausgesetzt, gut identifizieren.*

### Zielgruppe

Administratoren und Mitarbeiter aus sicherheitskritischen Bereichen, Softwareentwickler

### Hinweis

Eine kurze Einführung zu diesem Thema ist auch in den Kursen [Sicherheit in IP-Netzen](#) und [IPsec](#) enthalten.

### Überblick über Wireshark

- die Geschichte von Wireshark
- das Programm und seine Funktionen
- Navigieren im Wireshark
- Displayregeln

### Filter

- Was sind Filter?
- Displayfilter
- Capturefilter

### Sniffen

- Was ist sniffen?
- gesetzlicher Hintergrund zum Thema Sniffing
- sniffen in verschiedenen Umgebungen
- in einer Kollisionsdomäne
- in einer Broadcastdomäne
- im Netzwerk
- Hilfsmittel zum Sniffen
- arp spoof, ping, tracer
- unbeaufsichtigtes Sniffen
- einen TCP-Stream verfolgen

### Fileset

- Was ist ein Fileset?
- capture in ein Fileset
- verwenden eines Filesets zu Analysezwecken
- speichern des Datenstroms zur späteren Verwendung

### Statistiken

- erzeugen von Statistiken zur Weiterverarbeitung
- I/O Graphen erzeugen
- Server Response Time
- Endpoint Liste

### Vergleich

- Wireshark im Vergleich zu anderen Analysewerkzeugen
- Datenaustausch zwischen Netzwerkanalysetools

### zusätzliche Tools zu Wireshark

- tethereal
- mergenap
- editcap
- Winpcap-Treiber

**Kurs-ID: WireSha**

### Dauer

2 Tage / 8:00 - 15:30 Uhr

### Offener Kurs

Der Seminarpreis einschließlich Seminarunterlagen beträgt pro Teilnehmer 620,00 € zzgl. MwSt. (≙ 737,80 € inkl. MwSt.)

Termin laut [Terminplan](#) oder auf Anfrage

zur [Anmeldung](#)

Durchführung: ab 3 Pers.

### Firmenkurs

Termine nach Vereinbarung.

Preise für Individual- und Firmenschulungen auf Anfrage.

### Vorkenntnisse

Tiefere Kenntnisse zu TCP/IP z. B. entsprechend unserem Kurs [TCP/IP Protokolle](#) oder vergleichbare Kenntnisse sind unumgänglich.

Weitergehendes Wissen zu speziellen Protokollen z. B. VoIP, sicherheitsrelevante Themen o. a.

applikationsspezifische Protokollvarianten sind empfehlenswert.

Wie bei vielen unserer Kurse haben die meisten unserer Kursteilnehmer eine kurze Einarbeitungsphase in das Programm bereits hinter sich und nutzen den Kurs dazu, vertiefendes Wissen kurzer Zeit dazuzulernen.

### Weiterführende Kurse

- [Sicherheit in IP-Netzen](#)
- [IPsec](#)

0

1

2

3

4

5

6

7

8

9

0

1

2

3

4

5

6

7

8

