

# Security in IP-Netzen

## Sicherheitslücken erkennen und schließen

Die letzten Jahre waren eine Blütezeit neuartiger Angriffsmethoden. Aber auch die Anbieter von Schutzmaßnahmen sind nicht untätig geblieben. Das Thema Netzwerksicherheit hat dadurch an Komplexität gegenüber früher wesentlich zugenommen. Das in diesem Kurs vermittelte Know-how legt den Grundstein für die eigenverantwortliche Übernahme von Aufgaben in der Security-Planung und -Administration IP-basierter Netzwerke. Gleichzeitig ist er die Basis für eine Vielzahl von weiterführenden Kursen im Security-Bereich.

### Kursinhalt

- Ziele von Netzwerksicherheit
- Schwachstellen der TCP/IP-Architektur
- Besonderheiten bei IPv6
- Typische Angriffe: DoS, Spoofing, Cache Poisoning, etc.
- Symmetrische und asymmetrische Verschlüsselung (AES, 3DES, RSA, ECC, ...)
- Datenintegrität und Keyed Hash (MD5, SHA-1)
- Authentisierung, Signaturen und Zertifikate
- IPsec und SSL und ihr Einsatz für VPNs
- Anwendungen: SSH, SCP, PGP, HTTPS, etc.
- Endpoint Security: Virens Scanner, Festplattenverschl., Media Control, etc.
- LAN und WLAN Security: Port Security, WPA2, 802.1x
- Firewalls und DMZ
- Intrusion Detection and Prevention
- Security in virtualisierten Umgebungen / Cloud Security
- Demonstrationen am Testnetz

Jeder Teilnehmer erhält ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache.

### Zielgruppe

Wer aus Netzwerksicht detaillierte Kenntnisse zu den Sicherheitsproblemen in der TCP/IP-Welt benötigt und nach passenden Lösungen sucht, findet diese hier. Der Kurs eignet sich gleichermaßen für Administratoren, Planer und Consultants.

### Voraussetzungen

Optimale Voraussetzungen sind fundiertes Basiswissen im Umfeld LAN, Router und Internet sowie tiefer gehende Kenntnisse des IP-Protokolls.



### Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf [www.experteach.at](http://www.experteach.at) können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

4 Tage

€ 1.995,- zzgl. MwSt.

### Termin/Kursort

29.05.-01.06.12	Frankfurt	05.11.-08.11.12	München
06.08.-09.08.12	München	05.11.-08.11.12	Stuttgart
06.08.-09.08.12	Wien	03.12.-06.12.12	Frankfurt
27.08.-30.08.12	Frankfurt	03.12.-06.12.12	Zürich
18.09.-21.09.12	Düsseldorf	21.01.-24.01.13	München
16.10.-19.10.12	Berlin	18.02.-21.02.13	Frankfurt
16.10.-19.10.12	Hamburg		

Aktuelle Informationen finden Sie auf [www.experteach.at](http://www.experteach.at) SECU



EXPERTeach





## 1 Motivation für Netzwerksicherheit

- 1.1 Ziele von Netzwerksicherheit
  - 1.1.1 Vertraulichkeit
  - 1.1.2 Integrität
  - 1.1.3 Authentizität
  - 1.1.4 Verfügbarkeit
- 1.2 Die grundsätzlichen Bedrohungen
  - 1.2.1 Lauschen
  - 1.2.2 Spoofing
  - 1.2.3 Denial of Service
- 1.3 Das Internet Protocol
  - 1.3.1 Der IPv4-Header
  - 1.3.2 Der IPv6-Header
  - 1.3.3 UDP – Verbindungslos und ungesichert
  - 1.3.4 TCP – Verbindungsorientiert und gesichert
- 1.4 Schwachstellen der TCP/IP-Architektur
  - 1.4.1 IP Spoofing
  - 1.4.2 Malformed Packets
  - 1.4.3 Fragmentierungsangriffe
  - 1.4.4 SYN Flooding
  - 1.4.5 Blind Spoofing
  - 1.4.6 Angriffe auf bestehende Verbindungen
  - 1.4.7 Session Hijacking
  - 1.4.8 Der RST-Angriff
  - 1.4.9 Angriffe gegen DNS
  - 1.4.10 Angriffe gegen Routing
- 1.5 Typische Tools und Programme
  - 1.5.1 Informationsbeschaffung
  - 1.5.2 Metasploit
  - 1.5.3 Informationsquellen
  - 1.5.4 Die Grundschutzkataloge des BSI

## 2 Datenschutz durch Verschlüsselung

- 2.1 Anfänge der Kryptographie
- 2.2 Symmetrische Verschlüsselung
  - 2.2.1 Lebensdauer und Verteilung der Schlüssel
  - 2.2.2 Erzeugung von Schlüsseln
  - 2.2.3 Diffie-Hellman
  - 2.2.4 SPEKE
- 2.3 Asymmetrische Verschlüsselung
  - 2.3.1 RSA
  - 2.3.2 El Gamal
  - 2.3.3 Hybride Verfahren
- 2.4 Datenintegrität: Hash-Werte
  - 2.4.1 Typische Eigenschaften
  - 2.4.2 Angriffe auf Hash-Werte
  - 2.4.3 Keyed Hash

## 3 Authentisierung

- 3.1 Grundsätzliches
  - 3.1.1 Der Man in the Middle
  - 3.1.2 Authentisierung und Autorisierung
  - 3.1.3 User-bezogenes Logging
  - 3.1.4 Geräteauthentisierung und User-Authentisierung
  - 3.1.5 Architektur
  - 3.1.6 Aufrechterhaltung der Authentisierung

- 3.1.7 Replay-Angriffe
- 3.2 Identifikationsmöglichkeiten
  - 3.2.1 Statische Passwörter
  - 3.2.2 Einmal-Passwörter
  - 3.2.3 Biometrie
  - 3.2.4 Public-Key-Authentisierung
  - 3.2.5 Tickets und Zertifikate
- 3.3 Zertifikate
  - 3.3.1 Digitale Signatur
  - 3.3.2 Konzept
  - 3.3.3 PKI und CA
- 3.4 Authentisierungsprozeduren
  - 3.4.1 Verfahren mit Passwort-Übertragung
  - 3.4.2 Challenge – Response
  - 3.4.3 EAP
- 3.5 Zentrale Authentisierung
  - 3.5.1 RADIUS
  - 3.5.2 DIAMETER
  - 3.5.3 TACACS+
  - 3.5.4 LDAP
  - 3.5.5 Kerberos
  - 3.5.6 Konzept
  - 3.5.7 NTLM
- 3.6 Anonymisierer

## 4 Absichern von Verbindungen

- 4.1 VPN-Konzepte
- 4.2 Network Layer: IPsec
  - 4.2.1 IPsec – Die Betriebsarten
  - 4.2.2 IPsec Header
  - 4.2.3 Tunnelaufbau und -verwaltung
  - 4.2.4 Security Associations
  - 4.2.5 IKEv1
  - 4.2.6 IKEv2
- 4.3 Transport Layer: SSL
  - 4.3.1 SSL/TLSs
  - 4.3.2 Der SSL Verbindungsaufbau
  - 4.3.3 Architektur von SSL VPNs
- 4.4 Sichere Applikationen
  - 4.4.1 SSH
  - 4.4.2 PGP und S/MIME
  - 4.4.3 DNSSEC
  - 4.4.4 Absichern von VoIP

## 5 LAN- und WLAN-Security

- 5.1 Arbeitsweise eines LANs
  - 5.1.1 Das Ethernet-Protokoll
  - 5.1.2 Hubs
  - 5.1.3 Switches
  - 5.1.4 VLANs
- 5.2 Gefahren im LAN
  - 5.2.1 MAC Spoofing
  - 5.2.2 ARP Cache Poisoning
- 5.2.3 Neighbor Solicitation
- 5.2.4 Flooding der Switching Table
- 5.2.5 VLAN Hopping

- 5.2.6 Mirror Ports
- 5.2.7 DHCP Spoofing
- 5.2.8 Router Advertisements
- 5.2.9 ICMP-Angriffe
- 5.2.10 Spanning-Tree-Angriffe
- 5.3 LAN-Security
  - 5.3.1 Port Security
  - 5.3.2 Private VLANs
- 5.4 Arbeitsweise eines WLANs
  - 5.4.1 Service Set Identifier (SSID)
  - 5.4.2 Von Funkzelle zu Funkzelle und Roaming
- 5.5 WLAN-Security
  - 5.5.1 Unzureichende Maßnahmen
  - 5.5.2 Sicherheitsstandards
  - 5.5.3 Protected Management Frames
- 5.6 IEEE 802.1X
  - 5.6.1 Schlüsselgenerierung
  - 5.6.2 Automatische VLAN-Zuweisung

## 6 Firewalls

- 6.1 Firewalls
  - 6.1.1 Statische Paketfilter
  - 6.1.2 Dynamische Paketfilter – Stateful Firewalls
  - 6.1.3 Proxy Firewalls
  - 6.1.4 Mail Relays
  - 6.1.5 Data Loss Prevention
- 6.2 IDS und IPS
  - 6.2.1 Positionierung
  - 6.2.2 Arbeitsweise des IDS
  - 6.2.3 Maßnahmen
  - 6.2.4 Korrelationen
- 6.3 Netzdesign
  - 6.3.1 Network Address Translation (NAT) und Firewalls
  - 6.3.2 DMZ-Konzepte – Ein Überblick
  - 6.3.3 Firewalls und VPNs
  - 6.3.4 Ausfallsicherheit und Lastverteilung

## 7 Endpoint Security

- 7.1 Angriffe auf Betriebssysteme und Programme
  - 7.1.1 Malware
  - 7.1.2 Exploits
  - 7.1.3 Buffer Overflow
  - 7.1.4 Drive-by Infection
  - 7.1.5 Aktive Inhalte
  - 7.1.6 Phishing
- 7.2 Angriffe auf Webserver
  - 7.2.1 Cross Site Scripting
  - 7.2.2 SQL-Injection
- 7.3 Endpoint Security
  - 7.3.1 Virenschutzprogramm
  - 7.3.2 Patch Management
  - 7.3.3 Festplattenverschlüsselung
  - 7.3.4 Absicherung von Wechselmedien
- 7.4 Virtuelle Umgebungen



### ExperTeach GmbH Training Center Wien

Millennium Tower, 24. Etage  
Handelskai 94-96 • A-1200 Wien  
Telefon +43 66 43 45 39 64  
info@experteach.at • www.experteach.at

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 05.05.2012