

# Hackerwissen für Netzwerker

## Vom Port Scan bis zum Penetration Testing

Ein wirksamer Schutz vor Angriffen aus dem Internet oder dem eigenen Netzwerk kann nur gewährleistet werden, wenn die mit der Sicherheit betrauten Personen die Angriffsmethoden von Hackern kennen und verstehen. Die Informationsbeschaffung vor dem Angriff ist dabei genauso wichtig wie der Angriff selbst. Anhand praktischer Übungen lernen Sie die Denkweise und Methodik eines Hackers kennen, um dann in einem Testnetz einen aktiven Angriff zu simulieren. So ist es Ihnen möglich, Ihr eigenes Netzwerk auf Schwachstellen zu überprüfen und gegen Angriffe abzusichern.

### Kursinhalt

- Methodik und Werkzeuge von Hackern
- Schwächen der IP-Protokollfamilie
- Trojanische Pferde und Root Kits
- Sniffen in geschwitzen Netzen, ARP-Angriffe, Spoofing
- Reconnaissance und Enumeration
- DNS, Whois, RIPE und andere Informationsquellen
- Netzwerke auskundschaften
- Aktives und Passives Fingerprinting
- Port Scans und Vulnerability Checks
- Session Grabbing und Man-in-the-Middle-Angriff
- Google Hacking
- DNS Spoofing
- Passwörter knacken (Lexikon-Attacke, Brute Force, Social Engineering, Rainbow Tables)
- Cross Site Scripting und SQL Injection
- URL Spoofing
- Denial of Service
- Buffer Overflow Attacks, Exploits und das Metasploit-Framework
- Firewall Scanning und Piercing

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

### Zielgruppe

Diese Schulung richtet sich an Personen, zu deren Aufgabe die Sicherung des Netzwerks und der angeschlossenen Server vor Hackerangriffen zählt.

### Voraussetzungen

Gute IP-Kenntnisse sowie Grundkenntnisse zu Router-Netzen sind erforderlich. Praktische Erfahrung im Umgang mit Netzwerken ist sehr hilfreich. Der Kurs TCP/IP - Protokolle, Adressierung, Routing ist eine gute Vorbereitung.



### 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.

5 Tage

€2.495,- zzgl. MwSt.

### Termin/Kursort

|                 |            |                 |           |
|-----------------|------------|-----------------|-----------|
| 11.06.-15.06.12 | Wien       | 08.10.-12.10.12 | Frankfurt |
| 11.06.-15.06.12 | München    | 19.11.-23.11.12 | Wien      |
| 23.07.-27.07.12 | Düsseldorf | 19.11.-23.11.12 | München   |
| 13.08.-17.08.12 | Hamburg    |                 |           |

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



EXPERTeach





## 1 Netzwerk – Gefahren erkennen und vermeiden

- 1.1 Die Bedrohungslage erfassen
  - 1.1.1 Angriffsziele
  - 1.1.2 Klassifizierung von Angreifern
- 1.2 Übliche Vorgehensweise bei einem Angriff
  - 1.2.1 Angriff auf Clients
  - 1.2.2 Angriff auf Netzwerke
  - 1.2.3 Angriff auf Server
- 1.3 Hackertools – Für jeden verfügbar
- 1.4 Schutzmaßnahmen
  - 1.4.1 Bedrohungen kennen
  - 1.4.2 Schwachstellenanalyse
  - 1.4.3 Penetrationstest
  - 1.4.4 Reporting und Auswertung

## 2 Informationsbeschaffung

- 2.1 Unternehmensinformationen sammeln
  - 2.1.1 Geschäftliche und private Webseiten
  - 2.1.2 Google Groups
  - 2.1.3 Webarchive
  - 2.1.4 Google Hacking
- 2.2 Social Engineering
  - 2.2.1 Personenbezogene Daten sammeln
  - 2.2.2 Social Engineering Toolkit
  - 2.2.3 Zielnetze lokalisieren
  - 2.2.4 RIPE & Co. – Wem gehört das Netz?
  - 2.2.5 WHOIS – Wer hat die Domain registriert
  - 2.2.6 Dmity
- 2.3 Footprinting durch DNS
  - 2.3.1 Nslookup, dig und Co.
  - 2.3.2 Einen Zonentransfer initiieren
  - 2.3.3 Die Zonendatei durchsuchen
  - 2.3.4 Den Zonentransfer durchführen
- 2.4 Netzwerke auskundschaften
  - 2.4.1 Passive Suche
  - 2.4.2 Ping Varianten
  - 2.4.3 Traceroute-Varianten
  - 2.4.4 Firewall-Regeln erkunden
  - 2.4.5 IRPAS

## 3 LAN und WLAN-Angriffe

- 3.1 Gefahren im LAN
  - 3.1.1 VLAN Hopping
  - 3.1.2 Autokonfiguration von Trunks
  - 3.1.3 Mirror Ports
  - 3.1.4 Spanning-Tree-Angriffe
  - 3.1.5 VRRP und HSRP-Angriffe
- 3.2 IPv4-Angriffe
  - 3.2.1 ICMP-Angriffe
  - 3.2.2 DHCP-Angriffe
- 3.3 IPv6 – Das Protokoll und seine Schwächen
  - 3.3.1 ICMPv6-Angriffe
  - 3.3.2 Sicherheit von DHCPv6
- 3.4 Tools für Layer2/3-Angriffe
  - 3.4.1 Hyenae
  - 3.4.2 Yersinia
  - 3.4.3 Loki
  - 3.4.4 Scapy
- 3.5 Paketanalyse
  - 3.5.1 Voraussetzung für das Sniffing

- 3.5.2 Sniffen im LAN
- 3.5.3 Flooding des Switches
- 3.5.4 Port Stealing
- 3.5.5 IPv4 – ARP Cache Poisoning
- 3.5.6 IPv6 – NDP-Angriffe
- 3.6 WLAN-Angriffe
  - 3.6.1 Ein WLAN-Netz auskundschaften
  - 3.6.2 WLAN-Sniffing
  - 3.6.3 Authentisierungsangriffe
- 3.7 Sniffing Tools – Administrative Werkzeuge und mehr
- 3.8 LAN-Sicherheit verbessern
  - 3.8.1 Port Security
  - 3.8.2 Private VLANs
  - 3.8.3 ARP Inspection
  - 3.8.4 DHCP absichern
  - 3.8.5 Authentisierung mit IEEE 802.1X
  - 3.8.6 Sicherheit mit WPA / IEEE 802.11i

## 4 Port Scanning

- 4.1 Grundlagen des Port Scanning
  - 4.1.1 Dienste erforschen
  - 4.1.2 Ports von Interesse
- 4.2 Scanning Varianten
  - 4.2.1 TCP Scanning
  - 4.2.2 UDP Scanning
- 4.3 Advanced Scanning
  - 4.3.1 OS Detection
  - 4.3.2 Version Detection
- 4.4 Port Scanning in der Praxis
  - 4.4.1 Einfach aber schnell
  - 4.4.2 Shares scannen
  - 4.4.3 LANSpy und Look@LAN
  - 4.4.4 Scanning Apps
  - 4.4.5 Nmap
  - 4.4.6 Scans verschleiern

## 5 Schwachstellenanalyse

- 5.1 Mehr als nur Port Scan
  - 5.1.1 Mehrwert der Schwachstellenanalyse
  - 5.1.2 Arten von Schwachstellenanalysen
  - 5.1.3 Grenzen der Schwachstellenanalyse
- 5.2 Hintergründe der Schwachstellenanalyse
  - 5.2.1 Mit oder ohne Anmeldung
  - 5.2.2 Auf Patches scannen
- 5.3 Tools zur Schwachstellenanalyse
  - 5.3.1 Einzelne Schwachstellen scannen
  - 5.3.2 Nessus
  - 5.3.3 OpenVAS
  - 5.3.4 Nexpose
  - 5.3.5 GFI – LanGuard
  - 5.3.6 Eeye – Retina Network

## 6 Penetration Testing mit Metasploit

- 6.1 Überblick über Metasploit
  - 6.1.1 Aufbau des Metasploit Frameworks
  - 6.1.2 Exploits
  - 6.1.3 Payloads
  - 6.1.4 Weitere Module
- 6.2 Arbeiten mit dem Framework
  - 6.2.1 Die Konsole

- 6.2.2 Das Command Line Interface
- 6.2.3 Die GUI
- 6.2.4 Armitage
- 6.2.5 Metasploit Community Edition
- 6.2.6 Metasploit Pro – Die kommerzielle Variante
- 6.3 Exploitation mit Metasploit
  - 6.3.1 Angriff mit msfconsole
  - 6.3.2 Post Exploitation
  - 6.3.3 Privilege Escalation
- 6.3.4 Das System manipulieren
- 6.3.5 Informationen sammeln
- 6.3.6 Zugriff bewahren
- 6.3.7 Spuren verwischen
- 6.4 Exploitations verhindern
  - 6.4.1 Systeme sichern
  - 6.4.2 Die Sicherheitseinstellungen der Hersteller
- 6.5 Weitere Möglichkeiten von Metasploit
  - 6.5.1 Die Metasploit Database
  - 6.5.2 Port Scanning und Schwachstellenanalyse
  - 6.5.3 Automatisierte Angriffe
  - 6.5.4 Browser und PDF Angriffe
- 6.6 FastTrack für Eilige
- 6.7 Kommerzielle Penetration Tools

## 7 Kennwort-Angriffe

- 7.1 Kennwörter erraten
- 7.2 Password Cracking
  - 7.2.1 Die Kennwort-Datei auslesen
  - 7.2.2 Wörterbuchangriff
  - 7.2.3 Brute-Force-Angriffe
  - 7.2.4 Regenbogentabellen
  - 7.2.5 Cracking Tools
- 7.3 Password Guessing
  - 7.3.1 Die Authentisierung manipulieren
  - 7.3.2 Unterschiede bei den Diensten
  - 7.3.3 Tools zum Password Guessing
  - 7.3.4 Pass-the-Hash-Angriffe
- 7.4 Password Sniffing
  - 7.4.1 Kennwörter mitlesen
  - 7.4.2 Kennwörter cracken
  - 7.4.3 Tools zum Password Sniffing

## 8 Webangriffe

- 8.1 WWW – Angriffsziele
- 8.2 Angriffe auf Clients
  - 8.2.1 Browsereinstellungen
  - 8.2.2 Aktive Inhalte und Plug-Ins
- 8.3 Webserver sichern
- 8.4 Protokoll Angriffe
- 8.5 Angriffsarten
  - 8.5.1 Injection
  - 8.5.2 SQL Injection
  - 8.5.3 Cross Site Scripting – XSS
  - 8.5.4 Cross Site Request Forgery – CSRF
  - 8.5.5 Broken Authentication and Session Management
  - 8.5.6 Insecure Direct Object Reference
  - 8.5.7 Clickjacking
- 8.6 Websecurity Scanner



### 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 01.05.2012