# Hacking I

## Understanding Network Attacks

**In the context of cyber security, effective protection against attacks from the internet or your own network can only be guaranteed if the people responsible for security know and understand the motivation and approach of the various attackers. In this seminar, the methodical approach of a hacker is presented, from information gathering and planning to the execution of an attack. Another important aspect is the analysis of a security incident with the help of digital forensics. The course content is deepened by means of practical exercises. In a test environment, you will learn the methodology of a hacker and then simulate active attacks in a test network. This enables you to check your own network for vulnerabilities and secure it against attacks.**

### Course Contents

- Motivation and methodology of attacks
- Tools used by hackers
- Malware - from viruses to rootkits
- Sniffing and man-in-the-middle attacks
- LAN and WLAN attacks
- Abusing protocols
- Information gathering - reconnaissance and enumeration
- Exploring networks
- Portscan and fingerprinting
- Vulnerability checks
- Exploitation with Metasploit
- Password attacks
- Digital forensics methods
- Securing attack traces
- Analyzing security incidents

### Target Group

This training is aimed at people who are responsible for securing the network and connected servers against hacker attacks.

### Prerequisites

Good IP knowledge and basic knowledge of router networks are required. Practical experience in dealing with networks is very helpful. The course TCP/IP - Protocols, Addressing, Routing is a good preparation.

### This Course in the Web

You can find the up-to-date information and options for ordering under the following link:
www.experteach-training.com/go/**HACK**

### Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

### Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

### Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

### Premium Print Package

You can optionally purchase the high-quality Premium Print Package for this course at a price of € 200 (plus VAT).

| Training | | Prices, excl. of V.A.T. |
|---|---|---|
| **Classes in Germany** | **5 Days** | **€ 2,795** |
| **Classes in Austria** | **5 Days** | **€ 2,795** |
| **Classes in Switzerland** | **5 Days** | **€ 3,490** |
| **Online Training** | **5 Days** | **€ 2,795** |

**Date/course venue** — Course language German

| | | | |
|---|---|---|---|
| 09/11-13/11/26 | ONOnline | 05/07-09/07/27 | HYOnline |
| 14/12-18/12/26 | HYDüsseldorf | 26/07-30/07/27 | HYBerlin |
| 14/12-18/12/26 | HYOnline | 26/07-30/07/27 | HYHamburg |
| 01/02-05/02/27 | HYBerlin | 26/07-30/07/27 | HYOnline |
| 01/02-05/02/27 | HYHamburg | 26/07-30/07/27 | HYOnline |
| 01/02-05/02/27 | HYOnline | 30/08-03/09/27 | HYFrankfurt |
| 01/02-05/02/27 | HYOnline | 30/08-03/09/27 | HYOnline |
| 15/03-19/03/27 | HYFrankfurt | 30/08-03/09/27 | HYOnline |
| 15/03-19/03/27 | HYOnline | 30/08-03/09/27 | HYZürich |
| 15/03-19/03/27 | HYOnline | 11/10-15/10/27 | HYOnline |
| 15/03-19/03/27 | HYZürich | 11/10-15/10/27 | HYWien |
| 19/04-23/04/27 | HYOnline | 08/11-12/11/27 | HYDüsseldorf |
| 19/04-23/04/27 | HYWien | 08/11-12/11/27 | HYOnline |
| 31/05-04/06/27 | HYDüsseldorf | 06/12-10/12/27 | HYMünchen |
| 31/05-04/06/27 | HYOnline | 06/12-10/12/27 | HYOnline |
| 05/07-09/07/27 | HYMünchen | | |

Status 11/04/2026

Hacking I

# Table of Contents

## Hacking I – Understanding Network Attacks


**1 Netzwerkangriffe – Ein Überblick**
1.1 Angriffsziele
1.1.1 Angriff auf Clients
1.1.2 Mobile Endgeräte angreifen
1.1.3 Angriff auf Netzwerke
1.1.4 Angriff auf Server
1.2 Klassifizierung von Angreifern
1.2.1 Freizeithacker
1.2.2 Professionelle Angreifer
1.2.3 Politische Motive
1.2.4 Wirtschaftliche Interessen
1.2.5 Cyberterrorismus
1.2.6 Bedrohungen kennen
1.3 Struktur eines Angriffs
1.4 Quellen für Hackertools
1.4.1 Pen Testers Framework – PTF
1.4.2 Linux-Hacking-Distributionen
1.4.3 Kali -Linux anpassen
1.4.4 Mobile Endgeräte als Angriffswerkzeug

**2 Informationsbeschaffung**
2.1 Unternehmensinformationen sammeln
2.1.1 Das WWW als Informationsquelle
2.1.2 Soziale Plattformen ausnutzen
2.1.3 Suchmaschinen verwenden
2.2 Zielnetze lokalisieren
2.2.1 RIPE & Co. – Wem gehört das Netz?
2.2.2 WHOIS – Wer hat die Domain registriert
2.2.3 Verräterische Mails
2.3 Footprinting durch DNS
2.3.1 Nslookup, dig und Co.
2.3.2 Zonentransfers
2.3.3 Wörterbuchangriff auf die Zone
2.3.4 Reverse Lookups
2.4 Discover Scripts
2.5 Netzwerke auskundschaften
2.5.1 Passiv – Einfach nur lauschen
2.5.2 Aktiv-Ping Varianten
2.5.3 Traceroute ermittelt den Aufbau
2.5.4 Firewallregeln ermitteln

**3 Sniffing in LAN und WLAN**
3.1 Pakete mitlesen
3.1.1 Sniffing im LAN
3.1.2 Netzwerksniffer
3.2 Sniffing in geswitchten Netzen
3.2.1 Flooding des Switches
3.2.2 Port Stealing
3.2.3 IPv4 – ARP Cache Poisoning
3.2.4 Ettercap
3.2.5 IPv6 – NDP-Angriffe
3.3 Paketinformationen auswerten
3.4 Schutz gegen Sniffing-Angriffe
3.4.1 Port Security
3.4.2 ARP Inspection
3.4.3 Authentisierung mit IEEE 802.1X

**4 Netzwerke angreifen**
4.1 Gefahren im LAN
4.1.1 VLAN Hopping
4.1.2 Autokonfiguration von Trunks
4.1.3 Spanning-Tree-Angriffe
4.1.4 VRRP und HSRP-Angriffe
4.2 IPv4-Angriffe
4.2.1 ICMP-Angriffe
4.2.2 DHCP-Angriffe
4.3 Tools für Layer2/3-Angriffe
4.3.1 Hyenae
4.3.2 Yersinia
4.3.3 Scapy
4.4 IPv6 – Das Protokoll und seine Schwächen
4.4.1 ICMPv6-Angriffe
4.4.2 Sicherheit von DHCPv6

**5 WLAN-Angriffe**
5.1 Sicherheit im WLAN
5.1.1 Verschlüsselung und Integrität
5.1.2 Authentisierung
5.1.3 WEP – Wired Equivalent Privacy
5.1.4 WPA – Wi-Fi Protected Access
5.1.5 IEEE 802.11i – WPA2
5.2 Angriffe im WLAN
5.3 Ein WLAN-Netz auskundschaften
5.3.1 Die SSID ermitteln
5.3.2 Kismet und Giskismet
5.3.3 WLAN-Sniffing
5.4 Authentisierungsangriffe
5.4.1 WLAN-Cracking-Tools
5.4.2 Wifite
5.4.3 Fern-Wifi-Cracker
5.4.4 WPS-Angriffe – Reaver, Bully und Co.
5.5 MDK3 – DoS auf WLANs
5.6 Wifi Honeypots

**6 Port Scanning**
6.1 Grundlagen des Port Scanning
6.1.1 Dienste erforschen
6.1.2 Ports von Interesse
6.2 Scanning Varianten
6.2.1 Direct Scanning
6.2.2 Indirect Scanning
6.2.3 TCP Scanning
6.2.4 UDP Scanning
6.3 Advanced Scanning
6.3.1 OS Detection
6.3.2 Version Detection
6.4 Port Scanning in der Praxis
6.4.1 Einfach aber schnell
6.4.2 Nmap
6.4.3 Shares scannen
6.4.4 LAN- Scanning
6.4.5 Scanning Apps
6.4.6 Scans verschleiern

**7 Schwachstellenanalyse**
7.1 Mehr als nur Port Scan
7.1.1 Mehrwert der Schwachstellenanalyse
7.1.2 Arten von Schwachstellenanalysen
7.1.3 Grenzen der Schwachstellenanalyse
7.2 Hintergründe der Schwachstellenanalyse
7.2.1 Mit oder ohne Anmeldung
7.2.2 Auf Patches scannen
7.3 Tools zur Schwachstellenanalyse
7.3.1 Nessus
7.3.2 OpenVAS
7.3.3 Nexpose
7.3.4 GFI – LanGuard
7.3.5 Retina Network Security Scanner
7.3.6 Qualys Guard

**8 Metasploit – Ein Einstieg**
8.1 Überblick über Metasploit
8.1.1 Exploits
8.1.2 Payloads
8.1.3 Weitere Module
8.2 Arbeiten mit dem Framework
8.2.1 Exploitation mit Metasploit
8.2.2 Msfconsole
8.3 Armitage
8.3.1 Vorbereitung zum Start
8.3.2 Die GUI
8.3.3 Targets suchen
8.3.4 Schwachstellen lokalisieren
8.3.5 Exploitation
8.4 Post Exploitation
8.4.1 Meterpreter – Shell mit Erweiterungen
8.4.2 Der Shell Payload
8.5 Hail Mary

**9 Passwortangriffe im Überblick**
9.1 Default Passwords
9.2 Angriffsvarianten
9.2.1 Password Cracking (offline)
9.2.2 Password Cracking (online)
9.2.3 Password Sniffing
9.3 Tools für Kennwortangriffe
9.3.1 Offline Cracking Tools
9.3.2 Online cracking Tools
9.3.3 Tools zum Password Sniffing

**10 Digitale Forensik**
10.1 Forensik und Digitale Forensik
10.2 Forensik-Modelle
10.2.1 Secure – Beweissicherung
10.2.2 Analyse – Daten auswerten
10.2.3 Present – Bericht erstellen
10.2.4 Das BSI Modell für Digitale Forensik
10.3 Computer und Laptops
10.3.1 Live Response und Post Mortem Analyse
10.3.2 Die Festplatte auswerten
10.3.3 Computer Forensik Tools
10.4 Mobile Devices
10.4.1 Informationssicherung mobiler Endgeräte
10.4.2 Interaktion hinterfragen
10.4.3 Die SIM-Karte auswerten
10.4.4 Tools für Mobile-Device-Forensik
10.5 Betriebssysteme
10.5.1 Windows
10.5.2 Linux
10.5.3 Mac OS X
10.5.4 Android
10.5.5 iOS
10.6 Anwendungen
10.6.1 Browser-Artefakte
10.6.2 Chat und Instant Messaging
10.6.3 E-Mail
10.7 Netzwerk Forensik
10.7.1 Netzwerkverkehr aufzeichnen
10.7.2 Netzwerk Analyse Tools
10.7.3 Log-Dateien auswerten
10.7.4 Cloud Forensik
10.8 Linux-Forensik-Distributionen



**ExperTeach Benelux B.V.**
Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com