

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

E-Book The detailed digital documentation package, consisting of an e-book and PDF, is included in the price of the course.

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 a 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.

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	€ 3,690
Online Training	5 Days	€ 2,795
Date/course venue	Course language German	
05/05-09/05/25 Online	04/08-08/08/25 Hamburg	
05/05-09/05/25 Wien	04/08-08/08/25 Online	
02/06-06/06/25 Düsseldorf	08/09-12/09/25 Frankfurt	
02/06-06/06/25 Online	08/09-12/09/25 Online	
30/06-04/07/25 Zürich	13/10-17/10/25 Online	
07/07-11/07/25 Frankfurt	13/10-17/10/25 Wien	
07/07-11/07/25 Online	01/12-05/12/25 Düsseldorf	
04/08-08/08/25 Berlin	01/12-05/12/25 Online	

Status 03/13/2025



EXPERTeach



Table of Contents

Hacking I – Understanding Network Attacks

1 Netzwerkangriffe – Ein Überblick	4.2 DHCP-Angriffe	8 Metasploit – Ein Einstieg
1.1 Angriffsziele	4.3 Tools für Layer2/3-Angriffe	8.1 Überblick über Metasploit
1.1.1 Angriff auf Clients	4.3.1 Hyenae	8.1.1 Exploits
1.1.2 Mobile Endgeräte angreifen	4.3.2 Yersinia	8.1.2 Payloads
1.1.3 Angriff auf Netzwerke	4.3.3 Scapy	8.1.3 Weitere Module
1.1.4 Angriff auf Server	4.4 IPv6 – Das Protokoll und seine Schwächen	8.2 Arbeiten mit dem Framework
1.2 Klassifizierung von Angreifern	4.4.1 ICMPv6-Angriffe	8.2.1 Exploitation mit Metasploit
1.2.1 Freizeithacker	4.4.2 Sicherheit von DHCPv6	8.2.2 Msfconsole
1.2.2 Professionelle Angreifer		8.3 Armitage
1.2.3 Politische Motive	5 WLAN-Angriffe	8.3.1 Vorbereitung zum Start
1.2.4 Wirtschaftliche Interessen	5.1 Sicherheit im WLAN	8.3.2 Die GUI
1.2.5 Cyberterrorismus	5.1.1 Verschlüsselung und Integrität	8.3.3 Targets suchen
1.2.6 Bedrohungen kennen	5.1.2 Authentisierung	8.3.4 Schwachstellen lokalisieren
1.3 Struktur eines Angriffs	5.1.3 WEP – Wired Equivalent Privacy	8.3.5 Exploitation
1.4 Quellen für Hackertools	5.1.4 WPA – Wi-Fi Protected Access	8.4 Post Exploitation
1.4.1 Pen Testers Framework – PTF	5.1.5 IEEE 802.11i – WPA2	8.4.1 Meterpreter – Shell mit Erweiterungen
1.4.2 Linux-Hacking-Distributionen	5.2 Angriffe im WLAN	8.4.2 Der Shell Payload
1.4.3 Kali -Linux anpassen	5.3 Ein WLAN-Netz auskundschaften	8.5 Hail Mary
1.4.4 Mobile Endgeräte als Angriffswerkzeug	5.3.1 Die SSID ermitteln	
	5.3.2 Kismet und Giskismet	9 Passwortangriffe im Überblick
	5.3.3 WLAN-Sniffing	9.1 Default Passwords
2 Informationsbeschaffung	5.4 Authentisierungsangriffe	9.2 Angriffsvarianten
2.1 Unternehmensinformationen sammeln	5.4.1 WLAN-Cracking-Tools	9.2.1 Password Cracking (offline)
2.1.1 Das WWW als Informationsquelle	5.4.2 Wifite	9.2.2 Password Cracking (online)
2.1.2 Soziale Plattformen ausnutzen	5.4.3 Fern-Wifi-Cracker	9.2.3 Password Sniffing
2.1.3 Suchmaschinen verwenden	5.4.4 WPS-Angriffe – Reaver, Bully und Co.	9.3 Tools für Kennwortangriffe
2.2 Zielnetze lokalisieren	5.5 MDK3 – DoS auf WLANs	9.3.1 Offline Cracking Tools
2.2.1 RIPE & Co. – Wem gehört das Netz?	5.6 Wifi Honeybots	9.3.2 Online cracking Tools
2.2.2 WHOIS – Wer hat die Domain registriert		9.3.3 Tools zum Password Sniffing
2.2.3 Verräterische Mails		
2.3 Footprinting durch DNS	6 Port Scanning	10 Digitale Forensik
2.3.1 Nslookup, dig und Co.	6.1 Grundlagen des Port Scanning	10.1 Forensik und Digitale Forensik
2.3.2 Zonentransfers	6.1.1 Dienste erforschen	10.2 Forensik-Modelle
2.3.3 Wörterbuchangriff auf die Zone	6.1.2 Ports von Interesse	10.2.1 Secure – Beweissicherung
2.3.4 Reverse Lookups	6.2 Scanning Varianten	10.2.2 Analyse – Daten auswerten
2.4 Discover Scripts	6.2.1 Direct Scanning	10.2.3 Present – Bericht erstellen
2.5 Netzwerke auskundschaften	6.2.2 Indirect Scanning	10.2.4 Das BSI Modell für Digitale Forensik
2.5.1 Passiv – Einfach nur lauschen	6.2.3 TCP Scanning	10.3 Computer und Laptops
2.5.2 Aktiv-Ping Varianten	6.2.4 UDP Scanning	10.3.1 Live Response und Post Mortem Analyse
2.5.3 Traceroute ermittelt den Aufbau	6.3 Advanced Scanning	10.3.2 Die Festplatte auswerten
2.5.4 Firewallregeln ermitteln	6.3.1 OS Detection	10.3.3 Computer Forensik Tools
	6.3.2 Version Detection	10.4 Mobile Devices
3 Sniffing in LAN und WLAN	6.4 Port Scanning in der Praxis	10.4.1 Informationssicherung mobiler Endgeräte
3.1 Pakete mitlesen	6.4.1 Einfach aber schnell	10.4.2 Interaktion hinterfragen
3.1.1 Sniffing im LAN	6.4.2 Nmap	10.4.3 Die SIM-Karte auswerten
3.1.2 Netzwerksniffer	6.4.3 Shares scannen	10.4.4 Tools für Mobile-Device-Forensik
3.2 Sniffing in gewichteten Netzen	6.4.4 LAN- Scanning	10.5 Betriebssysteme
3.2.1 Flooding des Switches	6.4.5 Scanning Apps	10.5.1 Windows
3.2.2 Port Stealing	6.4.6 Scans verschleiern	10.5.2 Linux
3.2.3 IPv4 – ARP Cache Poisoning		10.5.3 Mac OS X
3.2.4 Ettercap	7 Schwachstellenanalyse	10.5.4 Android
3.2.5 IPv6 – NDP-Angriffe	7.1 Mehr als nur Port Scan	10.5.5 iOS
3.3 Paketinformationen auswerten	7.1.1 Mehrwert der Schwachstellenanalyse	10.6 Anwendungen
3.4 Schutz gegen Sniffing-Angriffe	7.1.2 Arten von Schwachstellenanalysen	10.6.1 Browser-Artefakte
3.4.1 Port Security	7.1.3 Grenzen der Schwachstellenanalyse	10.6.2 Chat und Instant Messaging
3.4.2 ARP Inspection	7.2 Hintergründe der Schwachstellenanalyse	10.6.3 E-Mail
3.4.3 Authentisierung mit IEEE 802.1X	7.2.1 Mit oder ohne Anmeldung	10.7 Netzwerk Forensik
	7.2.2 Auf Patches scannen	10.7.1 Netzwerkverkehr aufzeichnen
4 Netzwerke angreifen	7.3 Tools zur Schwachstellenanalyse	10.7.2 Netzwerk Analyse Tools
4.1 Gefahren im LAN	7.3.1 Nessus	10.7.3 Log-Dateien auswerten
4.1.1 VLAN Hopping	7.3.2 OpenVAS	10.7.4 Cloud Forensik
4.1.2 Autokonfiguration von Trunks	7.3.3 Nexpose	10.8 Linux-Forensik-Distributionen
4.1.3 Spanning-Tree-Angriffe	7.3.4 GFI – LanGuard	
4.1.4 VRRP und HSRP-Angriffe	7.3.5 Retina Network Security Scanner	
4.2 IPv4-Angriffe	7.3.6 Qualys Guard	
4.2.1 ICMP-Angriffe		

