

# Hacking II

## Angriffe auf Endgeräte und Applikationen

Für einen Angriff auf ein Netzwerk steht eine Vielzahl an Möglichkeiten zur Verfügung. Um Hacker effektiv abzuwehren und ein Netzwerk zu sichern, müssen Sicherheitsverantwortliche einer Firma die unterschiedlichen Methoden von Angriffen verstehen. Neben der theoretischen Erläuterung der Angriffsvarianten liegt ein Schwerpunkt dieses Seminars auf praktischen Übungen in einem Testnetz. Dadurch werden die Teilnehmer in die Lage versetzt, Schwachstellen innerhalb ihres Netzwerks und die resultierenden Angriffsmöglichkeiten bewerten und Abwehrmaßnahmen ergreifen zu können.

### Kursinhalt

- Angriffsvarianten und Motivation
- DoS und DDoS
- IPv4 und IPv6 missbrauchen
- Applikationen ausnutzen
- Von Trinoo zu #RefRef
- Bot-Netze
- Social Engineering
- Personen auskundschaften und manipulieren
- Phishing und seine Varianten
- Das Social Engineering Toolkit
- Das Metasploit Framework
- Exploits und ihre Anpassung
- Payloads von Shell bis Meterpreter
- Targets missbrauchen
- Kennworte brechen, raten und mitlesen
- Wörterbücher erstellen und anpassen
- Vor- und Nachteile von Brute Force
- Rainbow Tables
- Cain & Abel vs. John the Ripper
- Angriffe im WWW
- SQL Injection
- Cross Site Scripting
- Cross Site Request Forgery
- Webseiten scannen
- Daten manipulieren – Burp Suite und Co.

**E-Book** Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

### Zielgruppe

Dieser Kurs wurde für Personen konzipiert, die mit der Sicherung der Firmeninfrastruktur vor den unterschiedlichsten Arten von Angriffen betraut sind.

### Voraussetzungen

Neben guten IP-Kenntnissen sowie Grundkenntnissen zu Router-Netzen ist für diesen Kurs ein Grundwissen im Hinblick auf Angriffe und Schutzmaßnahmen erforderlich. Der Kurs Hacking I – Angreifer verstehen, Netze schützen ist hierfür eine gute Vorbereitung.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/HAC2](http://www.experteach.at/go/HAC2)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.	
<b>Termine in Deutschland</b>	<b>5 Tage</b>	<b>€ 3.195,-</b>
<b>Termine in Österreich</b>	<b>5 Tage</b>	<b>€ 3.195,-</b>
<b>Online Training</b>	<b>5 Tage</b>	<b>€ 3.195,-</b>
<b>Termin/Kursort</b>	Kurssprache Deutsch	
23.06.-27.06.25	Frankfurt	22.09.-26.09.25  Online
23.06.-27.06.25	Online	27.10.-31.10.25  Online
11.08.-15.08.25	Hamburg	27.10.-31.10.25  Wien
11.08.-15.08.25	Online	15.12.-19.12.25  Frankfurt
22.09.-26.09.25	Frankfurt	15.12.-19.12.25  Online

Stand 26.03.2025



# Inhaltsverzeichnis

## Hacking II – Angriffe auf Endgeräte und Applikationen

<b>1 Der Hintergrund von Angriffen</b>	<b>3.5.2</b> Technische Maßnahmen	<b>6.7.2</b> Powershell Script Attacks
<b>1.1</b> Motivation zum Angriff	<b>3.5.3</b> Den Provider einbinden	<b>6.7.3</b> Powersploit
<b>1.1.1</b> Sabotage		<b>6.7.4</b> Powershell Attacks mit dem SEToolkit
<b>1.1.2</b> Spionage		<b>6.7.5</b> Client Side Powershell Attacks 1/3
<b>1.1.3</b> Missbrauch		<b>6.7.6</b> Powershell in Meterpreter 1/3
<b>1.2</b> Angriff – Viele Möglichkeiten	<b>4 Exploitation Attacks</b>	<b>6.7.7</b> Fileless Powershell Attacks
<b>1.2.1</b> DoS und DDoS	<b>4.1</b> Schwachstellen ausnutzen	<b>6.7.8</b> Empire
<b>1.2.2</b> Sniffing	<b>4.1.1</b> Schadhafte Programme	
<b>1.2.3</b> Social Engineering	<b>4.1.2</b> Buffer Overflows	
<b>1.2.4</b> Advanced Persistent Threats	<b>4.1.3</b> Fuzzing – Vulnerabilities erkennen	
<b>1.2.5</b> Exploitation	<b>4.2</b> Exploits verwenden	
<b>1.2.6</b> Kennwortangriffe	<b>4.2.1</b> Exploits erstellen (1/3)	
<b>1.3</b> Angriffe strukturiert durchführen	<b>4.2.2</b> Exploits herunterladen	
<b>1.3.1</b> Targets lokalisieren	<b>4.2.3</b> Exploits anpassen	
<b>1.3.2</b> Angriffsziel festlegen	<b>4.3</b> Exploitation Attacks mit Metasploit	
<b>1.3.3</b> Angriffsplan erstellen	<b>4.3.1</b> Exploit auswählen	
<b>1.3.4</b> Angriff ausführen	<b>4.3.2</b> Payloads zuweisen	
<b>1.3.5</b> Nachbereitung des Angriffs	<b>4.3.3</b> Die Attacke	
	<b>4.4</b> Zugriffsvarianten	
	<b>4.4.1</b> Der Shell Payload	
	<b>4.4.2</b> VNC – Grafischer Zugriff	
	<b>4.4.3</b> Meterpreter – Shell mit Erweiterungen	
<b>2 Metasploit – Das Angriffs-Rahmenwerk</b>	<b>5 Client Side Attacks</b>	
<b>2.1</b> Hintergründe zu Metasploit	<b>5.1</b> Social Engineering	
<b>2.1.1</b> Die Bedeutung von Ruby	<b>5.1.1</b> Mining – Personendaten ermitteln	
<b>2.1.2</b> Aufbau des Frameworks	<b>5.1.2</b> Phishing	
<b>2.1.3</b> Die Module im Dateisystem	<b>5.1.3</b> Vishing	
<b>2.2</b> Interfaces zum Framework	<b>5.1.4</b> Smishing	
<b>2.2.1</b> Armitage	<b>5.1.5</b> Einen Webserver nutzen	
<b>2.2.2</b> Cobalt Strike	<b>5.1.6</b> Fake Domains	
<b>2.2.3</b> Metasploit Community / Pro	<b>5.2</b> Social Engineering Toolkit	
<b>2.2.4</b> Die Metasploit Konsole	<b>5.2.1</b> Fast-Track	
<b>2.3</b> Die Datenbank anbinden	<b>5.2.2</b> Social Engineering Attacks	
<b>2.3.1</b> Workspaces	<b>5.3</b> Client-Side-Angriffe mit Metasploit	
<b>2.3.2</b> Den Prompt anpassen	<b>5.3.1</b> Msfvenom – Payloads ausführbar	
<b>2.4</b> Informationsbeschaffung mit Metasploit	<b>5.3.2</b> Bösertige Dokumente erstellen (1/3)	
<b>2.4.1</b> Nach Targets scannen	<b>5.4</b> Veil Evasion	
<b>2.4.2</b> Einbinden externer Scans	<b>5.4.1</b> Die Konsole	
<b>2.4.3</b> Die Datenbank auslesen	<b>5.4.2</b> Malware erzeugen	
	<b>5.4.3</b> Malware verstecken (1/3)	
	<b>5.4.4</b> Hyperion	
	<b>5.4.5</b> Macros nutzen	
	<b>5.4.6</b> Shellter	
	<b>5.4.7</b> Backdoor Factory	
<b>3 Denial of Service</b>	<b>6 Post Exploitation</b>	
<b>3.1</b> Hintergründe von DoS und DDoS	<b>6.1</b> Nach dem Angriff	
<b>3.1.1</b> DoS vs. DDoS	<b>6.2</b> Privilege Escalation	
<b>3.1.2</b> Motivation des Angriffs	<b>6.2.1</b> Lokaler Exploit 1/3	
<b>3.1.3</b> Arten von Angriffern	<b>6.2.2</b> Post Exploitation Modul 1/3	
<b>3.2</b> Angriffsmethoden	<b>6.2.3</b> Privilege Escalation mit Meterpreter	
<b>3.2.1</b> Leitungen überlasten	<b>6.2.4</b> Privilege Escalation bei Windows 7, 8 und 10 (1/3)	
<b>3.2.2</b> Protokollabläufe stören	<b>6.3</b> Das System manipulieren	
<b>3.2.3</b> Systeme lähm legen	<b>6.4</b> Zugriff sicherstellen	
<b>3.2.4</b> Reflection-Angriffe	<b>6.4.1</b> Benutzer anlegen	
<b>3.3</b> Angriffsarten	<b>6.4.2</b> Backdoors bauen 1/3	
<b>3.3.1</b> IPv4-Angriffe	<b>6.5</b> Spuren verwischen	
<b>3.3.2</b> IPv6-Angriffe	<b>6.6</b> Informationen sammeln	
<b>3.3.3</b> TCP/UDP-Angriffe	<b>6.6.1</b> Lokale Kennwörter auslesen	
<b>3.3.4</b> Amplification Attack	<b>6.6.2</b> Applikations-Kennwörter	
<b>3.4</b> Angriffstools	<b>6.6.3</b> Meterpreter als Keylogger	
<b>3.4.1</b> ICMP, TCP und UDP missbrauchen	<b>6.6.4</b> ScreenDumps	
<b>3.4.2</b> Protokoll-Angriffe von Innen	<b>6.6.5</b> Sniffing	
<b>3.4.3</b> Historisch – Trinoo, Stacheldraht & Co.	<b>6.7</b> Powershell Attacks	
<b>3.4.4</b> Low Orbit Ion Cannon – LOIC & Co.	<b>6.7.1</b> Powershell Scripts	
<b>3.4.5</b> Slowloris & Co.		
<b>3.4.6</b> DDOSIM – Layer 7 DDOS Simulator		
<b>3.4.7</b> DAVOSET		
<b>3.4.8</b> DoS mit Metasploit		
<b>3.4.9</b> Bot-Netze nutzen		
<b>3.5</b> Schutz gegen DoS und DDoS		
<b>3.5.1</b> Systemeinstellungen anpassen		
		<b>7 Alternative Angriffswege</b>
		<b>7.1</b> USB-Angriffe
		<b>7.1.1</b> USB Drop Attacks
		<b>7.1.2</b> Keystroke Injection Attack
		<b>7.1.3</b> Rubber Ducky
		<b>7.1.4</b> Digispark
		<b>7.1.5</b> Bash Bunny
		<b>7.1.6</b> Überlast Angriffe
		<b>7.2</b> Mobile Endgeräte angreifen
		<b>7.2.1</b> Diebstahl oder Verlust
		<b>7.2.2</b> Kommunikationsbeziehungen attackieren
		<b>7.2.3</b> WLAN-Angriffe
		<b>7.2.4</b> Bluetooth-Angriffe
		<b>8 Webangriffe</b>
		<b>8.1</b> Web Attacks im Überblick
		<b>8.2</b> Server Side Attacks
		<b>8.2.1</b> Web Crawling
		<b>8.2.2</b> Web-Schwachstellen-Scanner
		<b>8.2.3</b> Web Security Proxies
		<b>8.2.4</b> Die Burp Suite
		<b>8.2.5</b> SQL Injection
		<b>8.3</b> Angriffe auf Clients
		<b>8.3.1</b> Cross Site Scripting (XSS)
		<b>8.3.2</b> Cross Site Request Forgery
		<b>8.3.3</b> Browser
		<b>8.3.4</b> Flash & Co
		<b>8.3.5</b> Das Beef Framework
		<b>9 Kennwortangriffe effektiv umsetzen</b>
		<b>9.1</b> Hintergründe
		<b>9.2</b> Offline Password Cracking
		<b>9.2.1</b> Hashdump
		<b>9.2.2</b> Mimikatz und Kiwi in Metasploit
		<b>9.3</b> Online Password Cracking
		<b>9.4</b> Password Sniffing
		<b>9.5</b> Wörterbücher verwenden
		<b>9.5.1</b> Default Passwords
		<b>9.5.2</b> Benutzerspezifische Kennwortlisten
		<b>9.5.3</b> Ein einfaches Wörterbuch erstellen
		<b>9.5.4</b> Hilfreiche Werkzeuge
		<b>9.6</b> Brute Force – Einfach nur raten
		<b>9.7</b> Rainbow Cracking
		<b>9.7.1</b> Rainbow Tables
		<b>9.7.2</b> Die Hintergründe verstehen
		<b>9.7.3</b> Rainbow Cracking in der Praxis
		<b>9.7.4</b> Schutz gegen Rainbow Cracking
		<b>9.8</b> Tools für Kennwort-Angriffe
		<b>9.8.1</b> John the Ripper
		<b>9.8.2</b> Hashcat
		<b>9.8.3</b> Cain and Abel
		<b>9.8.4</b> Hydra
		<b>9.8.5</b> Medusa

