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.

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.

Kursziel

Der Kurs vermittelt Ihnen ein fundiertes Verständnis moderner Sicherheitsmaßnahmen. Anhand verschiedener Angriffsarten und typischer Post-Exploitation-Methoden lernen Sie, Risiken realistisch einzuschätzen und ihre Netze gezielt widerstandsfähiger zu machen.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/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.

Premium Print Paket

Zu diesem Kurs können sie optional das hochwertige Premium Print Paket zum Preis von € 225,- (zzgl. MwSt) erwerben.

Training	Preise zzgl. MwSt.
Termine in Deutschland	**5 Tage CHF 3.515,-**
Termine in Österreich	**5 Tage CHF 3.515,-**
Online Training	**5 Tage CHF 3.515,-**

Termin/Kursort — Kurssprache Deutsch

30.11.-04.12.26	HY Online	14.06.-18.06.27	HY Online
30.11.-04.12.26	HY Wien	02.08.-06.08.27	HY München
15.02.-19.02.27	HY Hamburg	02.08.-06.08.27	HY Online
15.02.-19.02.27	HY Online	25.10.-29.10.27	HY Frankfurt
12.04.-16.04.27	HY Frankfurt	25.10.-29.10.27	HY Online
12.04.-16.04.27	HY Online	13.12.-17.12.27	HY Online
14.06.-18.06.27	HY Düsseldorf	13.12.-17.12.27	HY Wien

Stand 01.11.2026

Inhaltsverzeichnis

Hacking II – Angriffe auf Endgeräte und Applikationen

1 Der Hintergrund von Angriffen
1.1 Motivation zum Angriff
1.1.1 Sabotage
1.1.2 Spionage
1.1.3 Missbrauch
1.2 Angriff – Viele Möglichkeiten
1.2.1 DoS und DDos
1.2.2 Sniffing
1.2.3 Social Engineering
1.2.4 Advanced Persistent Threats
1.2.5 Exploitation
1.2.6 Kennwortangriffe
1.3 Angriffe strukturiert durchführen
1.3.1 Targets lokalisieren
1.3.2 Angriffsziel festlegen
1.3.3 Angriffsplan erstellen
1.3.4 Angriff ausführen
1.3.5 Nachbereitung des Angriffs

2 Metasploit – Das Angriffs-Rahmenwerk
2.1 Hintergründe zu Metasploit
2.1.1 Die Bedeutung von Ruby
2.1.2 Aufbau des Frameworks
2.1.3 Die Module im Dateisystem
2.2 Interfaces zum Framework
2.2.1 Armitage
2.2.2 Cobalt Strike
2.2.3 Metasploit Community / Pro
2.2.4 Die Metasploit Konsole
2.3 Die Datenbank anbinden
2.3.1 Workspaces
2.3.2 Den Prompt anpassen
2.4 Informationsbeschaffung mit Metasploit
2.4.1 Nach Targets scannen
2.4.2 Einbinden externer Scans
2.4.3 Die Datenbank auslesen

3 Denial of Service
3.1 Hintergründe von DoS und DDoS
3.1.1 DoS vs. DDoS
3.1.2 Motivation des Angriffs
3.1.3 Arten von Angreifern
3.2 Angriffsmethoden
3.2.1 Leitungen überlasten
3.2.2 Protokollabläufe stören
3.2.3 Systeme lahm legen
3.2.4 Reflection-Angriffe
3.3 Angriffsarten
3.3.1 IPv4-Angriffe
3.3.2 IPv6-Angriffe
3.3.3 TCP/UDP-Angriffe
3.3.4 Amplification Attack
3.4 Angriffstools
3.4.1 ICMP, TCP und UDP missbrauchen
3.4.2 Protokoll-Angriffe von Innen
3.4.3 Historisch – Trinoo, Stacheldraht & Co.
3.4.4 Low Orbit Ion Cannon – LOIC & Co.
3.4.5 Slowloris & Co.
3.4.6 DDOSIM—Layer 7 DDOS Simulator
3.4.7 DAVOSET
3.4.8 DoS mit Metasploit
3.4.9 Bot-Netze nutzen
3.5 Schutz gegen DoS und DDos
3.5.1 Systemeinstellungen anpassen
3.5.2 Technische Maßnahmen
3.5.3 Den Provider einbinden

4 Exploitation Attacks
4.1 Schwachstellen ausnutzen
4.1.1 Schadhafte Programme
4.1.2 Buffer Overflows
4.1.3 Fuzzing – Vulnerabilities erkennen
4.2 Exploits verwenden
4.2.1 Exploits erstellen (1/3)
4.2.2 Exploits herunterladen
4.2.3 Exploits anpassen
4.3 Exploitation Attacks mit Metasploit
4.3.1 Exploit auswählen
4.3.2 Payloads zuweisen
4.3.3 Die Attacke
4.4 Zugriffsvarianten
4.4.1 Der Shell Payload
4.4.2 VNC – Grafischer Zugriff
4.4.3 Meterpreter – Shell mit Erweiterungen

5 Client Side Attacks
5.1 Social Engineering
5.1.1 Mining – Personendaten ermitteln
5.1.2 Phishing
5.1.3 Vishing
5.1.4 Smishing
5.1.5 Einen Webserver nutzen
5.1.6 Fake Domains
5.2 Social Engineering Toolkit
5.2.1 Fast-Track
5.2.2 Social Engineering Attacks
5.3 Client-Side-Angriffe mit Metasploit
5.3.1 Msfvenom – Payloads ausführbar
5.3.2 Bösartige Dokumente erstellen (1/3)
5.4 Veil Evasion
5.4.1 Die Konsole
5.4.2 Malware erzeugen
5.4.3 Malware verstecken (1/3)
5.4.4 Hyperion
5.4.5 Macros nutzen
5.4.6 Shellter
5.4.7 Backdoor Factory

6 Post Exploitation
6.1 Nach dem Angriff
6.2 Privilege Escalation
6.2.1 Lokaler Exploit 1/3
6.2.2 Post Exploitation Modul 1/3
6.2.3 Privilege Escalation mit Meterpreter
6.2.4 Privilege Escalation bei Windows 7, 8 und 10 (1/3)
6.3 Das System manipulieren
6.4 Zugriff sicherstellen
6.4.1 Benutzer anlegen
6.4.2 Backdoors bauen 1/3
6.5 Spuren verwischen
6.6 Informationen sammeln
6.6.1 Lokale Kennwörter auslesen
6.6.2 Applikations-Kennwörter
6.6.3 Meterpreter als Keylogger
6.6.4 ScreenDumps
6.6.5 Sniffing
6.7 Powershell Attacks
6.7.1 Powershell Scripts
6.7.2 Powershell Script Attacks
6.7.3 Powersploit
6.7.4 Powershell Attacks mit dem SEToolkit
6.7.5 Client Side Powershell Attacks 1/3
6.7.6 Powershell in Meterpreter 1/3
6.7.7 Fileless Powershell Attacks
6.7.8 Empire

7 Alternative Angriffswege
7.1 USB-Angriffe
7.1.1 USB Drop Attacks
7.1.2 Keystroke Injection Attack
7.1.3 Rubber Ducky
7.1.4 Digispark
7.1.5 Bash Bunny
7.1.6 Überlast Angriffe
7.2 Mobile Endgeräte angreifen
7.2.1 Diebstahl oder Verlust
7.2.2 Kommunikationsbeziehungen attackieren
7.2.3 WLAN-Angriffe
7.2.4 Bluetooth-Angriffe

8 Webangriffe
8.1 Web Attacks im Überblick
8.2 Server Side Attacks
8.2.1 Web Crawling
8.2.2 Web-Schwachstellen-Scanner
8.2.3 Web Security Proxies
8.2.4 Die Burp Suite
8.2.5 SQL Injection
8.3 Angriffe auf Clients
8.3.1 Cross Site Scripting (XSS)
8.3.2 Cross Site Request Forgery
8.3.3 Browser
8.3.4 Flash & Co
8.3.5 Das Beef Framework

9 Kennwortangriffe effektiv umsetzen
9.1 Hintergründe
9.2 Offline Password Cracking
9.2.1 Hashdump
9.2.2 Mimikatz und Kiwi in Metasploit
9.3 Online Password Cracking
9.4 Password Sniffing
9.5 Wörterbücher verwenden
9.5.1 Default Passwords
9.5.2 Benutzerspezifische Kennwortlisten
9.5.3 Ein einfaches Wörterbuch erstellen
9.5.4 Hilfreiche Werkzeuge
9.6 Brute Force – Einfach nur raten
9.7 Rainbow Cracking
9.7.1 Rainbow Tables
9.7.2 Die Hintergründe verstehen
9.7.3 Rainbow Cracking in der Praxis
9.7.4 Schutz gegen Rainbow Cracking
9.8 Tools für Kennwort-Angriffe
9.8.1 John the Ripper
9.8.2 Hashcat
9.8.3 Cain and Abel
9.8.4 Hydra
9.8.5 Medusa

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch