



Ethical Hacking Advanced - Ethical Hacking Specialist CERT/EHS

Cyber Security und Hacking-Kenntnisse für Penetrationstester

Ethical Hacking Advanced ist unser 5-tägiger Aufbaukurs der sich gezielt an Fortgeschrittene und angehende Penetrationstester richtet. In diesem Hacking Kurs werden komplexe Angriffe gegen Windows-Server, Active Directory, Linux und Web Services behandelt und praktisch umgesetzt.

Außerdem werden Voice-over-IP, Bluetooth und RFID behandelt. Natürlich kommen aber auch die Klassiker Metasploit und Mimikatz nicht zu kurz.

Unser Experten-Zertifikat ermöglicht es Ihnen als Mitarbeiter Ihre Kompetenz im Umfeld Informationssicherheit eindeutig zu belegen.

Listenpreis

3.390,00 € exkl. MwSt

4.034,10 € inkl. MwSt

Dauer

5 Tage

Gebühr für Prüfungen/Examen

420,00 € exkl. MwSt / 499,80 € inkl. MwSt

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin



Manuela Krämer
Leitung
Informationssicherheit

Kontakt/Fragen:

m.kraemer@cbt-training.de

Telefon: +49 (0)89-4576918-12

Inhalte

Dieses Seminar richtet sich primär an Interessenten, die fortschrittliche Hacking-Techniken kennenlernen wollen. In diesem Workshop werden grundsätzliche Kenntnisse zu Portscanning, Vulnerability Scanning, Web Application Hacking und Exploit Frameworks vorausgesetzt und die Angriffe vertieft. In verschiedenen Übungsaufgaben müssen Sie Schwachstellen selbst identifizieren, einen geeigneten Angriff finden und diesen umsetzen.

Unterlagen und praktische Labs

Jeder Teilnehmer erhält die Schulungsunterlagen komplett mit Schulungspräsentation und ergänzenden Erklärungen sowie den Lab Guide, beides komplett in deutscher Sprache. Die Schulungsunterlagen werden kontinuierlich ergänzt und korrigiert, um auch aktuelle Themen abzubilden.

Alle Hacking-Tools werden in einer Umgebung mit verschiedenen virtuellen Maschinen praktisch eingesetzt, insbesondere können alle besprochenen Angriffe auch aktiv getestet und umgesetzt werden. Der Praxisanteil am Seminar beträgt ca. 50%.

Jeder Teilnehmer erhält außerdem einen Download-Link mit allen Hacking-Tools, um Angriffe auch auf den eigenen Systemen ausprobieren zu können

1. Tag

- **Port- und Vulnerability Scanning mit Kali Linux**
 - Port Scanning Wiederholung
 - Nmap Script Scanning
 - Vulnerability Scanning mit OpenVAS



- Praktischer Teil:
 - TCP- und UDP-Scanning mit Nmap
 - Script-Scanning mit Nmap (SNMP-Enumeration, Password Cracking, Vulnerability Detection)
 - Installation und Konfiguration von OpenVAS
 - Vulnerability Scanning mit OpenVAS
 - **Advanced Exploitation mit Metasploit**
 - Metasploit Exploits
 - Post Exploitation mit Metasploit
 - Funktionsweise des Meterpreter
 - Meterpreter-Module
 - Praktischer Teil:
 - Exploits und Exploit-Anpassung mit Metasploit
 - Privilege Escalation mit Metasploit
 - **Advanced Malware**
 - Powershell Malware
 - Obfuscated Malware
 - Praktischer Teil:
 - Malware Obfuscation mit msfvenom
2. Tag

- **Windows Server Hacking**
 - Funktionsweise der Namensdienste
 - Angriffe gegen LLMNR und MDNS
 - Funktionsweise von Shares
 - Angriffe gegen SMB
 - Angriffe gegen RDP
 - Angriffe gegen SQL
 - Praktischer Teil:
 - Name Service Spoofing mit Responder
 - SMB-Hash-Cracking mit Hashcat
 - SMB-Relay Angriff mit Metasploit
- **Windows Active Directory Hacking**
 - Kerberos-Authentifizierung
 - Praktischer Teil:
 - AD Enumeration mit Bloodhound

3. Tag

- **Angriffe gegen Webanwendungen**
 - Sicherheitsanalyse von Webanwendungen
 - Web Application Vulnerability Scanning
 - Passwort Cracking Angriffe
 - Praktischer Teil:
 - Passwort Brute Force mit OWASP ZAP
 - Passwort Brute Force mit Hydra
- **Advanced SQL Injection**
 - SQL-Injection
 - Advanced SQL Injection
 - Blind SQL Injection
 - PHP Shells
 - Praktischer Teil:
 - SQL-Injection mit OWASP ZAP
 - Blind SQL-Injection mit OWASP ZAP
- **Angriffe gegen Web Services APIs**
 - Funktionsweise von Web Services



- JSON-basierte Angriffe
- Brute Force Angriffe
- Praktischer Teil:
 - Import der Web API in OWASP ZAP
 - Angriffe gegen Web Services mit OPWAS ZAP

4. Tag

- **Angriffe in Netzwerken**
 - ARP-Spoofing
 - DHCP-Spoofing
 - Man-in-the-Middle-Angriffe
 - Spanning Tree Angriffe
 - Angriffe gegen SDN
 - Praktischer Teil:
 - ARP-Spoofing mit Ettercap
 - ARP-Spoofing mit Bettercap
 - TLS-Man-in-the-Middle mit SSLsplit
 - DHCP Starvation Angriff
- **Angriffe gegen VoIP**
 - Angriffe gegen VoIP-Devices und Asterisk
 - VoIP abhören
- **Angriffe gegen Firewall und VPN**
 - Tunnel durch die Firewall
 - Angriffe gegen IPsec und PPTP
 - Praktischer Teil:
 - Tunneling mit HTTP-Tunnel
- **Angriffe in IPv6-Netzwerken**
 - IPv6 Scanning
 - NDP Spoofing
 - Praktischer Teil:
 - IPv6-Scanning mit Nmap
 - IPv6-Angriffe mit dem THC IPv6 Attack Toolkit
- **Angriffe gegen IoT**
 - IoT Sicherheitskonzepte
 - Angriffe gegen SmartHome-Protokolle
- **Bluetooth und RFID Hacking**
 - Angriffe gegen Bluetooth
 - Angriffe gegen RFID

5. Tag

- **Unix Hacking**
 - Schwachstellen in Unix/Linux-Diensten (X11)
 - Angriffe gegen RPC-Dienste (NIS, NFS)
 - Linux Exploitnutzung
 - Kernel Based Rootkits unter Linux
 - Metasploit und Meterpreter auf Linux
 - Praktischer Teil:
 - Linux Enumeration mit Nmap
 - Angriffe gegen NFS
 - Angriffe gegen SSH Authorized_Keys
 - Linux Privilege Escalation
 - Post Exploitation mit Metasploit
 - Anwendung des Meterpreter
- **Planung und Durchführung von Penetrationstests**



- Notwendige vertragliche Vereinbarungen
- Vorgehensweisen und Methodiken
- Das Open Source Security Testing Methodology Manual (OSSTMM)
- Der OWASP Web Security Testing Guide (WSTG)

OPTIONAL: Prüfung im Anschluss CERT EHS

Ziele Vulnerability Checks und Penetrationstests dienen der Prüfung der Sicherheit Ihrer IT-Systeme. Selbstverständlich ist es oft notwendig, regelmäßig spezialisierte Penetrationstester zu beauftragen. Gleichzeitig ist jedoch sinnvoll, Wissen im eigenen Unternehmen aufzubauen. Einerseits können Sie die Qualität durchgeführter Penetrationstests und die tatsächlichen Risiken der aufgedeckten Schwachstellen besser bewerten. Andererseits können Sie vor der produktiven Inbetriebnahme wichtiger Systeme selbst prüfen, wie es um die Sicherheit bestellt ist. Neben klassischen Angriffen und Exploits werden auch exotischere Angriffe mit bössartiger Hardware und modifizierten Ladekabel, die sogar Mobilfunkgeräte angreifen, betrachtet und praktisch umgesetzt.

Der Hacking Kurs baut auf unserem 5-tägigen Ethical Hacking Basic auf. Ein Schwerpunkt des Kurses liegt auf der Vermittlung wichtiger technischer Hintergrunddetails zu Hacking-Tools und Exploits. Einzelne Übungsaufgaben müssen von den Teilnehmern vollständig selbst erarbeitet werden. Der Hacking Kurs setzt deshalb Kenntnisse von Nmap, Metasploit, Windows- und Linux-Grundlagen voraus.

Zielgruppe

- Das Hacking Seminar richtet sich an:
 - Penetrationstester
 - IT-Sicherheitsbeauftragte
 - IT-Sicherheitsberater
 - Systemadministratoren

in Unternehmen, die Informationssicherheitsrisiken auch aus der Sicht des Angreifers betrachten möchten, um ihre Server und ihr Unternehmen besser vor Angriffen schützen zu können.



Voraussetzungen

Für diesen Hacking Kurs sollten Sie die im Expert Hacking Specialist vermittelten Kenntnisse mitbringen. Grundlegende Programmierkenntnisse sind hilfreich.

Dieses Seminar ist NICHT für Einsteiger in das Thema Hacking geeignet.

Wenn Sie schon

- Kali installiert und einzelne Tools genutzt haben
 - mit Nmap ein Netz gescannt haben
 - Schwachstellen mit einem Vulnerability Scanner gefunden haben
 - mit ZAP oder Burp Suite eine Formulareingabe geprüft haben
 - Little Bobby Tables kennen
 - ein einfaches PowerShell Skript programmiert haben
- dann sind Sie in diesem Kurs richtig.

Kenntnisse aus folgenden Kursen der CBT oder vergleichbare Hacking Grundlagen Kenntnisse:

- Expert Hacking - Angriffsszenarien und Gegenmaßnahmen
- Ethical Hacking Basic - White Hat Hacker
- CEH EC Council - ältere Versionen
- Metasploit (in Verbindung mit weiteren Hack Grund-Kenntnissen)

Im Hacking Kurs verpflichten Sie sich, die neu erworbenen Fähigkeiten nicht für rechtswidrige oder böswillige Angriffe zu verwenden, die Tools nicht zur Schädigung von Computersystemen einzusetzen und die CBT für den (beabsichtigten oder unbeabsichtigten) Missbrauch dieser Tools zu entschädigen.



Prüfung/Zertifizierung

CERT EHS Ethical Hacking Specialist - Ethical Hacking Advanced

Prüfung am 5. Seminartag, deutsch

1. Teil Prüfung: Multiple-Choice 60 Minuten

2. Teil Prüfung: Freitext 30 Minuten

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice/Freitext Prüfung. Die **CBT CERT Prüfung** wird direkt nach Kursende abgenommen. Sie gilt als bestanden, wenn mindestens 70% der Fragen richtig beantwortet wurden.

Nach Bestehen der Prüfung erhalten Sie ein personenbezogenes **CBT CERT Zertifikat**, das Ihnen die erfolgreiche Kursteilnahme inklusive bestandener Prüfung bestätigt.

Hat ein Teilnehmer die **CBT CERT Prüfung** nicht bestanden, so kann er diese entweder direkt im Anschluss an die erste Prüfung oder während unserer Öffnungszeiten Online Live mit Prüfungsüberwachung (Kamerapflicht, MS-Teams) nach vorheriger schriftlicher Anmeldung (mind. 14 Tage vor Termin) gegen die genannte Prüfungsgebühr wiederholen.

Die Prüfung kann höchstens 2-mal wiederholt werden. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Gültigkeit CBT CERT:

Das **CBT CERT ZERTIFIKAT** ist 3 Jahre gültig und muss anschließend durch eine erneute Prüfung bei CBT Training & Consulting GmbH aktualisiert / verlängert werden.

Alle Prüfungsunterlagen werden 3 Jahre aufbewahrt.