



Ethical Hacking Basic - White Hat Hacker CERT/WHH

Cyber Security und Hacking-Kenntnisse für IT-Sicherheitsbeauftragte und Penetrationstester

Ethical Hacking Basic WHH ist unser 5-tägiger Kurs der sowohl für Einsteiger als auch Fortgeschrittene geeignet ist. Kein anderer Hacking Kurs bietet Ihnen in einer Woche einen so umfangreichen und vollständigen Themeneinblick.

In 18 Modulen werden Port- und Vulnerability Scanning mit Nmap und Nessus, Exploit Frameworks und Post Exploitation am Beispiel von Metasploit sowie Social Engineering und Schadprogramme behandelt. Neben vielen anderen werden Angriffe gegen Windows mit Mimikatz, gegen Netzwerk mit ARP-Spoofing und gegen Webanwendungen mit dem ZAP Attack Proxy praktisch durchgeführt. Wireless LAN Hacking, Denial-of-Service Angriffe und Mobile Hacking runden das Thema ab. Außerdem werden in einem Ausblick zukünftige Risiken wie KI und Quantencomputer angesprochen.

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

390,00 € exkl. MwSt / 464,10 € inkl. MwSt

Prüfungsversicherung

159,00 € exkl. MwSt / 189,21 € 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

In diesem 5-tägigen Hacking Seminar erhalten Sie in einem intensiven Workshop einen einzigartigen Einblick in die Motive sowie die Taktiken, Techniken und Prozeduren (TTP) der Angreifer. Der Hacking Kurs steigt tief in alle aktuellen Themen ein und lässt keine Wünsche offen.

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 speziellen Schulungs-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



- **Rechtliche Bewertung des Hackings**
 - Strafrechtliche Bewertung von Angriffen
 - Einordnung des § 202c und Eigenschutz
 - Internationales Recht
- **Angreifer und Motive**
 - Hacker, Cracker und die Szene
 - Motive von Angreifern
- **Vorgehensweise und Schwachstellen**
 - Hacking Cycle
 - Vorgehensweise von Angreifern
 - CVE und CVSS
 - Typische Sicherheitslücken und Programmierfehler
 - OWASP TOP 10 Sicherheitslücken
 - MITRE ATT&ACK
 - Praktischer Teil:
 - Auswertung von Schwachstellen mit CVE und CVSS
 - Zuordnung von Angriffen mit Hilfe von MITRE ATT&ACK
 - Suche nach Exploits für vorhandene Schwachstellen
 - Zugriff auf das Darknet mit dem TOR-Browser
- **Linux Hacking Distributionen**
 - Kali Linux
 - Praktischer Teil:
 - Optional Installation von Kali Linux
- **Informationsbeschaffung (Footprinting)**
 - Informationsbeschaffung mit öffentlich zugänglichen Mitteln
 - Vertrauliche Daten in Suchmaschinen
 - Google Dorks
 - Praktischer Teil:
 - Identifikation von Angriffszielen mittels DNS
 - Zuordnung der IP-Adressen anhand der RIPE-Datenbank
 - Nutzung spezieller Google- und Bing-Suchanfragen zur Informationsbeschaffung
 - Nutzung von Online-Diensten zur Informationsbeschaffung (Netcraft, Robtex)

2. Tag

- **Port Scanning**
 - Scan-Techniken unter Windows
 - Portscanning und Fingerprinting
 - Portscanning mit Nmap
 - Scanning mit IKE-Scan und SNMP-Scan
 - Praktischer Teil:
 - Sweep Scanning mit Nmap
 - TCP Portscanning mit Nmap
 - UDP Portscanning mit Nmap
 - Verschiedene Scan-Optionen (z.B. -O -A -F)
 - Alternativen zu Nmap (SuperScan, Unicorn-Scanner)
 - Traceroute mit Nping
- **Vulnerability Scanning**
 - Vulnerability Scanning mit Nessus
 - Auswertung von Scan-Ergebnissen und dienstspezifischer Informationen
 - Praktischer Teil:
 - Installation von Nessus
 - Konfiguration von Nessus Scan-Profilen für das Scannen
 - Vulnerability Scan mit Nessus
 - Auswertung der Ergebnisse



- **Technische Grundlagen von Exploits**
 - Buffer Overflows und Schutzmaßnahmen
 - Race Conditions
- **Exploits und Exploit Frameworks**
 - Webseiten mit Exploits (Exploit-DB et. al.)
 - Exploit-Frameworks
 - Bedienung von Metasploit
 - Post-Exploitation mit Metasploit
 - Praktischer Teil:
 - Nutzung der Ergebnisse von Nmap und Nessus für die Exploit-Vorbereitung
 - Nutzung eines Exploits zum Einbruch in Windows 10
 - Verwendung von Post Exploitation Modulen mit dem Meterpreter
 - Auslesen der SAM mit Mimikatz
 - Cracken der Passwörter mit John the Ripper und Cain&Abel

3. Tag

- **Social Engineering**
 - Einführung in Social Engineering
 - Praktischer Teil:
 - Social Engineering mit Gophish
- **Viren, Trojaner, Schadsoftware**
 - Viren und Trojaner selbst basteln
 - Client-Side Exploits
 - Botnetze
 - Schwachstellen in Virencannern
 - Praktischer Teil:
 - Test verdächtiger Programme mit Virustotal.com
 - Erzeugen eines Trojaners zum Tarnen der Schadsoftware basierend auf Netbus
 - Veränderung von Schadprogrammen zum Täuschen von Virencannern
 - Trojanisierung von Programmen mit msfvenom
 - Einbetten von Schadsoftware in ein PDF
 - Einbetten des Meterpreters als Makro in ein Word-Dokument
- **Angriffe gegen Windows Systeme**
 - Enumeration von Benutzern und Diensten unter Windows
 - NetBIOS-spezifische Schwachstellen
 - Passwörter auslesen und Lateral Movement (Mimikatz)
 - Spuren verwischen und Hintertüren installieren
 - Praktischer Teil:
 - Windows Enumeration mit SuperScan
 - Auslesen des LSA Cache mit Cain&Abel
 - Auslesen der SAM und Logonpasswörter mit Mimikatz
 - Cracken der Passwort-Hashes
- **Angriffe gegen Windows Server-Dienste**
 - Gezielte Ausnutzung von fehlkonfigurierten Diensten und Anwendungen
 - Angriffe gegen Microsoft SQL-Server
 - Angriffe gegen Domain Controller (DSInternals, BloodHound)
 - Pass-the-Hash Angriffe
 - Offline Angriffe
 - Praktischer Teil:
 - Offline Angriffe gegen AD mit DSInternals
 - Pass-the-Hash Angriff mit Metasploit
 - Analyse der AD-Sicherheit mit BloodHound

4. Tag



- **Angriffe in Netzwerken**
 - ARP-Spoofing
 - Man-in-the-Middle-Angriffe
 - Abhören von Passwörtern
 - Passwort Cracking
 - Praktischer Teil:
 - ARP-Spoofing mit Cain&Abel
 - ARP-Spoofing mit Bettercap
 - Sniffing mit Cain&Abel und Wireshark
- **DoS-/DDoS-Angriffe**
 - Denial-of-Service Angriffe
 - Distributed Denial-of-Service Angriffe
 - Amplification Attacks
 - Praktischer Teil:
 - Denial-of-Service Angriffe mit Mausezahn
- **Wireless LAN Hacking**
 - WEP Cracking
 - WPA/WPA2 Cracking
 - Sicherheit von WPA3
 - Praktischer Teil:
 - WLAN-Analyse mit Kismet
 - Abhören der Kommunikation mit airodump-ng
 - Replay-Angriffe mit aireplay-ng
 - WEP-Cracking mit aircrack-ng
 - WPA-Cracking mit Hashdump

5. Tag

- **Angriffe gegen Webanwendungen**
 - Sicherheitsanalyse von Webanwendungen
 - Sichere TLS-Verschlüsselung
 - SQL-Injection
 - Command Injection
 - Cross Site Scripting und Cross Site Request Forgery
 - Praktischer Teil:
 - Angriffe gegen Webanwendungen mit dem OWASP Zed Attack Proxy (ZAP)
 - Fuzzing von Formularfeldern mit dem OWASP Zed Attack Proxy (ZAP)
 - Demonstration von Angriffen anhand der DVWA
 - Erkennung und Ausnutzung von Cross Site Scripting (XSS) Angriffen
 - Erkennung und Ausnutzung von SQL-Injection Angriffen
 - Auslesen der SQL-Datenbank mit sqlmap
 - Analyse von Wordpress mit WPscan
 - Brute Force Angriffe gegen Webanwendungen mit Hydra
- **Angriffe gegen Mobile Devices**
 - Mobile Hacking
 - Malicious Apps
 - Angriffe gegen Android
- **Aktuelle Trends**
 - Aktuelle Risiken und Gefahren
 - Blick in die Zukunft

OPTIONAL: Prüfung im Anschluss CERT WHH



Ziele

IT-Systeme und IT-Infrastrukturen sind auf vielfältige Art bedroht. Es genügt nicht mehr, nur Firewall und Virenschutz im Auge zu behalten. Moderne Schadprogramme tarnen sich klug vor Virenschaltern. Netzwerke werden angegriffen und abgehört. Schwachstellen in Windows-Servern und Webanwendungen werden rücksichtslos ausgenutzt. Unsichere oder falsch konfigurierte Wireless LAN Netze dienen als Einfallstor an der Firewall vorbei. Sie als Verteidiger müssen alle Lücken erkennen und schließen. Ein Angreifer muss dagegen nur eine einzige offene Lücke finden und kann damit hohen Schaden anrichten.

Ein Schwerpunkt des Hacking-Kurses liegt deshalb auf der Vermittlung wichtiger technischer Hintergrunddetails zu Hacking-Tools und Exploits. Neben der Vorgehensweise in aktuellen Angriffen lernen Sie, mit verbreiteten Hacking-Tools und vielen verschiedenen Techniken umzugehen, um die Sicherheit Ihrer Systeme zu testen und Schutzmaßnahmen verbessern zu können.

Zielgruppe

- **Das Seminar richtet sich an:**
 - Systemadministratoren
 - Netzwerkadministratoren
 - Web-Administratoren
 - IT-Sicherheitsbeauftragte
 - IT-Sicherheitsberater

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

Sie sollten grundsätzliche Kenntnisse als Windows-Systemadministrator sowie über TCP/IP-basierte Netzwerke und Webanwendungen mitbringen, um maximalen Nutzen aus diesem Seminar zu ziehen. Programmierkenntnisse sind hilfreich jedoch nicht erforderlich.

Der Kurs ist für "Einsteiger" in das Thema Hacking geeignet.

Nachfolgende Kurse können Sie als Aufbaukurse nutzen:

- Ethical Hacking Advanced - Ethical Hacking Specialist CERT/EHS
- Zertifizierung zum Technical Security Analyst - Pentester CERT /TSA
- Pentest Pro Akademie by CBT

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 WHH White Hat Hacker - Ethical Hacking Basic

Prüfung am 5. Seminartag, deutsch
Multiple-Choice 60 Minuten

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice 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.

Prüfungsversicherung zum CBT CERT:

Haben Sie zum Kurs und zur Prüfungsgebühr unsere Prüfungsversicherung bestellt, berechtigt diese zur **einmaligen kostenfreien Prüfungswiederholung** zu o.g. Bedingungen. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Ohne Prüfungsversicherung zahlen Sie bei Wiederholung die volle Prüfungsgebühr.

Gültigkeit CBT CERT ZERTIFIKAT:

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.
