Ethical Hacking Basic - White Hat Hacker CERT/WHH

Angriffsszenarien und Gegenmaßnahmen
Werden Sie White-Hat-Hacker um den Black-Hat-Hacker zu verstehen und die richtigen Gegenmaßnahmen zum Schutz Ihrer Unternehmenssicherheit ergreifen zu können. Lernen Sie vom Experten, wie Sie Ihr Unternehmen vor böswilligen Angriffen schützen.

Zertifikat "White Hat Hacker - Ethical Hacking Basic"

Unser Experten-Zertifikat, das die Teilnehmer nach bestandener Prüfung erhalten, ermöglicht es erfahrenen Beratern und Mitarbeitern im Umfeld der IT-Sicherheit, ihre Kompetenz eindeutig zu belegen.

Listenpreis
3.290,00 € exkl. MwSt
3.915,10 € 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
CBT-Remote-Lab-Umgebungen für die Kursteilnehmer:
Die Labs werden über unser sicheres Schulungsnetzwerk, auch für die Online Live Teilnehmer, durchgeführt. Die Teilnehmer müssen somit keinerlei Software für den Kurs installieren, da sie auf unser Netz über einen Browser auf den Kurs zugreifen.

- Deutsche Kursunterlagen
- Prüfung: 1 Stunde Multiple-Choice
- Hacking Zertifikat nach Bestehen: White Hat Hacker CERT/WHH

Jeder, der seine IT-Infrastruktur schützen will, muss sowohl die Schwachstellen vor Ort als auch die potentiellen Angreifer (Black Hat Hacker) kennen. Abwehrstrategien können deshalb nur dann wirksam sein, wenn man die Bedrohungen realistisch einschätzen kann und die Methoden und Vorgehensweisen der Angreifer kennt. Werden Sie White-Hat-Hacker und schützen Sie so Ihr Unternehmen!

Jeder Teilnehmer erhält zum Manuskript (DEUTSCH) u.g. Labs sowie Infos zu wertvollen "Werkzeugen".
Praxis-Workshop LABS - Cyber Security Offense/Defense
Erfolgreiche Abwehr von Hacker-Angriffen / Cyber-Angriffen und sicherer Schutz Ihres Netzwerks!

Viele Hacking Angriffe und Labs auf Netzwerk-Komponenten runden das Seminar ab. **Das Seminar wird stets den aktuellen Anforderungen angepasst.** Diverse LABs werden während der Schulung von allen Teilnehmern über unser Schulungs-Labor durchgeführt und anschließend besprochen, diskutiert.

- **1. Tag**
- **Recht**
  - Strafrechtliche Bewertung von Angriffen
- **Einführung**
  - Wer sind die Angreifer? - Organisation und Struktur
  - Begriffsdefinitionen der Szene - Skript Kiddies und Profihacker
- **Vorgehensweise**
  - Vorgehensweise von Angreifern (Hacking Cycle)
  - Sicherheitslücken und Schwachstellendatenbanken - CVE, OWASP
- **Informationsbeschaffung (Footprinting)**
  - Informationsbeschaffung mit öffentlich zugänglichen Mitteln
  - Google Hacking (Google Dorks)

- **2. Tag**
- **Port Scanning**
  - Scan-Techniken unter Windows
  - Portscanning und Fingerprinting
  - Portscanning mit Nmap
  - Alternative Scanner - SuperScan, IKE-Scan, SNMP-Scan
- **Vulnerability Scanning**
  - Vulnerability Scanning mit Nessus
  - Auswertung von Ergebnissen und dienstspezifischer Informationen
- **Exploits**
  - Buffer Overflows und Exploits - Ursachen und Funktionsweise
- **Exploit Frameworks (Penetration)**
  - Nutzung von Exploits zur Kompromittierung von Windows Systemen
  - Exploit Frameworks am Beispiel von Metasploit

- **3. Tag**
- **Social Engineering**
  - Angriffe auf Mitarbeiter
- **Malicious Code**
  - Viren und Trojaner
  - Rootkits
  - Client-side Exploits
- **Hacking Hardware**
  - Rubber Ducky & Co.
- **Windows Schwachstellen**
  - Windows Architektur und Design, Gruppenrichtlinien
  - Enumeration von Benutzern und Diensten unter Windows
  - NetBIOS-spezifische Schwachstellen (Exploits, IPC, Admin Shares)
  - Auslesen von Zugangsdaten (LSA Cache, Mimikatz, Lateral Movement)
  - Gezielte Ausnutzung von fehlkonfigurierten Diensten und Anwendungen
  - AD-/RDP-/SQL-spezifische Schwachstellen

- **4. Tag**
- **Netzwerkangriffe**
  - Angriffe gegen Netzwerkkomponenten
  - Sniffing und Passwörter abhören
  - Password Cracking
  - Man-in-the-Middle Angriffe
- **Denial of Service Angriffe**
  - DoS und DDoS
  - Amplification Attacks

- **Wireless LAN Hacking**
  - WLAN-Sicherheit
  - WEP Cracking
  - WPA Cracking

- **5. Tag**
- **Angriffe gegen Webanwendungen**
  - Schwachstellen in der Verschlüsselung (TLS)
  - Sicherheitsanalyse von Webanwendungen
  - Cross-Site Scripting und Cross-Site Request Forgery
  - SQL-Injection, Command Injection
- **Mobile Devices**
  - Angriffe gegen Android
  - Angriffe gegen iOS
  - Mobile Malware
  - Mobilgeräte als Hacking-Devices
- **Aktuelle Trends**
  - Angriffe gegen CPUs
  - In the News
- **Multiple-Choice Prüfung CERT WHH**
  - Prüfungsvorbereitung
  - anschließend 60 Minuten Multiple-Choice Prüfung deutsch

Weiterführende Kurse:
Für eine Beratung rufen Sie uns gerne an!

- Ethical Hacking Advanced
- IT-Forensik
- Advanced Privacy & Counter Surveillance Training
- IT-GRC Governance, Risk & Compliance Management Systems
- Technical Security Analyst (Pentester)
- CCS Cloud Computing
- SIEM / PKI Verschlüsselung
- Change Management

Ziele

Die Teilnehmer arbeiten in einer LAB-Umgebung und Testen selbst. 40-50% Praxisanteil in der Schulung.

- Verstehen der Angriffsverfahren aktueller Hacker
- Lernen und Anwenden der Hacker-Methodik
- Identifizieren von Schwachstellen im Netzwerk
- Anwenden vorhandener Hacker-Tools
- Durchführen von Angriffen und Exploits
- Absichern von Rechnern

Ein Schwerpunkt des Kurses liegt auf der Vermittlung wichtiger technische Hintergrunddetails zu Hacker-Tools und Exploits.

Der Hacking Zertifizierungskurs umfasst Angriffe gegen Windows Server und Clients, die im Übungsnetzwerk in voller Länge durchgeführt werden.

Angefangen mit der Informationsbeschaffung über Scannen der Systeme, Eindringen in Server einer DMZ bis zur Erlangung von Root-Rechten und Installation einer Hintertür werden alle Themen behandelt.

Zielgruppe

System- und Netzwerk-Administratoren sowie IT-Sicherheitsbeauftragte und IT-Manager, die Security-Risiken aus der Sicht des Angreifers betrachten und dadurch effiziente Lösungsszenarien aufbauen möchten um ihr Unternehmen besser vor Angriffsszenarien schützen zu können.

Voraussetzungen

Gute Kenntnisse in der Administration von Windows-Systemen sowie der Funktionsweisen der Kommunikationsprotokolle im Internet (TCP/IP) sind von Vorteil. Programmiersprache 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 Academie by CBT

Prüfung/Zertifizierung

CERT WHH White Hat Hacker - Ethical Hacking Basic
Multiple-Choice Prüfung, deutsch

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.
