Cyber Security Analyst CERT/CSA

Penetration Tester - Planung, Durchführung, Assessments.
Im Seminar werden allgemeine Vorgehensweisen bei der Planung, Durchführung und Dokumentation von Security Assessments, Security Audits und Penetrationstests behandelt.

Zertifikat "Technical Security / Cyber Security Analyst"
Unser Experten-Zertifikat 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
420,00 € exkl. MwSt / 499,80 € 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

Ihr Ansprechpartner


Manuela Krämer
Leitung
Informationssicherheit

Kontakt/Fragen:
m.kraemer@cbt-training.de
Telefon: +49 (0)89-4576918-12

Inhalte
Zum Einsatz kommen gängige Open Source Tools und kommerzielle Werkzeuge wie KALI Linux, Metasploit Framework, Nmap, Nessus, Wmap, Nikto u.a.

Tag 1 bis Tag 4 Penetrationstest Theorie & Praxis
Referent Senior Security Consultant & Pentester (Profil unter Dozent)

- **Inhaltsübersicht**
  - Theoretische Grundlagen
  - Umgang mit den technischen Werkzeugen
  - Best Practices und Vorgehensmodelle
  - Übungen und Labs

- **Theoretische Grundlagen**
  - Arten von Sicherheitsprüfungen
  - Kennzeichnende Eigenschaften dieser Sicherheitsprüfungen
  - Security Audit
  - Vulnerability Assessment
  - Penetrationstest
  - Source Code Analyse und Reverse Engineering
  - Informationsquellen und Internet-Recherche
  - Phasenmodell für das Vorgehen
  - Einführung in das technische Penetrationstesting / Vorbereitung eines Penetrationstests
- **Technische Werkzeuge und deren Gebrauch**
  - KALI Linux mit diversen Tools

  - Tenable Nessus und OpenVAS
  - Wmap und Nikto
  - Password-Cracking
  - Grundlagen Metasploit
- **Praxisübungen & Labs nach Phasen**
  - Footprinting: Vorgehen und Werkzeuge
  - Scanning: Vorgehen und Werkzeuge
  - Enumeration: Vorgehen und Werkzeuge
  - Exploitation: Vorgehen und Werkzeuge
  - Post-Entry: Datensammlung und Beweissicherung
- **Praxisübungen & Labs am Beispiel**
  - Durchführen der Phasen innerhalb der Laborumgebung
  - Durchführen der Phasen in der Praxis
  - Anpassung an lokale Gegebenheiten
  - Datensammlung und -korrelation
  - Erkennen falscher Positiver und falscher Negativer
  - Auflösen von widersprüchlichen Ergebnissen
  - Empfehlungen zur Berichterstellung
- **Durchführung nach der BSI Penetrationstest-Studie**
  - Aufbau und Inhalt der Penetrationsteststudie
  - Folgerungen für das eigene Vorgehen
  - Stärken und Schwächen des Modells
  - Durchführung nach Penetrationsteststudie
- **Durchführen und Vorgehen nach OSSTMM**
  - Aufbau und Inhalt des Manuals
  - Reporting Templates
  - Risk Assessment Value
  - Folgerungen für das eigene Vorgehen
  - Stärken und Schwächen des Manuals
  - Durchführung nach dem OSSTMM
- **Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)**

5. Tag Aktuelle rechtliche Betrachtung & Rechtsfallen mit Rechtsurteilen
Referent Rechtsanwalt

- **Einführung in das Recht der IT-Sicherheit**
- **Technische, organisatorische, strategische und rechtliche Aspekte der IT-Sicherheit**
- **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**
- **IT-Compliance im Detail**
- **Datenschutz BDSG und informationelles Selbstbestimmungsrecht**
- **IT-Sicherheit und Hackertools**
- **Maßgebliche Rechtsbereiche für Penetrationstests u.a.**
  - § 202a StGB "Ausspähen von Daten"
  - § 202b StGB "Abfangen von Daten"
  - § 202c StGB "Hackerparagraph"
  - § 204 StGB "Verwertung fremder Geheimnisse"
  - § 206 StGB "Verletzung des Post- oder Fernmeldegeheimnisses"
  - § 263 StGB "Computerbetrug"
  - § 303a StGB "Datenveränderung"
  - § 303b StGB "Computersabotage"
- **Insb. datenschutzkonforme Protokollierung / Logfiles**
- **Lösungsansätze**
- **Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)**

Alternative zum Kurs oder Erweiterung:
Kompakt-Ausbildung in der Pentesting Pro Academy der CBT. Rufen Sie bei Interesse gerne an oder klicken Sie auf:
Übersicht zur Gesamtzertifizierung

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

- IT-Forensik
- Advanced Privacy & Counter Surveillance Training
- IT-GRC Governance, Risk & Compliance Management Systems
- Ethical Hacking Basic
- Ethical Hacking Advaced
- CCS Cloud Computing
- SIEM / PKI Verschlüsselung
- Change Management

Ziele

Im Seminar werden allgemeine Vorgehensweisen bei der Planung, Durchführung und Dokumentation von Security Assessments, Security Audits und Penetrationstests behandelt. Als Grundlage dienen neben zahlreichen Referenz-Standards (z.B. ISO 2700x) die Penetrationstest-Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und das international anerkannte Open Source Security Testing Methodology Manual (OSSTMM).

Am 1. Kurstag werden v.a. theoretische Aspekte wie z.B. Planung, Durchführung von vor Ort Assessments und Dokumentation behandelt.

Der Schwerpunkt am 2. Tag liegt v.a. in der Durchführung von technischen Assessments und Penetrationstests unter Normalbedingungen. Hierbei werden eine Vielzahl von Angriffen praktisch ausgeführt, die aus dem Internet gegen Systeme gerichtet werden können. Der Fokus liegt dabei auf der Erkennung und Bewertung von Sicherheitslücken und weniger im konkreten Einbrechen.

Am 3. Tag liegt der Schwerpunkt auf der Auswertung der am Vortag gewonnen Ergebnisse. Erfahrungsgemäß ist die Bedienung der Scanner nach einer guten und fundierten Einführung weniger problematisch als die nachfolgende Interpretation der Ergebnisse. Da der Abschlussbericht auch das Endergebnis (also das Produkt) eines Penetrationstests, Audits oder Assessments ist, müssen hier prägnant und nachvollziehbar alle Schwächen aufgelistet und bewertet werden. Darüber hinaus müssen Handlungsanweisungen zur Behebung der Schwächen präsentiert werden.

Der 4. Tag des technischen Teils beschäftigt sich mit den Besonderheiten und Ausnahmen. Hier hat der Teilnehmer die Möglichkeit, tiefergehende Werkzeuge kennen zu lernen, die über das Maß des normalen Audits hinausgehen.

Der 5. Tag befasst sich mit den rechtlichen Rahmenbedingungen von Security Assessments im Allgemeinen und Penetration Tests im Besonderen. Bei der technischen Ausführung von Security Assessments ist eine Vielzahl an rechtlichen Anforderungen zu beachten, um einer Strafbarkeit oder Schadensersatzpflicht entgegenzuwirken. Zusammen mit dem Teilnehmer werden die einschlägigen Strafrechtsnormen erörtert. Im Bereich des Zivilrechts werden häufige Haftungsfallen aufgezeigt und Lösungsmöglichkeiten zur Risikominimierung dargestellt. Es werden Wege der zivilrechtlichen Absicherung im Unternehmen und als Freiberufler aufgezeigt.

Zielgruppe

- IT-Manager, Führungskräfte und Mitarbeiter des IT-Sicherheitsmanagements, Leiter der IT-Sicherheit
- zukünftige IT-Sicherheitsbeauftragte, Systemadministratoren, Penetrationstester
- sowie Mitarbeiter der IT die diese Funktionen übernehmen sollen.

Voraussetzungen

Die Teilnehmer sollten über grundlegende Kenntnisse in Netzwerktechnologien mit Schwerpunkt TCP/IP verfügen. Gute Anwenderkenntnisse von Windows- und Linux-Systemen sollten vorhanden sein. Kenntnisse aus dem Bereich der Systemverwaltung sind hilfreich.

Dieser Kurs stellt die Basis für Penetrationstests und ist somit auch für nicht so technisch versierte Teilnehmer geeignet.

Prüfung/Zertifizierung

CERT CSA Cyber Security Analyst

Prüfung, deutsch
1. Part Dauer 45Minuten Multiple-Choice
2. Part IT-Recht 20 Minuten Multiple-Choice

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.
