



## Technical Security Analyst CERT/TSA

**Penetration Tester - Planung, Durchführung, Assessments.**

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

Intensiv-Ausbildung Pentesting Spezialist in der Pentesting Pro Academy der CBT. [Übersicht zur Pentesting Pro Academy Gesamtzertifizierung](#)

**Deutsche Kursunterlagen / 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

3.390,00 € exkl. MwSt

4.034,10 € 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

### Ihre Ansprechpartnerin



**Manuela Krämer**  
Leitung  
Informationssicherheit

### Kontakt/Fragen:

[m.kraemer@cbt-training.de](mailto:m.kraemer@cbt-training.de)

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

## Inhalte

Dieses Training vermittelt das vollständige Wissen zur Durchführung erster eigener Penetrationstests, Vulnerability Assessments oder auch Security Audits.

Neben den technische Grundlagen werden auch die wichtigsten rechtlichen Aspekte und Notwendigkeiten vermittelt.

Zudem werden verbreitete Best-Practices vorgestellt und deren Inhalte erläutert.

Der große Praxisteil, bei dem zentrale Tools aus KALI Linux beispielhaft erklärt und praktisch benutzt werden, rundet das Training ab.

- **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
- **Rechtliche Grundlagen**



- Rechtliche Aspekte der IT-Sicherheit
- Haftung und Vertraulichkeitserklärung
- Testrelevante "Hackerparagrafen"
- Wichtige Artikel der DSGVO
- **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)**

### Weiterführende Kurse:

- Kompakt-Ausbildung in der Pentesting Pro Academy der CBT. [Übersicht zur Pentesting Pro Academy Gesamtzertifizierung](#)



### Ziele

Im Seminar Technical Security Analyst 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)**.

Im Kurs Technical Security Analyst werden alle relevanten **theoretischen und rechtlichen Aspekte** wie z.B. Planung, Durchführung oder Haftung von vor Ort Assessments und die erforderliche Dokumentation behandelt.

Der Schwerpunkt 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.

Weitere Schwerpunkte liegen 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 letzte Part 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.

---

### 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 Technical Security Analyst stellt die Basis für Penetrationstests und ist somit auch für nicht so technisch versierte Teilnehmer geeignet.

---



### Prüfung/Zertifizierung

CERT TSA Technical Security Analyst

Prüfung, deutsch

Dauer 90 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.

---