PPA 4 KALI Aufbau

Pentesting Pro Academy by CBT-Training
Professional IT Security Expert - PITSE

Die komplette Zertifizierungsreihe besteht aus 17 Tagen in Einzel-Terminblöcken und sollte in einem Zeitrahmen von 2 Jahren absolviert werden um das Gesamtzertifikat "Professional IT Security Expert" zu erhalten.
Status-Zertifikate werden direkt nach jeweiliger bestandener Prüfung ausgestellt.
Übersicht zur Gesamtzertifizierung

Alle Einzelkursthemen können ohne Zertifizierung (Prüfung) auch außerhalb der PITSE-Zertifizierungsreihe absolviert werden. Beachten Sie hierfür bitte die Kursvoraussetzungen zur Teilnahme oder rufen Sie uns für eine Beratung an.

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
1.550,00 € exkl. MwSt
1.844,50 € inkl. MwSt

Dauer
2 Tage

Gebühr für Prüfungen/Examen
250,00 € exkl. MwSt / 297,50 € inkl. MwSt

Prüfungsversicherung
79,00 € exkl. MwSt / 94,01 € 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
CERT Technical Security Testing mit Kali Linux 4 Tage PPA 3 + PPA 4
Status Paket-Buchungen erhalten auf die Einzel-Kurspreise einen Rabatt von 10%.
Prüfung Multiple-Choice im PPA 4

- Vermittlung des Praxiswissens für den effizienten Einsatz gegen ausgewählte Targets
  - Hinweise zum Labor
  - Weitere Werkzeuge
  - Praktischer Einsatz der Werkzeuge
  - Kombinieren des Werkzeugeinsatzes
  - Fallbeispiele mit steigendem Schwierigkeitsgrad

SEMINARINHALTE PPA 4

- Laborumgebung
  - Online-Übungsziele
  - Hinzufügen weiterer Ziele im Labor

    - Metasploitable 3
- Komplexere Fallbeispiele
    - Behandelte Werkzeugauswahl
    - Netcat & Co
        - Netcat
        - Socat
        - Powercat
    - Paketanalyse
        - Wireshark
        - Tcpdump
    - Shell-Scripting
        - Variablen
        - Kontrollstrukturen
        - Tests
    - Umgang mit Vulnerability Scannern
        - Nessus
        - OpenVAS
    - Passwortangriffe
        - Wörterlisten
        - Online / Offline
        - Hashes und Rainbowtables
    - NetBIOS und SMB
        - Discovery und Scanning
        - Gebrauch der Tools
        - Typische Schwächen
        - Ein- und Ausgabeumlenkung
        - UNIX Philosophie und Architektur
    - Vulnerabilities und Exploits
        - CVE Details
        - Exploit DB
        - GHDB und Shodan
- Schwerpunkte der Fallbeispiele
    - Encoding und Decoding
    - Cracking und Guessing
    - Versteckte Informationen
    - Einfaches Debugging
    - Port-Knocking
    - Datei- und Dump-Analyse

Ziele

ALLE KURSE AUS DER REIHE KÖNNEN OHNE ZERTIFIZIERUNG AUCH ALS EINZELNE KURSE GEBUCHT WERDEN.

PPA 3 führt an KALI Linux heran und grundlegende, enthaltene Tools werden besprochen und benutzt (Fokus: Pentesting).

PPA 4 baut auf PPA 3 auf; es werden fortgeschrittene Tools behandelt und auch ein Ausblick auf Debugging und Programmierung wird gegeben. Alternativ kann man als aktiver KALI Nutzer auch hier einsteigen (Linux Kenntnisse sind hier ein MUSS).

Ziele und Nutzen der Pentesting Pro Academy

Diese modulare Ausbildungsreihe (PPA 1 - 8) soll dem Einsteiger einen vollständigen Ausbildungsweg in das interessante und vielschichtige Gebiet der technischen IT-Sicherheit (Cyber-Security) bieten. Dabei kann der Teilnehmer selbst die Geschwindigkeit und Frequenz des Fortschreitens bestimmen und sich immer weiter fordern ohne überfordert zu werden.

Die bewusst offensive Ausrichtung der Trainingseinheiten schafft die Grundlage für effektive Abwehr- und Verteidigungsstrategien (Cyber-Defense). "Knowing Your Enemy" ist unabdingbare Voraussetzung für jeden Administrator, SOC-Mitarbeiter, Incident Responder oder Malware-Analysten.

Selbstverständlich stellt diese Ausbildungsfolge auch einen perfekten Start für jeden dar, der auf dem Gebiet des Penetration Testing erfolgreich arbeiten möchte.

Die einzelnen Module (PPA) bauen aufeinander auf und sind so strukturiert, dass nahezu keine Überlappung oder Wiederholung enthalten ist. Aus diesem Grund müssen die Module in entsprechender Reihenfolge und auch im nötigen Umfang bearbeitet werden.

Zwischen den einzelnen Modulgruppen sind Prüfungen angesiedelt, die den Lernerfolg prüfen und sicherstellen. In den späteren Prüfungen werden auch praktische Leistungen erwartet.

Da jeder erfolgreiche Abschluss einer Modulgruppe mit einem Zertifikat der entsprechenden Stufe belohnt wird, kann jeder Teilnehmer selbst bestimmen, wie weit er oder sie sich selbst fordert.

Don't hesitate, challange Yourself!

Zielgruppe

Teilnehmer der Pentesting Pro Academy by CBT-Training

- Zukünftige Penetrationstester
- Mitarbeiter aus Administration, Netzwerk und SOC
- Mitarbeiterausbildung für IT-Security
- Strafverfolgungsbehörden und Angehörige von Cyber-Defense/Offense Einheiten

... und alle Personen, die sich für die Einzel-Modul Inhalte Step 1- Step 4 interessieren.

Wenn Sie die Gesamt-Zertifizierung nicht anstreben, können Sie auch mit entsprechendem Basis-Wissen diese einzelnen Step Module ohne Prüfung absolvieren.

Voraussetzungen

BRONZE-STATUS der AUSBILDUNGSREIHE
Diese Stufe ist auf den Praxisgebrauch von KALI Linux mit den darin enthaltenen Tools fokussiert.

Voraussetzungen:

- Seminar PPA 1 und PPA 2 Grundlagen Pentesting
- Seminar PPA 3 KALI Grundlagen: Umgang mit Kali, Kenntnis wichtiger Kali Tools
- Umgang mit Kali und Kenntnis wichtiger Kali Tools
- weitere hilfreiche Kenntnisse sind:
  - Betriebssystemkenntnisse (MS Windows, Linux, etc.)
  - Sicherheitsbewusstsein ((C)ISO, SiBe, Penetrationstester, Administrator, etc.)
  - Weiteres IT-Wissen (Programmierung, Netzwerke, Web-Technologie, etc.)

CBT Kunden, die unseren Kurs "Metasploit Expert Training auf Kali Linux (Aufbau)" absolviert haben, können direkt die BRONZE PRÜFUNG "Technical Security Testing mit Kali Linux" absolvieren und anschl. den Silber Status mit Kursen belegen.

Prüfung/Zertifizierung

Pentesting Pro Academy - BRONZE STATUS
Prüfung "CERT Technical Security Testing mit Kali Linux"

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.
