Pentesting Pro Academy Paket C - PPA 1-8

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

14.200,00 € exkl. MwSt

16.898,00 € inkl. MwSt

Dauer

17 Tage

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

Paketangebot für die Ausbildungsreihe
Paketpreis 17 Schulungtage inkl. 4 Prüfungen (Gebühren enthalten) inkl. Schulungsunterlage pro PPA-Kursmodul

Details zu den PPA-Kursen und Terminreihen entnehmen Sie bitte der Seite: Pentesting Pro Academy

CERT Basic Security Testing
PPA 1 + PPA 2 nur Virtual Classroom LIVE
Prüfung Multiple-Choice im PPA 2

CERT Technical Security Testing mit Kali Linux
PPA 3 + PPA 4 Virtual Classroom LIVE oder Präsenz
Prüfung Multiple-Choice im PPA 4

CERT Exploitation mit Metasploit
PPA 5 + PPA 6 Virtual Classroom LIVE oder Präsenz
Prüfung Multiple-Choice & Praxis-Test im PPA 6

CERT Advanced Development / Reversing & Sophistic Exploitation ODER CERT Web Exploit Analysis & Development
PPA 7 - PPA 8 Virtual Classroom LIVE oder Präsenz
Prüfung Multiple-Choice & Praxis-Test im PPA 8

SEMINAR-INHALTE PPA 1: Penetrationstest Grundlagen Theorie

- Theoretische Grundlagen und Begriffe
- Arten technischer Sicherheitsprüfungen
- Voraussetzungen für die Durchführung
- Systematische Vorgehensmodelle
- Berichterstellung

SEMINAR-INHALTE PPA 2: Vorgehensmodelle Pentesting

- BSI Penteststudie
- OSSTMM
- CIS 18

SEMINAR-INHALTE PPA 3: KALI Grundlagen

- Grundlegende Informationen
- GNU-Linux-Debian-Kali
- Kali Tools
- Workshops Metasploitable 2 + 3

SEMINAR-INHALTE PPA 4: KALI Aufbau

- Laborumgebung
- Netcat & Co
- Paketanalyse
- Shell-Scripting
- Umgang mit Vulnerability Scannern
- Passwortangriffe
- NetBIOS und SMB
- Vulnerabilities und Exploits
- Exemplarische Behandlung ausgesuchter Tools

SEMINAR-INHALTE PPA 5: Metasploit Framework

- Einführung
- Metasploit-Framework und -Pro
- Architektur und Bestandteile
- Bedienung und Befehle
- Job- und Sessionmanagement
- Datenmanagement
- Payloads
- Sondermodule
- Ausführliches Fallbeispiel

SEMINAR-INHALTE PPA 6: Fortgeschrittener Einsatz von Metasploit / Exploitation mit Metasploit

- Metasploit Module
- PoC-Entwicklung

SEMINAR-INHALTE PPA 7: Exploit Development & Tools

- Tool Case
- Praxis
- Beispielszenario
- Einfache Schwachstellen und deren Exploitation

SEMINAR-INHALTE PPA 8A: Advanced Development / Reversing & Sophistic Exploitation

- Typische Schwachstellen und deren Exploitation

- Umgehen von Schutzmaßnahmen
- Reversing
- Weitere Werkzeuge
- Beispielszenarien

ODER

SEMINAR-INHALTE PPA 8B: Web Exploit Analysis & Development

- Tool Case
- Umgehen von client-seitigen Schutzeinrichtungen
- Angriff auf die Authentisierung
- Unterwandern des Session Managements
- Aushebeln der Zugriffskontrolle
- Analyse und Auslesen von Datenspeichern
- Verstehen und Ausnutzen der Applikationslogik
- Automatisieren von Angriffen
- Finden von Schwächen im Quelltext

Ausführlichere Seminarinhalte finden Sie in den jeweiligen Einzelmodulen.

Ziele

PPA 1 behandelt das allgemeine Vorgehen bei der Durchführung technischer Sicherheitsüberprüfungen

PPA 2 behandelt verbreitete Vorgehensweisen bei der Durchführung technischer Sicherheitsüberprüfungen auf Basis anerkannter Best Practices. Voraussetzung hierfür ist das Verständnis des allgemeinen Vorgehens bei der Durchführung technischer Sicherheitsüberprüfungen oder gleichwertige Praxiserfahrung.

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

PPA 4 baut auf 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).

PPA 5 erklärt Architektur und Bedienung von Metasploit anhand zahlreicher, praktischer Übungen

PPA 6 baut auf 5 auf und zeigt fortgeschrittene Möglichkeiten von Metasploit genauso wie Ansätze zur Automatisierung und Individualisierung

PPA 7 führt in den Entwicklungsprozess ein und stellt typische Unterstützungswerkzeuge und deren Gebrauch vor.

PPA 8Abeschäftigt sich mit der Umgehung von Schutzmaßnahmen, Reverse Engineering, Disassembling, Decompiling und komplexeren Exploits (als PPA 7). Voraussetzung: PPA 7.

ODER

PPA 8B beschäftigt sich mit Web-Exploitation, dem Umgehen von Schutzmaßnahmen, Fuzzing und Reverse Engineering. Voraussetzung: PPA 7..

Ziele und Nutzen der Pentesting Pro Academy
Diese modulare Ausbildungsreihe (PPA 1 - PPA 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´s) 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, die sich für das Thema Penetrationstest interessieren.

Voraussetzungen

Hier kann jeder einsteigen, auch technisch nicht ganz so versierte Teilnehmer, da PPA 1- PPA 2 die Basic vermittelt.

- Hilfreich
  - Betriebssystemkenntnisse (MS Windows, Linux, etc.)
  - Sicherheitsbewusstsein ((C)ISO, SiBe, Penetrationstester, Administrator, etc.)
  - Weiteres IT-Wissen (Programmierung, Netzwerke, Web-Technologie, etc.)

Weitere Kursvoraussetzung für die Ausbildungsreihe Pentesting Pro Academy by CBT-Training:
Ausbildung im Bereich der IT oder vergleichbare Kenntnisse,
sichere Bedienung von Betriebssystemen (Windows, Linux) auf Anwenderniveau und Netzwerkgrundkenntnisse.

Prüfung/Zertifizierung

Pentesting Pro Academy - GOLD Status
Prüfung 1 BASIC "CERT Basic Security Testing" im PPA 2
Prüfung 2 BRONZE "CERT Technical Security Testing" im PPA 4
Prüfung 3 SILBER "CERT Exploitation mit Metasploit" im PPA 6
Prüfung 4 GOLD "CERT Advanced Development / Reversing & Sophistic Exploitation" im PPA 8A ODER "CERT Web Exploit Analysis & Development" im PPA 8B
CERT 1-3 führt zum Gesamt-Zertifikat "Associate Penetration Tester"CERT 1-8 führt zum Gesamt-Zertifikat "Professional IT Security Expert"
