



PPA 8 A Advanced Development / Reversing & Sophistic Exploitation

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 Zeitraum 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

1.950,00 € exkl. MwSt

2.320,50 € inkl. MwSt

Dauer

3 Tage

Gebühr für Prüfungen/Examen

490,00 € exkl. MwSt / 583,10 € 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 Advanced Exploitation und Development 6 Tage PPA 7 - PPA 8
Status Paket-Buchungen erhalten auf die Einzel-Kurspreise einen Rabatt von 10%.
Prüfung Multiple-Choice & Praxis-Test

SEMINAR-INHALTE PPA 8 A

- Typische Schwachstellen und deren Exploitation
 - Structured Exception Handler
 - Return Oriented Programming
- Umgehen von Schutzmaßnahmen
 - ASLR
 - Stack Cookies
 - DEP und HW DEP
 - Egghunter
- Reversing
 - Umgang mit Debugger und Disassemble
 - Black-Box Analysetechniken
- Weitere Werkzeuge
 - Tools für Patching und HEX Tools
 - Decodieren von Dateiformaten
 - Analyse von Code und Datenstrukturen



- Beispielszenarien
 - Analyse der Applikationen
 - Analyse von Schutzeinrichtungen und Malware
 - Auffinden der Schwachstelle
 - Entwickeln des Exploits

Ziele

Ein Seiteneinstieg in PPA 8 ist nicht möglich!

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

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

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

O D E R

PPA 8 B 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 - 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, challenge 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

Voraussetzungen

GOLD-STATUS der AUSBILDUNGSREIHE

Diese finale Stufe beschäftigt sich nicht mehr mit der Benutzung fertiger Werkzeuge, sondern leitet zur eigenständigen Exploit-Entwicklung an.

Der Teilnehmer besitzt ausreichende Erfahrung bei der Durchführung von Pentests, gutes Netzwerkwissen und idealerweise Programmiererfahrung.

Ein Seiteneinstieg in PPA 8 ist nicht möglich!

Kursvoraussetzungen:

- Professional Security Expert (Silber)
 - Penetrationstest Grundlagen Theorie PPA 1 & PPA 2 (Basic)
 - Theoretisches Vorgehensmodell
 - BSI Penteststudie, OSSTMM, CIS Controls
 - Umgang mit Linux / Kali Linux PPA 3 & PPA 4 (Bronze)
 - Kenntnis und Anwendung wichtiger Kali Tools
 - Umgang mit Metasploit Framework PPA 5 & PPA 6 (Silber)
 - Benutzung und Bedienung des Metasploit Frameworks
 - Fortgeschrittener Einsatz des Frameworks
 - Grundverständnis der Funktionsweise von Exploits
 - Exploit Development & Tools PPA 7
- Hilfreich:
 - Betriebssystemkenntnisse (MS Windows, Linux, etc.)
 - Sicherheitsbewusstsein ((C)ISO, SiBe, Penetrationstester, Administrator, etc.)
 - Weiteres IT-Wissen (Programmierung, Netzwerke, Web-Technologie, etc.)



Prüfung/Zertifizierung

Pentesting Pro Academy - GOLD STATUS

Prüfung "CERT Advanced Development / Reversing & Sophistic Exploitation" Dauer 4 Stunden

GESAMTZERTIFIKAT nach bestandenen Prüfungen von Basic bis Gold

CBT CERT "Professional IT Security Expert - PITSE"

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice/Freitext 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 jederzeit 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.

Gültigkeit CBT CERT:

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.
