Zertifizierungsweg

- **Basic**
  - 2 Tage + Abschlusstest (T)
- **Bronze**
  - 4 Tage + Abschlusstest (T)
- **Silber**
  - 5 Tage + Abschlusstest (T+P)
- **Gold**
  - 6 Tage + Abschlusstest (T+P)

T: Theorie- / P: Praxisprüfung

Stand Juni 2023

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.

Interessenten, die entsprechendes Vorwissen mitbringen, können in dieser Ausbildungsreihe quer einsteigen bzw. ohne Zertifizierungsziel auch Einzelkurs-Module absolvieren.

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.

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. Die Teilnehmer erhalten für jeden PPA-Modulkurs eine personalisierte Teilnehmerbestätigung mit Kursinhalten.

"Don’t hesitate, challange Yourself!"

PPA 1 - Penetrationstest Grundlagen Theorie

Dauer: 1 Tag

- **Theoretische Grundlagen und Begriffe**
  - Ziele der IT-Sicherheit
  - "Hackerslang"
- **Arten technischer Sicherheitsprüfungen**
  - Security Audit
  - Vulnerability Assessment
  - Penetrationstest
- **Voraussetzungen für die Durchführung**
  - Klärung der Haftung
  - Risiken bei der Durchführung
  - Abgrenzung und Zieldefinition
  - Non Disclosure Agreement
- **Systematische Vorgehensmodell**
  - Reconnaissance
  - Attack Surface Detection
  - Enumeration
  - Vulnerability Detection
  - Exploitation
  - Escalation
  - Pillage
- **Berichterstellung**
  - Gliederung und Inhalt
  - Beweissicherung
  - Protokollierung
  - Dos und Don'ts

PPA 2 Vorgehensmodelle Pentesting

Dauer: 1 Tag, CERT Basic Status zum Kursende (optional)

- **BSI Penteststudie**
  - **Übersicht über die Dokumente beim BSI**
    - Durchführungskonzept für Pentests
    - Praxis-Leitfaden für Pentests
    - Praxis-Leitfaden für Webcheck
  - **Gliederung und Aufbau des DF-Konzepts**
    - Einleitung und Zielsetzung, IT-Sicherheit
    - Rechtliche Überlegungen und Bedingungen
    - Durchführung
    - Anhang
  - **Gliederung und Aufbau PL-Pentest**
    - Voraussetzungen (organisatorisch, fachlich)
    - Ablauf
    - Anhang
- **Gliederung und Aufbau PL-Webcheck**
  - Einleitung
  - Voraussetzungen (organisatorisch, fachlich)
  - Ablauf und Durchführung
  - Anhang
- **Praxisrelevanz**
  - Gebrauch der drei Dokumente
  - Vorgehen gemäß BSI-Vorgaben
  - Querverbindungen zu anderen Vorgehensmodellen
- **OSSTMM**
  - Aufbau der Module
  - Human Security Testing
  - Physical Security Testing
  - Wireless Security Testing
  - Telecommunications Security Testing
  - Data Networks Security Testing
- **CIS 18**

PPA 3 - KALI Grundlagen

Dauer: 2 Tage

- **Grundlegende Informationen**
  - Beschaffung und Installation
  - Geschichte und Überblick
  - Labor und Virtualisierung
- **GNU-Linux-Debian-Kali**
  - Entwicklung
  - Wichtige Befehle
  - Demos und Übungen
  - File-System und Software-Pakete
- **Kali Tools**
  - Kali Meta-Packages
  - Ausgewählte Tools
  - Demos und Übungen
- **Workshops**
  - Metasploitable2
  - Metasploitable3

PPA 4 - KALI Aufbau

Dauer: 2 Tage, CERT Bronze Status zum Kursende (optional)

- **Laborumgebung**
  - Online-Übungsziele
  - Hinzufügen weiterer Ziele im Labor
  - Verschiedene Target VMs
- **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

PPA 5 – Metasploit Framework

Dauer: 2 Tage

- **Einführung**
- **Metasploit-Framework und -Pro**
  - Übersicht und Struktur des Frameworks
  - Besonderheiten innerhalb KALI
- **Architektur und Bestandteile**
  - Philosophie
  - Modultypen
  - Schnittstellen
  - Erweiterungen
- **Bedienung und Befehle**
  - Hilfe zur Selbsthilfe
  - CLI Komandos
  - Grafische Benutzeroberfläche
  - Moduloptionen
- **Job- und Sessionmanagement**
  - Möglichkeiten
  - Nutzung
- **Datenmanagement**
  - Anbinden und Nutzen einer Datenbank
  - Verzeichnisstruktur
- **Payloads**
  - Shells
  - Reverse-Shells
  - Commands
  - Post-Exploitation
  - Standalone Payloads
- **Sondermodule**
  - Generic Listener
  - Breakpoint
- **Ausführliches Fallbeispiel Workshop**
  - Metasploitable 3

PPA 6 – Fortgeschrittener Einsatz von Metasploit

Dauer: 3 Tage, CERT Silber Status zum Kursende (optional)

- **Grundlagen**
  - Rechnerarchitektur und Speichermanagement
  - Debugger inkl. Plugin
  - Maschinensprache und Assembler
- **Metasploit-Tools**
  - pattern_create und pattern_offset
  - nasm_shell
  - msfvenom
- **PoC-Entwicklung**
  - Grundlagen Python
  - Befehle und Kontrollstrukturen
  - Verstehen von fertigen PoC's
  - Entwickeln neuer Exploits
  - Zusammenarbeit in der Community
- **Metasploit Module**
  - Grundlagen Ruby
    - Variablen
    - Klassen und Methoden
    - Befehle und Kontrollstrukturen
  - Verstehen bestehender Module
  - Anpassen von Modulen
  - Konvertieren von "Fremd"-Exploits
  - Entwickeln eigener Module
  - Zusammenarbeit in der Community
- **Fallbeispiele**
  - Einsatz von Metasploit
- **Prüfungsvorbereitung**
  - Wiederholung
  - Fallbeispiel

PPA 7 – Exploit Development & Tools

Dauer: 3 Tage

- **Einstieg**
  - CWE, CVE
  - Testing
- **Fuzzing**
  - Grundlagen
  - Tools und Ressourcen
  - Guided Lab und Labs
- **Exploiting**
  - Mona PyScript
  - Developer-Module & Tools MSF
  - Buffer Overflow
  - Format String Exploits
  - SEH-Exploits

Im letzten Modul wählen Sie zwischen 8A oder 8B Ihr Thema aus um zur Gesamt-Zertifizierung zu gelangen.

PPA 8A Advanced Development / Reversing & Sophistic Exploitation

Dauer: 3 Tage, CERT Gold Status zum Kursende (optional)

- **Einführung**
  - Ausgangssituation
  - Entwicklungsgeschichte
  - Web-Sicherheit bis dato
- **Grundlegende Verteidigungsmechanismen**
- **Aktuelle Technologien**
  - Client- und serverseitig
  - Header und Statuscodes
  - Codierung
- **Analyse der Angriffsfläche**
  - Tools
  - Web-Spidering
  - Durchführung und Ziele
- **Umgehen clientseitiger Kontrollen**
  - Abfangen und Manipulieren von Daten
  - Verschleierung und Verschlüsselung
  - Browser-Erweiterungen
- **Angriffe auf die Authentisierung**
  - Fehlerquellen und Ansatzpunkte

PPA 8B – Web Exploit Analysis & Development

Dauer: 3 Tage, CERT Gold Status zum Kursende (optional)

- **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

Ausführliche Informationen und Kurstermine finden Sie unter:
https://www.cbt-training.de/zertifizierungen/pentesting-pro-academy.html

Manuela Krämer

Leitung Informationssicherheit
Beratung / Vertrieb / Consulting

Telefon +49 89 4576918-12

Mail: m.kraemer@cbt-training.de

CBT Training & Consulting GmbH
Elektrastraße 6 a, D - 81925 München
Telefon +49 (0)89 4576918-0

beratung@cbt-training.de
www.cbt-training.de
www.it-informationssicherheit.de
www.secuta.de

Ich erstelle mit Ihnen gemeinsam Ihren terminlichen Zertifizierungsplan.
Rufen Sie mich gerne an.