



Kali Linux Einführung & Aufbau

Vermittlung des Basiswissens für den effizienten Einsatz einer auf Penetrationstests spezialisierten Plattform und des Praxiswissens für den effizienten Einsatz gegen ausgewählte Targets.

Listenpreis

3.100,00 € exkl. MwSt

3.689,00 € inkl. MwSt

Dauer

4 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

Modul 1 Kali Linux Einführung

- **Vermittlung des Basiswissens für den effizienten Einsatz einer auf Penetrationstests spezialisierten Plattform**
 - Installation, Wartung und Konfiguration
 - Struktur und Aufbau
 - LINUX Betriebssystem-Kenntnis und -Verständnis
 - Übersicht über die enthaltenen Werkzeuge
 - Praxiseinsatz der Werkzeuge an Beispielen
- **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
 - Viele diverse Demos und Übungen
- **Workshops**
 - Metasploitable2
 - Metasploitable3

Modul 2 Kali Linux Aufbau

- **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

- **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

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

Weiterhin werden fortgeschrittene Tools behandelt sowie ein Ausblick auf Debugging und Programmierung gegeben.

Zielgruppe

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

Voraussetzungen

- **Penetrationstest Grundlagen**
 - **Vorgehensmodelle Pentesting**
 - **weitere hilfreiche Kenntnisse sind:**
 - Betriebssystemkenntnisse (MS Windows, Linux, etc.)
 - Sicherheitsbewusstsein ((C)ISO, SiBe, Penetrationstester, Administrator, etc.)
 - Weiteres IT-Wissen (Programmierung, Netzwerke, Web-Technologie, etc.)
-