

PPA 3 KALI Grundlagen (S3KG)

ID S3KG Price on request Duration 2 days

Who should attend

- 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.

Prerequisites

[PPA 1 Penetrationstest Grundlagen Theorie \(S1PTGT\)](#) und [PPA 2 Vorgehensmodelle Pentesting \(S2VMPT\)](#)

Course Objectives

Diese modulare Ausbildungsreihe 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 (Steps) 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 sich selbst fordert.

Course Content

Vorüberlegungen

- Virtualisierung
- Laboraufbau

Beschaffung und Installation

- Quellen und Integritätsprüfung
- Direkt / Virtualisiert / USB

Linux Grundlagen

- Hilfe zur Selbsthilfe
- Shell
- Wichtige Kommandos
- Ein- und Ausgabeumlenkung
- Editoren
- UNIX Philosophie und Architektur

Aktualisierung und Wartung

- Paketmanagement

Konfiguration und Überwachung

- Prozesse und Logdateien

Übersicht über die Werkzeuggruppen

- Reconnaissance
- Scanning
- Vulnerability Detection
- Exploitation
- Passwortangriffe
- WLAN-Angriffe

- Web-Angriffe
- Forensik
- Reverse Engineering

Exemplarische Behandlung ausgesuchter Tools

- Maltego und recon-ng
- Nmap
- Aircrack-Suite

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>