PPA 4 KALI Aufbau (S4KA)

ID S4KA **Preis** auf Anfrage **Dauer** 2 Tage

Zielgruppe

- 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 PPA 1-PPA 4 interessieren.

Voraussetzungen

- PPA 1 Penetrationstest Grundlagen Theorie (S1PTGT)
- PPA 2 Vorgehensmodelle Pentesting (S2VMPT)
- PPA 3 KALI Grundlagen (S3KG)

Kursziele

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.

Kursinhalt

Laborumgebung

- Online-Übungsziele
- Hinzufügen weiterer Ziele im Labor
- Metasploitable 3

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

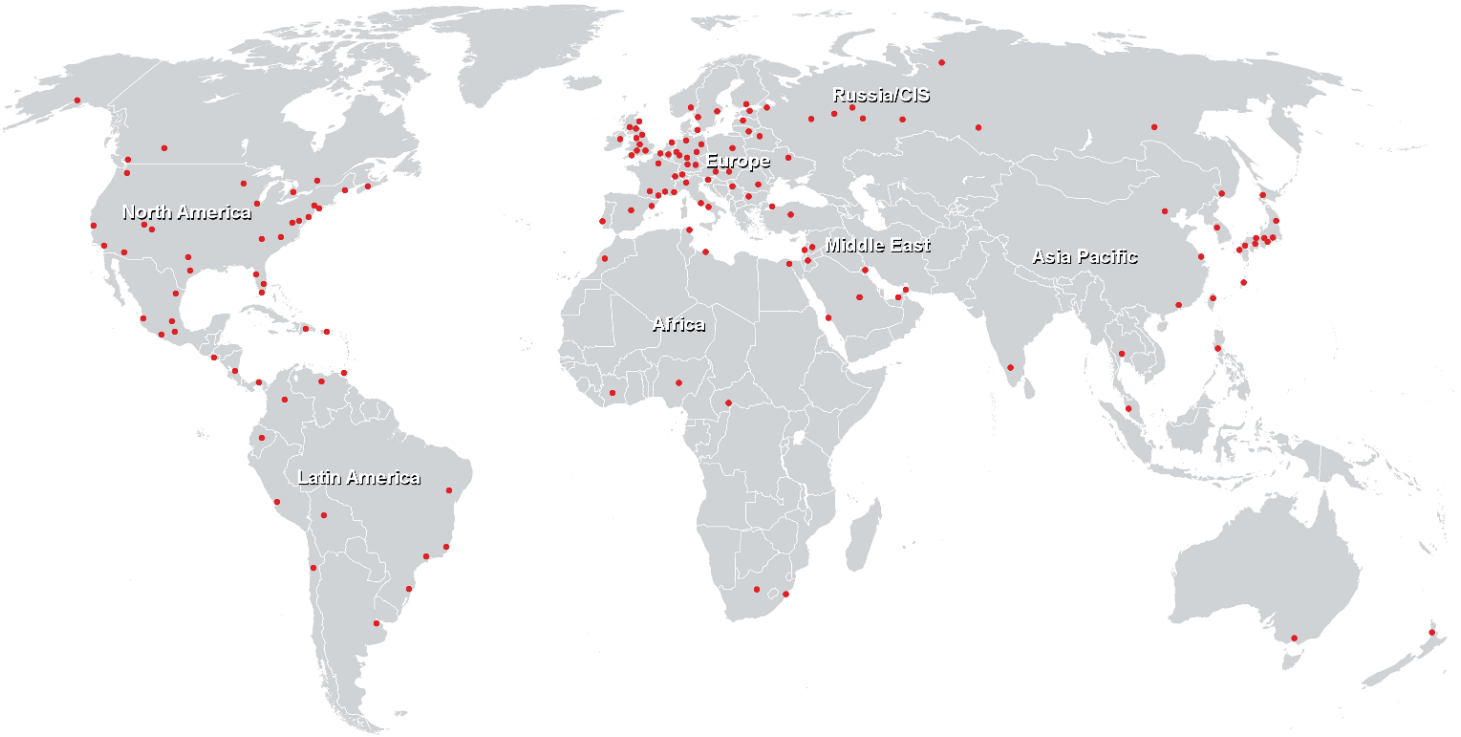
Vulnerabilities und Exploits

- CVE Details
- Exploit DB
- GHDB und Shodan

Exemplarische Behandlung ausgesuchter Tools

PPA 4 KALI Aufbau (S4KA)

Weltweite Trainingscenter



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