Kali Linux - Effizienter Einsatz für Pentrationstests (KLEPT)

ID KLEPT **Price** on request **Duration** 4 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 Interessierten

Prerequisites

- Penetrionstest 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.)

Course Objectives

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

Course Content

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 im Workshop Charakter mit Metaslpoittable 1 und 2

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

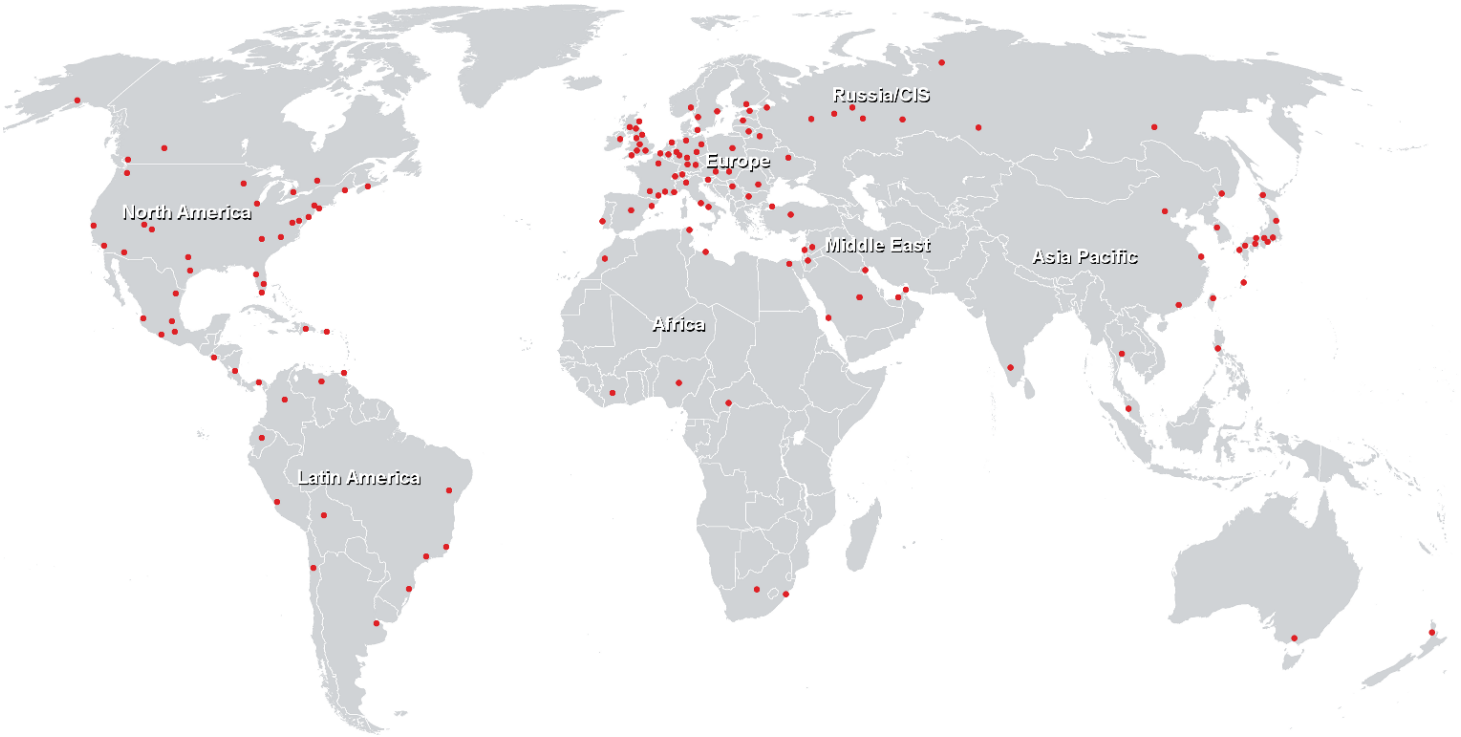
    - Wörterlisten
    - Online / Offline
    - Hashes und Rainbowtables
- NetBIOS und SMB
    - Discovery und Scanning
    - Gebrauch der Tools
    - Typische Schwächen
    - Ein- und Ausgabeumlenkung
    - UNIX Philosophie und Architektur
- Vulnerabilities und Exploits
    - CVE Details
    - Exploit DB
    - GHDB und Shodan

Schwerpunkte der Fallbeispiele

- Encoding und Decoding
- Cracking und Guessing
- Versteckte Informationen
- Einfaches Debugging
- Port-Knocking
- Datei- und Dump-Analyse

Kali Linux - Effizienter Einsatz für Pentrationstests (KLEPT)

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