Cyber Security Technical Analyst (CSA)

ID CSA **Price** on request **Duration** 5 days

Who should attend

- IT-Manager, Führungskräfte und Mitarbeiter des IT-Sicherheitsmanagements, Leiter der IT-Sicherheit
- zukünftige IT-Sicherheitsbeauftragte, Systemadministratoren, Penetrationstester
- sowie Mitarbeiter der IT die diese Funktionen übernehmen sollen.

Prerequisites

Die Teilnehmer sollten über grundlegende Kenntnisse in Netzwerktechnologien mit Schwerpunkt TCP/IP verfügen. Gute Anwenderkenntnisse von Windows- und Linux-Systemen sollten vorhanden sein. Kenntnisse aus dem Bereich der Systemverwaltung sind hilfreich.

Dieser Kurs Cyber Technical Security Analyst stellt die Basis für Penetrationstests und ist somit auch für nicht so technisch versierte Teilnehmer geeignet!

Course Objectives

Im Seminar Cyber Security Technical Analyst werden allgemeine Vorgehensweisen bei der Planung, Durchführung und Dokumentation von Security Assessments, Security Audits und Penetrationstests behandelt. Als Grundlage dienen neben zahlreichen Referenz-Standards (z.B. ISO 2700x) die Penetrationstest-Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und das international anerkannte Open Source Security Testing Methodology Manual (OSSTMM).

Im Kurs Cyber Security Technicial Analyst werden alle relevanten theoretischen und rechtlichen Aspekte wie z.B. Planung, Durchführung oder Haftung von vor Ort Assessments und die erforderliche Dokumentation behandelt.

Der Schwerpunkt liegt v.a. in der Durchführung von technischen Assessments und Penetrationstests unter Normalbedingungen. Hierbei werden eine Vielzahl von Angriffen praktisch ausgeführt, die aus dem Internet gegen Systeme gerichtet werden können. Der Fokus liegt dabei auf der Erkennung und Bewertung von Sicherheitslücken und weniger im konkreten Einbrechen.

Weitere Schwerpunkte liegen auf der Auswertung der am Vortag gewonnen Ergebnisse. Erfahrungsgemäss ist die Bedienung der Scanner nach einer guten und fundierten Einführung weniger problematisch als die nachfolgende Interpretation der Ergebnisse. Da der Abschlussbericht auch das Endergebnis (also das Produkt) eines Penetrationstests, Audits oder Assessments ist, müssen hier prägnant und nachvollziehbar alle Schwächen aufgelistet und bewertet werden. Darüber hinaus müssen Handlungsanweisungen zur Behebung der Schwächen präsentiert werden.

Der letzte Part des technischen Teils beschäftigt sich mit den Besonderheiten und Ausnahmen. Hier hat der Teilnehmer die Möglichkeit, tiefergehende Werkzeuge kennen zu lernen, die über das Mass des normalen Audits hinausgehen.

Course Content

Dieses Training vermittelt das vollständige Wissen zur Durchführung erster eigener Penetrationstests, Vulnerability Assessments, Schwachstellenanalyse oder auch Security Audits.

Neben den technischen Grundlagen werden auch die wichtigsten rechtlichen Aspekte und Notwendigkeiten vermittelt.

Zudem werden verbreitete Best-Practices vorgestellt und deren Inhalte erläutert.

Theoretische Grundlagen

- Arten von Sicherheitsprüfungen
- Kennzeichnende Eigenschaften dieser Sicherheitsprüfungen
- Security Audit
- Vulnerability Assessment
- Penetrationstest
- Source Code Analyse und Reverse Engineering
- Informationsquellen und Internet-Recherche

- Phasenmodell für das Vorgehen
- Einführung in das technische Penetrationstesting / Vorbereitung eines Penetrationstests

Rechtliche Grundlagen

- Rechtliche Aspekte der IT-Sicherheit
- Haftung und Vertraulichkeitserklärung
- Testrelevante "Hackerparagraphen"
- Wichtige Artikel der DSGVO

Technische Werkzeuge und deren Gebrauch

- KALI Linux mit diversen Tools
- Tenable Nessus und OpenVAS
- Wmap und Nikto
- Password-Cracking
- Grundlagen Metasploit

Praxisübungen & Labs nach Phasen

- Footprinting: Vorgehen und Werkzeuge
- Scanning: Vorgehen und Werkzeuge
- Enumeration: Vorgehen und Werkzeuge
- Exploitation: Vorgehen und Werkzeuge
- Post-Entry: Datensammlung und Beweissicherung

Praxisübungen & Labs am Beispiel

- Durchführen der Phasen innerhalb der Laborumgebung
- Durchführen der Phasen in der Praxis
- Anpassung an lokale Gegebenheiten
- Datensammlung und -korrelation
- Erkennen falscher Positiver und falscher Negativer
- Auflösen von widersprüchlichen Ergebnissen
- Empfehlungen zur Berichterstellung

Durchführung nach der BSI Penetrationstest-Studie

- Aufbau und Inhalt der Penetrationsteststudie
- Folgerungen für das eigene Vorgehen
- Stärken und Schwächen des Modells
- Durchführung nach Penetrationsteststudie

Durchführen und Vorgehen nach OSSTMM

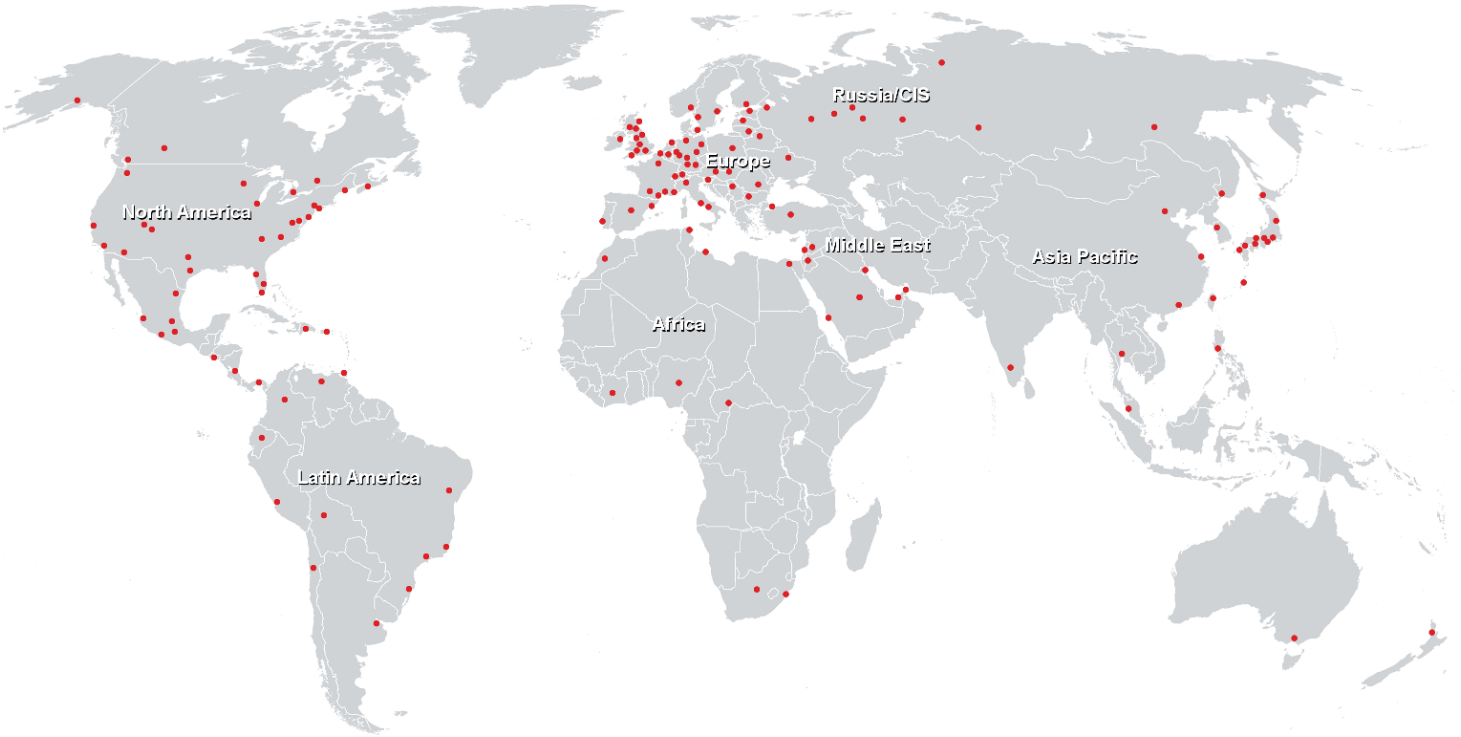
- Aufbau und Inhalt des Manuals
- Reporting Templates
- Risk Assessment Value
- Folgerungen für das eigene Vorgehen
- Stärken und Schwächen des Manuals
- Durchführung nach dem OSSTMM

Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)

Der grosse Praxisteil, bei dem zentrale Tools aus KALI Linux beispielhaft erklärt und praktisch benutzt werden, rundet das Training ab.

Cyber Security Technical Analyst (CSA)

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