Master Class: Hackers Demystified L2 (HDM2)

ID HDM2 **Price** on request **Duration** 5 days

Who should attend

Dieser Kurs wendet sich an erfahrene System-Administratoren, Consultants und Hyper-V-Designer.

Prerequisites

Mindestens 3 Jahre Erfahrung mit Windows Servern und 3 Jahre mit Active Directory

Course Objectives

Dieser Kurs richtet sich an fortgeschrittene Teilnehmer, die bereits über fundierte Kenntnisse in der Cybersecurity verfügen und mehr über die Erkennung, Abwehr und Analyse fortschrittlicher Bedrohungen lernen möchten. Durch die Vertiefung in spezialisierte Techniken und Angriffsvektoren, die von erfahrenen Angreifern genutzt werden, bietet dieser Kurs eine intensive Auseinandersetzung mit der Sicherheit moderner IT-Infrastrukturen.

Course Content

Web Application Attacks: Teilnehmer erlernen die Erkennung und Abwehr von Angriffen auf Webanwendungen, einschliesslich SQL-Injection, bei der Angreifer schädliche SQL-Befehle in Eingabefelder einschleusen, um Daten zu manipulieren oder zu stehlen. Cross-Site Scripting (XSS) wird ebenfalls behandelt, wobei Nutzer durch eingefügte Skripte in vertrauenswürdigen Webseiten angegriffen werden. Ausserdem werden File Inclusion-Schwachstellen thematisiert, die das Einschleusen von Dateien in Webanwendungen ermöglichen und so Zugriff auf den Server erlauben.

Kerberos Abuse: Dieser Abschnitt widmet sich dem Missbrauch des Kerberos-Authentifizierungssystems, einschliesslich Techniken wie Pass-the-Ticket, Kerberoasting und AS-REP Roasting. Diese fortgeschrittenen Methoden ermöglichen es Angreifern, ansonsten gut gesicherte Netzwerke zu kompromittieren.

Active Directory Enumeration and Exploitation: Hier lernen die Teilnehmer, wie sie Active Directory-Strukturen durchsuchen und ausnutzen können. Dazu gehören LDAP Enumeration, DCSync-Angriffe, die es erlauben, Benutzeranmeldeinformationen zu replizieren und Delegation Abuse, um unerlaubte Zugriffe im Netzwerk zu erlangen.

Privilege Escalation: Die Teilnehmer erfahren, wie sie Berechtigungen innerhalb eines Systems oder Netzwerks eskalieren können, um höhere Zugriffsrechte zu erlangen. Dies ist insbesondere dann notwendig, wenn der initiale Zugriff auf ein System erfolgreich ist, für das weitere Vorgehen jedoch erweiterte Berechtigungen benötigt werden. Dazu zählen Techniken wie Path Interception, Token Manipulation und das Umgehen der Benutzerkontensteuerung (UAC).

Lateral Movement: Hier wird vermittelt, wie sich Angreifer innerhalb eines Netzwerks bewegen, indem sie bestehende Zugriffsrechte ausnutzen oder erweitern. Methoden wie Pass-the-Hash, der Einsatz von Remote Services und Credential Dumping stehen dabei im Fokus.

Evading Endpoint Protections: Schliesslich lernen die Teilnehmer, wie Angreifer gängige Endpunktschutzmechanismen umgehen können. Dazu gehören Obfuscation (Verschleierung von Code), Living off the Land (Ausnutzung legitimer Tools für bösartige Zwecke) und fileless Malware, die ohne traditionelle Dateien auskommt und somit schwerer zu entdecken ist.

Schulungsumgebung

- Die Schulung läuft komplett virtualisiert.
- Jeder Teilnehmer bekommt einen eigenen Hardware-Server (!) mit mindestens zwei NVME-SSDs und mindestens 256 (!) GB RAM.
- Jeder Teilnehmer baut seine Umgebung mit dem Trainer komplett selber auf. Durch entsprechende Hardware sind neue Systeme in Sekunden (!) neu aufgesetzt.

Hardware

Jedem Teilnehmer steht ein dedizierter Server in einem

Rechenzentrum mit insgesamt 1 Gbit-Anschluss ins Internet zur Verfügung. Jeder Teilnehmer-Server ist folgendermassen ausgestattet:

- 128 GB RAM
- mind. 20 vCores
- 2 NVME-SSDs mit mind. 3.000 MB/s schreibend und mind. 2.000 MB/s lesend
- 1 Gbit ins Internet Gesamt-Bandbreite

Unsere Trainer

Wir haben lange nach unseren beiden Trainern gesucht, und haben sie vor einigen Jahren gefunden. Selten findet man technisch absolut hochrangige Trainer und Consultants, die auch noch als Speaker arbeiten und gleichzeitig auch noch sehr gute Trainer sind:

Sascha Schimmler ist Offensive Application Security Lead DACH bei einem Unternehmen für Cybersicherheitsdienstleistungen.

Hacker, nach meinem Verständnis sind nahezu NIE Hacker. Es sind bezahlte IT-Nomaden, die kaum grosse Kenntnisse ihrer Tools haben.

Deswegen: Lassen Sie uns reden; über Miss- und Verständnis zu aktuellen Themen und vielem mehr.

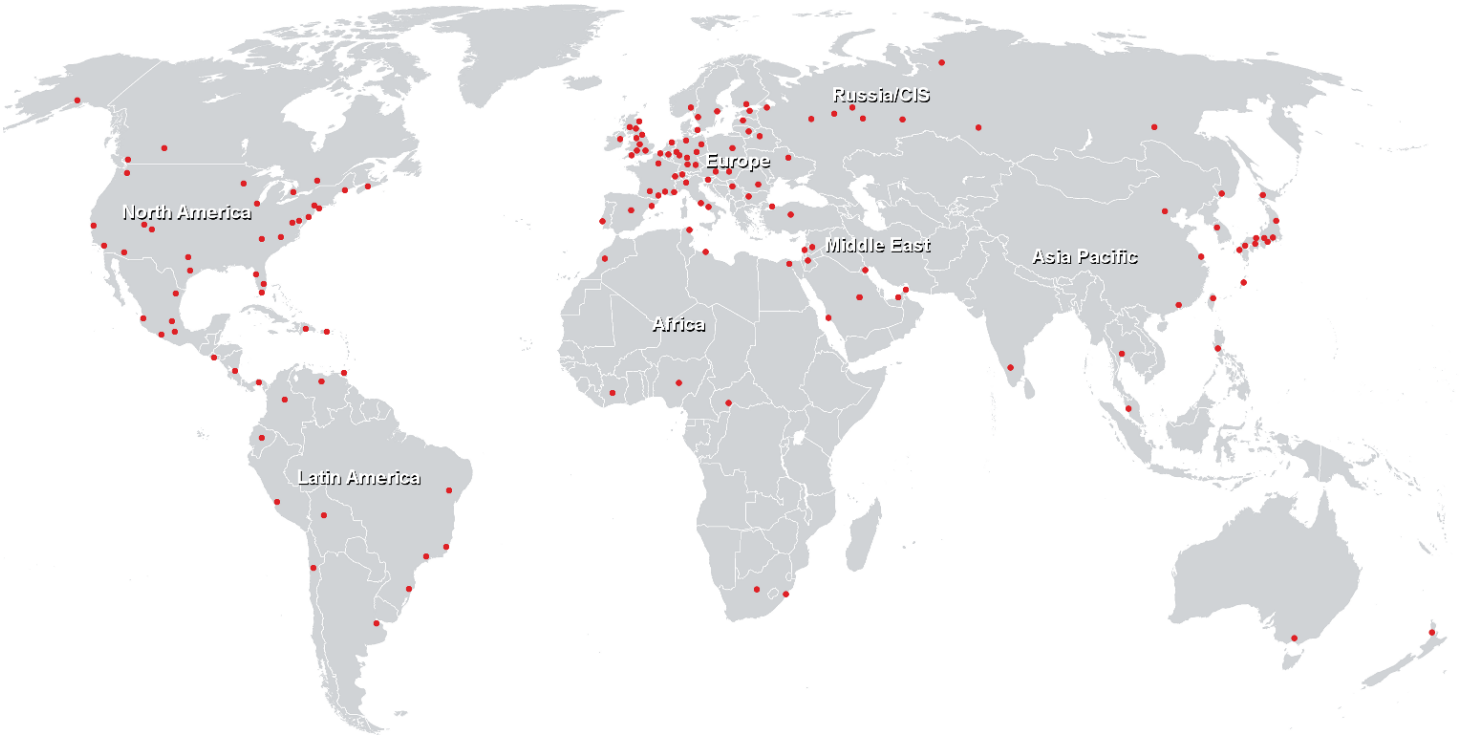
Seine Mission: Die Grundwerte Europas vor Cyber-Angriffen zu schützen.

Michael Oonk ist Senior Cyber Defense Engineer bei einem Enterprise-Unternehmen in Deutschland.

Seine absoluten Top-Kenntnisse sind das Red Teaming, Digital Forensics, Incident Response und das Security Consulting – und das alles from the field….

Master Class: Hackers Demystified L2 (HDM2)

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