Windows Domain Hacking & Security Hands-On («CYBADE»)

In diesem Hands-on Workshop lernen Sie die heutigen Techniken und Tools der Angreifer kennen (Offensive). Daneben werden defensive Aspekte zur Erkennung der Angriffe beleuchtet und gemeinsam Massnahmen zur Verhinderung der Angriffstechniken erarbeitet.

Dauer: 3 Tage
Preis: 3'900.– zzgl. 8.1% MWST
Kursdokumente: Digitale Kursunterlagen

Inhalt

Dieser hands-on Workshop bietet Ihnen folgende Inhalte:

- Anhand des MITRE ATT&CK® Frameworks (https://attack.mitre.org) werden die Taktiken und Techniken der Cyberkriminellen kennengelernt
- Es besteht die ultimative Möglichkeit in einer Laborumgebung (Windows Active Directory-Umgebung mit Client und Servern) die Tools der Angreifer kennenzulernen.
- Es werden Angriffssimulationen auf gängige IT-Infrastruktur von Unternehmen durchgeführt
- Anhand von angeleiteten Übungen können die für Sie und Ihr Unternehmen relevanten Techniken ausprobiert werden
- Zusammen mit den anderen Kursteilnehmern werden mögliche Erkennungs- und Gegenmassnahmen zu den Angriffen erarbeitet
- In der grossen Abschluss-Challenge wird die komplette Kill Chain eines Cyberangriffs anhand eines konkretes Cases durch gespielt

Key Learnings

- Aufzählen von mindestens drei Akteuren und deren Motivation bezüglich Cyberbedrohungen
- In Betrieb nehmen einer Lab-Umgebung (Windows Active Directory), um gängige Angriffe zu simulieren/üben
- Wissen, wo die Enterprise Matrix des MITRE ATT&CK® Frameworks zu finden ist
- Navigieren innerhalb der Matrix und herausfiltern der für Sie relevanten Techniken
- Benennen der 12 Taktiken der ATT&CK Matrix for Enterprise
- Beschreiben von mindestens drei Techniken pro Taktik und Ausprobieren von möglichen Angriffen im Lab
- Kenntnisse über mögliche Erkennungs- und Gegenmassnahmen zu den ausprobierten Angriffen

Methodik & Didaktik

Dieser Workshop beinhaltet aktive Lehrgespräche mit den Teilnehmenden, Reflexion und Austausch von Erfahrungen aus der eigenen Praxis im Kontext der Theorie und angeleitete Übungen in einer Hands-On Laborumgebung.

Zielpublikum

Dieser Workshop richtet sich an Informationssicherheitsverantwortliche, Informationssystemarchitekten, Sicherheitstester, Sicherheitsrevisoren, Sicherheitsberater, Sicherheitsingenieure, Netzwerkingenieure und Systemadministratoren.

Anforderungen

Gute Kenntnisse in Windows (Konfiguration und Wartung von Windows Servern, Active Directory-Infrastruktur, GPO, AppLocker, Windows Eventlog, PowerShell, Sysmon, SysInternals etc.) sind von Vorteil. Besuch der folgenden Kurse oder äquivalente breite praktische Hacking-Erfahrungen mit KALI Linux ist empfehlenswert:

- Cyber Security Tester – Hands-on Foundation («HAK»)
- Cyber Security Tester – Hands-on Professional («HAK2»)

Weiterführende Kurse

- CAS Cyber Security Analytics & Defense Expert («CSACAS»)
- Advanced Penetration Tester («ADVPEN»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-offense/workshop-windows-domain-hacking-security-hands-on