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

In this hands-on workshop, you will learn about the attackers' current techniques and tools (offensive). In addition, defensive aspects to detect the attacks will be highlighted and measures to prevent the attack techniques will be worked out together.

Duration: 3 days
Price: 3'900.–
Course documents: Digital courseware

Content

This hands-on workshop offers the following content:

- Using the MITRE ATT&CK® framework (https://attack.mitre.org), you will learn the tactics and techniques used by cybercriminals.
- The ultimate opportunity to learn the attackers' tools in a lab environment (Windows Active Directory environment with client and servers).
- Attack simulations on common IT infrastructure of companies are performed
- Guided exercises allow you to try out the techniques relevant to you and your company
- Together with the other course participants, possible detection and countermeasures to the attacks are developed
- In the big final challenge, the complete kill chain of a cyber attack is played out on the basis of a concrete case.

Key Learnings

- List at least three actors and their motivation regarding cyber threats.
- Commission a Lab environment (Windows Active Directory) to simulate/practice common attacks.
- Know where to find the enterprise matrix of the MITRE ATT&CK® framework.
- Navigate within the matrix and filter out the techniques that are relevant to you
- Name the 12 tactics of the ATT&CK Matrix for Enterprise
- Describing at least three techniques per tactic and trying out possible attacks in the lab
- Know about possible detection and countermeasures to the tried attacks

Methodology & didactics

This workshop includes active teaching conversations with the participants, reflection and exchange of experiences from own practice in the context of theory and guided exercises in a hands-on lab environment.

Target audience

This workshop is designed for information security managers, information system architects, security testers, security auditors, security consultants, security engineers, network engineers, and system administrators.

Requirements

Attendance of the following courses or equivalent broad hands-on hacking experience with KALI Linux. Good knowledge of Windows (configuration and maintenance of Windows servers, Active Directory infrastructure, GPO, AppLocker, Windows Eventlog, PowerShell, Sysmon, SysInternals, etc.) is a plus.

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

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-security/cyber-security-defense/workshop-windows-domain-hacking-security-hands-on