Cyber Security Tester/Analyst – Hands-On Exploiting («HAK4»)

In this course you will learn how to take advantage of vulnerabilities through exploits. With the acquired knowledge about exploiting techniques you will be able to detect attacks more quickly and thus suggest suitable countermeasures.

Duration: 2 days
Price: 1'900.–

Content

In the course we will work with KALI LINUX™ and various own codes. A corresponding LAB environment for hands-on exercises is available for all participants. They are introduced step by step to the exciting exploit topic in the guided LAB exercises. In addition to professional exploit tools such as the Metasploit™ framework, various own scripts are also used. In the LAB, attacks on client and server systems as well as on web applications are looked at. We gain access to systems via exploits and increase our system rights via privilege escalation. For a deeper understanding of current attacks, we look at the particularly interesting approach of «Living off the Land Hacking», against which basic protective measures are currently insufficient.

The course is rounded off with the essential attack techniques against web applications, since these are an exposed and popular target of criminal hackers. After this course, you will be able to analyze known and new exploit techniques in your own test environment and thus improve your own cyber security measures and detection rules. All participants explicitly commit themselves not to misuse the acquired knowledge. A written agreement to this effect must be signed before the course begins.

- Set up your own Exploiting Lab
- Classify computer architectures and assembler code in the context of exploits
- Introduction to debugging programs like gdb, OllyDbg and Immunity
- Detection of weak points by means of fuzzing
- Understand basic exploiting techniques such as buffer and heap overflows, format string vulnerabilities, etc
- Create your own exploit scripts together
- Understand the use of shellcodes within the exploit
- Generate shellcodes and embed them into your own exploit script
- Ensure that the exploit is executable (Bad Chars)
- Perform various user space exploits
- Using kernel exploits to gain root privileges
- Exploit vulnerable program libraries (DLLs)
- Classify protective effect and limits of DEP and ASLR in the context of system curing
- Testing protective measures with «Living off the Land Hacking»
- Understand basic attack techniques against web applications such as XSS, SQL injection, etc
- Tasks for own LABs for independent knowledge deepening

*KALI LINUX™ is a trademark of Offensive Security.
*Metasploit™ is a trademark of Rapid7 LLC.

Key Learnings

- Implementing known and new exploiting techniques
- Testing of security measures against exploits in test environments (hacking labs)
- Sharpening of analytical skills against targeted attacks
- Better understanding and faster detection of attack patterns

Target audience

This course is aimed at security professionals, computer scientists and managers who have attended the course «Cyber Security Tester - Hands-on Professional (HAK2)» and would like to deepen their previously acquired knowledge and analytical skills in a hands-on training with various exploiting techniques.

Requirements

Completion of one of the following courses or equivalent broad practical hacking experience with KALI LINUX™:

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

Certification

This compact seminar can be used together with own exercises to prepare for various IT security and hacking certificates and is part of the preparation for the renowned certificate: «OSSTMM Professional Security Analyst».

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-offense/course-cyber-security-testeranalyst-hands-on-exploiting