Hacking and Security, Level 1

Hands-on course of 5 days - 35h
Ref.: HAC - Price 2024: CHF3 530 (excl. taxes)

EDUCATIONAL OBJECTIVES

At the end of the training, the trainee will be able to:

Understand the techniques used by computer hackers and be able to counter their attacks

Measure your information system's security level

Carry out a penetration test

Define the impact and scope of a vulnerability

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@ORSYS.fr to review your request and its feasibility.

THE PROGRAMME

last updated: 07/2021

1) Hacking and security

- Forms of attacks, procedures, actors, challenges.
- Audits and intrusion tests, place in an ISMS.

2) Sniffing, interception, analysis, network injection

- Anatomy of a packet, tcpdump, Wireshark, tshark.
- Hijacking and intercepting communications (Man-in-the-Middle, VLAN attacks, honeypots).
- Packets: Sniffing, reading/analyzing from a pcap, extracting useful data, graphical representations.
- Scapy: Architecture, capacities, use.

Hands-on work : Listening to the network with sniffers. Creating a mini packet interceptor in C. Using scapy (command line, Python script): injections, interception, pcap reading, scanning, DoS, MitM.

3) Recognition, scanning, and enumeration

- Intelligence gathering, hot reading, operating the darknet, social engineering.
- Recognizing services, systems, topology, and architectures.
- Types of scans, filtering detection, firewalking, fuzzing.
- Camouflage using spoofing and bouncing, identifying paths with traceroute, source routing.
- Evading IDS and IPS: Fragmentations, covert channels.
- Nmap: Scanning and exporting results, options.
- Other scanners: Nessus, OpenVAS.

Hands-on work : Using the tool nmap, writing an NSE script in LUA. Filtering detection.

4) Web attacks

- OWASP: Organization, chapters, Top 10, manuals, tools.
- Discovering infrastructure and the corresponding technologies, strengths and weaknesses.
- Client-side: Clickjacking, CSRF, stealing cookies, XSS, components (flash, java). New vectors.
- Server-side: Authentication, session theft, injections (SQL, LDAP, files, commands).
- Including local and remote files, cryptographic attacks and vectors.
- Evading and bypassing protections: Example techniques for bypassing WAF.

- Burp Suite tools, ZAP, Sqlmap, BeEF

Hands-on work : Implementing different Web attacks under actual conditions, both server-side and client-side.

5) Application and post-operation attacks

- Microsoft authentication attack, PassTheHash.
- From C to the machine code assembler. Shellcodes.
- Encoding shellcodes, deleting null bytes
- Rootkits. Using processes: Buffer Overflow, ROP, Dangling Pointers.
- Protections and bypassing: Flag GS, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes with hardcoded addresses/LSD.
- Metasploit: Architecture, features, interfaces, workspaces, writing exploits, generating Shellcodes.

Hands-on work : Metasploit: Operating and using the database. Msfvenom: Generating Shellcodes, file trapping. Buffer overflow in Windows or Linux, exploit with shellcode Meterpreter.

DATES

REMOTE CLASS
2024 : 08 Jul, 21 Oct