Publication date : 04/05/2024

Course : Hacking and security with CyberRange

Practical course - 5d - 35h00 - Ref. HCR
Price : 3660 CHF E.T.

This advanced training course will teach you the techniques you need to measure the security level of your information system. Following these attacks, you'll learn how to trigger the appropriate response and raise the security level of your network.

Teaching objectives

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

- Understand hacker techniques and counter their attacks
- Measure the security level of your information system
- Perform a penetration test
- Defining the impact and scope of a vulnerability

Intended audience

Security managers and architects. System and network technicians and administrators.

Prerequisites

Good knowledge of IS security, networks, systems (especially Linux) and programming. Or knowledge equivalent to that acquired in the course "System and network security" (ref. SCR).

Practical details

Hands-on work

Airbus CyberSecurity's CyberRange is used to create and play out realistic scenarios involving real cyber-attacks.

Course schedule

1 Hacking and security

- Forms of attack.
- Operating procedures.
- Players and issues.

PARTICIPANTS

Security managers and architects. System and network technicians and administrators.

PREREQUISITES

Good knowledge of IS security, networks, systems (especially Linux) and programming. Or knowledge equivalent to that acquired in the course "System and network security" (ref. SCR).

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.

2 Sniffing, interception, analysis, network injection

- Packet anatomy, tcpdump, Wireshark, tshark.
- Hijacking and interception of communications (man-in-the-middle, VLAN attacks, honeypots).
- Packages: sniffing, reading/analysis from a pcap, extraction of useful data, graphical representations.
- Scapy: architecture, capabilities, use.
- Scenarios and tools available on CyberRange.

Hands-on work

Listen to the network with sniffers. Use scapy (command line, python script): injections, interception, pcap reading, scanning, DoS, man-in-the-middle (MITM).

3 Recognition, scanning and enumeration

- Intelligence gathering, hot reading, darknet exploitation, social engineering.
- Service, system, topology and architecture recognition.
- Types of scans, filtering detection, firewalking, fuzzing.
- Camouflage by spoofing and bouncing, path identification with traceroute, source routing.
- IDS and IPS evasion: fragmentations, covert channels.
- Nmap: scan and export results, options.
- Other scanners: Nessus, OpenVAS.
- Scenarios and tools available on CyberRange.

Hands-on work

Using the nmap tool and detecting filtering on the CyberRange platform.

4 Web attacks

- OWASP: organization, chapters, Top10, manuals, tools.
- Discover the infrastructure and associated technologies, strengths and weaknesses.
- Client-side: clickjacking, CSRF, cookie theft, XSS, components (Flash, Java). New vectors.
- Server side: authentication, session theft, injections (SQL, LDAP, files, commands).
- Inclusion of local and remote files, cryptographic attacks and vectors.
- Protection evasion and circumvention: WAF bypass techniques.
- Burp Suite, ZAP, SQLmap, BeEF tools.
- Scenarios available on CyberRange.

Hands-on work

Implementation of different web attacks under real conditions on both server and client sides using CyberRange.

5 Application attacks

- Metasploit: architecture, features, interfaces, workspaces.
- Exploit writing, shell code generation.

Dates and locations

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.

REMOTE CLASS
2026 : 20 Apr., 27 July, 2 Nov.