Publication date : 01/07/2025

Course : Hacking and security, level 2, expertise

Practical course - 3d - 21h00 - Ref. HKE
Price : 2470 CHF E.T.

4,6 / 5

BEST

This course will teach you advanced hacking techniques. You'll create shellcodes and payloads to exploit application vulnerabilities on operating systems, so you can better understand vulnerabilities and raise your system's security level to remedy them.

Teaching objectives

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

- Understanding recent attacks and system exploits
- Understand modern techniques for bypassing application protections
- Exploiting application vulnerabilities on Linux and Windows systems
- Create shellcodes and payloads (Linux and Windows)

Intended audience

Security managers, architects, system and network administrators. Pentesters.

Prerequisites

Good knowledge of IS security, C, Python and assembler is required.

Course schedule

1 State of the art in offense and defense

- A bit of current news: 5G, blockchain, smart contracts, IoTs (connected objects), AI, IPv4, IPv6.
- The latest attack techniques.
- The latest defensive strategies.

PARTICIPANTS

Security managers, architects, system and network administrators. Pentesters.

PREREQUISITES

Good knowledge of IS security, C, Python and assembler is required.

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 From C to assembler to machine code

- What is assembler and machine code. Compiling.
- How a processor works.
- Assembler basics and C language basics.
- Encoding concepts (addressing modes, registers, instructions, operations, etc.).

3 Application attacks

- The concepts of malware (virus, rootkit, etc.).
- State of the art of backdoors on Windows and Unix/Linux.
- Setting up backdoors and trojans.
- Shellcodes, TCP reverse shell, TCP bind shell.
- Shellcode encoding, NULL bytes removal.
- Process exploits: buffer overflow, ROP, Dangling Pointers.
- Protection and bypassing: GS flag, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes with hard-coded addresses, LSD.
- Advanced Metasploit: architecture, features, interfaces, workspaces, exploit writing, shellcode generation.

Hands-on work

Shellcode exploitation: buffer overflow (Windows or Linux). Bypass protections. Obtain a root shell using various types of buffer overflow. Use Metasploit to generate shellcode.

4 Analysis techniques

- Static analysis of binaries.
- Dynamic analysis tools.
- Safety in the sandbox.
- Reverse engineering and debugging.
- Modern packers and crypters.

Hands-on work

Malware analysis using different analysis techniques.

5 Cryptanalysis

- Cryptanalysis concepts (processes, encryption, etc.).
- Algorithm identification.
- Attacks on stream ciphers, ECB and CBC modes.
- Side-channel attacks.
- Attacks on blockchain.

Dates and locations

REMOTE CLASS
2026 : 16 Mar., 22 June, 7 Oct., 16 Nov.

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.