Publication date : 01/09/2024

Course : Intrusion detection and SOC

Practical course - 4d - 28h00 - Ref. TRU
Price : 2520 € E.T.

3,8 / 5

This highly practical course presents the most advanced attack techniques to date and shows how to detect them. Using attacks on identified targets (Web servers, clients, networks, firewalls, databases, etc.), you will learn how to trigger the most appropriate response. You'll also learn about the SOC concept and the tools you'll need as an SOC analyst.

Teaching objectives

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

- Identify and understand analysis and detection techniques
- Acquire the knowledge to deploy different intrusion detection tools
- Implement intrusion prevention and detection solutions
- Understand SOC concepts and environment
- Know how to use analysis tools

Intended audience

Systems and network technicians and administrators.

Prerequisites

Good knowledge of networks and security. Familiarity with the ANSSI security hygiene guide. Completion of the introductory cybersecurity course.

Course schedule

PARTICIPANTS

Systems and network technicians and administrators.

PREREQUISITES

Good knowledge of networks and security. Familiarity with the ANSSI security hygiene guide. Completion of the introductory cybersecurity course.

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.

1 Understanding network protocols

- Other aspects of the IP, TCP and UDP protocols.
- Focus on ARP and ICMP.
- Forced routing of IP packets (source routing).
- IP fragmentation and reassembly rules.
- The need for serious filtering.
- Securing your servers: a must.
- Technology-based countermeasures: from filtering routers to stateful inspection firewalls; from proxies to reverse proxies.
- Quick overview of solutions and products.

Hands-on work

Viewing and analyzing classic traffic. Use of various sniffers.

2 Attacks on TCP/IP

- How hackers implement "Spoofing" IP.
- Carry out denial-of-service attacks.
- The TCP sequence number prediction technique.
- TCP session theft: Hijacking (Hunt, Juggernaut).
- Understand how hackers carry out attacks on SNMP.
- TCP Spoofing attack (Mitnick): demystification.

Hands-on work

Injection of packets manufactured on the network. Participants can choose to use graphical tools, Perl, C or dedicated scripts.

3 Intelligence Gathering

- Search for traces: query Whois databases, DNS servers, search engines.
- Learn how to implement server identification.
- Understanding the context: analyzing results, determining filtering rules, specific cases.

Hands-on work

Non-intrusive search for information on a potential target (chosen by participants). Use of network scanning tools.

4 Detecting trojans and backdoors

- State of the art in Windows and Unix backdoors. What is a backdoor?
- How to set up backdoors and trojans.
- Downloading scripts to clients, exploiting browser bugs.
- Covert Channels": client-server applications using ICMP.
- Example of communication with distributed Denial of Service agents.

Hands-on work

Analysis of Loki, a client-server using ICMP. Accessing private information with your browser.

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.

5 Attacks and exploiting vulnerabilities

- Server takeover: finding and exploiting vulnerabilities.
- Examples of how to set up "backdoors" and remove traces.
- How to bypass a firewall (netcat and bounces)?
- Denial of service research techniques.
- What is distributed denial of service (DDoS)? How do hackers organize themselves to carry out such an attack?
- Buffer overflow attacks.
- Exploiting vulnerabilities in source code. Similar techniques: "Format String", "Heap Overflow".
- What are the vulnerabilities in Web applications? How can they be detected and protected?
- How malicious people manage to steal information from a database.
- What are RootKits?

Hands-on work

Exploitation of the bug used by the "Code Red" worm. Obtain a root shell using various types of buffer overflow. Testing a denial of service (Jolt2, Ssping). Use netcat to bypass a firewall. Use [[SQL Injection]] techniques to break Web authentication.

6 The SOC (Security Operation Center)

- What is a SOC?
- What is it used for? Why are more and more companies using it?
- SOC functions: logging, monitoring, audit and security reporting, post-incident analysis.
- The benefits of a SOC.
- SOC solutions.
- SIM (Security Information Management).
- SIEM (Security Information and Event Management).
- SEM (Security Event Management).
- Example of a monitoring strategy.

7 The SOC analyst's job

- What does a SOC analyst do?
- What are its skills?
- Monitor and sort alerts and events.
- Know how to prioritize alerts.

8 How do you manage an incident?

- Signs of successful IS intrusion.
- What have the hackers achieved? How far did they get?
- How do you react to a successful intrusion?
- Which servers are affected?
- Find the entry point and fill it.
- The Unix/Windows toolbox for evidence retrieval.
- Clean-up and return to production of compromised servers.

Dates and locations

REMOTE CLASS **PARIS LA DÉFENSE**

2026 : 9 June, 15 Sep., 17 Nov.

2026 : 9 June, 15 Sep., 17 Nov.