Publication date : 06/17/2024

Course : Intrusion detection

how to manage security incidents

Practical course - 4d - 28h00 - Ref. INT

Price : 2960 CHF E.T.

3,9 / 5

This theoretical and practical training course presents the most advanced attack techniques to date, and shows how to deal with them. Based on attacks carried out on identified targets (Web servers, clients, networks, firewalls, databases, etc.), participants will learn how to trigger the appropriate response (anti-trojan filtering, malformed URL filtering, spam detection and real-time intrusion detection with IDS probes).

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
- Managing an intrusion incident
- Understanding the legal framework

Intended audience

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

Prerequisites

Good knowledge of TCP/IP networks. Basic knowledge of IT security.

Practical details

Hands-on work

Secure and "normally " protected architectures (multi-DMZ firewalls, secure applications) will be the target of attacks.

Course schedule

PARTICIPANTS

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

PREREQUISITES

Good knowledge of TCP/IP networks. Basic knowledge of IT security.

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 The world of IT security

- Definitions "official": hacker, hacking.
- The world's hacker community, the "gurus", the "script kiddies".
- The hacker mindset and culture.
- Conferences and major safety sites.

Hands-on work

Underground navigation. Locate useful information.

2 TCP/IP for firewalls and intrusion detection

- IP, TCP and UDP from another angle.
- 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.

3 Understanding attacks on TCP/IP

- The "Spoofing" IP.
- Denial-of-service attacks.
- TCP sequence number prediction.
- TCP session theft: Hijacking (Hunt, Juggernaut).
- 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. Hijacking a telnet connection.

4 Intelligence Gathering: the art of camouflage

- Search for traces: query Whois databases, DNS servers, search engines.
- 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.

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 Protect your data

- Password systems "in clear", by challenge, encrypted.
- An update on Windows authentication.
- Reminders on SSH and SSL (HTTPS).
- Sniffing a switched network: ARP poisoning.
- Attacks on encrypted data : Man in the Middle" on SSH and SSL, Keystoke Analysis" on SSH.
- Sniffer detection: advanced tools and methods.
- Password attacks.

Hands-on work

SSH session decryption and theft: "Man in the Middle" attack. Password cracking with LophtCrack (Windows) and John The Ripper (Unix).

6 Detecting trojans and backdoors

- State of the art of backdoors on Windows and Unix.
- Setting 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.

7 Defending online services

- Server takeover: finding and exploiting vulnerabilities.
- Examples of how to set up "backdoors" and remove traces.
- How to bypass a firewall (netcat and bounces)?
- The search for denial of service.
- Distributed denial of service (DDoS).
- Buffer overflow attacks.
- Exploiting vulnerabilities in source code. Similar techniques: "Format String", "Heap Overflow".
- Vulnerabilities in Web applications.
- Theft of information from a database.
- 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.

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.

9 Conclusion: what legal framework?

- The right answer to hackers.
- French hacking law.
- The role of the State, official bodies.
- What can we expect from the Office Central de Lutte contre la Criminalité (OCLCTIC)?
- The search for evidence and perpetrators.
- And in an international context?
- Intrusive testing or domesticated hacking?
- Stay within a legal framework, choose the service provider, be sure of the result.

Dates and locations

REMOTE CLASS
2026 : 19 May, 6 Oct., 8 Dec.