System and Network Security, Level 1

Hands-on course of 4 days - 28h
Ref.: FRW - Price 2024: €2 990 (excl. taxes)

EDUCATIONAL OBJECTIVES

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

Know the flaws and threats of information systems

Learn the role of various security devices

Design and create a suitable security architecture

Implement the most common means of securing networks

Securing a Windows and Linux system

Participants

Implementing an HTTP proxy solution in Windows or Linux, an antivirus solution for network flows. Designing and implemen

TRAINING PROGRAM

Implementing an HTTP proxy solution in Windows or Linux, an antivirus solution for network flows. Designing and implementing a multi-firewall, multi-DMZ architecture. Implementing fundamental techniques to make the operating system secure.

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: 01/2018

1) Risks and threats

- Introduction to security.
- Overview of IT security.
- IT security vocabulary.
- "Low-level" attacks.
- Strengths and weaknesses of the TCP/IP protocol.
- Illustration of ARP, IP Spoofing, TCP-SYNflood, SMURF, and other attacks.
- Denial of service and distributed denial of service.
- Application attacks.
- Intelligence gathering.
- HTTP: A particularly vulnerable protocol (SQL injection, Cross Site Scripting, etc.).
- DNS: Dan Kaminsky attack.
- Hands-on work ¤Installation and use of the Wireshark network analyzer. Implementing an application solution.

Installation and use of the Wireshark network analyzer. Implementing an application solution.

2) Security architectures

- What architectures for what needs?
- Secure addressing plan: RFC 1918.
- Address translation (FTP as an example).
- The role of demilitarized zones (DMZ).
- Example architectures.
- Making the architecture secure through virtualization.
- Firewalls: Cornerstone of security.
- Actions and limits of traditional network firewalls.
- Technological change in firewalls (Appliance, VPN, IPS, UTM, etc.).

- Firewalls and virtual environments.
- Proxy server and application relay.
- Proxy or firewall: Conflicting or complementary?
- Reverse proxy, content filtering, cache, and authentication.
- SMTP relay, a must?
- Hands-on work ¤Implementation of a Caching proxy/Authentication.
Implementation of a Caching proxy/Authentication.

3) Data security
- Cryptography.
- Symmetrical and asymmetrical encryption. Hash functions.
- Cryptographic services.
- User authentication.
- Importance of reciprocal authentication.
- X509 certificates. Electronic signature. Radius. LDAP.
- Worms, virus, Trojans, malware, and keyloggers.
- Current trends. Antiviruses available, complementary nature of elements. EICAR, a “virus” to recognize.
- Hands-on work ¤Deploying an SMTP relay and an HTTP/FTP antivirus proxy. Implementing a server certificate.
Deploying an SMTP relay and an HTTP/FTP antivirus proxy. Implementing a server certificate.

4) Transfer security
- WiFi security.
- Risks inherent in wireless networks.
- The limits of WEP. WPA and WPA2 protocol.
- Types of attacks.
- Man in the Middle attack with Rogue AP.
- The IPSec protocol.
- Overview of the protocol.
- Tunnel and transport modes. ESP and AH.
- Analyzing the protocol and associated technologies (SA, IKE, ISAKMP, ESP, AH, etc.).
- The SSL/TLS protocols.
- Overview of the protocol. Details of the negotiation
- Analysis of main vulnerabilities.
- Sslstrip and sslsnif attacks.
- The SSH protocol. Overview and features
- Differences with SSL.
- Hands-on work ¤Carrying out a Man in the Middle attack on an SSL session. Implementing IPSec transport mode/PSK.
Carrying out a Man in the Middle attack on an SSL session. Implementing IPSec transport mode/PSK.

5) Making a system secure, “Hardening”
- Presentation.
- Insufficiency of default installations.
- Evaluation criteria (TCSEC, ITSEC, and common criteria).
- Making Windows secure.
- Account and authorization management.
- Control of services.
- Network configuration and auditing.
- Making Linux secure.
- Kernel configuration.
- File system.
- Network and service management.

- Hands-on work ¤Example of making a Windows and Linux system secure.
Example of making a Windows and Linux system secure.

6) Auditing and security on an everyday basis

- Tools and techniques available
- Intrusion tests: Tools and means.
- Detecting vulnerabilities (scanners, IDS probes, etc.).
- Real-time IDS-IPS detection tools, agent, probe, or cut-off.
- Reacting effectively in all circumstances.
- Supervision and administration.
- Organizational impacts.
- Technological monitoring.

7) Case study

- Prior study.
- Analysis of needs.
- Creating an architecture.
- Defining the action plan.
- Deployment.
- Approach to installing elements.
- Implementing the filtering policy.
- Hands-on work ¤Creating flow management.
Creating flow management.

DATES

REMOTE CLASS
2024 : 02 Jul, 15 Oct