System and Network Security, Level 2

Hands-on course of 4 days - 28h
Ref.: SEA - Price 2024: CHF2 860 (excl. taxes)

EDUCATIONAL OBJECTIVES

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

Measuring the information system's security level

Using intrusion detection, vulnerability detection, and auditing tools

Strengthening information system security.

How an AAA (Authentication, Authorization, Accounting) architecture works.

Implementing SSL/TLS.

HANDS-ON WORK

Many tools will be deployed by the participants. IDS SNORT detector, vulnerability scan with NESSUS, network analysis and scan with ETHEREAL and NMAP. Making a Wi-Fi network 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: 07/2021

1) Refreshers.

- The TCP/IP protocol.
- Address translation.
- Network architecture.
- Firewall: Benefits and limits.
- Proxys, reverse-proxy: Application protection.
- Demilitarized zones (DMZ).

2) Attack tools

- Attack classification and security paradigms.
- Principles of attacks: Spoofing, flooding, injection, capture, etc.
- Libraries: Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Tools: Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.

Hands-on work : Analyzing protocols with Wireshark. Using Scapy and Arpspoof.

3) Cryptography, application

- Security services.
- Cryptographic algorithms and principles (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Specific certificates and profiles for various servers and clients (X509).
- IPSEC protocol and virtual private networks (VPN).
- SSL/TLS and VPN-SSL protocols. Data compression issues.

Hands-on work : Getting started with openssl and implementing OpenPGP. Generating X509 v3 certificates.

4) AAA architecture (Authentication, Authorization, Accounting).

- The AAA network: Authentication, authorization, and accounting.
- One Time Password: OTP, HOTP, Google Authenticator, SSO (Kerberos protocol).
- The role of the LDAP directory in authentication solutions.
- The modules PAM and SASL.
- Radius architecture and protocol (Authentication, Authorization, Accounting).
- Possible attacks.

- How to protect yourself.
Hands-on work : Attacking an AAA server.

5) Detecting intrusions
- Operating principles and detection methods.
- Market players, overview of systems and applications involved.
- Network scanners (Nmap) and application scanners (Web applications).
- IDSs (Intrusion Detection Systems).
- The benefits of these technologies and their limits.
- How to place them in the enterprise architecture.
- Overview of the market, detailed study of SNORT.
Hands-on work : Installation, configuration, and implementation of SNORT, writing attack signatures.

6) Verifying a system's integrity
- Operating principles.
- What are the products available?
- Overview of Tripwire or AIDE (Advanced Intrusion Detection Environment).
- Vulnerability auditing.
- Principles and methods and organizations for managing vulnerabilities.
- Reference site and overview of auditing tools.
- Defining a security policy.
- Study and implementation of Nessus (status, operation, evolution).
Hands-on work : Vulnerability auditing of the network and servers using Nessus and Nmap. Website vulnerability auditing.

7) Managing security events
- Handling information reported by various security equipment.
- Consolidation and correlation.
- Overview of SIM (Security Information Management).
- SNMP management and protocol: Security strengths and weaknesses.
- SNMP security solution.
Hands-on work : Setting up a SNMP attack.

8) Wi-Fi network security
- How do you make a WiFi network secure?
- Intrinsic weaknesses of WiFi networks.
- SSID Broadcasting, MAC Filtering: What do they add?
- Is WEP still useful?
- The WPA protocol, the first acceptable solution.
- WPA implementation in shared key mode, is it enough?
- WPA, Radius and AAA server, enterprise implementation.
- The 802.11i and WPA2 standards: Which solution is the most advanced today?
- Injecting traffic, cracking WiFi keys.
Hands-on work : Configuring tools for traffic capture, scanning networks and analyzing Wi-Fi traffic. Configuring an AP (access point) and implementing security solutions.

9) Telephony-over-IP security
- Voice-over-IP concepts. Overview of applications.
- Architecture of a VoIP system.
- The SIP protocol, an open voice-over-IP standard.
- Weaknesses of the SIP protocol.
- Problems with NAT.
- Attacks on telephony-over-IP.
- What are the security solutions?

10) Email security

- Architecture and operation of email.
- Protocols and access to emails (POP, IMAP, Webmail, SMTP, etc.).
- Problems and classifications of email attacks (spam, phishing, identity theft, etc.).
- Spam fighters.
- Methods, architectures, and tools for fighting spam.
- Email address collection tools.
- Solutions implemented against spam.

DATES

REMOTE CLASS
2024 : 04 Jun, 17 Sep, 03 Dec