Publication date : 03/14/2024

Course : System and network security

Face up to threats with the CyberRange from Airbus CyberSecurity

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

Price : 2900 CHF E.T.

4,4 / 5

BEST

This practical course will show you how to implement the main means of securing systems and networks. After studying a few threats to the information system, you will learn about the role of various security equipment in protecting the company.

Teaching objectives

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

- Understand information system vulnerabilities and threats
- Understand the role of various safety devices
- Design and implement an appropriate security architecture
- Implement the main network security measures
- Securing Windows and Linux systems

Intended audience

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

Prerequisites

Good knowledge of networks and systems.

Practical details

Hands-on work

Airbus CyberSecurity's CyberRange is used to create and play out realistic scenarios involving real cyber-attacks.

Course schedule

PARTICIPANTS

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

PREREQUISITES

Good knowledge of networks and systems.

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 Risks and threats

- Lower layer" attacks.
- TCP/IP protocol strengths and weaknesses.
- Illustration of ARP and IP Spoofing attacks, TCP-SYNflood, SMURF, etc.
- Denial of service and distributed denial of service.
- Application attacks.
- HTTP, a particularly exposed protocol (SQL injection, Cross Site Scripting, etc.).
- DNS: attack Dan Kaminsky.

Hands-on work

Log on to the CyberRange platform, take control of a Linux/Windows machine to navigate in command and graphics mode. Use of the Wireshark network analyzer.

2 Everyday tools

- Available tools and techniques.
- Penetration testing: tools and resources.
- Types of scans, filtering detection, firewalking.
- Vulnerability detection (scanners, IDS probes, etc.).
- Real-time detection tools IDS-IPS, agent, probe or cut-off.
- Build an architecture and train with CyberRange (architecture, operating system, components, etc.).
- CyberRange scenarios: cyber-attacks (network, system, web), traffic (dns, ftp, ping, http), etc.

Hands-on work

Run a scenario on CyberRange to perform web vulnerability scans (ping, port scan, web vulnerability scan, user database dump, traffic generation).

3 Security architectures

- Which architectures for which needs?
- Secure addressing plan: RFC 1918.
- Address translation (FTP as an example).
- The role of demilitarized zones (DMZs).
- Secure architecture through virtualization.
- Firewall: the cornerstone of security. Actions and limitations of traditional network firewalls.
- Proxy server, firewall, application relay.
- Reverse proxy, content filtering, caching and authentication.

Hands-on work

Implementation of a web cache proxy (Squid) on CyberRange.

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.

4 Data security

- Fundamental concepts of cryptography. The main tools on the market, and what vendors have to offer.
- Current trends. The antiviral offer, complementary elements. EICAR, a "virus" you need to know about.
- Symmetrical and asymmetrical encryption. Hash functions.
- Cryptographic services and concepts.
- Cryptographic principles and algorithms (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- User authentication. The importance of mutual authentication.
- Public key management and certification, revocation, renewal and archiving.
- Key management infrastructure (PKI).
- Diffie-Hellman algorithm. Man-in-the-middle attack.
- X509 certificates. Electronic signature. Radius. LDAP.
- Worms, viruses, trojans, malware and keyloggers.

Hands-on work
Deployment of SMTP relay and HTTP/FTP Antivirus proxy.

5 Exchange security

- The IPSec protocol.
- Presentation of the protocol.
- Tunnel and transport modes. ESP and AH.
- Analysis of protocol and associated technologies (SA, IKE, ISAKMP, ESP, AH, etc.).
- SSL/TLS protocols.
- Presentation of the protocol. Negotiation details.
- Analysis of the main vulnerabilities.
- sslstrip and sslsnif attacks.
- The SSH protocol. Overview and features.
- Differences with SSL.

Hands-on work
Run an SSL vulnerability scanning scenario on CyberRange to highlight SSL/TLS vulnerabilities. Perform a man-in-the-middle attack on an SSL session.

6 Hardening a system

- Introducing hardening.
- Insufficient default installations.
- Evaluation criteria (TCSEC, ITSEC and common criteria).
- Securing Windows.
- Account and authorization management.
- Service control.
- Network configuration and auditing.
- Securing Linux.
- Kernel configuration.
- File system.
- Service and network management.

Hands-on work
Example of securing a Windows and Linux system.

7 Audit

- Supervision and administration.
- Organizational impact.
- Real-time detection tools IDS-IPS, agent, probe or cut-off. What products are available?
- Processing information from the various safety devices.
- React effectively in all circumstances.
- Technology watch. Reference site and overview of auditing tools.

Hands-on work
Analysis of machine system log files on CyberRange.

Dates and locations

REMOTE CLASS
2026 : 4 May, 30 June, 6 Oct.