Publicatiedatum : 14/03/2024

# Opleiding : Beveiliging van systemen en netwerken

**Omgaan met bedreigingen met de CyberRange van Airbus CyberSecurity**

*Praktijkcursus - 4d - 28u00 - Ref. SCR*

*Prijs : 2470 € V.B.*

4,4 / 5

BEST

Deze praktische cursus laat je zien hoe je de belangrijkste middelen om systemen en netwerken te beveiligen kunt implementeren. Na het bestuderen van enkele bedreigingen voor het informatiesysteem, leer je over de rol van verschillende beveiligingsapparatuur bij het beschermen van het bedrijf.

## Pedagogische doelstellingen

**Aan het einde van de training is de deelnemer in staat om:**

- Inzicht in de kwetsbaarheden en bedreigingen van informatiesystemen
- De rol van verschillende veiligheidsuitrustingen begrijpen
- Een geschikte beveiligingsarchitectuur ontwerpen en implementeren
- De belangrijkste netwerkbeveiligingsmaatregelen implementeren
- Een Windows- en Linux-systeem beveiligen

## Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

## Voorafgaande vereisten

Goede kennis van netwerken en systemen.

## Praktische modaliteiten

**Praktisch werk**

De CyberRange van Airbus CyberSecurity wordt gebruikt om realistische scenario's met echte cyberaanvallen te maken en uit te spelen.

## Opleidingsprogramma

**DEELNEMERS**

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

**VOORAFGAANDE VEREISTEN**

Goede kennis van netwerken en systemen.

**VAARDIGHEDEN VAN DE CURSUSLEIDER**

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

**BEOORDELINGSMODALITEITEN**

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

## 1 Risico's en bedreigingen

- Laag-laag" aanvallen.
- Sterke en zwakke punten van het TCP/IP-protocol.
- Illustratie van ARP en IP Spoofing aanvallen, TCP-SYNflood, SMURF, etc.
- Ontzegging van service en gedistribueerde ontzegging van service.
- Aanvallen van toepassingen.
- HTTP, een bijzonder blootgesteld protocol (SQL-injectie, Cross Site Scripting, enz.).
- DNS: aanval door Dan Kaminsky.

### Praktisch werk

Inloggen op het CyberRange platform, met behulp van een Linux/Windows machine om te navigeren in opdracht- en grafische modus. Gebruik van de Wireshark netwerkanalyser.

## 2 Dagelijkse hulpmiddelen

- De beschikbare hulpmiddelen en technieken.
- Penetratietests: tools en hulpmiddelen.
- Soorten scans, detectie van filters, firewalking.
- Kwetsbaarheidsdetectie (scanners, IDS-sondes, enz.).
- IDS-IPS, agent, probe of cut-off real-time detectietools.
- Bouw een architectuur en train met CyberRange (architectuur, besturingssysteem, componenten, enz.).
- Scenario's beschikbaar op CyberRange: cyberaanvallen (netwerk, systeem, web), verkeer (dns, ftp, ping, http), enz.

### Praktisch werk

Voer een scenario uit op CyberRange om kwetsbaarheden op het web te scannen (ping, poortscan, kwetsbaarheden op het web, database user dump, verkeer genereren).

## 3 Beveiligingsarchitecturen

- Welke architecturen voor welke behoeften?
- Plan voor veilige adressering: RFC 1918.
- Adresvertaling (FTP als voorbeeld).
- De rol van gedemilitariseerde zones (DMZ's).
- Veilige architectuur door virtualisatie.
- Firewall: de hoeksteen van beveiliging. Acties en beperkingen van traditionele netwerkfirewalls.
- Proxyserver, firewall, applicatie relay.
- Reverse proxy, inhoud filteren, caching en authenticatie.

### Praktisch werk

Implementatie van een webcache proxy (Squid) op CyberRange.

**PEDAGOGISCHE EN TECHNISCHE MIDDELEN**

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

**TOEGANGSMODALITEITEN EN TERMIJNEN**

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

**TOEGANKELIJKHEID VOOR MINDERVALIDEN**

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

## 4 Gegevensbeveiliging

- De fundamentele concepten van cryptografie. De belangrijkste tools op de markt, wat uitgevers te bieden hebben.
- Huidige trends. Het antivirale aanbod, aanvullende elementen. EICAR, een "virus" waarvan je op de hoogte moet zijn.
- Symmetrische en asymmetrische encryptie. Hashfuncties.
- Cryptografische diensten en concepten.
- Cryptografische principes en algoritmen (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Gebruikersauthenticatie. Het belang van wederzijdse authenticatie.
- Beheer en certificering van openbare sleutels, intrekking, vernieuwing en archivering van sleutels.
- Sleutelbeheerinfrastructuur (PKI).
- Diffie-Hellman algoritme. Man-in-the-middle aanval.
- X509-certificaten. Elektronische handtekening. Radius. LDAP.
- Wormen, virussen, trojans, malware en keyloggers.

**Praktisch werk**
Implementatie van een SMTP-relay en een HTTP/FTP Antivirus proxy.

## 5 Wisselzekerheid

- Het IPSec-protocol.
- Presentatie van het protocol.
- Tunnel- en transportmodi. ESP en AH.
- Analyse van het protocol en bijbehorende technologieën (SA, IKE, ISAKMP, ESP, AH, etc.).
- SSL/TLS-protocollen.
- Presentatie van het protocol. Details van de onderhandelingen.
- Analyse van de belangrijkste kwetsbaarheden.
- sslstrip en sslsnif aanvallen.
- Het SSH-protocol. Overzicht en functies.
- Verschillen met SSL.

**Praktisch werk**
Een SSL-kwetsbaarhedenscanscenario uitvoeren op CyberRange om SSL/TLS-kwetsbaarheden aan het licht te brengen. Een man-in-the-middle aanval uitvoeren op een SSL sessie.

## 6 Een systeem beveiligen: hardening

- Presentatie van uitharding.
- Onvoldoende standaardinstallaties.
- Evaluatiecriteria (TCSEC, ITSEC en gemeenschappelijke criteria).
- Windows beveiligen.
- Account- en autorisatiebeheer.
- Servicecontrole.
- Netwerkconfiguratie en -audit.
- Linux beveiligen.
- Kernelconfiguratie.
- Bestandssysteem.
- Service- en netwerkbeheer.

**Praktisch werk**
Voorbeeld van het beveiligen van een Windows en Linux systeem.

### 7 Controle

- Toezicht en administratie.
- Organisatorische impact.
- IDS-IPS real-time detectietools, agent, probe of cut-off. Welke producten zijn beschikbaar?
- Informatie verwerken die wordt gerapporteerd door de verschillende veiligheidsvoorzieningen.
- Effectief reageren in alle omstandigheden.
- Technologiebewaking. Referentiesite en overzicht van audittools.

**Praktisch werk**
Analyse van logbestanden van machinesystemen op CyberRange.

## Data en plaats

**KLAS OP AFSTAND**
2026 : 4 mei, 30 juni, 6 okt.

**PARIS LA DÉFENSE**
2026 : 27 apr., 23 juni, 29 sep.