Publicatiedatum : 22/05/2024

Opleiding : De basisprincipes van systeem- en netwerkbeveiliging

Praktijkcursus - 3d - 21u00 - Ref. BSR
Prijs : 2100 € V.B.

4,1 / 5

In deze zeer praktische cursus leer je hoe je de belangrijkste middelen om systemen en netwerken te beveiligen kunt implementeren. Je zult zien welke bedreigingen er zijn voor het informatiesysteem en hoe je daarmee om kunt gaan.

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
- De belangrijkste netwerkbeveiligingsmaatregelen implementeren

Doelgroep

Systeem- en netwerktechnici en -beheerders.

Voorafgaande vereisten

Goede kennis van netwerken en beveiliging. Bekend zijn met de ANSSI-beveiligingshygiënegids. De introductiecursus cyberbeveiliging hebben afgerond.

Opleidingsprogramma

1 De baan van beveiligingsintegrator

- Wat doet een beveiligingsintegrator?
- Welke vaardigheden heeft het?
- Deelnemen aan het onderhouden van OS in optimale veiligheidsomstandigheden.
- Beveiligingsoplossingen integreren, implementeren en onderhouden.
- Essentiële beveiligingsoplossingen.

DEELNEMERS

Systeem- en netwerktechnici en -beheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van netwerken en beveiliging. Bekend zijn met de ANSSI-beveiligingshygiënegids. De introductiecursus cyberbeveiliging hebben afgerond.

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.

2 Risico's en bedreigingen

- Inleiding tot veiligheid.
- Sterke en zwakke punten van het TCP/IP-protocol.
- Illustratie van ARP en IP Spoofing aanvallen, TCP SYN Flood, SMURF, etc.
- Ontzegging van service en gedistribueerde ontzegging van service.
- HTTP, een bijzonder blootgesteld protocol (SQL-injectie, Cross Site Scripting, enz.).
- Aanvallen op het DNS.

Praktisch werk

De Wireshark netwerkanalyser installeren en gebruiken. Een applicatie-aanval uitvoeren.

3 Beveiligingsarchitecturen

- Welke architecturen voor welke behoeften?
- Veilige architectuur door virtualisatie.
- Firewall: de hoeksteen van beveiliging.
- Technologische ontwikkelingen in firewalls (Appliance, VPN, IPS, UTM, enz.).
- Firewalls en virtuele omgevingen.
- Reverse proxy, inhoud filteren, caching en authenticatie.

Praktisch werk

Implementatie van een cache/authenticatie proxy.

4 Gegevensbeveiliging

- Cryptografie.
- Symmetrische en asymmetrische encryptie. Hashfuncties.
- Cryptografische diensten.
- Gebruikersauthenticatie.
- X509-certificaten. Elektronische handtekening. Radius. LDAP.
- Wormen, virussen, trojans, malware en keyloggers.

Praktisch werk

Inzetten van een HTTP/FTP antivirus proxy. Een servercertificaat implementeren.

5 Wisselzekerheid

- WiFi-beveiliging.
- De beperkingen van WEP. De protocollen WPA en WPA2.
- Val Man in the Middle aan met de AP rogue.
- Het IPSec-protocol.
- Tunnel- en transportmodi. ESP en AH.
- Analyse van het protocol en bijbehorende technologieën (SA, IKE, ISAKMP, ESP, AH, etc.).
- SSL/TLS-protocollen.
- Het SSH-protocol. Overzicht en functies.

Praktisch werk

Een Man in the Middle aanval uitvoeren op een SSL sessie. IPSec transport/PSK modus implementeren.

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.

6 Een systeem beveiligen, de "Hardening"

- Evaluatiecriteria (TCSEC, ITSEC en gemeenschappelijke criteria).
- Windows beveiligen.
- Account- en autorisatiebeheer.
- Servicecontrole.
- Netwerkconfiguratie en -audit.
- Linux beveiligen.

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

Data en plaats

KLAS OP AFSTAND
2026 : 3 juni, 16 sep., 16 nov.

PARIS LA DÉFENSE
2026 : 3 juni, 16 sep., 16 nov.