Publicatiedatum : 19/01/2024

Opleiding : Check Point R81, netwerkbeveiliging, niveau 1

Praktijkcursus - 4d - 28u00 - Ref. CPB
Prijs : 2520 € V.B.

In deze cursus maakt u kennis met de nieuwste versie van Check Point-producten: R81.20. Aan het einde van deze cursus bent u in staat om een uniform beveiligingsbeleid (Toegangscontrole en Dreigingspreventie) en gedeelde beveiligingsbeleidsregels (Geo Policy en HTTPS Inspection) te implementeren en te beheren.

Pedagogische doelstellingen

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

- Check Point R81 installeren en configureren
- Een beveiligingsbeleid implementeren
- Logboekcontrole en filteren implementeren
- Inbraken blokkeren met SAM (Suspicious Activity Monitor)

Doelgroep

Systeem-/netwerk-/beveiligingsbeheerders en -ingenieurs, technici.

Voorafgaande vereisten

Goede kennis van TCP/IP. Basiskennis van IT-beveiliging.

Opleidingsprogramma

1 Bediening en installatie

- Implementaties (gedistribueerd, standalone).
- Server voor beveiligingsbeheer.
- Back-up, herstel, snapshots en CLI-interface.

Praktisch werk
Installeer Check Point onder Gaïa in versie R81.

DEELNEMERS
Systeem-/netwerk-/beveiligingsbeheerders en -ingenieurs, technici.

VOORAFGAANDE VEREISTEN
Goede kennis van TCP/IP.
Basiskennis van IT-beveiliging.

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 Uniform beveiligingsbeleid

- Regels en subregels per zone.
- Impliciete regels, objecten met Object Explorer, anti-spoofing.

Praktisch werk
SmartConsole installeren. Aanmaken van beveiligingsobjecten en -beleid, gedeeld beleid. Tags beheren.

3 Adresomzetting (NAT)

- Regels en RFC 1918.
- NAT statisch/verbergen, ARP, VPN.
- Handmatig, automatische modus.

Praktisch werk
Automatische NAT (verbergen, statisch) en handmatige transactieregels.

4 Site-to-site en client-to-site VPN

- Virtual Private Network-principes, IPSEC, IKEv1/v2, Software Blade Mobile Access.
- Traditionele en vereenvoudigde modus.
- Endpoint Security Heavy Client, Check Point Mobile.
- Mobiele toegangsverificatie: Check Point Mobile, iOS/Android clients, SSL Network Extender (SNX) captive portal.

Praktisch werk
Installeren van een site-to-site IPSec tunnel en toegang op afstand met IPSec VPN. Check Point Mobile activeren en instellen.

5 Firewall en gebruikersbeheer

- Logboeken en waarschuwingen van Smartcenter beheren.
- Tabbladen Logboeken & Monitoren, Gateways & Servers.
- SAM-functionaliteit (Suspicious Activity Monitor) met Check Point SmartView Monitor R81.
- Gebruikersauthenticatie.
- Beheer van identiteitscollectoren.
- Gebruik van toegangsrollen.

Praktisch werk
Identity Awareness, logboekcontrole en filteren implementeren. Inbraak blokkeren met SAM.

6 IPS-module

- Kwetsbaarheden, beveiligingslekken, CVE-verwijzingen.
- Beveiligingsprofiel, IPS-beleid.

Voorbeeld
Bescherming tegen kwetsbaarheden met de IPS-module.

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.

7 Applicatiebeheer

- Noties van toepassingshandtekeningen.
- Aanmaken van aangepaste toepassingen.
- Beheer van limieten, UserCheck, URL-filtering.

Voorbeeld
Implementatie van een beveiligingsbeleid voor inhoud.

8 Bedreigingspreventie

- Antivirus en Antibot modules.
- Bedreigingsextractie/emulatie.

Praktisch werk
Implementatie van een bedreigingspreventiebeleid.

Data en plaats

KLAS OP AFSTAND
2026 : 10 maa., 16 juni, 27 okt.

PARIS LA DÉFENSE
2026 : 10 maa., 16 juni, 27 okt.