CCSA, Check Point Certified Security Administrator R81, voorbereiding op certificering

Praktijkcursus van 4 dagen - 28u
Ref : CPQ - Prijs 2024 : € 3 280 excl. BTW

In deze cursus leert u alle technieken en methodieken die u nodig hebt om te slagen voor het CCSA R81 certificeringsexamen. U leert hoe u een beveiligingsbeleid, adresvertaling (NAT) en de Intrusion Prevention System (IPS) module implementeert.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Check Point R81 installeren en configureren

Adresomzetting (NAT) implementeren

Een beveiligingsbeleid implementeren en verkeer monitoren

Voorbereiding op het officiële examen dat leidt tot CCSA-certificering

CERTIFICERING

Om deel te nemen aan het certificeringsexamen hoeft u zich alleen maar te registreren op de Check Point website. U kunt het examen dan direct online afleggen of in een erkend centrum.

HET PROGRAMMA

laatste update: 10/2021

1) Inleiding

- Check Point-producten.
- Nieuwigheden van de R80-versie.

2) Werking en installatie

- Architectuur in gedistribueerde modus en in zelfstandige modus.
- Beheerserver. SIC-protocol.
- Back-up- en herstelopdrachten.
- Voorstelling van het Gaïa-systeem.

Installatie van Check Point R80.

3) Implementatie van een beveiligingsbeleid

- Aan de slag met SmartConsole.
- SmartDashboard R80 starten en gebruiken.
- Beveiligingsbeleid. Regelbeheer.

Installatie van SmartConsole. Objecten maken. Een beveiligingsbeleid realiseren. Anti-adresvervalsing activeren.

4) Adresomzetting (NAT)

- Regels voor adresomzetting met IPv4 en IPv6.
- Statische NAT (One To One NAT) en dynamische NAT (.Many To One NAT)/PAT.
- ARP-problematiek en routering.

Implementatie van automatische NAT van het statisch type, Hide en regels voor manuele transacties.

5) Monitoring en logboekbeheer

- Beleid inzake logboekbeheer.

DEELNEMERS

Systeem-/netwerk-/beveiligingstechnici, -beheerders en -ingenieurs.

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.

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.

- Verbindingen opvolgen met SmartView Tracker.
- SmartView Monitor, functies en alarmdrempels.

Activering van monitoring, gebruik van het Suspicious Activity Monitoring Protocol, visualisatie van verkeer, monitoring van de status van het beveiligingsbeleid.

6) R80-clientauthenticatie

- Identity Awareness. Application Control.
- Soorten authenticaties.

Implementatie van Identity Awareness.

7) Site-naar-site-VPN en mobiel VPN

- VPN-architectuur. Grondbeginselen van versleuteling.
- Inleiding tot IKE en IPSec.
- Certificeringsinstantie (CA). Domain-Based VPN.
- SecureClient en SSL Network Extender.

Implementatie van een IPSec site-naar-site-tunnel met behulp van een preshared key en een certificaat. Configuratie van externe toegang met IPSec VPN en SSL VPN.

8) IPS-module

- Voorstelling van IPS.
- Web Intelligence. Application Intelligence.
- IPS- en IDS-beveiligingsprofielen.

Voorbeeld van bescherming tegen kwetsbaarheden met de IPS-module.

DATA

KLAS OP AFSTAND
2024 : 02 jul, 26 nov

BRUSSEL
2024 : 02 jul, 26 nov