Sécurité réseaux, niveau 1

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Installer et configurer Check Point R81
- Mettre en œuvre une politique de sécurité
- Mettre en œuvre l'examen et le filtrage des logs
- Bloquer les intrusions avec SAM (Suspicious Activity Monitor)

Public concerné

Administrateurs et ingénieurs systèmes/réseaux/sécurité, techniciens.

Prérequis

Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises**.**

Durée de la Formation : 4 jours (28heures)

Prix de la Formation : 2750 euros TTC

Programme de la formation

1 Fonctionnement et installation

- Déploiements (distribué, standalone).
- Serveur de management (Security Management Server).
- Sauvegarde, restauration, snapshots et interface CLI.

Travaux pratiques

Installer Check Point sous Gaïa

2 Politique de sécurité unifiée

- Règles, sous-règles par zone.
- Règles implicites, objets avec Object Explorer, l'anti-spoofing.

Travaux pratiques

Installer SmartConsole. Créer des objets et une politique de sécurité, des politiques partagées (shared policies). Gérer les tags.

3 Translation d'adresses (NAT)

- Règles et RFC 1918.
- NAT static/hide, ARP, VPN.
- Mode manuel, automatique.

Travaux pratiques

Mise en place de NAT automatique (type hide, static) et de règles de transaction manuelle.

4 VPN site à site et client vers site

- Principes du Réseau Privé Virtuel, IPSEC, IKEv1/v2, Software Blade Mobile Access.
- Mode traditionnel et simplifié.
- Client lourd Endpoint Security, Check Point Mobile.
- Authentification en Mobile Access : Check Point Mobile, Clients iOS/Android, Portail captif SSL Network Extender (SNX).

Travaux pratiques

Installer un tunnel IPSec site à site, un accès distant en VPN IPSec. Activation et mise en place de Check Point Mobile.

5 Firewall et gestion des utilisateurs

- Gérer des logs sur le Smartcenter, des alertes.
- Onglets Logs & Monitor, Gateways & Servers.
- Fonctionnalités SAM (Suspicious Activity Monitor) avec Check Point SmartView Monitor R81.

- Authentification des utilisateurs.
- Gestion de l'Identity Collector.
- Utilisation des Access Roles.

Travaux pratiques

Mise en oeuvre d'Identity Awareness, de l'examen et du filtrage des logs. Bloquer les intrusions avec SAM.

6 Module IPS

- Vulnérabilités, failles de sécurité, référencement CVE.
- Profil de sécurité, politique IPS.

Exemple

Protection contre les vulnérabilités avec le module IPS.

7 Contrôle applicatif

- Notions de signatures applicatives.
- Créations d'applications personnalisées.
- Gestion des limites, des UserCheck, filtrage URL.

Exemple

Déploiement d'une politique de sécurité de contenu.

8 Threat Prevention

- **Modules Antivirus, Antibot.**
- **Threat Extraction/Emulation.**

Travaux pratiques

Mise en oeuvre d'une politique de Threat Prevention.

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.
Découvrez-les sur notre page Comment financer sa formation