Administrateur Firewalls ASA certifié Cisco

Administrateur Firewalls ASA certifié Cisco

durée : 5 jour(s) code formation : ASA

Description :

La sécurité des données est une condition indispensable dans les échanges sur les réseaux locaux et distants. Il est primordial, pour un administrateur, de connaître et de réévaluer en permanence les risques qu`encourent les systèmes informatiques. Les premières étapes dans la sécurisation d`un réseau informatique concernent l`accès aux dispositifs actifs du réseau (routeurs, commutateurs), la mise en place et la configuration d`un pare-feu.

Pré-requis :

Avoir déjà réalisé la configuration de base d?un routeur Cisco
Savoir utiliser un système d?exploitation Windows ou Unix/Linux

Programme :

Sécurisation des dispositifs réseaux Cisco

- Les menaces concernant les infrastructures réseaux modernes
- Les menaces courantes sur les installations physiques
- Les méthodes usuelles d'attaques réseau
- Les vers, les virus, les trojan
- Le cycle de vie de la sécurité
- Les politiques de sécurité
- La description de l'architecture d'autodéfense de Cisco
- La sécurisation des routeurs Cisco
- La sécurisation des routeurs grâce au SDM (Security Device Manager)
- La sécurisation des droits d'accès pour l'administration des routeurs
- Les privilèges d'accès multiples
- La sécurisation de l'image IOS et des fichiers de configuration
- L'implémentation d'AAA sur les routeurs Cisco
- Les fonctions d'AAA (Authentication, Authorization et Accounting)
- Les propriétés des protocoles RADIUS et TACACS+
- Les méthodes d'authentification pour fournir un accès au routeur ou à travers un routeur
- Les ACLS
- Le rappel sur les listes de contrôle d'accès
- La configuration et la vérification des ACL pour éviter les denis de service
- La configuration des ACL pour éviter l'usurpation d'identité (IP address spoofing)
- L'implémentation du management de la sécurité réseau et du reporting
- La planification de la sécurité
- La configuration de SSH

La configuration de Syslog

SNMPv3 et NTPv3

L'évitement des attaques de couche 2

Les attaques communes de couche 2 : VLAN hopping, STP attacks, ARP spoofing, MAC spoofing, CAM overflow...

Les propriétés de sécurité au niveau des commutateurs Catalyst Cisco (PVLAN, SPAN port, IBNS...)

Les attaques communes sur les réseaux sans-fil

Les principales fonctions de sécurité du protocole 802.11

La mise en place d'IOS Firewall

La présentation des principaux avantages et inconvénients des différents types de firewall (parefeu)

Les tables d'état

La configuration du NAT sur un pare-feu

La configuration du firewall grâce à SDM

L'implémentation de Cisco IPS

La détection d'intrusion basée sur le réseau ou sur le client

La définition des technologies de détection d'intrusion, les réponses aux attaques et les options de monitoring

L'activation de l'IPS et de la configuration

La configuration du VPN IPSec sur un routeur Cisco

IKE Protocol

Le hachage des messages (HMAC)

Les méthodes de cryptage

La clé Diffie-Hellman

L'authentification IPSec

L'environnement PLI

La configuration et la vérification d'un VPN intersites avec des clés partagées

Cisco Easy VPN Server et Cisco Easy VPN Remote

La configuration d'accès distant VPN

Les ateliers pratiques

La sécurisation d'un routeur Cisco

atelier : sécuriser les accès administratifs à un routeur Cisco, One-Step lockdown, mots de passe cryptés, exec timout

Les listes de contrôles d'accès

Lors de ce TP, le stagiaire apprendra à configurer, optimiser et dépanner les listes de contrôle d'accès afin d'éviter les attaques par Telnet, SNMP, l'IP Spoofing ou encore les attaques par dénis de service distribués.

SSH et Syslog

Cet atelier enseignera au stagiaire à configurer un lien SSH sur des routeurs Cisco afin d'en sécuriser les accès et de configurer un serveur Syslog qui recueillera tous les messages d'alerte.

Les parefeux et les systèmes de détection d'intrusion

Ce TP consiste à configurer le firewall et l'IPS Cisco sur un routeur, à partir de la console de gestion de sécurité SDM Cisco.

Le VPN

A la fin de cet atelier, le stagiaire sera en mesure de configurer une liaison VPN entre 2 sites, de configurer un routeur Cisco afin qu'il accepte les connexions d'accès réseau à distance.

Sécurisation d'un réseau avec PIX Firewall et ASA

Configuration d'un système de sécurité de base

Description de la sécurité logicielle et physique

Utilisation des commandes show

Configuration de NAT

Mise en place d'une route par défaut

Configuration des options de log

Decription des technologies de parefeu

Configuration d'un net static

Limitation des connexions embryonnaires

Configuration d'une solution de sécurité pour limiter les accès non fiables

Configuration des ACL basées sur les adresses, l'heure et les protocoles

Configuration des groupes d'objets pour optimiser les ACL

Configuration du filtrage de java/activeX

Configuration de l'URL filtering

Vérification des restrictions de trafic entrant

Configuration d'une solution pour sécuriser les connexions VPN intersites et d'accès distant

Les certificats

Configuration de IKE

Configuration des paramètres IPSec

Configuration des crypto-map

EasyVPN

Configuration de WebVPN Configuration de firewall transparent et virtuel, options de haute disponibilité

Les firewall transparents

Configuration d'un parefeu transparent

Monitoring et maintien du parefeu virtuel

Le fail-over

Configuration du système de sécurité pour le fail-over

Configuration du routage et de la commutation sur un dispositif de sécurité

Activation du serveur DHCP et des relais DHCP

Configuration des VLAN

Configuration de RIP et OSPF

Configuration du multicast

Configuration de ICMP

Configuration d'une politique modulaire de sécurité

Configuration d'une class-map

Configuration d'une policy-map

Configuration d'une service-policy

Configuration d'une ftp-map

DNS-guard

Ateliers pratiques

Configuration d'un dispositif de sécurité

exercice pratique : configurer PIX Firewall