TD – sécurisation switch

Objectif : sécuriser les switches Cisco

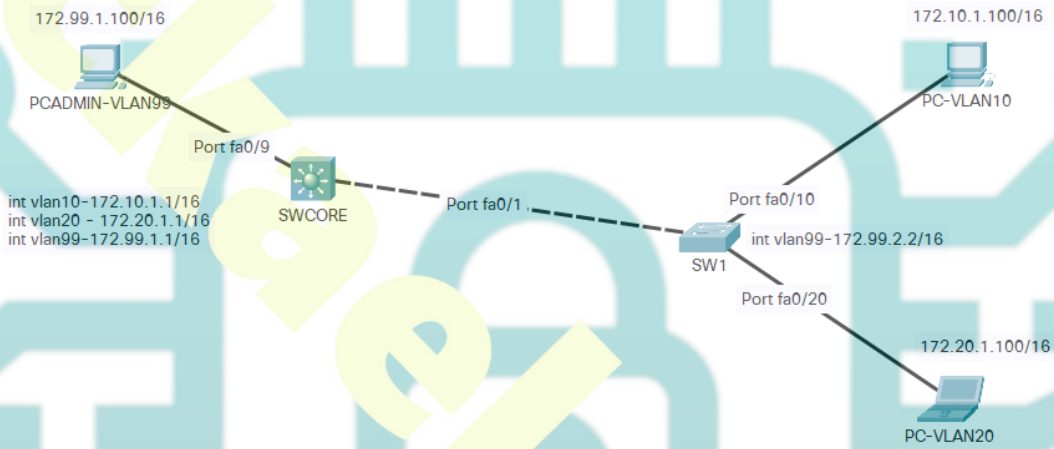


Schéma du TD

Configuration du swcore

en
conf t
hostname swcore
!désactivation de la recherche DNS
no ip domain-lookup
!désactivation du service CDP de découverte des voisins
no cdp run
vlan 10
name 10
int vlan 10
ip address 172.10.1.1 255.255.0.0
vlan 20
name 20
int vlan 20

ip address 172.20.1.1 255.255.0.0
!création de l'interface d'administration
vlan 99
name svi
int vlan 99
ip address 172.99.1.1 255.255.0.0
int fa0/9
switchport access vlan 99
!activation du trunk
int fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!activation du routage
ip routing

Configuration du sw1

en
conf t
hostname sw1
!désactivation de la recherche DNS
no ip domain-lookup
!désactivation du service CDP de découverte des voisins
no cdp run
vlan 10
name 10
vlan 20
name 20
int fa0/10
switchport access vlan 10
int fa0/20
switchport access vlan 20
!activation du trunk
int fa0/1
switchport mode trunk
!création de l'adresse d'administration
vlan 99
name svi

int vlan99
ip address 172.99.2.2 255.255.0.0

Sécurisation des accès console et distant
Configuration accès sécurisé local sur SWCORE

!chiffrement mot de passe
conf t
service password-encryption
!création du mot de passe pour le mode exec
enable password Pa$$en

- Tester l'accès lors de la saisie de la commande enable
- Faire un sh run pour vérifier le mot de passe

Configuration accès sécurisé distant SSH

conf t
!création de l'utilisateur
username admin password Pa$$
!gestion des noms (obligatoire pour SSH)
ip domain-name cisco.com
!génération de la clé
crypto key generate rsa
1024
!affectation des consoles simultanées
line vty 0 4
!activation de SSH à la place de Telnet
transport input ssh
login local
exit
ip ssh version 2
!gestion des tentatives de connexion max
ip ssh authentication-retries 3

!délai avant deconnexion
ip ssh time-out 60

- Tester l'accès via ssh de plusieurs PC, cela doit fonctionner

Limitation de l'accès SSH

ip access-list standard SSH
permit host 172.99.1.100
deny any
!on affecte l'ACL SSH à la console
line vty 0 4
access-class SSH in

- tester l'accès via ssh de plusieurs PC, seul le PC admin peut y accéder

Protection des ports des requêtes STP sur le SW1

conf t
interface range fa0/10,fa0/20
shutdown
!limiter le spanning tree sur les ports non trunk
spanning-tree portfast
spanning-tree bpduguard enable
no shutdown

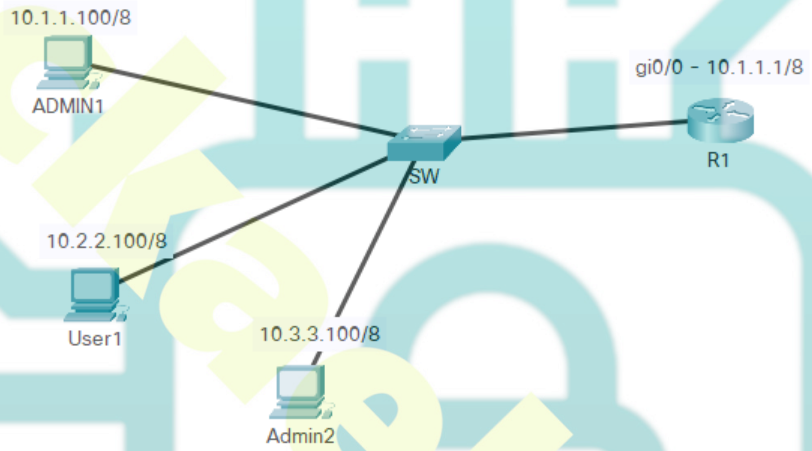
Protection du port du PC admin sur swcore

!activation de la protection des ports sur swcore
int fa0/9
switchport mode access
shut
switchport port-security
!désactivation du port si mauvaise adresse MAC
switchport port-security violation shutdown
!demande d'associer une adresse MAC à un port en dynamique
switchport port-security mac-address sticky
no shut

Tests de la configuration

- Tenter de se connecter avec un autre PC sur le port 9 du swcore, le port doit passer en down.

Niveau de privilèges des utilisateurs sur routeur



Configuration du routeur R1

en
conf t
hostname R1
int gi0/0
ip address 10.1.1.1 255.0.0.0
no shut
!mettre une longueur de mot de passe minimum
security passwords min-length 4
service password-encryption
enable password Pa$$

Mise en place des privilèges sur R1

!création des utilisateurs
username user1 privilege 0 password user1
username admin1 privilege 15 password admin1

username admin2 privilege 5 password admin2
privilege exec level 5 show vlan
!mise en place de SSH
ip domain-name cisco.com
!génération de la clé
ip ssh version 2
crypto key generate rsa
1024
!affectation des consoles simultanées
line vty 0 4
!activation de SSH à la place de Telnet
transport input ssh
login local
exit
!gestion des tentatives de connexion max
ip ssh authentication-retries 3
!délai avant deconnexion
ip ssh time-out 60

Tests à effectuer

- Se connecter avec le compte user1 et taper la commande sh run (elle doit échouer) puis faire ? pour voir les commandes disponibles.
- Se connecter avec le compte admin2 et tenter de taper la commande sh run (elle doit échouer) puis taper la commande sh vlan (elle doit fonctionner)
- Se connecter avec admin1 et taper la commande sh run (elle doit fonctionner)