Cisco

Sécurisation des périphériques Cisco

Objectifs

Comment restreindre l'accès via une politique de mots de passes,

Mise en place d'une bannière pour les informations légales

Mise en place de mots de passes pour accès à distance et chacun des niveaux de cisco IOS

Chiffrement des mots de passes dans le fichier de configuration

SCALAR

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

PRINCIPES DE BASES

La base de la sécurité sur un périphérique :

- **Fermer physiquement l'accès** au local technique
- **Journaliser les accès**
- **Sécuriser a minima avec un mot de passe**
- Mettre en place une politique de **mots de passes robustes**

SCALAR

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

PRINCIPES DE BASES

La base de la sécurité sur un périphérique :

- **Éteindre** les ports/interfaces/services **inutilisés**
- **Chiffrer** les **mots de passes** !
- Utilisez une **`clé SSH`** pour une **gestion à distance**

SCALAR

Plus précisément dans un environnement Cisco

SÉCURISER SON APPAREIL CISCO

- **Mettre un mot de passe sur le port console !**
- Mettre un **mot de passe sur le mode privilégié !**
- Mettre **les interfaces** dans un **autre VLAN que celui par défaut !**
- Mettre le **VLAN 1 sur OFF !**

SCALAR

SÉCURISER SON APPAREIL CISCO

- Configurer **le SSH** pour la gestion distante de l'appareil
  - **N'utilisez PAS le Telnet !!**
- Configurer une **déconnexion après délai d'inactivité**
- Configurer **la protection des ports**

SCALAR

Démonstrations concrètes

Sécuriser le port console & l'accès aux commandes avec privilèges

Sécuriser le mode **USER** *(port console)*

```
# enable
# conf terminal
# line console 0
# password VOTRE_MOT_DE_PASSE
# login
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Sécuriser le mode **EXEC USER**

```
# enable
# conf terminal
# enable secret exemple
# exit
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Chiffrer les mots de passes crées et présents dans le fichier de config

Chiffrer les mots de passe !

```
service password-encryption
```

Autrement, les mots de passes sont en clair

dans le fichier de configuration !

SCALAR

Changer les interfaces de VLAN et Mettre le VLAN 1 sur OFF

Pourquoi faire?

- **Tous les appareils Cisco ont un VLAN 1 implémenté par défaut et non-supprimable.**
- Il faut **le désactiver pour compliquer la tâche aux attaquants.**
- **Et donc déplacer dans un autre VLAN les interfaces se trouvant actuellement dans le VLAN 1 !**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

METTRE LES INTERFACES DANS UN AUTRE VLAN

```
# enable
# configure terminal
# vlan 45
# exit
# interface range fa0/1-24
# switchport mode access
# switchport access vlan 45
```

N'oubliez pas d'activer le VLAN45 en allant dans l'interface vlan45, avec 'no shutdown' !

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

ÉTEINDRE LE VLAN ACTIF PAR DÉFAUT

```
# enable
# configure terminal
# interface vlan 1
# shutdown
# exit
```

SCALAR

Mettre en place une déconnexion suite à inactivité

Configurer la déconnexion par inactivité

```
# enable
# configure terminal
# line console 0 / line vty 0-15
# exec-timeout 10
# exit
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Configurer le SSH

LE SSH — ÉTAPES THÉORIQUES

1. Changer le nom de l'appareil
2. **Donner un nom de domaine à l'appareil**
3. **Créer un compte utilisateur et un mot de passe**
4. **Générer une clef SSH**
5. **L'appliquer à des lignes vty ou une interface**
6. Forcer la version 2 du SSH

SCALAR

Configurer le SSH sur Cisco IOS

```
# ip domain name cisco.com
# username NOM_USER secret MDP
# crypto key generate rsa
# line vty 0-15 / line console 0
# login local
# transport input ssh
# exit
# ip ssh version 2
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Protéger les ports utilisés

PROTÉGER LES PORTS !

Principe :

- **Dire à un port qu'il ne peut communiquer qu'avec une ou plusieurs autres adresses MAC précises !**

- **Lui dire quoi faire si l'adresse MAC détectée en face n'est plus celle attendue !**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

PROTÉGER LES PORTS !

Principe :

- **On peut rentrer l'adresse MAC, ou demander au port de retenir la 1ère** *(ou les suivantes)* **qui le contacte.**

- **Et dire au port de s'éteindre en cas de violation, ou autre !**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

PROTÉGER LES PORTS !

```
# interface TYPE PORT
# switchport mode access
# switchport port-security maximum 1
# switchport port-security mac-adress sticky
# switchport port-security violation shutdown
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25