Conformité d’un switch Cisco

IOS pris en charge

Le switch Cisco doit exécuter une version IOS actuellement prise en charge par Cisco Systems.

Vérifiez que le switch est conforme à cette exigence en demandant à l'administrateur du switch de saisir la commande suivante :

```
show version
```

Vérifiez que la version est toujours prise en charge par Cisco. Toutes les versions prises en charge par Cisco sont disponibles à l'URL suivante :

www.cisco.com/c/en/us/support/ios-nx-os-software

Conformité d’un switch Cisco

Présence de Syslog

Le switch Cisco doit être configuré pour envoyer des logs à au moins deux syslog centraux dans le but de transmettre des alertes aux administrateurs et au responsable de la sécurité du système d'information (ISSO).

La configuration devrait ressembler à l'exemple ci-dessous :

```
logging a.b.c.d
logging e.f.g.h
```

Où a.b.c.d et e.f.g.h sont les adresses IP des deux serveurs Syslog

Conformité d’un switch Cisco

Présence de serveur d’authentification

Le switch Cisco doit être configuré pour utiliser au moins deux serveurs d'authentification afin d'authentifier les utilisateurs avant d'accorder un accès administrateur.

Examinez la configuration du switch Cisco pour vérifier que le périphérique est configuré pour utiliser au moins deux serveurs d'authentification comme source principale d'authentification. Vérifiez la conformité comme indiqué dans l'exemple suivant :

```
aaa new-model
!
aaa authentication CONSOLE local
aaa authentication login LOGIN_AUTHENTICATION group radius local


ip http authentication aaa login-authentication LOGIN_AUTHENTICATION
ip http secure-server


radius-server host x.x.x.x auth-port 1812 acct-port 1813 key xxxxxxx
radius-server host x.x.x.x auth-port 1812 acct-port 1813 key xxxxxxx



line con 0
exec-timeout 5 0
login authentication CONSOLE
line vty 0 1
exec-timeout 5 0
login authentication LOGIN_AUTHENTICATION
```

Conformité d’un switch Cisco

Présence de mécanismes cryptographiques

Le switch Cisco doit être configuré pour mettre en œuvre des mécanismes cryptographiques afin de protéger la confidentialité des sessions de maintenance à distance.

Examinez la configuration du switch Cisco pour vérifier qu'elle est conforme à cette exigence.

```
ip ssh version 2
ip ssh server algorithm encryption aes256-ctr aes192-ctr aes128-ctr
```

Conformité d’un switch Cisco

Présence de code d’authentification

Le switch Cisco doit être configuré pour utiliser le code d'authentification de message Keyed-Hash (HMAC) validé par FIPS afin de protéger l'intégrité des sessions de maintenance à distance.

Examinez la configuration du switch Cisco pour vérifier qu'elle est conforme à cette exigence, comme indiqué dans l'exemple ci-dessous :

```
ip ssh version 2
ip ssh server algorithm mac hmac-sha2-512 hmac-sha2-256
```

Conformité d’un switch Cisco

Gestion de l’inactivité

Le switch Cisco doit être configuré pour mettre fin à toutes les connexions réseau associées à la gestion des périphériques après cinq minutes d'inactivité.

Examinez la configuration du switch Cisco pour vérifier que toutes les connexions réseau associées à une gestion de périphérique ont une valeur de délai d'inactivité définie sur cinq minutes ou moins, comme indiqué dans l'exemple suivant :

```
ip http secure-server
ip http timeout-policy idle 300 life nnnn requests nn

line con 0
exec-timeout 5 0
line vty 0 1
exec-timeout 5 0
```

Conformité d’un switch Cisco

Crypter l’affichage des mots de passe

Le switch Cisco doit uniquement stocker des représentations cryptographiques des mots de passe.

Examinez la configuration du switch pour déterminer si les mots de passe sont chiffrés, comme indiqué dans l'exemple ci-dessous :

```
service password-encryption

Enable secret 5 xxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Conformité d’un switch Cisco

Désactiver les services inutiles

Le switch Cisco doit être configuré pour interdire l'utilisation de toutes les fonctions et services inutiles et non sécurisés.

Vérifiez qu'aucun port, protocole ou service inutile ou non sécurisé n'est activé sur le switch. Par exemple, les commandes suivantes ne doivent pas figurer dans la configuration :

```
boot network
ip boot server
ip bootp server
ip dns server
ip identd
ip finger
ip http server
ip rcmd rcp-enable
ip rcmd rsh-enable
service config
service finger
service tcp-small-servers
service udp-small-servers
service pad
service call-home
```