Vidéo - Méthodes de sécurisation d'accès (9 min)

Avant toute chose, lorsque vous installez un périphérique sur votre réseau, par exemple un commutateur Cisco, faites en sorte que son accès soit sécurisé afin que seul un administrateur puisse le configurer ou modifier ses paramètres. Pour ce faire, il faut définir certains paramètres de configuration initiaux. Je clique sur l'icône du PC, puis sur le programme d'émulation de terminal. Je dispose maintenant d'une connexion de console au commutateur.

Dans cette démo, j'utilise l'interface en ligne de commande directement sur le commutateur. Vous voyez que je suis connecté au commutateur en mode d'exécution utilisateur sans authentification. Le risque de sécurité est élevé, d'autant plus que, à ce stade, je peux saisir la commande « enable » et passer en mode d'exécution privilégié, toujours sans aucun mot de passe ou authentification. Sauf que ce mode d'exécution permet de configurer le commutateur. Donc, la première chose à faire est de sécuriser l'accès à ce mode.

Pour ce faire, je passe en mode de configuration globale, je saisis la commande « enable secret », puis le mot de passe. Utilisez des mots de passe forts autant que possible. Dans notre scénario de test, je vais utiliser « class ». Avec le paramètre « secret », je sais que ce mot de passe sera chiffré dans le fichier de configuration. Une autre possibilité est de taper « enable password class ». Cette formulation ne permet pas de chiffrer le mot de passe dans le fichier de configuration. Je préfère donc l'effacer. Voyons si notre commande « enable secret class » a fonctionné. Je tape Ctrl+C pour passer en mode d'exécution privilégié, puis je quitte le commutateur. J'appuie sur « Entrée ». Je suis en mode d'exécution privilégié. Je tape « enable ». Je suis invité à saisir le mot de passe. Lorsque je le fais, aucun des caractères saisis ne s'affiche. Je tape « class » et j'appuie sur « Entrée ». Je suis maintenant en mode d'exécution privilégié.

Examinons la configuration en cours jusqu'à ce point. Pour ce faire, je saisis la commande « show running-config » pour examiner la consultation en cours. J'appuie sur « Entrée ». Regardez ici, en haut : la commande « enable secret » est affichée. Le 5 signifie qu'il s'agit d'un hachage MD5 et voilà notre mot de passe en hachage unidirectionnel. Vous voyez donc que la commande « enable secret » permet de masquer le mot de passe dans le fichier de configuration. Pour afficher le reste du fichier de configuration, il suffit d'appuyer sur la barre d'espace du clavier. Nous avons donc chiffré le mot de passe actif ou l'accès au mode d'exécution privilégié. Voyons maintenant l'accès au commutateur via la console. Nous pouvons également le sécuriser. Pour cela, je saisis « enable » et le mot de passe « class ». Je passe en mode de configuration globale en tapant « conf t », puis en mode de configuration de ligne pour la console de ligne 0. Je saisis « line console 0 ». Je suis en mode de configuration de ligne. Je peux saisir un mot de passe pour la connexion de console. Je tape « password ». Je devrais utiliser un mot de passe complexe, mais, pour cette démo, je vais juste choisir « cisco ». J'appuie sur « Entrée ». Je tape la commande « login » pour me connecter comme administrateur global sur la console de ligne 0. Maintenant que j'ai sécurisé le port de console, je vais aussi sécuriser l'accès au terminal virtuel pour les connexions à distance. Je tape « line vty », pour le terminal ou le télétype virtuel, puis le nombre de lignes auxquelles j'autorise l'accès à distance. Le commutateur Cisco permet 16 connexions à distance simultanées via les terminaux virtuels. Pour configurer les 16, il faut taper 0 pour le premier terminal, un espace, puis le numéro du dernier terminal que je veux configurer. Dans ce cas, je vais saisir 15. Ainsi, je peux configurer les terminaux virtuels de 0 à 15. Je saisis « password cisco » puis la commande « login ».

Examinons ces mots de passe dans la configuration en cours. Pour ce faire, je tape Ctrl+C pour passer en mode d'exécution privilégié, puis je saisis « show run », l'abréviation de « show running-config ». J'appuie sur Tab. La commande complète s'affiche. Voici le fichier de configuration en cours. J'appuie sur la barre d'espace et je navigue vers le bas. Vous voyez des configurations pour « line con 0 », « line vty 0 4 » et « line vty 5 15 ». Dans IOS, les lignes de terminal virtuel sont réparties en deux groupes : de 0 à 4 et de 5 à 15. Le mot de passe « cisco » s'affiche en texte brut, contrairement à la commande « enable secret password » où le mot de passe est chiffré via un hachage unidirectionnel. Pour renforcer la sécurité du commutateur, nous pouvons chiffrer ces mots de passe afin qu'ils ne soient plus visibles en texte brut.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Pour ce faire, je reviens au mode de configuration globale et je saisis la commande « service password-encryption ». Cette commande offre un chiffrement faible de tous les mots de passe du commutateur. Allons vérifier en mode d'exécution privilégié, dans le fichier de configuration en cours. J'appuie sur la barre d'espace pour descendre. Vous voyez que le mot de passe « cisco » est désormais chiffré à l'aide d'un chiffrement de type 7. Ce n'est pas un chiffrement très fort, mais il augmente tout de même la sécurité. Autre commande de configuration initiale importante pour sécuriser l'accès au commutateur : définir un message de bannière. Pour ce faire, je passe en mode de configuration globale, et je saisis la commande « banner motd » pour « message of the day ». Je peux saisir un message que les utilisateurs voient lorsqu'ils se connectent, par exemple une mention légale informant les personnes non autorisées qu'elles sont en infraction et risquent des poursuites. Je peux désormais saisir mon message de sécurité entre deux délimiteurs. Pour vos délimiteurs, optez pour un caractère non utilisé dans le message. Par exemple, j'utilise des guillemets dans mon message. Entre les guillemets, je saisis le message « Aucun accès non autorisé n'est permis. Les contrevenants seront poursuivis dans les limites légales autorisées. » Ainsi, les pirates potentiels sauront qu'ils essaient d'accéder à un périphérique ou réseau sécurisé, et qu'il s'agit d'un environnement protégé par la loi. J'appuie sur « Entrée ». La bannière est configurée. Examinons ces configurations de sécurité. Je tape Ctrl+C, puis je saisis « exit » pour quitter le commutateur. J'appuie sur « Entrée ». L'avertissement de la bannière s'affiche ainsi qu'une demande de mot de passe rien que pour accéder à la console. Je saisis le mot de passe « cisco ». Je suis en mode d'exécution utilisateur. Je tape « enable ». Je dois saisir un autre mot de passe pour accéder au mode d'exécution privilégié. Je saisis le mot de passe « class ». J'ai désormais un accès complet au commutateur.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.