16.4.1 - Sécurité des périphériques

Cisco AutoSecure

Un domaine des réseaux qui nécessite une attention particulière pour maintenir la sécurité est les appareils. Vous disposez probablement déjà d'un mot de passe pour votre ordinateur, votre smartphone ou votre tablette. Est-il aussi fort que possible? Utilisez-vous d'autres outils pour améliorer la sécurité de vos appareils? Cette rubrique vous explique comment.

les paramètres de sécurité sont définis à l'aide des valeurs par défaut, Lorsqu'un nouveau système d'exploitation est installé sur un périphérique. Dans la pluPartie des cas, le niveau de sécurité correspondant n'est pas suffisant. Sur les routeurs Cisco, la fonction Cisco AutoSecure permet de sécuriser le système, comme le montre la figure.

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

Voici également quelques étapes simples qu'il convient d'effectuer sur la pluPartie des systèmes d'exploitation:

- Changement immédiat des noms d'utilisateur et des mots de passe par défaut.
- Accès aux ressources du système limité strictement aux personnes autorisées à utiliser ces ressources.
- Désactivation des services et des applications qui ne sont pas nécessaires et désinstallation dans la mesure du possible.

Souvent, les périphériques expédiés par les fabricants ont été entreposés pendant un certain temps et ne disposent pas des correctifs les plus récents. Il est important de mettre à jour les logiciels et d'installer les correctifs de sécurité avant toute mise en œuvre.

16.4.2

Mots de passe

Pour protéger les périphériques réseau, il est important d'utiliser des mots de passe forts. Voici quelques recommandations classiques à suivre:

- Utilisez un mot de passe d'au moins 8 caractères et de préférence au moins 10 caractères. Plus le mot de passe est long, plus qu'il est fort.
- Choisissez des mots de passe complexes. Utilisez une combinaison de lettres majuscules et minuscules, de chiffres, de symboles et d'espaces si elles sont autorisées.
- Évitez de répéter un même mot, d'utiliser des mots communs du dictionnaire, des lettres ou des chiffres consécutifs, les noms d'utilisateur, les noms des membres de votre famille ou de vos animaux domestiques, des informations biographiques telles que la date de naissance, les numéros d'identification, les noms de vos ascendants ou toute autre information facilement identifiable.
- Faites volontairement des fautes d'orthographe. Par exemple, Smith = Smyth = 5mYth ou Sécurité = 5ecur1te.
- Modifiez régulièrement votre mot de passe. Si un mot de passe est compromis sans le savoir, la possibilité pour l'acteur de menace d'utiliser le mot de passe est limitée.
- Ne notez pas les mots de passe sur des bouts de papier placés en évidence sur votre bureau ou sur votre écran.

Weak Passwords

Mot de passe faible	Raison de sa faiblesse
secret	Mot de passe simple tiré du dictionnaire
Dupont	Maiden name of mother
toyota	Marque d'une voiture
bob1967	Nom et année de naissance de l'utilisateur
Blueleaf23	Mots et chiffres simples

Strong Passwords

Mot de passe fort	Raison de sa force
b67n42d39c	Il combine des caractères alphanumériques.
12^h u4@1p7	Il combine des caractères alphanumériques, des symboles et comprend un espace.

Sur les routeurs Cisco, les espaces en début de mot de passe sont ignorés, mais ceux situés après le premier caractère sont pris en compte. Par conséquent, vous pouvez utiliser la barre d'espace pour créer un mot de passe fort composé d'une expression de plusieurs mots. On parle dans ce cas de phrase secrète. Une phrase de passe est souvent plus facile à retenir qu'un simple mot de passe. Elle est également plus longue et plus difficile à deviner.

16.4.3

Sécurité supplémentaire des mots de passe

Les mots de passe forts sont efficaces uniquement s'ils sont secrets. Plusieurs mesures permettent de s'assurer que les mots de passe restent secrets sur un routeur et un commutateur Cisco, y compris ceux-ci :

- Cryptage tous les mots de passe en texte clair.
- Définition d'une longueur de mot de passe minimale acceptable
- Empêcher les attaques par force de deviner les mots de passe
- Désactivation d'un accès en mode EXEC privilégié inactif après une durée spécifiée.

Comme le montre l'exemple de configuration dans la figure, la commande de configuration **service password-encryption** globale empêche les personnes non autorisées de connaître les mots de passe en texte clair dans le fichier de configuration. Cette commande chiffre tous les mots de passe en texte clair. Notez dans l'exemple que le mot de passe «cisco» a été chiffré en tant que «03095A0F034F».

En outre, pour garantir la longueur minimale de tous les mots de passe configurés, utilisez la commande **security passwords min-length** *length* en mode de configuration globale. Dans la figure, chaque nouveau mot de passe configuré devrait avoir une longueur minimale de huit caractères.

Les acteurs de menace peuvent utiliser un logiciel de craquage de mot de passe pour mener une attaque par force sur un périphérique réseau. Cette attaque tente continuellement de deviner les mots de passe valides jusqu'à ce que l'un d'entre eux fonctionne. Utilisez la commande de configuration globale **login block-for # attempts # within #** pour dissuader ce type d'attaque. Dans l'illustration la commande **login block-for 120 attempts 3 within 60** bloque les tentatives de connexion pendant 120 secondes après trois échecs de connexion en l'espace de 60 secondes.

Les administrateurs réseau peuvent être distraits et laisser accidentellement une session en mode EXEC privilégiée ouverte sur un terminal. Cela pourrait permettre à un acteur de menace interne de modifier ou d'effacer la configuration du périphérique.

Par défaut, les routeurs Cisco déconnectent une session EXEC après 10 minutes d'inactivité. Toutefois, vous pouvez réduire ce paramètre à l'aide de la commande de configuration de ligne **exec-timeout** *minutes secondes*. Cette commande peut être appliquée à la console en ligne, aux lignes auxiliaires et aux lignes vty. Dans la figure, nous demandons au périphérique Cisco de déconnecter automatiquement un utilisateur inactif sur une ligne vty après que l'utilisateur a été inactif pendant 5 minutes et 30 secondes.

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco123
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
R1# show running-config | section line vty
line vty 0 4
 password 7 094F471A1A0A
 exec-timeout 5 30
 login
 transport input ssh
R1#
```

Activation de SSH

Telnet simplifie l'accès aux périphériques à distance, mais il n'est pas sécurisé. Les données contenues dans un paquet Telnet sont transmises en clair. Par conséquent, il est vivement recommandé d'activer SSH sur les périphériques pour assurer la sécurité des accès à distance.

Il est possible de configurer un périphérique Cisco pour supporter SSH en suivant les six étapes suivantes :

Étape 1. Configurez un nom d'hôte unique pour le périphérique. Un appareil doit avoir un nom d'hôte unique autre que celui par défaut.

Étape 2. Configurez le nom de domaine IP. Configurez le nom de domaine IP du réseau en utilisant la commande de configuration globale **ip-domain name**.

Étape 3. Générez une clé pour chiffrer le trafic SSH. SSH crypte le trafic entre la source et la destination. Toutefois, pour effectuer cette opération, une clé d'authentification unique doit être générée en utilisant la commande de configuration globale **crypto key generate rsa general-keys modulus** *bits*. Le module de *bits* détermine la taille de la clé et peut être configuré de 360 bits à 2048 bits. Plus la valeur du bit est grande, plus la clé est sécurisée. Cependant, les valeurs de bits plus importantes prennent également plus de temps pour chiffrer et déchiffrer les informations. Il est recommandé d'utiliser un module d'au moins 1024 bits.

Étape 4. Vérifiez ou créer une entrée dans la base de données locale. Créez une entrée de nom d'utilisateur dans la base de données locale à l'aide de la commande de configuration globale **username** . Dans l'exemple, le paramètre **secret** est utilisé pour que le mot de passe soit chiffré à l'aide de MD5.

Étape 5. Authentification par rapport à la base de données locale. Utilisez la commande **login local** de configuration de ligne pour authentifier la ligne vty par rapport à la base de données locale.

Étape 6. Activez les sessions SSH entrantes de vty. Par défaut, aucune session d'entrée n'est autorisée sur les lignes vty. Vous pouvez spécifier plusieurs protocoles d'entrée, y compris Telnet et SSH à l'aide de la commande **transport input [ssh | telnet]** .

Comme indiqué dans l'illustration, le routeur R1 est configuré dans le domaine span.com. Ces informations sont utilisées avec la valeur binaire spécifiée dans la commande **crypto key generate rsa general-keys modulus** pour créer une clé de chiffrement.

Ensuite, une entrée de base de données locale pour un utilisateur nommé Bob est créée. Enfin, les lignes vty sont configurées pour s'authentifier auprès de la base de données locale et pour accepter uniquement les sessions SSH entrantes.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

Désactiver les services inutilisés

Les routeurs et les commutateurs Cisco démarrent avec une liste de services actifs qui peuvent ou non être requis dans votre réseau. Désactivez tous les services inutilisés pour préserver les ressources système, telles que les cycles CPU et la RAM, et empêcher les acteurs de menace d'exploiter ces services. Le type de services activés par défaut varie en fonction de la version d'IOS. Par exemple, IOS-XE n'a généralement que les ports HTTPS et DHCP ouverts. Vous pouvez le vérifier avec la commande **show ip ports all** , comme indiqué dans l'exemple.

Modifié le: mardi 5 mars 2024, 14:19

◄ 16.2.2 - Atténuation des attaques du réseau

Aller à...

BTS SIO Lycée CFA Robert Schuman Metz