Travaux pratiques – Sécurisation des périphériques réseau

Topologie

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	NA
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1

Objectifs

1re partie : Configurer les paramètres de base du périphérique

2e partie : Configurer les mesures de sécurité de base sur le routeur

3e partie : Configurer les mesures de sécurité de base sur le commutateur

Contexte/scénario

Il est recommandé de configurer tous les périphériques réseau avec, au moins, un nombre minimum de commandes de sécurité basées sur les meilleures pratiques. Cela inclut les périphériques d'utilisateur final, les serveurs et les périphériques réseau, tels que les routeurs et les commutateurs.

Au cours de ces travaux pratiques, vous allez configurer les périphériques réseau dans la topologie pour qu'ils acceptent les sessions SSH et permettent une gestion à distance. Vous utiliserez également l'interface de ligne de commande IOS pour configurer les mesures de sécurité communes et basiques en matière de meilleures pratiques. Vous testerez ensuite les mesures de sécurité pour vérifier qu'elles sont correctement mises en œuvre et qu'elles fonctionnent correctement.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs ISR Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960s équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Ressources requises

- 1 routeur (Cisco 1941 équipé du logiciel Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)

- 1 ordinateur (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet tel qu'indiqués dans la topologie

1re partie : Configurer les paramètres de base des périphériques

Dans la première partie, vous allez configurer la topologie du réseau et configurer les paramètres de base, tels que les adresses IP des interfaces, l'accès des périphériques et les mots de passe sur le routeur.

Étape 1 : Câblez le réseau conformément à la topologie.

Connectez les équipements représentés dans la topologie et effectuez le câblage nécessaire.

Étape 2 : Initialisez et redémarrez le routeur et le commutateur.

Étape 3 : Configurez le routeur.

Reportez-vous aux travaux pratiques précédents pour obtenir de l'aide sur les commandes requises pour SSH.

a. Accédez au routeur par la console et activez le mode d'exécution privilégié.

b. Passez en mode de configuration.

c. Attribuez le nom R1 au routeur.

d. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

e. Définissez **class** comme mot de passe chiffré d'exécution privilégié.

f. Définissez **cisco** comme mot de passe de console et activez la connexion.

g. Définissez **cisco** comme mot de passe vty et activez la connexion.

h. Chiffrez tous les mots de passe en clair.

i. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

j. Configurez et activez l'interface G0/1 sur le routeur à l'aide des informations contenues dans la table d'adressage.

k. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Étape 4 : Configurez le commutateur.

a. Accédez au commutateur par la console et activez le mode d'exécution privilégié.

b. Passez en mode de configuration.

c. Attribuez le nom S1 au commutateur.

d. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

e. Définissez **class** comme mot de passe chiffré d'exécution privilégié.

f. Définissez **cisco** comme mot de passe de console et activez la connexion.

g. Définissez **cisco** comme mot de passe vty et activez la connexion.

h. Chiffrez tous les mots de passe en clair.

i. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

j. Configurez l'interface SVI par défaut avec les informations d'adresse IP figurant dans la table d'adressage.

k. Enregistrez la configuration en cours dans le fichier de configuration initiale.

2e partie : Configurer les mesures de sécurité de base sur le routeur

Étape 1 : Renforcez les mots de passe.

Un administrateur doit s'assurer que les mots de passe respectent les consignes standard pour les mots de passe forts. Les consignes peuvent être d'inclure des lettres, des chiffres et des caractères spéciaux dans le mot de passe et de définir une longueur minimale.

Remarque : les consignes visant à promouvoir les meilleures pratiques requièrent l'utilisation de mots de passe forts, comme ceux affichés ici, dans un environnement de production. Cependant, les autres travaux pratiques de ce cours utilisent les mots de passe cisco et class par souci de facilité lors de l'exécution des travaux pratiques.

a. Modifiez le mot de passe chiffré du mode d'exécution privilégié pour satisfaire aux instructions.

```
R1(config)# enable secret Enablep@55
```

b. Imposez l'utilisation d'au moins 10 caractères pour tous les mots de passe.

```
R1(config)# security passwords min-length 10
```

Étape 2 : Activez les connexions SSH.

a. Attribuez le nom de domaine **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Créez une entrée de base de données d'utilisateur local à utiliser lors de la connexion au routeur via SSH. Le mot de passe doit être conforme aux normes des mots de passe forts et l'utilisateur doit disposer d'un accès de niveau administrateur.

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

c. Configurez transport input pour les lignes vty de façon à ce que les connexions SSH soient autorisées, mais pas les connexions Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. Les lignes vty doivent utiliser la base de données des utilisateurs locaux pour l'authentification.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Générez une clé de chiffrement RSA en utilisant un module de 1 024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.CCNA-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Étape 3 : Sécurisez les lignes de console et VTY.

a. Vous pouvez configurer le routeur pour qu'une connexion inactive pendant une durée définie soit automatiquement fermée. Si un administrateur réseau est connecté à un périphérique réseau et doit soudainement s'absenter, cette commande déconnecte automatiquement l'utilisateur au terme du délai spécifié. Les commandes suivantes déconnectent la ligne après cinq minutes d'inactivité.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. La commande suivante empêche les tentatives de connexion par force brute. Le routeur bloque les tentatives de connexion pendant 30 secondes si quelqu'un effectue deux tentatives infructueuses en l'espace de 120 secondes. Ce minuteur a été défini à une valeur particulièrement faible pour les besoins de ces travaux pratiques.

```
R1(config)#login block-for 30 attempts 2 within 120
```

Que signifie **2 within 120** dans la commande ci-dessus ?

Que signifie **block-for 30** dans la commande ci-dessus ?

Étape 4 : Vérifiez que tous les ports inutilisés sont désactivés.

Les ports du routeur sont désactivés, par défaut, mais il est toujours prudent de vérifier que tous les ports inutilisés se trouvent dans un état administratively down. Vous pouvez rapidement vérifier cela en tapant la commande **show ip interface brief**. Tous les ports inutilisés qui ne se trouvent pas en état administratively down doivent être désactivés au moyen de la commande **shutdown** en mode de configuration d'interface.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Étape 5 : Vérifiez que vos mesures de sécurité ont été mises en œuvre correctement.

a. Utilisez Tera Term pour établir une connexion telnet vers R1.

R1 accepte-t-il la connexion Telnet ?

Justifiez votre réponse.

b. Utilisez Tera Term pour établir une connexion SSH vers R1.

R1 accepte-t-il la connexion SSH ?

c. Tapez intentionnellement les informations d'utilisateur et de mot de passe pour voir si l'accès est bloqué au bout de deux tentatives.

Que s'est-il passé lorsque vous n'êtes pas parvenu à vous connecter la deuxième fois ?

d. À partir de votre session de console sur le routeur, entrez la commande **show login** pour afficher l'état de la connexion. Dans l'exemple ci-dessous, la commande **show login** a été exécutée dans les 30 secondes du délai de blocage des connexions et indique que le routeur est en mode silencieux (Quiet-Mode). Le routeur n'acceptera plus aucune tentative de connexion pendant 14 secondes supplémentaires.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. Au terme du délai des 30 secondes, envoyez à nouveau SSH à R1 et connectez-vous au moyen du nom d'utilisateur **admin** et du mot de passe **Admin15p@55**.

Une fois que vous vous êtes connecté avec succès, qu'est-ce qui s'est affiché ?

f. Passez en mode d'exécution privilégié et utilisez **Enablep@55** pour le mot de passe.

Si vous n'avez pas tapé correctement ce mot de passe, êtes-vous déconnecté de votre session SSH après deux tentatives infructueuses en l'espace de 120 secondes ?

Justifiez votre réponse.

g. Exécutez la commande **show running-config** à l'invite du mode d'exécution privilégié pour afficher les paramètres de sécurité que vous avez appliqués.

3e partie : Configurer les mesures de sécurité de base sur le commutateur

Étape 1 : Renforcez les mots de passe sur le commutateur.

Modifiez le mot de passe chiffré du mode d'exécution privilégié pour satisfaire aux consignes relatives aux mots de passe forts.

```
S1(config)# enable secret Enablep@55
```

Remarque : la commande **password min-length** de sécurité n'est pas disponible sur le commutateur 2960.

Étape 2 : Activez les connexions SSH.

a. Attribuez le nom de domaine **CCNA-lab.com**.

```
S1(config)# ip domain-name CCNA-lab.com
```

b. Créez une entrée de base de données d'utilisateur local à utiliser lors de la connexion au routeur via SSH. Le mot de passe doit être conforme aux normes des mots de passe forts et l'utilisateur doit disposer d'un accès de niveau administrateur.

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

c. Configurez le transport input pour les lignes vty de façon à autoriser les connexions SSH mais pas les connexions Telnet.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. Les lignes vty doivent utiliser la base de données des utilisateurs locaux pour l'authentification.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Générez une clé de chiffrement RSA en utilisant un module de 1 024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Étape 3 : Sécurisez les lignes de console et VTY.

a. Configurez le commutateur pour qu'il désactive toute ligne inactive depuis 10 minutes.

```
S1(config)#line console 0
S1(config-line)#exec-timeout 10 0
S1(config-line)#line vty 0 15
S1(config-line)#exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. Pour empêcher toute tentative de connexion par la force brute, configurez le commutateur pour qu'il bloque les accès pendant 30 secondes lorsque 2 tentatives infructueuses sont effectuées en l'espace de 120 secondes. Ce minuteur a été défini à une valeur particulièrement faible pour les besoins de ces travaux pratiques.

```
S1(config)#login block-for 30 attempts 2 within 120
S1(config)# end
```

Étape 4 : Vérifiez que tous les ports inutilisés sont désactivés.

Par défaut, les ports du commutateur sont activés. Désactivez tous les ports inactifs sur le commutateur.

a. Vous pouvez vérifier l'état des ports du commutateur au moyen de la commande **show ip interface brief**.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
```

```
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

b. Utilisez la commande **interface range** pour désactiver plusieurs interfaces à la fois.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. Vérifiez que toutes les interfaces inactives ont été désactivées administrativement.

```
S1# showip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
```

```
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Étape 5 : Vérifiez que vos mesures de sécurité ont été mises en œuvre correctement.

a. Vérifiez que la connexion Telnet a été désactivée sur le commutateur.

b. Envoyez SSH au commutateur et effectuez volontairement une faute en tapant les informations de l'utilisateur et du mot de passe pour vérifier si l'accès est bloqué.

c. Au terme du délai des 30 secondes, envoyez à nouveau SSH à S1 et connectez-vous au moyen du nom d'utilisateur **admin** et du mot de passe **Admin15p@55**.

   La bannière s'est-elle affichée après vous être connecté avec succès ?

d. Passez en mode d'exécution privilégié en utilisant **Enablep@55** comme mot de passe.

e. Exécutez la commande **show running-config** à l'invite du mode d'exécution privilégié pour afficher les paramètres de sécurité que vous avez appliqués.

Remarques générales

1. La commande **passwordcisco** a été entrée pour les lignes console et vty dans votre configuration de base dans la première partie. Quand ce mot de passe est-il utilisé lorsque les mesures de sécurité des meilleures pratiques ont été appliquées ?

2. Les mots de passe préconfigurés, comportant moins de 10 caractères, sont-ils concernés par la commande **security passwords min-length 10** ?

Tableau récapitulatif de l'interface du routeur

Récapitulatif de l'interface du routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des combinaisons possibles des interfaces Ethernet et série dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes de Cisco IOS.