Travaux pratiques - Sécurisation des périphériques réseau

Topologie

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A
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

Partie 1 : Configurer les paramètres de base des périphériques

Partie 2 : Configurer les mesures de sécurité de base sur le routeur

Partie 3 : 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 des utilisateurs finaux, 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 en ligne de commande de Cisco IOS pour configurer des mesures de sécurité communes et basiques conformes aux meilleures pratiques. Vous testerez ensuite ces mesures de sécurité pour vérifier qu'elles sont correctement mises en œuvre et qu'elles fonctionnent correctement.

Remarque: les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 équipé de version 16.9.4 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (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 ce qui est indiqué 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 les commutateurs ont été effacés et n'ont pas de configuration de démarrage. En cas de doute, contactez votre instructeur.

Ressources requises

- 1 Routeur (Cisco 4221 équipé de Cisco IOS version 16.9.4, image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.2(2) image lanbasek9 ou similaire)
- 1 ordinateur (Windows équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Instructions

Partie 1 : 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 les périphériques.

Étape 1: Câblez le réseau conformément à la topologie.

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

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

Étape 3: Configurez le routeur et le commutateur.

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

b. Attribuez le nom du périphérique comme indiqué dans la table d'adressage.

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

d. Attribuez class comme mot de passe chiffré d'exécution privilégié.

e. Attribuez cisco comme mot de passe de console et activez la connexion.

f. Attribuez cisco comme mot de passe VTY et activez la connexion.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

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

i. Configurez l'interface SVI par défaut sur le commutateur avec les informations d'adresse IP figurant dans la table d'adressage.

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

Étape 4: Configurez PC-A.

a. Configurez PC-A avec une adresse IP et un masque de sous-réseau.

b. Configurez une passerelle par défaut pour PC-A.

Étape 5: Vérifiez la connectivité du réseau.

Envoyez une requête ping de PC-A vers R1. Si la requête ping échoue, dépannez la connexion.

Partie 2 : Configurer les mesures de sécurité de base sur le routeur

Étape 1: Configuration des mesures de sécurité

a. Chiffrez tous les mots de passe.

b. Configurez le système pour qu'il nécessite un mot de passe de 12 caractères minimum.

c. Modifiez les mots de passe (privilège exec, console et vty) pour répondre à la nouvelle exigence de longueur.

   1) Définissez le mot de passe exec privilégié sur **$cisco!PRIV***

   2) Définissez le mot de passe de connexion de la console sur **$cisco!!CON***

   3) Définissez le mot de passe de la ligne vty sur **$cisco!!VTY***

d. Configurer le routeur pour accepter uniquement les connexions SSH à partir d'emplacements distants

   1) Configurez le nom d'utilisateur **SshAdmin** avec un mot de passe crypté de **55HAdm!n2020**

   2) Le nom de domaine du routeur doit être défini sur ccna-lab.com

   3) Le module de la clé doit être de 1024 bits.

e. Définissez les configurations de sécurité et les meilleures pratiques sur la console et les lignes vty.

1) Les utilisateurs doivent être déconnectés après 5 minutes d'inactivité.
2) Le routeur ne doit pas autoriser les connexions vty pendant 2 minutes si 3 tentatives de connexion échouées se produisent dans une minute.

Partie 3 : Configuration des mesures de sécurité

Étape 1: 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 à l'état d'arrêt administratif (administratively down). Vous pouvez rapidement vérifier cela en tapant la commande **show ip interface brief**. Tous les ports inutilisés qui ne se trouvent à l'état d'arrêt administratif doivent être désactivés au moyen de la commande **shutdown** en mode de configuration d'interface.

Étape 2: 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 ? Expliquez votre réponse.

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

   R1 accepte-t-il la connexion SSH ?

c. Effectuez volontairement une faute en tapant les informations de l'utilisateur et du 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 120 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 111 secondes supplémentaires.

e. Au terme du délai des 30 secondes, envoyez à nouveau SSH à R1 et connectez-vous au moyen du nom d'utilisateur **SSHadmin** et du mot de passe **Admin1p@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** comme 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 60 secondes ? Expliquez 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.

Partie 4 : Configurer les mesures de sécurité de base sur le commutateur

Étape 1: Configuration des mesures de sécurité

a. Chiffrez tous les mots de passe.

b. Configurez le système pour exiger un mot de passe de 12 caractères minimum

c. Modifiez les mots de passe (privilège exec, console et vty) pour répondre à la nouvelle exigence de longueur.

1) Définissez le mot de passe exec privilégié sur **$cisco!PRIV***

2) Définissez le mot de passe de connexion de la console sur **$cisco!!CON***

3) Définissez le mot de passe de la ligne vty sur **$cisco!!VTY***

d. Configurez le commutateur pour accepter uniquement les connexions SSH provenant d'emplacements distants.

1) Configurez le nom d'utilisateur **SshAdmin** avec un mot de passe crypté de **55HAdm!n2020**

2) Le nom de domaine des commutateurs doit être défini sur ccna-lab.com

3) Le module de la clé doit être de 1024 bits.

e. Définissez les configurations de sécurité et les meilleures pratiques sur la console et les lignes vty.

1) Les utilisateurs doivent être déconnectés après 5 minutes d'inactivité.

2) Le commutateur ne doit pas autoriser les connexions pendant 2 minutes si 3 tentatives de connexion échouées se produisent dans une minute.

f. Désactivez tous les ports non utilisés.

Étape 2: 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**.

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

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

Étape 3: 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 R1 et connectez-vous au moyen du nom d'utilisateur **SSHadmin** et du mot de passe **Admin1p@55**.

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

d. Passez en mode d'exécution privilégié et utilisez **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.

Questions de réflexion

1. La commande **password cisco** a été entrée pour les lignes console et VTY dans votre configuration de base dans la première partie. Quand ce mot de passe sera-t-il utilisé une fois les mesures de sécurité des meilleures pratiques 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 des interfaces des routeurs

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)	Série 0/0/0 (S0/0/0)	Série 0/0/1 (S0/0/1)
1.900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Série 0/0/0 (S0/0/0)	Série 0/0/1 (S0/0/1)
2.801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Série 0/1/0 (S0/1/0)	Série 0/1/1 (S0/1/1)
2.811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Série 0/0/0 (S0/0/0)	Série 0/0/1 (S0/0/1)
2.900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Série 0/0/0 (S0/0/0)	Série 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Série 0/1/0 (S0/1/0)	Série 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Série 0/1/0 (S0/1/0)	Série 0/1/1 (S0/1/1)

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 différentes combinaisons d'interfaces Ethernet et série possibles dans l'appareil. Il 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 Cisco IOS.