Packet Tracer – Résilience des routeurs et des commutateurs

Table d'adressage

Appareil	Adresse IP	Masque de sous-réseau	Passerelle par défaut	Site
HQ_Router	10.44.1.1	255.255.255.0	N/A	Metropolis Bank HQ

Objectifs

Partie 1 : Renforcer la configuration IOS

Partie 2 : Activer la fonctionnalité de configuration résiliente de Cisco IOS

Contexte

Au cours de cette activité, vous renforcerez la configuration IOS d'un routeur sur le réseau de Metropolis. Vous activerez ensuite la fonctionnalité de résilience IOS sur un routeur Cisco. L'adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez les terminaux clients du réseau de Metropolis pour déployer la configuration résiliente d'IOS.

Partie 1 : Renforcer la configuration IOS

Étape 1 : Accédez à l'invite de commandes sur l'ordinateur de Sally.

a. Cliquez sur le site du **siège social de la Metropolis Bank**, puis sur l'ordinateur de **Sally**.

b. Cliquez sur l'onglet **Poste de travail**, puis sur **Invite de commande**.

Étape 2 : Connectez-vous à distance au routeur HQ_Router.

a. SSH au routeur **HQ_Router** en saisissant **ssh –l admin 10.44.1.1** dans l'invite de commandes. Utilisez le mot de passe **cisco12345** lorsque vous y êtes invité.

b. À l'invite, tapez **enable** et, lorsque vous y êtes invité, saisissez le mot de passe actif **class**.

L'invite suivante devrait s'afficher :

```
HQ_Router#
```

c. Avez-vous reçu un message d'avertissement destiné à protéger le routeur HQ_Router contre toute intrusion d'utilisateurs non autorisés ?

Étape 3 : Créez un message d'avertissement légal sur le routeur HQ_Router.

a. À l'invite `HQ_Router#`, passez en mode de configuration globale à l'aide de la commande **configure terminal**.

b. À l'invite `HQ_Router(config)#`, collez les commandes suivantes :

```
banner motd #
ACCÈS INTERDIT À TOUT UTILISATEUR NON AUTORISÉ
Vous devez disposer d'une autorisation explicite pour accéder à ce terminal
ou le configurer.
```

```
Toute tentative d'accès à ce système ou d'utilisation non autorisée sera passible de
poursuites civiles et pénales.
Toutes les activités effectuées sur ce terminal sont enregistrées et contrôlées.
#
```

c. À l'invite `HQ_Router(config)#`, utilisez les commandes **end** et **logout** pour couper votre connexion au routeur **HQ_Router**.

d. SSH dans le routeur **HQ_Router** à nouveau depuis l'ordinateur **Sally**. Le mot de passe SSH est **cisco12345**.

Avez-vous reçu des informations ou messages supplémentaires lorsque vous avez réussi à vous connecter au routeur **HQ_Router** ? Quels sont les éléments affichés ?

Étape 4 : Sécurisez le routeur HQ_Router à l'aide d'un mot de passe.

a. À l'invite, tapez **enable** et, lorsque vous y êtes invité, saisissez le mot de passe actif **class**.

b. Passez en mode de configuration globale au moyen de la commande **configure terminal**. À l'invite `HQ_Router(config)#`, collez les commandes suivantes :

```
!chiffre des mots de passe en clair dans la configuration running-config
service password-encryption

!impose un minimum de 10 caractères pour tout nouveau mot de passe
security passwords min-length 10
```

Partie 2 : Activer la fonctionnalité de configuration résiliente de Cisco IOS

Étape 1 : Affichez l'image IOS actuelle.

a. Une fois connecté via SSH sur l'ordinateur de **Sally**, saisissez la commande **exit** pour retrouver l'invite `HQ_Router#`.

b. Saisissez la commande **dir flash:** pour afficher le fichier IOS.bin actuel.

Quel est le nom du fichier .bin dans flash ?

Étape 2 : Sécurisez l'image et la configuration en cours d'exécution.

a. À l'invite `HQ_Router#`, passez en mode de configuration globale à l'aide de la commande **configure terminal**.

b. Utilisez la commande **secure boot-image** à l'invite `HQ_Router(config)#` pour activer la résilience de l'image IOS et éviter que le fichier IOS apparaisse dans le répertoire affiché dans les résultats tout en rendant impossible la suppression du fichier IOS sécurisé.

c. Utilisez la commande **secure boot-config** à l'invite `HQ_Router(config)#` pour enregistrer une copie sécurisée de la configuration en cours d'exécution et rendre impossible la suppression du fichier de configuration sécurisé.

d. Revenez en mode d'exécution privilégié avec la commande **exit**. Saisissez la commande **dir flash:** pour afficher le fichier IOS.bin actuel.

   Y a-t-il des fichiers IOS.bin répertoriés ?

e. À l'invite `HQ_Router#`, saisissez la commande **show secure bootset** pour afficher l'état de la résilience de l'image et de la configuration IOS Cisco.

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Renforcer la configuration IOS	Étape 2	10	
	Étape 3	10	
Partie 2 : Activer la fonctionnalité de configuration résiliente pour IOS Cisco	Étape 1	10	
	Étape 2	10	
	Questions	**40**	
	Score relatif à Packet Tracer	**60**	
	Score total	**100**	