Packet Tracer - Sécurisation des périphériques réseau

Table d'adressage

Périphérique	Interface	Adresse	Masque	Passerelle
RTR-A	G0/0/0	192.168.1.1	255.255.255.0	N/A
	G0/0/1	192.168.2.1	255.255.255.0	N/A
SW-1	Interface SVI	192.168.1.254	255.255.255.0	
PC	Carte réseau	192.168.1.2	255.255.255.0	
Ordinateur portable	Carte réseau	192.168.1.10	255.255.255.0	
Ordinateur distant	Carte réseau	192.168.2.10	255.255.255.0	

Exigences

Remarque: Pour que cette activité soit brève et facile à gérer, certains paramètres de configuration de sécurité n'ont pas été définis. Dans d'autres cas, les meilleures pratiques en matière de sécurité n'ont pas été suivies.

Dans cette activité, vous configurerez un routeur et un commutateur selon la liste d'exigences.

Instructions

Étape 1: Documentez la configuration de réseau

Complétez la table d'adressage avec les informations nécessaires.

Étape 2: Configuration requise du routeur:

- Empêchez l'IOS de tenter à résoudre des commandes mal tapées sur les noms de domaine.
- Les noms d'hôte correspondant aux valeurs de la table d'adressage.
- Les mots de passe nouvellement créés requis au moins 10 caractères de longueur.
- Un mot de passe fort à dix caractères pour la ligne de console. Utilisez **@Cons1234!**

- Assurez-vous que les sessions console et VTY se ferment après exactement 7 minutes .
- Un mot de passe de dix caractères fort et chiffré pour le mode d'exécution privilégié. Pour cette activité, il est permis d'utiliser le même mot de passe que la ligne de console.
- Une bannière MOTD qui met en garde contre l'accès aux périphériques non autorisés.
- Le cryptage de tous les mots de passe.
- Un nom d'utilisateur de **NetAdmin** avec un mot de passe chiffré **LogAdmin!9**.
- Activez le routage SSH.
  - Utilisez **security.com** comme un nom de domaine.
  - Utilisez un module de **1024**.
- Les lignes VTY doivent utiliser SSH pour les connexions entrantes.
- Les lignes VTY doivent utiliser le nom d'utilisateur et le mot de passe qui ont été configurés pour authentifier les connexions.
- Empêcher les tentatives de connexion de force brute en utilisant une commande qui bloque les tentatives de connexion pendant 45 secondes si quelqu'un échoue trois tentatives dans un délai de 100 secondes.

Étape 3: La Configuration requise du commutateur:

- Tous les ports de commutateur inutilisés sont administrativement désactivés.
- L'interface de gestion par défaut SW-1 doit accepter les connexions via le réseau. Utilisez les information répertorié dans la table d'adressage. Le commutateur doit être accessible à partir de réseaux distants.
- Utilisez **@Cons1234!** comme un mot de passe d'exécution privilégié.
- Configurer SSH comme on l'a fait pour le routeur.
- Créer un nom d'utilisateur **NetAdmin** avec le mot de passe secret crypté **LogAdmin! 9**
- Les lignes VTY ne doivent pas accepter que les connexions via SSH.
- Les lignes VTY ne doivent autoriser que le compte d'administrateur réseau pour accéder à l'interface de gestion du commutateur.
- Les hôtes des deux réseaux locaux doivent pouvoir envoyer une requête ping vers l'interface de gestion du commutateur.