Packet Tracer : configuration de SSH

Topologie

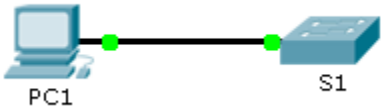

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objectifs

Partie 1 : sécurisation des mots de passe

Partie 2 : chiffrement des communications

Partie 3 : vérification de l'implémentation de SSH

Contexte

SSH doit remplacer Telnet pour les connexions relatives à la gestion. Telnet utilise des communications non sécurisées en texte clair. SSH assure la sécurité des connexions distantes en fournissant un chiffrement efficace de toutes les données transmises entre les périphériques. Dans cet exercice, vous allez sécuriser un commutateur distant avec le chiffrement de mot de passe et SSH.

Partie 1 : Sécurisation des mots de passe

a. À partir de l'invite de commande de **PC1**, établissez une connexion Telnet vers **S1**. Le mot de passe d'exécution privilégié et utilisateur est **cisco**.

b. Enregistrez la configuration actuelle de sorte que toutes les éventuelles erreurs commises soient annulées en basculant l'interrupteur de **S1**.

c. Affichez la configuration en cours et notez que les mots de passe sont en texte clair. Entrez la commande permettant de chiffrer les mots de passe en clair **:**

service password-encryption

d. Vérifiez que les mots de passe sont chiffrés.

Partie 2 : Chiffrement des communications

Étape 1 : Définissez le nom de domaine IP et générez des clés sécurisées.

L'utilisation de Telnet n'est généralement pas fiable, car les données sont transmises en texte clair. Par conséquent, utilisez SSH chaque fois qu'il est disponible.

a. Définissez le nom de domaine sur **netacad.pka.**

b. Des clés sécurisées sont nécessaires pour chiffrer les données. Générez des clés RSA en spécifiant une longueur de 1024.

Étape 2 : Créez un utilisateur SSH et reconfigurez les lignes VTY pour un accès SSH uniquement.

a. Créez l'utilisateur **administrator** en lui attribuant **cisco** comme mot de passe.

b. Configurer les lignes VTY pour vérifier les informations de connexion dans la base de données et pour autoriser uniquement l'accès à distance SSH. Supprimez le mot de passe existant pour les lignes vty.

Partie 3 : Vérification de l'implémentation SSH

a. Quittez la session Telnet et tentez de vous reconnecter en utilisant Telnet. La tentative doit échouer.

b. Tentez de vous connecter via SSH. Tapez **ssh** et appuyez sur **Entrée** sans définir aucun paramètre afin d'afficher les instructions d'utilisation de la commande. Indice : l'option `-l` est la lettre « L », et non pas le chiffre 1.

c. Une fois correctement connecté, passez en mode d'exécution privilégié et enregistrez la configuration. Si vous n'avez pas pu accéder à **S1**, mettez-le hors tension et recommencez depuis la Partie 1.