Packet Tracer: Configuración de SSH

Topología

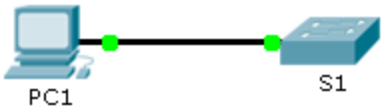

Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objetivos

Parte 1: Proteger las contraseñas

Parte 2: Cifrar las comunicaciones

Parte 3: Verificar la implementación de SSH

Aspectos básicos

SSH debe reemplazar a Telnet para las conexiones de administración. Telnet usa comunicaciones inseguras de texto no cifrado. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro de todos los datos transmitidos entre los dispositivos. En esta actividad, protegerá un switch remoto con el cifrado de contraseñas y SSH.

Parte 1: Proteger las contraseñas

a. Desde el símbolo del sistema en la **PC1**, acceda al **S1** mediante Telnet. La contraseña de los modos EXEC del usuario y EXEC privilegiado es **cisco**.

b. Guarde la configuración actual, de manera que pueda revertir cualquier error que cometa reiniciando el **S1**.

c. Muestre la configuración actual y observe que las contraseñas están en texto no cifrado. Introduzca el comando para cifrar las contraseñas de texto no cifrado.

s1 (config) #service password-encryption

d. Verifique que las contraseñas estén cifradas.

© 2017 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 2: Cifrar las comunicaciones

Paso 1: Establecer el nombre de dominio IP y generar claves seguras

En general no es seguro utilizar Telnet, porque los datos se transfieren como texto no cifrado. Por lo tanto, utilice SSH siempre que esté disponible.

a. Configure el nombre de dominio **netacad.pka.**

s1 (config) #ip domain-name netacad.pka

b. Se necesitan claves seguras para cifrar los datos. Genere las claves RSA con la longitud de clave 1024.

s1 (config) #crypto key generate rsa

Paso 2: Crear un usuario de SSH y reconfigurar las líneas VTY para que solo admitan acceso por SSH

a. Cree un usuario **administrador** con **cisco** como contraseña secreta.

s1 (config) #username administrator secret cisco

b. Configure las líneas VTY para que revisen la base de datos local de nombres de usuario en busca de las credenciales de inicio de sesión y para que solo permitan el acceso remoto mediante SSH. Elimine la contraseña existente de la línea vty.

s1 (config) #line vty 0 15

s1 (config) #no password

s1 (config-line) #transport input ssh

Parte 3: Verificar la implementación de SSH

a. Cierre la sesión de Telnet e intente iniciar sesión nuevamente con Telnet. El intento debería fallar.

b. Intente iniciar sesión mediante SSH. Escriba **ssh** y presione la tecla **Enter**, sin incluir ningún parámetro que revele las instrucciones de uso de comandos. Sugerencia: la opción `-l` representa la letra “L”, no el número 1.

c. Cuando inicie sesión de forma correcta, ingrese al modo EXEC privilegiado y guarde la configuración. Si no pudo acceder de forma correcta al **S1**, reinicie y comience de nuevo en la parte 1.

© 2017 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.