Laboratorio: dispositivos de red seguros

Topología

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: configurar ajustes básicos de los dispositivos

Parte 2: Configurar medidas básicas de seguridad en el router

Parte 3: configurar medidas de seguridad básicas en el switch

Aspectos básicos/situación

Se recomienda que todos los dispositivos de red se configuren con al menos un conjunto de comandos de seguridad recomendados. Esto incluye dispositivos para usuarios finales, servidores y dispositivos de red, como routers y switches.

En esta actividad de laboratorio, configurará los dispositivos de red en la topología a fin de que acepten sesiones de SSH para la administración remota. También utilizará la CLI del IOS para configurar medidas de seguridad básicas según las prácticas recomendadas. Luego, probará las medidas de seguridad para verificar que estén implementadas de manera apropiada y que funcionen correctamente.

Nota:Los routers utilizados con los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.4 (universalk9 image). Los switches utilizados en los laboratorios son Cisco Catalyst 2960s con Cisco IOS Release 15.2 (2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.4 o comparable)
- 1 Switch (Cisco 2960 con Cisco IOS Release 15.2 (2) imagen lanbasek9 o comparable)
- 1 PC (Windows 7 u 8 con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Instrucciones

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los ajustes básicos, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas de los dispositivos.

Paso 1: Realice el cableado de red tal como se muestra en la topología.

Conecte los dispositivos que se muestran en la topología y realice el cableado necesario.

Paso 2: Inicie y vuelva a cargar el router y el switch.

Paso 3: Configure el router y el switch.

a. Acceda al dispositivo mediante el puerto de la consola e ingrese al modo EXEC privilegiado.

b. Asigne un nombre al dispositivo de acuerdo con la tabla de direccionamiento.

c. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

d. Asigne class como la contraseña cifrada de EXEC privilegiado.

e. Asigne cisco como contraseña de la consola y habilite el inicio de sesión.

f. Asigne cisco como la contraseña de VTY y habilite el inicio de sesión.

g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

h. Configure y active la interfaz G0 / 0/1 en el enrutador utilizando la información contenida en la Tabla de direccionamiento.

i. Configure la SVI predeterminada con la información de dirección IP incluida en la tabla de direccionamiento.

j. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Configurar PC-A

a. Configure PC-A con una dirección IP y una máscara de subred.

b. Configure una puerta de enlace predeterminada para PC-A.

Paso 5: Verifique la conectividad de red.

Haga ping a R1 y S1 desde la PC-A. Si alguno de los pings falla, solucione los problemas de la conexión.

Parte 2: Configurar medidas de seguridad básicas en el router

Paso 1: Configurar medidas de seguridad.

a. Cifre todas las contraseñas de texto sin cifrar.

b. Configure el sistema para que requiera una contraseña mínima de 12 caracteres.

c. Cambie las contraseñas (exec privilegiado, console y vty) para cumplir con el nuevo requisito de longitud.

   1) Establezca la contraseña de exec privilegiada en **$cisco! PRIV***

   2) Establezca la contraseña de la consola en **$cisco!!CON***

   3) Establezca la contraseña de la línea vty en **$cisco!! VTY***

d. Configurar el router para que acepte sólo conexiones SSH desde ubicaciones remotas

   1) Configure el nombre de usuario **sshAdmin** con una contraseña cifrada de **55hAdm! n2020**

   2) El nombre de dominio del router debe establecerse en ccna-lab.com

   3) El módulo clave debe ser de 1024 bits.

e. Establezca configuraciones de seguridad y prácticas recomendadas en las líneas de consola y vty.

   1) Los usuarios deben desconectarse después de 5 minutos de inactividad.

   2) El router no debe permitir inicios de sesión vty durante 2 minutos si se producen 3 intentos fallidos de inicio de sesión dentro de 1 minuto.

Parte 3: Configurar medidas de seguridad.

Paso 1: Verifique que todos los puertos sin usar estén inhabilitados.

Los puertos del router están inhabilitados de manera predeterminada, pero siempre es prudente verificar que todos los puertos sin utilizar tengan un estado inactivo en términos administrativos. Esto se puede verificar rápidamente emitiendo el comando **show ip interface brief**. Todos los puertos sin utilizar que no estén en un estado inactivo en términos administrativos se deben inhabilitar por medio del comando **shutdown** en el modo de configuración de la interfaz.

Paso 2: Verifique que las medidas de seguridad se hayan implementado correctamente.

a. Use Tera Term en la PC-A para hacer telnet a R1.

   ¿R1 acepta la conexión Telnet? Explique.

b. Use Tera Term en PC-A a SSH a R1.

   ¿R1 acepta la conexión SSH?

c. Escriba intencionalmente un nombre de usuario y una contraseña erróneos para ver si se bloquea el acceso al inicio de sesión luego de dos intentos.

   ¿Qué sucedió después de dos intentos fallidos de inicio de sesión?

d. Desde su sesión de consola en el router, emita el comando **show login** para ver el estado de inicio de sesión. En el siguiente ejemplo, el comando **show login** se emitió dentro del período de bloqueo de inicio de sesión de 120 segundos y muestra que el enrutador está en modo silencioso. El enrutador no aceptará ningún intento de inicio de sesión durante 111 segundos más.

e. Después de que hayan expirado los 120 segundos, vuelva a SSH a R1 e inicie sesión con el nombre de usuario **SSHadmin** y **55HAdm!n2020** para la contraseña.

Luego de haber iniciado sesión satisfactoriamente, ¿qué apareció en la pantalla?

f. Ingrese al modo EXEC privilegiado y use **$cisco!PRIV*** para la contraseña.

Si escribe incorrectamente esta contraseña, ¿se desconecta de su sesión SSH después de tres intentos fallidos en 60 segundos? Explique.

g. Emita el comando **show running-config** en la petición del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Parte 4: Configurar medidas de seguridad básicas en el switch

Paso 1: Configurar medidas de seguridad.

a. Cifre todas las contraseñas de texto sin cifrar.

b. Configure el sistema para que requiera una contraseña mínima de 12 caracteres

c. Cambie las contraseñas (exec privilegiado, consola y vty) para cumplir con el nuevo requisito de longitud.

1) Establezca la contraseña ejecutiva privilegiada en **$cisco!PRIV***

2) Establezca la contraseña de la consola en **$cisco!!CON***

3) Establezca la contraseña de la línea vty en **$cisco!!VTY***

d. Configure el conmutador para que acepte sólo conexiones SSH desde ubicaciones remotas.

1) Configure el nombre de usuario **SSHadmin** con una contraseña cifrada de **55HAdm!n2020**

2) El nombre de dominio de los switches debe establecerse en ccna-lab.com

3) El módulo clave debe ser 1024 bits.

e. Establezca configuraciones de seguridad y mejores prácticas en la consola y las líneas vty.

1) Los usuarios deben desconectarse después de 5 minutos de inactividad.

2) El switch no debe permitir inicios de sesión durante 2 minutos si se producen 3 intentos fallidos de inicio de sesión dentro de 1 minuto.

f. Deshabilite todos los puertos no utilizados.

Paso 2: Verifique que todos los puertos sin usar estén inhabilitados.

Los puertos del switch están habilitados de manera predeterminada. Desactive todos los puertos que no se estén usando en el switch.

a. Puede verificar el estado de los puertos del switch emitiendo el comando **show ip interface brief**.

b. Use el comando **interface range** para desactivar varias interfaces a la vez.

c. Verifique que todas las interfaces inactivas tengan un estado inactivo en términos administrativos.

Paso 3: Verifique que las medidas de seguridad se hayan implementado correctamente.

a. Verifique que Telnet se haya inhabilitado en el switch.

b. Acceda al switch mediante SSH y escriba intencionalmente un nombre de usuario y una contraseña erróneos para ver si se bloquea el acceso al inicio de sesión.

c. Una vez que hayan transcurrido los 30 segundos, vuelva a SSH a S1 e inicie sesión con el nombre de usuario **SSHadmin**y **55HAdm!n2020** para la contraseña.

¿Apareció el banner luego de haber iniciado sesión correctamente?

d. Ingrese al modo EXEC privilegiado usando **$cisco!PRIV*** como contraseña.

e. Emita el comando **show running-config** se ingresó para la consola y las líneas VTY en su configuración básica en la Parte 1.

Preguntas de reflexión

1. El **comando password cisco** command was entered for the console and VTY lines in your basic configuration in Part 1. ¿Cuándo se utiliza esta contraseña después de haberse aplicado las medidas de seguridad según las prácticas recomendadas?

2. ¿Las contraseñas preconfiguradas de menos de 10 caracteres se ven afectadas por el **comando de contraseñas de seguridad min-length 12?**

Tabla de resumen de interfaces de router

Modelo de router	Interfaz Ethernet 1	Interfaz Ethernet #2	Interfaz serial 1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Nota: Para conocer la configuración del router, observe las interfaces para identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles

combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, aunque puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.