Práctica de laboratorio: Protección de dispositivos de red

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
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 parámetros básicos de los dispositivos

Parte 2: Configurar medidas básicas de seguridad en el router

Parte 3: Configurar medidas básicas de seguridad en el switch

Información básica/Situación

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

En esta práctica 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 conforme a las prácticas recomendadas. Luego, probará las medidas de seguridad para verificar que estén implementadas de manera apropiada y que funcionen correctamente.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son ISR Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos 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 con el instructor.

Recursos necesarios

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)

- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

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

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

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

Paso 3: Configurar el router.

Consulte la práctica de laboratorio anterior para obtener ayuda con los comandos necesarios para SSH.

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

b. Entre al modo de configuración.

c. Asigne el nombre R1 al router.

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

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

g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

h. Encripte las contraseñas de texto no cifrado.

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

j. Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.

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

Paso 4: Configure el switch.

a. Acceda al switch mediante el puerto de consola y habilite al modo EXEC privilegiado.

b. Entre al modo de configuración.

c. Asigne el nombre S1 al switch.

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

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

g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

h. Encripte las contraseñas de texto no cifrado.

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

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

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

Parte 2: Configurar medidas básicas de seguridad en el router

Paso 1: Aportar seguridad a las contraseñas

Un administrador debe asegurar que las contraseñas cumplan con las pautas estándar para contraseñas seguras. Entre estas pautas, se podría incluir combinar letras, números y caracteres especiales en la contraseña y establecer una longitud mínima.

Nota: las pautas de prácticas recomendadas requieren el uso de contraseñas seguras, como las que se muestran aquí, en ambientes de producción. Sin embargo, las otras prácticas de laboratorio en este curso utilizan las contraseñas cisco y class para facilitar la realización de las prácticas.

a. Cambie la contraseña encriptada del modo EXEC privilegiado conforme a las pautas.

```
R1(config)# enable secret Enablep@55
```

b. Exija que se utilice un mínimo de 10 caracteres para todas las contraseñas.

```
R1(config)# security passwords min-length 10
```

Paso 2: Habilitar conexiones SSH

a. Asigne el nombre **CCNA-lab.com** al dominio.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

c. Configure la entrada de transporte para las líneas vty de modo que acepten conexiones SSH, pero no permitan conexiones Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. Las líneas vty deben utilizar la base de datos de usuarios local para realizar la autenticación.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.CCNA-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```


Paso 3: Implementar medidas de seguridad en las líneas de consola y vty

a. Puede configurar el router para que se cierre la sesión de una conexión que estuvo inactiva durante el lapso especificado. Si un administrador de red inicia sesión en un dispositivo de red y, de repente, se debe ausentar, este comando cierra la sesión del usuario en forma automática después de un tiempo especificado. Los siguientes comandos harán que se cierre la sesión de la línea después de cinco minutos de inactividad.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. El comando siguiente impide los intentos de inicio de sesión por fuerza bruta. Si alguien falla en dos intentos en un período de 120 segundos, el router bloquea los intentos de inicio de sesión por 30 segundos. Este temporizador se establece en un valor especialmente bajo para esta práctica de laboratorio.

```
R1(config)# login block-for 30 attempts 2 within 120
```

¿Qué significa **2 within 120** en el comando anterior?

¿Qué significa **block-for 30** en el comando anterior?

Paso 4: Verifique que todos los puertos sin utilizar estén deshabilitados.

Los puertos del router están deshabilitados de manera predeterminada, pero siempre es prudente verificar que todos los puertos sin utilizar tengan un estado administrativamente inactivo. Esto se puede verificar rápidamente emitiendo el comando **show ip interface brief**. Todos los puertos sin utilizar que no estén en el estado administratively down (administrativamente inactivo) se deben deshabilitar por medio del comando **shutdown** en el modo de configuración de interfaz.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Paso 5: Verificar que las medidas de seguridad se hayan implementado correctamente

a. Utilice Tera Term para acceder al R1 mediante Telnet.

¿R1 acepta la conexión Telnet?

¿Por qué o por qué no?

b. Utilice Tera Term para acceder al R1 mediante SSH.

¿R1 acepta la conexión SSH?

c. Escriba incorrectamente a propósito la información de usuario y contraseña para ver si el acceso de inicio de sesión se bloquea después de dos intentos.

¿Qué ocurrió después del segundo inicio de sesión fallido?

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 30 segundos y muestra que el router está en modo silencioso. El router no aceptará ningún intento de inicio de sesión por 14 segundos más.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. Cuando hayan pasado los 30 segundos, vuelva a acceder al R1 mediante SSH e inicie sesión utilizando el nombre de usuario **admin** y la contraseña **Admin15p@55**.

Una vez que inició sesión correctamente, ¿qué se mostró?

f. Ingrese al modo EXEC privilegiado y utilice la contraseña **Enablep@55**.

Si escribe esta contraseña incorrectamente, ¿se desconectará la sesión de SSH después de dos intentos fallidos en el lapso de 120 segundos?

¿Por qué o por qué no?

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

Parte 3: Configurar medidas básicas de seguridad en el switch

Paso 1: Aportar seguridad a las contraseñas en el switch

Cambie la contraseña encriptada del modo EXEC privilegiado conforme a las pautas de contraseña segura.

```
S1(config)# enable secret Enablep@55
```

Nota: el comando de seguridad **password min-length** no está disponible en el switch 2960.

Paso 2: Habilitar conexiones SSH

a. Asigne el nombre **CCNA-lab.com** al dominio.

```
S1(config)# ip domain-name CCNA-lab.com
```


b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

c. Configure la entrada de transporte para las líneas vty para permitir las conexiones SSH, pero no las conexiones Telnet.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. Las líneas vty deben utilizar la base de datos de usuarios local para realizar la autenticación.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Paso 3: Implementar medidas de seguridad en las líneas de consola y vty

a. Haga que el switch cierre sesión en una línea que haya estado inactiva durante 10 minutos.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. Para impedir intentos de inicio de sesión por fuerza bruta, configure el switch para que bloquee el acceso de inicio de sesión por 30 segundos en caso de que haya dos intentos fallidos en un período de 120 segundos. Este temporizador se establece en un valor especialmente bajo para esta práctica de laboratorio.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Paso 4: Verifique que todos los puertos sin utilizar estén deshabilitados.

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

a. Para verificar el estado de los puertos del switch, utilice el comando **show ip interface brief**.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
```



```
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

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

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. Verifique que todas las interfaces inactivas tengan un estado administrativamente inactivo.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
```



```
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Paso 5: Verificar que las medidas de seguridad se hayan implementado correctamente

a. Verifique que Telnet esté deshabilitado en el switch.

b. Acceda al switch mediante SSH y escriba incorrectamente a propósito la información de usuario y contraseña para ver si el acceso de inicio de sesión se bloquea.

c. Cuando hayan pasado los 30 segundos, vuelva a acceder al S1 mediante SSH e inicie sesión utilizando el nombre de usuario **admin** y la contraseña **Admin15p@55**.

¿Apareció el anuncio después de iniciar sesión correctamente?

d. Ingrese al modo EXEC privilegiado utilizando la contraseña **Enablep@55**.

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

Reflexión

1. En la configuración básica de la parte 1, se introdujo el comando **password cisco** para las líneas de consola y vty. ¿Cuándo se utiliza esta contraseña después de haberse aplicado las medidas de seguridad conforme a las prácticas recomendadas?

2. ¿Se vieron afectadas por el comando **security passwords min-length 10** las contraseñas configuradas previamente con menos de 10 caracteres?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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)

Nota: para conocer la configuración del router, observe las interfaces a fin de 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, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.