Actividad de laboratorio: protección de dispositivos de red

Topología

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	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 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). 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 obtenidos pueden diferir de los que se muestran en las actividades de laboratorio. Consulte la tabla de resumen de interfaces del router que figura 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 1941 con software Cisco IOS versión 15.2(4)M3, imagen universal o similar)
- Un switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 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

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 del modo EXEC privilegiado.

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

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

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

h. Configure y active la interfaz G0/1 en el router utilizando la información de 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.

Parte 2: Configurar medidas de seguridad básicas en el router

Paso 1: Cifre las contraseñas de texto no cifrado.

```
R1(config)# service password-encryption
```

Paso 2: Refuerce las contraseñas.

Un administrador debe garantizar que las contraseñas cumplan con las pautas estándar para contraseñas seguras. Estas pautas podrían incluir combinar letras, números y caracteres especiales en la contraseña y establecer una longitud mínima.

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

a. Cambie la contraseña cifrada del modo EXEC privilegiado según las pautas.

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

b. Establezca el requisito de que todas las contraseñas tengan como mínimo 10 caracteres.

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


Paso 3: Habilite conexiones SSH.

a. Asigne **CCNA-lab.com** como nombre de dominio.

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

b. Cree una entrada en la 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 al modo EXEC usuario. Si no se indica el modo privilegiado en el comando, el usuario tendrá acceso predeterminado al modo EXEC usuario (nivel 15).

```
R1(config)# username SSHadmin privilege 1 secret Admin1p@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 usar la base de datos de usuarios local para 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
```

Paso 4: Proteja las líneas de consola y VTY.

a. Puede configurar el router para que se cierre la sesión de una conexión que estuvo inactiva durante un período especificado. Si un administrador de red inicia sesión en un dispositivo de red y, de repente, se debe ausentar, este comando cierra automáticamente la sesión del usuario después de un plazo 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 siguiente comando 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 durante 30 segundos. Este temporizador está configurado en un valor especialmente bajo para esta actividad 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 5: 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.

```
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 6: Verifique que las medidas de seguridad se hayan implementado correctamente.

a. Use Tera Term para acceder a R1 a través de Telnet.

¿R1 acepta la conexión Telnet? Explique.

b. Use Tera Term para acceder a R1 a través de SSH.

¿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 ejemplo a continuación, 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 durante 14 segundos más.

```
R1# show login
     Se aplica una demora de inicio de sesión predeterminada de 1 segundo.
     No se ha configurado ninguna lista de acceso de modo silencioso.

     Router habilitado para detectar los ataques de inicio de sesión.
     Si ocurren más de 2 fallas de inicio de sesión en 120 segundos o menos,
     se desactivarán los inicios de sesión durante 30 segundos.

     Router actualmente en modo silencioso.
     Seguirá en el modo silencioso durante 14 segundos.
     Denegación de inicios de sesión de todas las fuentes.
R1#
```

e. Pasados 30 segundos, vuelva a acceder a R1 mediante SSH e inicie sesión utilizando el nombre de usuario **SSHadmin** y la contraseña **Admin1p@55**.

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

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

Si escribe mal esta contraseña, ¿se desconectará la sesión de SSH después de dos intentos fallidos en el plazo de 120 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 3: Configurar medidas de seguridad básicas en el switch

Paso 1: Encripte las contraseñas de texto no cifrado.

```
S1(config)# service password-encryption
```

Paso 2: Refuerce las contraseñas en el switch.

Cambie la contraseña cifrada del modo EXEC privilegiado según las pautas de contraseñas seguras.

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

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

Paso 3: Habilite conexiones SSH.

a. Asigne **CCNA-lab.com** como nombre de dominio.

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

b. Cree una entrada en la base de datos de usuarios local para que se utilice al conectarse al switch a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso al modo EXEC usuario. Si no se indica el modo privilegiado en el comando, el usuario tendrá acceso predeterminado al modo EXEC usuario (nivel 1).

```
S1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

c. Configure la entrada de transporte para las líneas VTY para que permitan conexiones SSH pero no conexiones Telnet.

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

d. Las líneas VTY deben usar la base de datos de usuarios local para 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 4: Proteja las líneas de consola y VTY.

a. Configure el switch para que se cierre 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 al inicio de sesión durante 30 segundos en caso de que haya 2 intentos fallidos en un plazo de 120 segundos. Este temporizador está configurado en un valor especialmente bajo para esta actividad de laboratorio.

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

Paso 5: 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**.

```
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. Use 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 inactivo en términos administrativos.

```
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 6: 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. Pasados 30 segundos, vuelva a acceder al S1 mediante SSH e inicie sesión usando el nombre de usuario **SSHadmin** y la contraseña **Admin1p@55**.

¿Apareció el banner luego de haber iniciado sesión correctamente?

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

e. Emita el comando **show running-config** en la petición 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 según las prácticas recomendadas?

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

Tabla de resumen de interfaces de router

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 (S0/0/0)	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 hacer 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 haber 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 un comando de Cisco IOS para representar la interfaz.