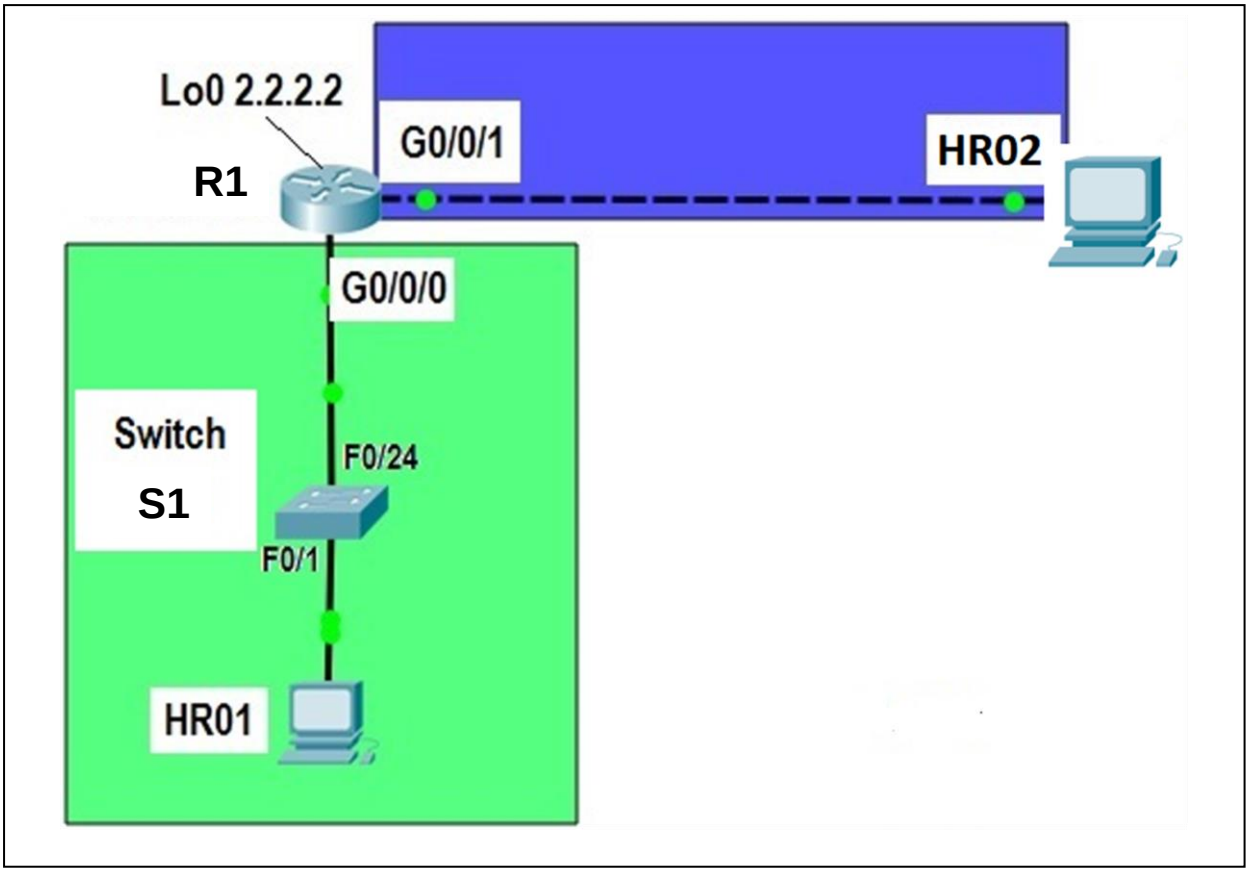
Ejercicio 11. Protección de dispositivos de red

Topología física



Introducción

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 este ejercicio 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.

Parte 1. Configurar medidas de seguridad básicas en el router

1. Encripte las contraseñas de texto no cifrado.

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

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.

a. Cambie la contraseña cifrada del modo EXEC privilegiado según 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
```

3. Proteja las líneas de consola y VTY.

c. 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)#
```

d. 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
```

4. 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
```

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

Parte 2. Configurar medidas de seguridad básicas en el switch

1. Encripte las contraseñas de texto no cifrado.

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

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.

3. Proteja las líneas de consola y VTY.

f. 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)#
```

4. 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.

g. 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                  172.16.0.33     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
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  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
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  up                    up
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

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

```
S1(config)# interface range f0/2-23 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

i. 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  up                    up
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  administratively down down
FastEthernet0/6        unassigned      YES unset  administratively down down
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  up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

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

Reflexión

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

_____

_____