Packet Tracer: recuperabilidad de router y switch

Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred	Gateway predeterminado	Sitio
HQ_Router	10.44.1.1	255.255.255.0	N/D	Metropolis Bank HQ

Objetivos

Parte 1: fortalecer la configuración de IOS

Parte 2: activar la función de configuración de recuperabilidad de Cisco IOS

Aspectos básicos

En esta actividad, se endurecerá la configuración de IOS de un router dentro de la red Metropolis. Luego, habilitará la característica de recuperabilidad de IOS en un router de Cisco. La asignación de direcciones IP, la configuración de red y las configuraciones de servicio ya están completas. Usará los dispositivos cliente en la red de Metropolis para implementar la configuración de recuperabilidad de IOS.

Parte 1: Fortalecer la configuración de IOS

Paso 1: Acceda a la petición de ingreso de comando en la computadora de Sally.

a. Haga clic en el sitio **Metropolis Bank HQ** y luego haga clic en la computadora **Sally**.

b. Haga clic en la ficha **Escritorio** y luego haga clic en **Petición de ingreso de comando**.

Paso 2: Conéctese de manera remota al router HQ_Router.

a. Conéctese por SSH al router **HQ_Router** al introducir **ssh –l admin 10.44.1.1** en la petición de ingreso de comando. Utilice la contraseña **cisco12345** cuando se le solicite.

b. En la petición de ingreso, escriba **enable** e introduzca la contraseña de habilitación **class** cuando se le solicite.

Su solicitud debe mostrar:

```
HQ_Router#
```

c. ¿Recibió un mensaje de advertencia que le impida a los usuarios no autorizados acceder al router HQ_Router?

Paso 3: Cree un mensaje de notificación legal en el router HQ_Router.

a. En la petición de ingreso `HQ_Router#`, introduzca un modo de configuración global usando el comando **configurar terminal**.

b. En la petición de ingreso `HQ_Router(config)#` pegue los siguientes comandos:

```
banner motd #
ESTÁ PROHIBIDO EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO
```

```
Debe contar con permiso explícito y autorizado para acceder o configurar este
dispositivo.
Los intentos y las acciones no autorizados de acceder o usar este sistema
pueden ocasionar sanciones
civiles o penales.
Todas las actividades realizadas en este dispositivo se registran y se
supervisan.
#
```

c. En la petición de ingreso `HQ_Router(config)#` utilice los comandos **finalizar** y **cerrar sesión** para finalizar su conexión a **HQ_Router**.

d. Conéctese por SSH al router **HQ_Router** nuevamente desde la computadora **Sally**. La contraseña de SSH es **cisco12345**.

¿Le solicitaron información o texto adicional cuando se conectó correctamente al router **HQ_Router**? ¿Qué es lo que se muestra?

Paso 4: Aplique la seguridad de la contraseña en el router HQ_Router.

a. En la petición de ingreso, escriba **enable** e introduzca la contraseña de habilitación **class** cuando se le solicite.

b. Ingrese al modo de configuración global mediante el comando **configurar terminal**. En la petición de ingreso `HQ_Router(config)#` pegue los siguientes comandos:

```
!cifra contraseñas de texto simple en la configuración de ejecución
service password-encryption

! aplica cualquier contraseña nueva configurada para tener un mínimo de 10
caracteres
security passwords min-length 10
```

Parte 2: Active la función de configuración de recuperabilidad de Cisco IOS

Paso 1: Ver la imagen de IOS actual.

a. Mientras esté conectado por SSH desde la computadora de **Sally**, introduzca el comando **exit** para volver a la petición de ingreso `HQ_Router#`.

b. Ahora introduzca el comando **dir flash:** para ver el archivo IOS.bin actual.

¿Cuál es el nombre del archivo .bin actual en flash?

Paso 2: Garantizar la imagen y la configuración en ejecución.

a. En la petición de ingreso `HQ_Router#`, introduzca un modo de configuración global usando el comando **configurar terminal**.

b. Utilice el comando **imagen de arranque seguro** en la petición de ingreso `HQ_Router (config)#` para activar la recuperabilidad de la imagen de IOS y para evitar que el archivo de IOS se muestre en el resultado del directorio y evite la eliminación del archivo de IOS seguro.

c. Utilice el comando **configuración de arranque seguro** en la petición de ingreso `HQ_Router (config)#` para guardar una copia segura de la configuración en ejecución y evitar la eliminación del archivo de configuración seguro.

d. Vuelva al modo EXEC con privilegios al introducir el comando **exit**. Ahora introduzca el comando **dir flash**: para ver el archivo IOS.bin actual.

¿Aparece algún archivo IOS.bin en el listado?

e. En la petición de ingreso `HQ_Router#` , introduzca el comando **mostrar conjunto de arranque seguro** para ver el estado de recuperabilidad de la imagen IOS de Cisco y de la configuración.

Tabla de puntuación sugerida

Sección de la actividad	Ubicación de la consulta	Puntos posibles	Puntos obtenidos
Parte 1: fortalecer la configuración de IOS	Paso 2	10	
	Paso 3	10	
Parte 2: activar la función de configuración de recuperabilidad de Cisco IOS	Paso 1	10	
	Paso 2	10	
Preguntas		**40**	
Puntuación de Packet Tracer		**60**	
Puntuación total		**100**	