Packet Tracer - Resiliência de Encaminhador e comutador

Tabela de Endereçamento

Dispositivo	Endereço IP	Másc. sub-rede	Gateway predefinido	Local
HQ_Router	10.44.1.1	255.255.255.0	N/A	Metropolis Bank HQ

Objetivos

Parte 1: Blindar a configuração do IOS

Parte 2: Ativar a funcionalidade de configuração resiliente do Cisco IOS

Segundo Plano

Nesta atividade, blindará a configuração IOS de um encaminhador dentro da rede Metropolis. Posteriormente, irá ativar a resiliência do IOS num encaminhador Cisco. O endereçamento IP, a configuração de rede e as configurações de serviço já foram realizados. Você usará os dispositivos cliente na rede Metropolis para implantar a configuração da resiliência do IOS.

Parte 1: Blindar a configuração do IOS

Passo 1: Aceda ao terminal de linha de comando no computador da Sally.

a. Clique no site **Metropolis Bank HQ** e, em seguida, clique no computador da **Sally**.

b. Clique na aba **Desktop** e depois em **Command Prompt**.

Passo 2: Ligue-se remotamente ao encaminhador HQ_Router.

a. Ligue-se por SSH ao **HQ_Router** inserindo **ssh —l admin 10.44.1.1** na linha de comando. Use a senha **cisco12345** quando solicitada.

b. No prompt, digite **enable** e a senha de enable **class** quando solicitado.

O seu prompt deve exibir:

```
HQ_Router#
```

c. Você foi solicitado com alguma mensagem de aviso, informando que utilizadores não autorizados não devem aceder ao HQ_Router?

_____

Passo 3: Crie uma mensagem de notificação legal no HQ_Router.

a. No prompt `HQ_Router#` , insira o modo de configuração global usando o comando **configure terminal** .

b. No prompt `HQ_Router (config) #` , cole os seguintes comandos:

```
banner motd #
O ACESSO NÃO AUTORIZADO A ESTE DISPOSITIVO É PROIBIDO
Você deve ter permissão explícita e autorizada para aceder ou configurar este
dispositivo. Tentativas e ações não autorizadas para aceder ou usar este
```

```
sistema podem resultar em penalizações criminais. Todas as atividades
realizadas neste dispositivo são registadas e monitorizadas.
#
```

c. No prompt `HQ_Router (config) #` use o comando **end** e **logout** para terminar a sua ligação ao **HQ_Router**.

d. Ligue-se por SSH ao **HQ_Router** novamente a partir do computador da **Sally**. A senha SSH é **cisco12345**.

Você foi solicitado com algum texto/informação adicional quando você se conectou com sucesso ao **HQ_Router**? O que é mostrado?

_____

_____

Passo 4: Imponha a segurança de senha no HQ_Router.

a. No prompt, digite **enable** e a senha de enable **class** quando solicitado.

b. Entre no modo de configuração global usando o comando **configure terminal**. No prompt `HQ_Router (config) #` , cole os seguintes comandos:

```
!encripta as senhas em claro no running-config
service password-encryption

!impõe novas senhas configuradas para ter um mínimo de 10 caracteres
security passwords min-length 10
```

Parte 2: Ativar a funcionalidade de configuração resiliente do Cisco IOS

Passo 1: Visualize a imagem atual do IOS.

a. Enquanto ligado via SSH a partir **do computador da Sally**, digite o comando **exit** para retornar ao prompt `HQ_Router#` .

b. Digite o comando **dir flash:** para ver o ficheiro IOS.bin atual.

Qual é o nome do ficheiro.bin atual em flash?

_____

Passo 2: Proteja a imagem e a configuração em execução.

a. No prompt `HQ_Router#` , insira o modo de configuração global usando o comando **configure terminal** .

b. Use o comando **secure boot-image** dentro do prompt `HQ_Router (config) #` para ativar a resiliência de imagem IOS e impedir que o ficheiro IOS apareça na saída do diretório e evitar a eliminação do ficheiro IOS seguro.

c. Use o comando **secure boot-config** dentro do prompt `HQ_Router (config) #` para armazenar uma cópia segura da configuração running e impedir a eliminação do ficheiro de configuração protegido.

d. Retorne ao modo EXEC privilegiado inserindo o comando **exit**. Agora digite o comando **dir flash:** para visualizar o ficheiro IOS.bin atual.

Há algum ficheiro IOS.bin listado? _____

e. No prompt `HQ_Router#` , incorpore o comando **show secure bootset** para ver o estado da resiliência da imagem IOS e da configuração.

Pontuação Sugerida

Secção da Atividade	Localização da Questão	Pontos Possíveis	Pontos Ganhos
Parte 1: Blindar a configuração do IOS	Passo 2	10	
	Passo 3	10	
Parte 2: Ativar a funcionalidade de configuração resiliente do Cisco IOS	Passo 1	10	
	Passo 2	10	
	Perguntas	**40**	
	Pontuação do Packet Tracer	**60**	
	Pontuação Total	**100**	