Packet Tracer – Resiliência do roteador e do switch

Tabela de Endereçamento

Dispositivo	Endereço IP	Máscara de sub-rede	Gateway padrão	Site
HQ_Router	10.44.1.1	255.255.255.0	N/D	Metropolis Bank HQ

Objetivos

Parte 1: Blindagem da configuração do IOS

Parte 2: Ativação do recurso de Configuração resiliente do Cisco IOS

Histórico

Nessa atividade, você endurecerá a configuração do IOS de um roteador na rede do Metropolis. Depois disso, você ativará o recurso de resiliência do IOS em um roteador Cisco. O endereçamento IP, a configuração de rede e as confirmações de serviço já foram realizados. Você usará os dispositivos clientes na rede do Metropolis para implantar a configuração de resiliência do IOS.

Parte 1: Blindagem da configuração do IOS

Passo 1: Acesse o command prompt (prompt de comando) no computador da Sally.

a. Clique no site **Metropolis Bank HQ** e clique no notebook **Sally**.

b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Command Prompt (Prompt de Comando)**.

Passo 2: Conecte-se, remotamente, ao roteador HQ_Router.

a. Usando SSH para o **HQ_Router** digite **ssh –l admin 10.44.1.1** no command prompt (prompt de comando). Use a senha **cisco12345** quando solicitado.

b. No prompt, digite **enable** (ativar) e digite a senha **class** quando solicitado.

Seu prompt deverá exibir:

```
HQ_Router#
```

c. Você recebeu uma mensagem de aviso impedindo usuários não autorizados de acessar o HQ_Router?

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

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

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

```
banner motd #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
É necessário ter permissão explícita e autorizada para acessar ou configurar
esse dispositivo.
```



```
Tentativas e ações não autorizadas para acessar ou usar este sistema pode
resultar em penalidades civis
E/ou criminais.
Todas as atividades realizadas neste dispositivo são registradas e
monitoradas.
#
```

c. No prompt `HQ_Router(config)#`, use o comando **end** e **logout** para encerrar a conexão com o **HQ_Router**.

d. Execute SSH no **HQ_Router** novamente no computador da **Sally**. A senha do SSH é **cisco12345**.

Você foi solicitado a fornecer informações/texto adicionais quando se conectou com sucesso ao **HQ_Router**? O que é mostrado?

Passo 4: Aplique segurança de senha no HQ_Router.

a. No prompt, digite **enable** (ativar) e digite a senha **class** quando solicitado.

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

```
!criptografa senhas de texto simples na configuração em execução
service password-encryption

!faz com que todas as novas senhas configuradas tenham um mínimo de dez
caracteres
security passwords min-length 10
```

Parte 2: Ativação do recurso de Configuração resiliente do Cisco IOS

Passo 1: Visualize a imagem do IOS atual.

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

b. Digite o comando **dir flash:** para visualizar o arquivo IOS.bin atual.

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

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

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

b. Use o comando **secure boot-image** no prompt `HQ_Router(config)#` para ativar a resiliência de imagem IOS e impedir que o arquivo de IOS seja mostrado na saída do diretório e impeça a exclusão do arquivo de IOS protegido.

c. Use o comando **secure boot-config** no prompt `HQ_Router(config)#` para armazenar uma cópia protegida da configuração em execução e impedir a exclusão do arquivo de configuração protegido.

d. Retorne ao modo EXEC com privilégios com o comando **end**. Agora, digite o comando **dir flash:** para visualizar o arquivo IOS.bin atual.

Há algum arquivo IOS.bin listado?

e. No prompt `HQ_Router#`, digite o comando **show secure bootset** para visualizar o status da resiliência da imagem e da configuração do Cisco IOS.

Pontuação Sugerida

Seção da Atividade	Etapa da Pergunta	Pontos Possíveis	Pontos Obtidos
Parte 1: Blindagem da configuração do IOS	Etapa 2	10	
	Etapa 3	10	
Parte 2: Ativação do recurso de Configuração resiliente do Cisco IOS	Etapa 1	10	
	Etapa 2	10	
	Perguntas	**40**	
	Pontuação do Packet Tracer	**60**	
	Pontuação Total	**100**	

