

Packet Tracer - Router and Switch Resilience

Addressing Table

Device	IP Address	Subnet Mask	Default Gateway	Site
HQ_Router	10.44.1.1	255.255.255.0	N/A	Metropolis Bank HQ

Objectives

Part 1: Hardening the IOS Configuration

Part 2: Activating the Cisco IOS Resilient Configuration Feature

Background

In this activity, you will harden the IOS configuration of a router within the Metropolis network. Afterwards, you will enable the IOS resiliency feature on a Cisco router. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the Metropolis network to deploy the IOS resiliency configuration.

Part 1: Hardening the IOS configuration

Step 1: Access the command prompt on Sally's computer.

- a. Click the Metropolis Bank HQ site and then click the computer Sally.
- b. Click the **Desktop** tab and then click **Command Prompt**.

Step 2: Remotely connect to the router HQ_Router.

- a. SSH to the HQ_Router by entering ssh –I admin 10.44.1.1 in the command prompt. Use the password of cisco12345 when prompted.
- b. At the prompt, type **enable** and enter the enable password **class** when prompted.

Your prompt should display:

HQ Router#

c. Were you prompted with any warning message preventing unauthorized users from accessing the HQ_Router?

NO

Step 3: Create a legal notification message on the HQ Router.

- a. At the HQ Router# prompt, enter global configuration mode using the configure terminal command.
- b. At the HQ Router (config) # prompt, paste in the following commands:

banner motd #

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

You must have explicit, authorized permission to access or configure this device.

Unauthorized attempts and actions to access or use this system may result in civil and/or $\,$

criminal penalties. All activities performed on this device are logged and monitored.

- C. At the HQ_Router (config) # prompt use the end and logout command to end your connection to HQ_Router.
- d. SSH into the HQ Router again from the computer Sally. The SSH password is cisco12345.

Were you prompted with any additional text/information when you connected successfully to the **HQ_Router**? What is shown?

YES

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

You must have explicit, authorized permission to access or configure this device. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

Step 4: Enforce password security on the HQ_Router.

- a. At the prompt, type **enable** and enter the enable password **class** when prompted.
- b. Enter global configuration mode using the configure terminal command. At the HQ_Router(config) # prompt, paste in the following commands:

!encrypts plain-text passwords in the running-config
service password-encryption

!enforces any new configured passwords to have a minimum of 10 characters security passwords \min -length 10

Part 2: Activating the Cisco IOS Resilient Configuration Feature

Step 1: View the current IOS image.

- a. While connected via SSH from Sally's computer, enter the exit command to return to the HQ_Router# prompt.
- b. Enter the command dir flash: to view the current IOS.bin file.

What is the name of the current .bin file in flash?

151-4.M4.bin

Step 2: Secure the running image and configuration.

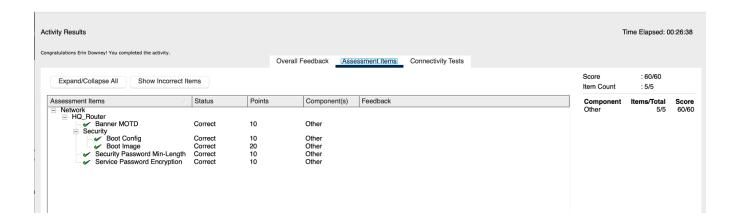
- $\textbf{a.} \quad \textbf{At the} \ \mathtt{HQ_Router\#} \ \ \textbf{prompt}, \ \textbf{enter global configuration mode using the } \ \textbf{configure terminal command}.$
- b. Use the **secure boot-image** command within the HQ_Router(config) # prompt to activate IOS image resilience and prevent the IOS file from both showing in the directory output and prevents the deletion of the secured IOS file.
- c. Use the secure boot-config command within the HQ_Router(config) # prompt to store a secure copy of the running configuration and prevent deletion of the secured configuration file.

d. Return to privileged EXEC mode by entering the **exit** command. Now enter the command **dir flash:** to view the current IOS.bin file.

Are there any IOS.bin file listed?

NO

e. At the HQ_Router# prompt, enter the command show secure bootset to view the status of the Cisco IOS image and configuration resilience.



Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Harden the IOS	Step 2	10	
configuration	Step 3	10	
Part 2: Activate the Cisco	Step 1	10	
IOS resilient configuration feature	Step 2	10	
	Questions	40	
Pack	60		
	100		