Packet Tracer - Router and Switch Resilience (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

1. 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 |

1. Objectives

Part 1: Hardening the IOS Configuration

Part 2: Activating the Cisco IOS Resilient Configuration Feature

1. 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.

1. Hardening the IOS configuration
   * 1. Access the command prompt on Sally’s computer.
        1. Click the **Metropolis Bank HQ** site and then click the computer **Sally**.
        2. Click the **Desktop** tab and then click **Command Prompt**.
     2. Remotely connect to the router HQ\_Router.
        1. SSH to the **HQ\_Router** by entering **ssh –l admin 10.44.1.1** in the command prompt. Use the password of **cisco12345** when prompted.
        2. At the prompt, type **enable** and enter the enable password **class** when prompted.

Your prompt should display:

HQ\_Router#

* + - 1. Were you prompted with any warning message preventing unauthorized users from accessing the HQ\_Router?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

No

* + 1. Create a legal notification message on the HQ\_Router.
       1. At the HQ\_Router# prompt, enter global configuration mode using the **configure terminal** command.
       2. 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.

#

* + - 1. At the HQ\_Router(config)# prompt use the **end** and **logout** command to end your connection to **HQ\_Router**.
      2. 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, the MOTD banner configured in step 3.b is displayed after successfully forming an SSH connection with router **HQ\_Router**.

* + 1. Enforce password security on the HQ\_Router.
       1. At the prompt, type **enable** and enter the enable password **class** when prompted.
       2. 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**

1. Activating the Cisco IOS Resilient Configuration Feature
   * 1. View the current IOS image.
        1. While connected via SSH from **Sally’s** computer, enter the **exit** command to return to theHQ\_Router# prompt.
        2. Enter the command **dir flash:** to view the current IOS.bin file.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c2900-universalk9-mz.SPA.151-4.M4.bin

* + 1. Secure the running image and configuration.
       1. At the HQ\_Router# prompt, enter global configuration mode using the **configure terminal** command.
       2. 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.
       3. 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.
       4. 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

* + - 1. At the HQ\_Router# prompt, enter the command **show secure bootset** to view the status of the Cisco IOS image and configuration resilience.
      2. Enter the command **reload** to reload the router. Press **Enter** to confirm the reload.

HQ\_Router#reload

Proceed with reload? [confirm]

% Connection timed out; remote host not responding

C:\>

1. Suggested Scoring Rubric

|  |  |  |  |
| --- | --- | --- | --- |
| Activity Section | Question Location | Possible Points | Earned Points |
| Part 1: Harden the IOS configuration | Step 2 | 10 |  |
| Step 3 | 10 |  |
| Part 2: Activate the Cisco IOS resilient configuration feature | Step 1 | 10 |  |
| Step 2 | 10 |  |
| **Questions** | | **40** |  |
| **Packet Tracer Score** | | **60** |  |
| **Total Score** | | **100** |  |