10.15 Lab: Restrict Telnet and SSH Access

Candidate: COMPTIA COMPTIA ()
Time Spent: 00:11

Score: 0%

Task Summary

Required Actions

- ✕ Create Standard Access List 5
- ✕ Permit Network 192.168.1.0 0.0.0.255
- ✕ Permit Network 192.168.2.0 0.0.0.255
- ✕ Permit Network 192.168.3.0 0.0.0.255
- ✕ Apply Access List 5 to VTY lines 0-4 Show Details
- ✕ Save your changes in the startup-config file Show Details

Explanation

Complete this lab as follows:

1. Enter the configuration mode for the router:
   a. From the exhibit, select the router.
   b. From the terminal, press **Enter**.
   c. Type **enable** and then press **Enter**.
   d. Type **config term** and then press **Enter**.
2. From the terminal, create a standard numbered access list using number 5. Add a **permit** statement for each network to the access list.
   a. Type **access-list 5 permit 192.168.1.0 0.0.0.255** and then press **Enter**.
   b. Type **access-list 5 permit 192.168.2.0 0.0.0.255** and then press **Enter**.
   c. Type **access-list 5 permit 192.168.3.0 0.0.0.255** and then press **Enter**.
3. Apply the access list to VTY lines 0–4. Filter incoming traffic.
   a. Type **line vty 0 4** and then press **Enter**.
   b. Type **access-class 5 in** and then press **Enter**.
   c. Press **Ctrl** + **Z**.
4. Save your changes in the **startup-config** file.
   a. Type **copy run start** and then press **Enter**.
   b. Press **Enter** to begin building the configuration.

c. Press **Enter**.