10.6.13 Packet Tracer - Research and Execute Password Recovery Procedures - Physical Mode

Objectives

Part 1: Research the Configuration Register

Part 2: Document the Password Recovery Procedure for a Specific Cisco Router

Background / Scenario

The purpose of this activity is to research the procedure for recovering or resetting the enable password on a specific Cisco router. The enable password protects access to privileged EXEC and configuration mode on Cisco devices. The enable password can be recovered, but the enable secret password is encrypted and would need to be replaced with a new password.

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

In this activity, you will begin by researching the purpose and settings of the configuration register for Cisco devices. You will then research and detail the exact procedure for password recovery for a specific Cisco router. Finally, using Packet Tracer, you will practice the procedure by using the configuration register to recover a password on a Cisco 2911 router.

Note: By design, the activity will open with a completion percentage of 12%.

Instructions

Part 1: Research the Configuration Register

To recover or reset an enable password, you will access the ROMMON interface to instruct the router to ignore the startup configuration when booting. When booted, access privilege EXEC mode, overwrite the running configuration with the saved startup configuration. You will then recover or reset the password and restore the boot process of the router to include the startup configuration.

The configuration register of the router plays a vital role in the process of password recovery. In the first part of this activity, you will research the purpose of the configuration register of a router and the meaning of certain configuration register values.

Step 1: Describe the purpose of the configuration register.

What is the purpose of the configuration register?

What command changes the configuration register in global configuration mode?

What command changes the configuration register in ROMMON mode?

Step 2: Determine configuration register values and their meanings.

Research and list the router behavior for the following configuration register values.

0x2102

0x2142

What is the difference between these two configuration register values?

Part 2: Document the Password Recovery Procedure for a Specific Cisco Router

For Part 2, you will describe the exact procedure for recovering or resetting a password from a 2900 series Cisco router and answer questions based on your research.

Step 1: Detail the process to recover a password on a specific Cisco router.

Research and list the steps and commands to recover or reset the enable or enable secret password from your Cisco router. Summarize the steps in your own words.

Step 2: Using Packet Tracer, execute the recovery of an enable password and a secret password on a Cisco 2911 router.

Imagine that you have just returned from a week-long conference. You try to log into the main company router but while you were away, someone changed the enable password. You are unable to log into the router.

a. From the desktop of the laptop, use the terminal mode to connect to the router. Because the passwords are unknown to you, you will not be able to log in.

b. In Physical Mode, go to the rear view of the router in the rack and switch the router off.

c. Power the router back on and quickly return to terminal mode on the laptop and enter **CTRL+c** before the hash loading marks (#####) have finished displaying. If you are not quick enough, power cycle the router another time. You should end up in ROMMON mode.

Note: On real equipment, you might have to type **ALT-b** instead of **CTRL-c**

```
rommon 1 >
```

Note: On real equipment, you must be physically near the router to execute this procedure. It is essential that a corporation ensure that there is strong physical security for all networking devices.

d. Change the value of the configuration register and reboot.

```
rommon 1 > confreg 0x2142
rommon 2 > reset
```

e. Ensure that you enter **N** to the initial configuration dialog question. You will be in user EXEC mode. Go to privileged EXEC mode.

f. Copy the startup configuration to the running configuration. The Router prompt should have changed to Main#

g. Make the following modifications to the running configuration:

1) Change the router prompt to Branch.

2) Change the secret password to **branch1**.

3) Change the console vty line passwords to **branch2**.

4) Add a banner of “Password Recovered”.

5) Verify the value of the configuration register.
6) Change the configuration register to 0x2102 in global config mode.

```
Branch(config)# config-register 0x2102
```

7) Save the running configuration to the startup configuration.

h. Reload the router and login with the new passwords.

i. Display the running configuration. Notice that the interfaces are in shutdown mode. Reactivate interfaces G0/0 and G0/2.

Step 3: Answer questions about the password recovery procedure.

Using the process for password recovery, answer the following questions.

Describe how to find the current setting for your configuration register.

Describe the process for entering ROMMON mode.

What commands do you need to enter the ROMMON interface?

What message would you expect to see when the router boots?

Why is it important to load the startup configuration into the running configuration?

Why is it important to change the configuration register back to the original value after recovering password?

Reflection Question

Why is it of critical importance that a router be physically secured to prevent unauthorized access?