Lab – Researching Password Recovery Procedures (Instructor Version)

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

Objectives

Part 1: Research the Configuration Register

- Identify the purpose of the configuration register.
- Describe router behavior for different configuration register values.

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

- Research and record the process for password recovery on a specific Cisco router.
- Answer questions based on the researched procedure.

Background / Scenario

The purpose of this lab 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 lab, 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.

Required Resources

- Device with Internet access

Part 1: Research the Configuration Register

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

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

Instructor Note: Have students visit the **Use of Configuration Register on All Cisco Routers** page at http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a008022493f.shtml on the Cisco Website.

Step 1: Describe the purpose of the configuration register.

What is the purpose of the configuration register?

_____

_____

_____

_____

The configuration register can be used to change how the router boots, options for booting, and console speed.

What command changes the configuration register in configuration mode?

_____

config-register

What command changes the configuration register in the ROMMON interface?

_____

confreg

Step 2: Determine configuration register values and their meanings.

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

0x2102 _____

_____

For the configuration register value 0x2102, a router will load the IOS from the flash memory then load the start-up configuration from the NVRAM if present. If no operating system is found, then the router will boot to ROMMON.

0x2142 _____

_____

For the configuration register value 0x2142, a router will load the IOS from the flash memory, ignore the start-up configuration in NVRAM, and provide a prompt for initial configuration dialog. If no operating system is found, then the router will boot to ROMMON.

What is the difference between these two configuration register values?

_____

_____

The 0x2102 setting is for normal router operation. The 0x2142 setting bypasses the start-up configuration allowing a user to recovery or reset the enable password.

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 specific Cisco router and answer questions based on your research. Your instructor will provide you with the exact router model to research.

Instructor Note: Have students visit the **Password Recovery Procedures** page on the Cisco website at http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml for password recovery procedures for a variety of Cisco devices.

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

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

_____

To recover or reset the enable password on the Cisco 1900 series router, complete the following steps:

1. Establish a terminal connection with the router using Tera Term or other terminal emulator.
2. Boot to ROMMON by either removing flash and rebooting or selecting Alt-b during a reboot.
3. Type **confreg 0x2142** at the rommon prompt.
4. Type **reset** at the next rommon prompt.
5. Type **no** at the initial configuration dialog.
6. Type **enable** at the router prompt.
7. Type **copy startup-config running-config** to load the startup configuration.
8. Type **show running-config**.
9. Record an unencrypted enable password. Reset an encrypted enable password.
10. In configuration mode, type **config-register 0x2102**.
11. In privilege mode, type **copy running-config startup-config** in order to save configuration.
12. Use the **show version** command to verity configuration register settings.

Step 2: 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.

The **show version** command will provide the current setting for the configuration register.

Describe the process for entering ROMMON.

A user can remove the flash memory and restart the router to boot to the ROMMON utility. A user can also boot the router and select **alt**+**b** if using Tera Term.

What commands do you need to enter the ROMMON interface?

A user would need to enter **confreg 0x2142** to change the configuration setting followed by **reset** to restart the router.

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

If a router does not load the startup configuration, a user would expect to see the message “Continue with configuration dialog?”

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

Loading the startup configuration into the running configuration ensures that the original startup configuration remains intact if the user saves during the password recovery process.

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

Returning the configuration register to the original value will ensure that the router will load the startup configuration during the next reload.

Reflection

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

Because the password recovery procedure is based on a console connection, which requires direct physical access to the device, preventing unauthorized users access to the physical device is an imperative part of an overall security plan.