Lab – Researching Password Recovery Procedures

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 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 a 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 the privileged 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.

Step 1: Navigate to Cisco Website.

At the time of writing this lab, the **Use of Configuration Register on All Cisco Routers** page can be found at http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html on the Cisco Website.

Navigate to the aforementioned web page or use a search engine to answer the questions in following steps.

Step 2: Describe the purpose of the configuration register.

What is the purpose of the configuration register?

What command changes the configuration register in configuration mode?

What command changes the configuration register in the ROMMON interface?

Step 3: 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 specific Cisco router and answer questions based on your research. Your instructor will provide you with the exact router model to research.

Step 1: Navigate to the Cisco website.

At the time of writing this lab, the **Password Recovery Procedures** page can be found at http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/6130-index.html on the Cisco Website.

Navigate to the aforementioned web page or use a search engine to answer the questions in following steps.

Step 2: 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.

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.

What commands do you need to enter to bypass the startup configuration while in the ROMMON mode?

What message would you expect to see when the router boots? And how should you answer the message?

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 the password?

Reflection

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