Lab – Configure and Verify Password Recovery

Topology

Objectives

Part 1: Configure Basic Device Settings

Part 2: Reboot Router and Enter ROMMON

Part 3: Reset Password and Save New Configuration

Part 4: Verify the Router is Loading Correctly

Background / Scenario

The purpose of this lab is to reset 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 will 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 change the configuration register in order to reset the enable password on a Cisco router.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to connect to the Cisco IOS device via the console port

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and copy the basic configuration into R1. The password is encrypted to setup the scenario of needing to recover from an unknown enabled password.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings on the router.

a. Console into the router and enter global configuration mode.

b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
hostname R1
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyMLl5/
```

```
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
logging sync
end
write
exit
```

c. Press **Enter** and try to enable Privileged Exec mode.

As you can see, access to a Cisco IOS device is very limited if the enable password is unknown. It is important for a network engineer to be able to recover from an unknown enable password issue on a Cisco IOS device.

Part 2: Reboot Router and Enter ROMMON

Step 1: Reboot the router.

a. While still consoled into R1, remove the power cord from the back of R1.

Note: If you are working in a NETLAB pod, ask your instructor how to power cycle the router.

b. From the console session on PC-A, issue a hard break to interrupt the routers normal boot process and enter ROMMON mode.

Note: To issue a hard break in Tera Term, press the **Alt** and the **B** keys simultaneously.

Step 2: Reset the configuration register.

a. From the ROMMON prompt, type a **?**, then press **Enter**. This will display a list of available ROMMON commands. Look for the **confreg** command in this list.

```
rommon 1 > ?
alias              set and display aliases command
boot               boot up an external process
break              set/show/clear the breakpoint
confreg            configuration register utility
cont               continue executing a downloaded image
context            display the context of a loaded image
cookie             display contents of motherboard cookie PROM in hex
dev                list the device table
dir                list files in file system
frame              print out a selected stack frame
help               monitor builtin command help
history            monitor command history
iomemset           set IO memory percent
meminfo            main memory information
repeat             repeat a monitor command
reset              system reset
rommon-pref        Select ROMMON
set                display the monitor variables
showmon            display currently selected ROM monitor
stack              produce a stack trace
sync               write monitor environment to NVRAM
```

```
sysret              print out info from last system return
tftpdnld            tftp image download
unalias             unset an alias
unset               unset a monitor variable
hwpart              Read HW resources partition
rommon 2 >
```

Note: The number at the end of the ROMMON prompt will increment by one each time a command is entered.

b. Type **confreg 0x2142** and press **Enter**. Changing the register to Hex 2142 tells the router not to automatically load the startup configuration when booting. The router will need to be rebooted for the configuration register change to take effect.

```
rommon 2 > confreg 0x2142


You must reset or power cycle for new config to take effect
rommon 3 >
```

c. Issue the **reset** ROMON command to reboot the router.

```
rommon 3 > reset

System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled


Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340


IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x480ce0c
Self decompressing the image :
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
###################################################### [OK]
< output omitted >
```

d. When asked if you would like to enter the initial configuration dialog, type **no** and press **Enter**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

e. The router will complete its boot process and display the User Exec prompt. Enter Privileged Exec mode.

```
Router> enable
Router#
```

Part 3: Reset Password and Save New Configuration

a. While in Privileged Exec mode, copy the startup configuration to the running configuration.

```
Router# copy startup-config running-config
Destination filename [running-config]?
1478 bytes copied in 0.272 secs (5434 bytes/sec)

R1#
```

b. Enter global configuration mode.

c. Reset the enable secret password to **cisco**.

```
R1(config)# enable secret cisco
```

d. Reset the configuration register back to 0x2102 to allow the startup configuration to automatically load the next time the router is rebooted.

```
R1(config)# config-register 0x2102
```

e. Exit global configuration mode.

f. Copy the running configuration to the startup configuration.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

You have successfully reset the enable password on a router.

Part 4: Verify the Router is Loading Correctly

Step 1: Reboot R1.

Step 2: Verify that the startup configuration loaded automatically.

Step 3: Enter Privileged Exec mode.

The new enable secret password should be cisco. If you are able to enter Privileged Exec mode, then you have successfully completed this lab.

Reflection

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