实验 - 配置并验证密码恢复

拓扑

目标

第 1 部分：配置基本设备设置

第 2 部分：重启路由器并进入 ROMMON

第 3 部分：重置密码并保存新配置

第 4 部分：验证路由器是否正确加载

背景/场景

本实验的目的是重置特定思科路由器中的启用密码。使能密码用于保护在思科设备上对特权 EXEC 模式和配置模式的访问。启用密码可恢复，但启用加密密码已加密，将需要替换为新密码。

为了绕过密码，用户必须熟悉 ROM 监控 (ROMMON) 模式，以及思科路由器的配置寄存器设置。ROMMON 是存储在 ROM 中的基本 CLI 软件，找不到 IOS 时，可使用此软件来排除启动错误以及恢复路由器。

在本实验中，您将更改配置寄存器以重置思科路由器中的启用密码。

所需资源

- 1 台路由器（采用思科 IOS 15.2(4)M3 版通用映像的思科 1941 或同类路由器）
- 1 台 PC（采用 Windows 7、Vista 或 XP 且支持终端模拟程序，比如 Tera Term）
- 通过控制台电缆将控制台端口连接思科 IOS 设备。

第 1 部分：配置基本设备设置

在第 1 部分中，您将设置网络拓扑并将基本设置复制到 R1 中。密码已加密，以设置需要从未知启用密码恢复的应用场景。

步骤 1： 建立如拓扑图所示的网络。

步骤 2： 如有必要，请初始化并重新加载路由器。

步骤 3： 在路由器上配置基本设置。

a. 通过控制台连接到路由器，然后进入全局配置模式。

b. 复制以下基本配置并将其粘贴到路由器上的运行配置中。

```
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. 按 **Enter**，并尝试启用特权 EXEC 模式。

您可以看到，如果启用密码未知，思科 IOS 设备的访问权限会非常有限。网络工程师务必能够从思科 IOS 设备的未知启用密码问题中恢复设备。

第 2 部分：重启路由器并进入 ROMMON

步骤 1： 重新启动路由器。

a 在仍登录到 R1 控制台时，从 R1 后面移除电源线。

注：如果您操作的是 NETLAB pod，请询问教师如何断电重启路由器。

b 从 PC-A 的控制台会话中，发出一个硬中断命令以中断路由器正常启动进程并进入 ROMMON 模式。

注：要在 Tera Term 中发出硬中断，请同时按下 **Alt** 键和 **B** 键。

步骤 2： 重置配置寄存器。

a 从 ROMMON 提示符处，输入 **?**，然后按 **Enter**。这将显示可用的 ROMMON 命令列表。在该列表中查找 **confreg** 命令。

```
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 >
```

注：每次输入一个命令时，ROMMON 提示符末尾的数字将增加 1。

b 键入 **Confreg 0x2142**，并按 Enter。将寄存器更改为 Hex 2142 将告知路由器不要在启动时自动加载启动配置。路由器将需要重启，才能使配置寄存器更改生效。

```
rommon 2 > confreg 0x2142


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

c 发出 **reset** ROMON 命令重启路由器。

```
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 当系统询问您是否确定进入初始配置对话框时，请键入 **no**，并按 **Enter**。

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

e 路由器将完成启动过程并显示用户执行提示符。进入特权 EXEC 模式。

```
Router> enable
Router#
```

第 3 部分：重置密码并保存新配置

a 在特权 EXEC 模式下，将启动配置复制到运行配置中。

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

R1#
```

b 进入全局配置模式。

c 将启用加密密码重置为 **Cisco**。

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

d 将配置寄存器重置为 0x2102 以允许在下一次重启路由器时自动加载启动配置。

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

e 退出全局配置模式。

f 将运行配置复制到启动配置中。

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

您已成功重置路由器的启用密码。

第 4 部分：验证路由器是否正确加载

步骤 1： 重启 R1。

步骤 2： 验证启动配置是否自动加载。

步骤 3： 进入特权 EXEC 模式。

新的启用加密密码应为 cisco。如果您能够进入特权 EXEC 模式，则已成功完成本实验。

思考

为什么路由器必须具有物理安全性，以防止未经授权的访问？

_____

_____

_____