Securing Network Devices

etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+2+Securing+the+Network/Securing+Network+Devices/

Physically Secure the Devices

All network devices need to be in a physically secure environment, whether in a locked data closet, a locked cabinet, or both. In most cases, if routers and switches can be physically accessed, they can be compromised. With Cisco devices, the only things required to compromise the system are a console cable kit and a terminal system, which today can include many palm-sized devices. Password recovery techniques are well known and easy to implement.

While password recovery lets a person with less than CCNA skills take control of the device, an equal fear should be the person with a screwdriver who decides to take the device(s) and worry about accessing them later. Cisco devices are typically hot items on web auction sites, often with several thousand listings on any given day. While corporate data centers typically have secure facilities, many small businesses and small branch offices might rely on Telco closets for router placement. Before agreeing to place devices in a Telco closet, consider that, in many cases, every building tenant has direct or indirect access to that closet.

Other reasons for centralizing network devices into a single room include facilitating environmental features like climate control (heating and cooling), stable power with Uninterruptible Power Supply (UPS) backups, secure access including locks and protection from over the wall or under the floor access, and possibly increased human presence to provide a deterrent. If the data room is busy with many people having access, it might make good sense to put key devices into locked cabinets.

Securing Administrative Access

One of the fundamental requirements in protecting the network is to secure the administrative access to any network device. With Cisco devices, administrative access to the device could allow someone to reconfigure features or even possibly use that device to launch attempts on other devices. Some of the basic techniques for securing administrative access would include the following:

- Setting User mode passwords
- Setting Privilege mode passwords
- Encrypting passwords in the configuration files
- Setting an MOTD banner to advise about the security restrictions
- Setting access privilege levels
- Restricting Telnet access to the device
- Restricting web browser access to the device
- Restricting SNMP access to the device

The first five techniques are covered in this chapter, while the last three are covered in Chapter 3, which deals with access control lists.

User Mode Passwords

This section reviews and expands on the techniques for assigning passwords to the three potential access points to the *User* mode, the entry level into a Cisco device. In Chapter 3, you learn how to use authentication servers, such as TACACS+ and RADIUS, with AAA authentication services for securing access to Cisco devices.

The User level on a Cisco router often has three potential access points. They include the following:

- **Console (con) port** Access for the console cable. Figure 2-2 shows a typical console port on a router.
- **Auxiliary (AUX) port** A console-like access that can be attached to an external modem for a dial-up connection.
- **Virtual terminal (vty) ports** The access points for Telnet sessions.

Click To expand

Figure 2-2: Console port on an 800 model telecommuter router

The default configuration for each of these interfaces, shown in the following code listing, doesn't include a password. Since the release of version 12.0 of the IOS, the virtual terminals and AUX ports require that a password is set. If none is set, the user will be rejected with the message "password required, but none set." The console port doesn't have this requirement, so it's a good idea always to set a password to prevent anyone with a laptop and a console cable from accessing the device.

```
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!
line con 0 ????????<-Console connection
 login
line aux 0 ????????<-AUX connection
 login
line vty 0 4 ??????<-Virtual terminal
connections
 login
end
```

The basic password configuration for each is the same. The password is defined with the **password** command and the **login** command. Passwords can be 1 to 25 character, and can include uppercase and lowercase letters, as well as numbers, to comply with complex password requirements in the password policy. The result might look like the following listing:

```
!
line con 0
 password
cisco1
 login
line aux 0
 password
cisco2
 login
line vty 0 4
 password
cisco3
 login
end
```

The passwords used should comply with the password policy portion of the network security policy. You could use the same password for all three, but this isn't a secure solution. Someone attempting to access the device through one of these three methods will be prompted only for a password, at which time they need to supply the appropriate one.

User Name/Password with Login Local

You can require both a user name and a password, as well as have the opportunity to create different combinations for different users. The first step is to develop a local database of acceptable user name and password combinations in the Global Configuration mode. Like all passwords, these are case- ensitive, can include text and numerals, and should comply with the password policy. The user names aren’t case sensitive. Two examples might include the following:

```
Rtr1(config)#username remote password
acC3ss
Rtr1(config)#username scott password woLfe7
```

To finish the configuration, change the login command to **login local** for the interface(s) that you want to use this feature. In the following example, only the virtual terminal lines are being changed.

```
username remote password
access
username scott password wolfe
!
line con 0
 password cisco1
 login
line aux 0
 password cisco2
 login
line vty 0 4
 login local
end
```

After making the changes, the next Telnet session login might look like the following:

```
User Access Verification

Username: remote ????????????<-Used the remote / acC3ss combination
Password:
Rtr1>exit ???????????????????<-Successful attempt

User Access Verification

Username: scott ?????????????<-Used scott / WOLFE7 combination - note case
Password:
% Login invalid ?????????????<-Wrong case on the password)

Username: ScOtT ?????????????<-Used ScOtT / woLfe7 combination - note
case)
Password:
Rtr1> ???????????????????????<-Used the correct case on the password)
```

The important things to remember are that the user name isn’t case sensitive, while the password is. Furthermore, if more than one entry is in the local database, then any valid combination is acceptable.

Privilege Mode Passwords

Access security for the Privilege mode involves being prompted for a password only if an **enable password** or **enable secret** password has been previously defined in Global Configuration mode. If neither is set, no security allowing any user to view and/or change the device configuration exists for the Privilege mode. Someone could even set a password and lock out other users.

The older **enable password** command followed by the desired password creates a cleartext entry in the running configuration that could be viewed by anyone seeing the configuration. The more secure **enable secret** command followed by the desired password creates an encrypted entry in the running configuration that can't be understood by anyone just seeing the configuration. If both **enable password** and **enable secret** are configured, only the **enable secret** is used. The **enable password** is ignored.

The following entries demonstrate both commands, and then use a **show run** command to display the configuration. All passwords are case sensitive and should comply with the password policy.

```
Rtr1#conf t
Rtr1(config)#enable password test
Rtr1(config)#enable secret cisco
Rtr1(config)#^z
Rtr1(config)#show run
!
enable secret 5
$1$4F6c$D5iYCm31ri1cA9WwvAU220
enable password test
```

Notice the enable secret password can't be recognized, but the enable password is easily recognized. If only the enable password had been set, anyone seeing the configuration could get the password that would let them reconfigure the router.

Password Encryption

If you look over the previous examples, you'll notice all passwords are in cleartext, except for the enable secret password. This means prying eyes might gather a password. You can secure the passwords in Global Configuration mode by typing the **service password-encryption** command. This permanently encrypts all passwords, so make sure you know what they are. The following abbreviated output demonstrates the command and the results:

```
Rtr1#conf t
Rtr1(config)#service password-encryption ????????????<-command
Rtr1(config)#^Z
Rtr1#sho run
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption ?????????????????????????<-command
!
hostname Rtr1
!
enable secret 5 $1$4F6c$D5iYCm31ri1cA9WwvAU220
enable password 7 15060E1F10 ?????????????????????????<-enable password
!
username remote password 7 070E224F4B1A0A ??????????<-local database
username scott password 7 02110B570D03 ?????????????<-local database
!
line con 0
 password 7 121A0C041104 ???????????????????????????<-line con
password
 login
line aux 0
 password 7 121A0C041104 ???????????????????????????<-line aux
password
 login
line vty 0 4
 login local
!
end
```

Note, typing **no service password-encryption** won't cause the passwords to revert to cleartext. The system will no longer encrypt new passwords, but the existing ones remain encrypted. Make sure you know a password before you encrypt it.

Message of the Day Banner (MOTD)

It's possible and prudent to create a message that will appear to everyone logging in to the User mode. This message should be a polite warning of company security policies for unauthorized access. Some courts have held that if this isn't explicitly stated—telling people to stay out, then it's an implicit invitation to come in and raise havoc.

To configure this message, use the **banner motd** command in the Global Configuration mode. The syntax is a little unusual in that you type the command, followed by a character you don't plan to include in the message. This character becomes a delimiter, in that everything you type after it until the character appears again will be part of the message. An example would be **banner motd *No Unauthorized Access*** where the asterisks indicate the beginning and the end of the message. The asterisks won't appear in the message.

You can make multiple-line messages by using SHIFT-ENTER at the end of the line and ignoring the warning message that appears the first time you try it. The following lines demonstrate this technique. Typing a new MOTD replaces any existing one.

```
Rtr1#conf t
Rtr1(config)#banner motd * Unauthorized Access Could Result In
Termination
Enter TEXT message. ?End with the character '*'. ??????????<-Ignore this

If you have any trouble with this device, call:
Mark Smith in IT Tech Support
Phone: (555) 555-1111 ext 1234*
Rtr1(config)#^Z
Rtr1#
```

The next login attempt would look like the following:

```
Unauthorized Access Could Result In Termination

If you have any trouble with this device, call:
Mark Smith in IT Tech Support
Phone: (555) 555-1111 ext 1234
User Access Verification
Password:
```

Three other options can be used with the **banner {exec | incoming | login | motd}** command that allow for variations on when the banner can be used. The MOTD option has been included because it causes the warning to appear at login for all users and is the most frequently used. You can use the help feature to see the other options.

Privilege Levels

Cisco devices numbered 0 through 15 have 16 privilege levels. By default, any user who can furnish the user-level password or user name/password combination can gain User exec mode access to the device, which is privilege level 1. From there, if the user knows the enable secret password, they can access the Privilege exec mode, or privilege level 15. The three predefined privilege levels on Cisco devices include the following:

- **1** User exec mode only (prompt is router>), the default level for login
- **15** Privileged exec mode (prompt is router#), the Enable mode
- **0** Seldom used, but includes five commands: disable, enable, exit, help, and logout

To determine or confirm the current privilege level, type the **show privilege** command. It would look like this in Privilege mode:

```
Rtr1#show privilege
Current privilege level is
15
Rtr1#
```

Privilege levels 2 through 14 can be defined by the admin to provide limited features to some users by assigning specific commands to the level using the **privilege** command.

The syntax is

> *privilege mode {level level command* | *reset command}, where*

mode	Indicates the configuration level being assigned. This includes all router configuration modes, including exec, configure, and interface.
level	Indicates the level being defined.
command	Indicates the command to be included. If you specify exec mode, then the command must be an **exec mode** command.
reset	Resets the privilege level of the command to the default privilege level.

A possible application of this feature might look like the following lines, which are creating a new Privilege mode for a part-time administrator.

```
Rtr1(config)#privilege exec level 7 ping
Rtr1(config)#privilege exec level 7 show startup-
config
Rtr1(config)#privilege exec level 7 show ip route
Rtr1(config)#privilege exec level 7 show ip int brief
Rtr1(config)#enable secret level 7 tESt7
```

The following lines show how the new privilege level would be accessed and a confirmation of the new level:

```
Rtr1>enable 7
Password:
Rtr1#show privilege
Current privilege level is
7
Rtr1#
```

Any attempt to run a command other than those specifically defined for this privilege level returns the same error message as any attempt to run a command from the wrong mode. As you will see in Chapter 4, AAA authentication provides some additional options for this feature.

Note that the privilege feature only limits user access if the user only knows the enable secret password for the defined level. If the user knows any other level password, then they can go there as well.