Global Information Assurance Certification Paper

Restricting commands on a Cisco Router with Privilege Levels

GIAC LevelOne Security Essentials Practical for Pepin C. Barrameda Jr
For Capital Sans, December 2000, Washington D.C.

Initially, I had a hard time finding my way around Cisco's CCO(Cisco Connection Online) because of the tremendous amount of information. It took some time for me to find my way around but eventually I became comfortable. I discovered sites that had links directly to different sections of the huge site. One of my favorites is ciscoinanutshell.com owned by a CCIE named Randall S. Benn. As I was browsing his site, I noticed the word "looking glass" and ever the curious techie, telneted to route-server.ip.att.net. Wow, I was in an ATT router which I could use to do some network troubleshooting! I had a box outside my network wherein I could ping/traceroute to myself or anywhere in the world. Of course as the curious techie, I typed a "?" at the Cisco IOS(Internetworking Operating System) prompt to see what commands I could execute, low and behold a lot of commands were missing. Obviously, the router had to be hardened, but how does one restrict IOS commands, one aspect of hardening a Cisco router. I will cover one way of doing that.

I have always wanted shell accounts external to my network for testing purposes. This looking glass is the next best thing. I know hackers can cover their tracks by telneting into so many boxes that the trail would be almost next to impossible to follow. So I tried to telnet from the ATT router(as a **security experiment**). Telnet was denied. Even typing in an IP addresses which defaults to "Telnet to this IP address" was prevented. What did the router guy do?

In the greeting of the router, it stated that "For questions about this route-server, send email to: jayb@att.com." So I did. Of course, I thanked him for sharing this resource and if it was not against policy to share how he did this on a Cisco IOS and point me to the right direction. Mr. Jay Borkenhagen responded and was very helpful with his information. He pointed me to his Cisco resources and explained that the command to restrict the telnet application, which is allowed at the user mode, was "privilege exec level 15 telnet". This command, in a nut shell, restricted telnet to the enable mode, the highest level of access.

By default, the Cisco IOS software has two modes of password security. They are the user mode(exec) and the privilege mode (enable) . You can tell which mode you are in by looking at the prompt. If the prompt looks like "router>", you are in the user mode where you can do a lot of show commands, ping, traceroute and other troubleshooting commands but no configuration commands. If the prompt looks like "router#", then you are in the enable mode where you can configure the router. Its like root on Unix boxes or administrator on NT. Within both modes, you can type "?" to find out what commands are authorized for that mode.

With the privilege exec level command, you can configure commands to run in other than their default mode. The format is as follows:

Router (config)# privilege exec level *level command*

For example, the ping command works for both modes. Let's say for some reason, you may want to restrict the ping command to only be executed in the enable mode. You would type in at the global configuration mode "privilege exec level 15 ping". The number 15 represents the highest level of the 16 possible hierarchical levels of modes. And this highest mode, 15, can only be accessed with the enable password. The levels that can be configured are 0 to 15. Level 1 is the normal user mode. Level 0, which is rarely used has 5 commands associated with it which are disable, enable, exit, help, and logout. In the following example, the router is logged in at level 0 and only 5 commands are allowed. Even the "**show privilege**" command which shows what privilege level you are logged in as, is not allowed.

```
Router>?
Exec commands:
  disable  Turn off privileged commands
  enable   Turn on privileged commands
  exit     Exit from the EXEC
  help     Description of the interactive help system
  logout   Exit from the EXEC

Router>show privilege
          ^
% Invalid input detected at '^' marker.
```

With 16 possible levels, you can configure multiple levels of command access and users/passwords to access those levels. For example, with the ping command, we can set it to level 7 by typing in "privilege exec level 7 ping". And the password to get to level 7 can be set by "enable password level 7 *password*". To access a level, from the prompt, type "enable 7" and the password associated with that level once prompted. Ping can then be executed from level 7 and up. Usernames with corresponding passwords can be set to a specific level. In the global configuration mode, as part of the username-based authentication system and after entering "**username *name* password *password***" , type "**username *name* privilege *level***". The user specified will automatically login at the specified privilege level.

An important thing to remember when setting a command at a certain level, all subsets of that command are also set to that level. That is, if you set "show ip route" to level 7, all show commands and show ip commands are automatically set to level 7 unless the commands are set individually at different levels.

For example:

The command in the following example places all show ip commands, which includes all show commands, at privilege level 7:

privilege exec level 7 show ip route

This is the same as following command:

privilege exec level 7 show

The commands in the following example place "show ip route" at level 7 and the "show" and "show ip" commands at level 1:

privilege exec level 7 show ip route
privilege exec level 1 show ip
privilege exec level 1 show

Privilege levels can also be set on lines. By going to the line configuration and typing "privilege level *level"* a default privilege level is specified for that line.

At a higher level of security, AAA (authentication, authorization, accounting) servers can provide a centralized user account management instead of relying on the user/password local to the configuration of the router. This is beyond the scope of this paper.

There are many steps in hardening a Cisco Router. One way is by restricting commands in the Cisco IOS as demonstrated by the shared ATT router. Try it. The box is there as a resource for everyone.

Sources:

Benn, Randall S., "Links to Cisco.com and ATT looking glass",www.ciscoinanutshell.com

jayb@att.com, Jay Borkenhagen, ATT Network Engineer

telnet route-server.ip.att.net

"Passwords and privileges commands"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_r/srprt5/srpass.htm

"Configuring passwords and privileges"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt5/scpass.htm

"Configuring Terminal Access Security"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/112cg_cr/2cbook/2cauthen.htm#xtocid2183020

"Multiple Levels of Privileges Examples"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt5/scpasswd.htm#37123