Router Security?

Gaurab Raj Upadhaya
gaurab@lahai.com
Packet Clearing House

Topics

- IOS Version
- Access Control
- Privilege Levels
- Passwords
- Unnecessary Services and Protocols
- SNMP
- Routing Security
- Logging

Why Router security?

- Routers are edge of your network. A compromised router provides an entry to your network
- Compromised routers can be used for initiating attacks into other networks
- Break-in into routers that act as firewalls create more problems.

Some Secure Use of Routers

- As firewalls
  - Properly configured routers are more robust firewalls
  - Using access routers with authentication
- In Routing and Data collection
  - Prefix lists, and traffic shaping and control
  - For flow generation, collection and analysis

Cisco IOS Versions

- The IOS version you use may not always be the latest, but must be patched properly
- The current stable Cisco IOS train is 12.xx

- Command
  - `show version`

Cisco Slides on IOS

Access Control

- Ways of Access to a Router
  - Console Access
    - Through a cable connected to the serial port
    - Console Access is the default mode of access
    - Password recovery functions can only be performed over the console port
    - Physical security of the equipment is thus important
  - Auxiliary Port
    - Generally used for out of band access
    - Also used for connecting to other routers' console port

Access Control

- Virtual TTY (VTY)
  - Virtual Terminal are provided over the network
  - By default, it's telnet, other modes also possible
- HTTP
  - Newer routers have a web configuration utility
- TFTP
  - Most routers use TFTP to get their image and configuration at boot time
- SNMP
  - Provides both read-only and readwrite abilities

Access Control Don'ts

- Don't set password to 'cisco' or 'router'
- Dont' leave the password in clear text
- Don't use the same password for the different modes of access
- Don't use the same password for different privileage levels
- Don't keep raw configs with password on text files

Access List

- Access lists cannot be edited one line at a time
  - Best strategy is to write the complete access list on a text editor and paste it to the router
  - Make sure the last statement is always the
    - Access-list nn deny any
  - Access list numbers can be from 10 to 99, beyond that are extended access list.
  - Same access list can be applied to different processes

Authorization Levels

- In Cisco routers, there are two levels
  - User Mode or Level 1
    - Default mode when someone logs in
    - Allows users to view information but cannot change configurations
    - When you login, it's this mode
  - Privileged Mode or Level 15
    - Router configuration mode
    - This is also known as enable mode
    - You still have to enter the configuration mode.

Local Username Access

- By default, cisco routers don't require usernames.
- But it's a good idea to assign username and password
- Routers can also use TACACS and AAA to authenticate users
- Additionally, you should limit the IP address from which remote access can be done

Privilege Levels

- By default, three privileges are configured
  - Zero Level, has only 5 commands
  - One Level, limited read-only access
  - 15 level, full access to the router
- You can configure additional privilege level
  - You can assign specific privilege level to users
  - You can assign specific privilege level on access ports

Warning Banners

- In some jurisdictions, civil and/or criminal prosecution of crackers who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. One way of providing this notification is to put it into a banner message configured with the Cisco IOS `banner login` command.
- From a security, rather than a legal, point of view, your login banner usually should not contain any specific information about your router, its name, its model, what software it's running, or who owns it; such information may be abused by crackers.

Questions ?????