**Experiment 6**

**Date:** 31-08-2021

**Aim:** To secure the USER and EXEC mode and VTY lines of a switch and check its authentication using telnet command.

**Software Used:** Cisco Packet Tracer.

**Theory:**

**Password Guidelines:** The use of weak or easily guessed passwords continues to be the biggest security concern of organizations. Network devices, including home wireless routers, should always have passwords configured to limit administrative access.

Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device.

All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

When choosing passwords, use strong passwords that are not easily guessed. There are some key points to consider when choosing passwords:

* Use passwords that are more than eight characters in length.
* Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
* Avoid using the same password for all devices.
* Do not use common words because they are easily guessed.

Use an internet search to find a password generator. Many will allow you to set the length, character set, and other parameters.

**Note:** Most of the labs in this course use simple passwords such as cisco or class. These passwords are considered weak and easily guessable and should be avoided in production environments. We only use these passwords for convenience in a classroom setting, or to illustrate configuration examples.

**Configure Passwords:**

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using the line console 0 global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the password password command. Finally, enable user EXEC access using the login command.

Text

Description automatically generated

Console access will now require a password before allowing access to the user EXEC mode.

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. It is the most important access method because it provides complete access to the device.

To secure privileged EXEC access, use the enable secret password global config command, as shown in the example.

**Text

Description automatically generated**

Virtual terminal (VTY) lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

To secure VTY lines, enter line VTY mode using the line vty 0 15 global config command. Next, specify the VTY password using the password password command. Lastly, enable VTY access using the login command.

An example of securing the VTY lines on a switch is shown.

Text

Description automatically generated

**Observations:**

1. **Securing the USER and EXEC mode and VTY Lines:**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. **Checking the Authentication of the Switch using TELNET command:**

Text

Description automatically generated

**Results:** Securing the USER and EXEC mode and VTY lines of a switch and check its authentication using telnet command.