Lab Activity 1.0.1.0 - Switch Security Implementation

Using your packet tracer, answer the following:

The topology will be based upon the scenario, create a table for your addressing.

Objectives

1. Think about a scenario in a company, a school or any establishment you need to apply a port security. Apply the Core, Distribution, Access.
2. Develop your own network topology in packet tracer
3. Group the computers using Layer 2 implementation. ex. Lab 1, Lab 2, AcctgOffice, HROffice... etc.
4. Use IPv6 address in this topology
5. Verify the Layer 2 configuration of a switch port connected to an end station.
6. Configure the initial configuration of the switch (hostname, console password, SSH password, banner MOTD, enable secret), use **cisco** as password for the terminals
7. Configure the ports of a switch a permanent MAC address (one MAC address per port) and a security shutdown feature.
8. Validate security implementation and explain the process below.
9. The grades will be based on the level of difficulty of your work. Depends upon the layers of switches in the LAN.
10. List all your commands for checking (copy and paste) "notepad style"

Reflection

1. Why would one port on a switch be secured on a switch using these scenario parameters (and not all the ports on the same switch)?

The use of ports would be restricted to specific devices if security measures were implemented in each port of a switch, which might hinder laptop mobility because users would not be able to connect to the switch unless they knew which port they could use.

2. Why would a network administrator use a network simulator to create, configure, and validate a security plan, instead of using the small- to medium-sized business' actual, physical equipment?

A network administrator would use a network simulator to create, configure, and validate a security plan before using actual equipment because you can save time and prevent any mistakes in the network. You can preserve your equipment before you use it because you have already prepared it virtually. Cisco Packet Tracer is a network simulator which meets all requirements.

3. What are the steps or processes in implementing port security and what is its relation to information assurance?

1. Activate port security on all the active access ports on switch
2. Configure the active ports to allow as many MAC addresses needed to be learned on the ports.
3. For the port on the switch connected to a server, statically configure the MAC address using port security.

4. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration.
5. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but not disable the ports.

Information assurance is related to it in that it contributes to network security by stopping unauthorized devices from forwarding packets or watching information transfer via the network.

4. What happened when you add computers on ports with port security?

It doesn't connect because it only allows a specific number of MAC addresses to connect to the port. In this case, only 1.

5. What happens when you replace a rogue laptop to the on the port with port security? Why?

Same thing, it doesn't connect because it only allows a specific number of MAC addresses to connect to the port. In this case, only 1. Since the MAC address has changed, then it will not be recognized.

Submission:

a. packet tracer file with filename - port-sercurity_familyname.pkt

   Include your reflection inside the packet tracer file.

b. Rubrics in checking:

- topology and addressing - 20pts
- initial configuration - 10pts
- port security configuration - 20pts
- connectivity and verification - 20pts
- reflection - 15 pts
- list of commands - 15 pts