Exercise 24: Securing your system - Part 2

I. Prepare the environment

1. Login to the CentOS server with user student and install the following packages:

   - Nmap
   - Xinetd
   - telnet-server and telnet

II. Setup host security

1. Login to the CentOS server with student
2. Scan all the TCP port of the CentOS server to specify the opening ports using nmap
3. Specify the TCP opening ports that is allowed by firewall using nmap.
4. List all the tcp sockets in listening state with ss utility.
5. Re-do the step 3 with lsof utility
6. Show the process ID and user that hold the tcp port 22 with fuser utility
7. Configure the xinetd to manage the telnet server (/usr/sbin/in.telnetd). Start the xinetd and check if the telnet port (23) is open and you can use telnet client to connect to the telnet server.
8. Using tcp wrappers to deny the telnet connection from your local host. Try to connect via telnet again. Could you connect?
9. Assume that you don't use the xinetd service and decide to disable it. Do the commands to stop and disable the xinetd

Exercise Instructions

I. Prepare the environment

1. Login to the CentOS server with user student and install the following packages:

   - Nmap
   - Xinetd
   - telnet-server and telnet

   $ sudo yum install nmap

   $ sudo yum install xinetd

   $ sudo yum install telnet-server telnet

II. Setup host security

1. Login to the CentOS server with user/password: **student/lpic1@123**

2. Scan all the TCP port of the CentOS server to specify the opening ports using nmap
   $ nmap -sT 127.0.0.1

3. Specify the TCP opening ports that is allowed by firewall using nmap.
   $ nmap -sT

4. List all the tcp sockets in listening state with ss utility.
   $ sudo ss -ltn

5. Re-do the step 3 with lsof utility
   $ sudo lsof -i TCP -sTCP:LISTEN

6. Show the process ID and user that hold the tcp port 22 with fuser utility
   $ sudo fuser -vn tcp 22

7. Configure the xinetd to manage the telnet server (/usr/sbin/in.telnetd). Start the xinetd and check if the telnet port (23) is open and you can use telnet client to connect to the telnet server.
   - *Create the file telnet inside the directory /etc/xinetd.d/ with the following content*

     service telnet
     {
     disable = no
     socket_type = stream
     protocol = tcp
     port = 23
     server = /usr/sbin/in.telnetd

```
    wait            = no
    user            = root
}
```

- *Start the xinetd service*
  $ sudo systemctl start xinetd

- *Check if the telnet server port (23) is open*
  $ netstat -ltn |grep 23

- *Using telnet client to connect to the CentOS server*
  $ telnet localhost

8. Using tcp wrappers to deny the telnet connection from your local host. Try to connect via telnet again. Could you connect?
   - *Edit the /etc/hosts.deny file and add your server IP to the restricted list*
     $ sudo vi /etc/hosts.deny
     In.telnetd: <your server IP address>
     :wq!
   - *Now try to telnet from your server, you could not connect to your server any more*
     $ telnet <your server IP address>

9. Assume that you don't use the xinetd service and decide to disable it. Do the commands to stop and disable the xinetd
   $ sudo systemctl stop xinetd
   $ sudo systemctl disable xinetd