Firewall Lab

Submission Requirements

In your lab report you must document all the commands and all the required screenshots in the main markdown file(s) for all the steps in the Lab. Ensure that all relevant commands are entered in plain text as well and that all your screenshots show up in your markdown file. Remember you need to prove you did the lab and that you had an effective solution in your Lab report to receive a passing mark.

```
FirewallLab-shi-89/
    ├── FirewallLabReport-shi-89.md
    ├── BeforeFirewall-shi-89.txt
    ├── BlockLAMPServer-shi-89.txt
    ├── AfterFirewall-shi-89.txt
    └── img/ # All your screenshots here
```

Purpose and Intent

The purpose of this lab is for students to become farmiliar with firewalling. The Lab should be done in parts and students should be able to verify that their solution works.

The following tools will be helpful in this lab (in addition to standard Linux Commands):

Tool	Comments
`nmap`	Comments
`gufw`	Comments
`ss`	Comments

It should be noted that this lab will require the network setup you did in Lab2, both of your machines should be on your isolated network. This is particularly important as you will be doing some network scanning and you are not permitted to scan hosts outside of your network.

Firewall Lab setup

Using your ubuntu server that you setup in your previous lab, you will do the following:

```
# Update the package repository
sudo apt-get update
# Install XFCE4
sudo apt-get install xfce4
sudo apt-get install xfce4-terminal
# Install gufw
sudo apt-get install python-gi
sudo apt-get install gufw
```

You will then restart your ubuntu server, once you have logged in as your normal user and type `startxfce4`, you will then be put into the default xfce4 desktop. You can always get back here by logging into the local terminal and typing `startxfce4`

Steps for this Lab.

1. Use `nmap` on your kali machine to scan your ubuntu server (by hostname). Use text redirection to save the file as `BeforeFirewall-shi-89.txt`
2. On your Ubuntu machine, block off all the ports associated with your LAMP installation using gufw. Use text redirection to save the file as `BlockLAMPServices-shi-89.txt`
3. Then change the sshd service to use a port number that corresponds to the last **three**. Digits of your student number. Without using an external computer or network scan verify that the port is open on the appropriate port. Prove it in your lab report, use a screenshot and relevant commands.
4. Then open the new updated sshd service port in the ufw firewall.
5. Use `nmap` on your kali machine to scan your ubuntu server (by hostname). Use text redirection to save the file as `AfterFirewall-shi-89.txt`.
6. > **Note** you may need to direct nmap to scan the port range 0-999 in order for your ssh server to be listed.
7. Use the `diff` command to show the difference between the "Before" and "After" files.

Reflection Questions

1. What was the easiest part of this lab?
2. What was the most difficult part of this lab?
3. What List all the different types of `nmap` scans, which one seems most interesting to you?
4. By asking you to output the `diff` between Before and After, what information does this tell me? Be specific.
5. Why might you have to specify the port range in order for your port to show up?

References:

https://phoenixnap.com/kb/gufw https://stackoverflow.com/questions/71369726/no-module-named-gi

---
