INFOTC 3001 - Computer Network Security
Laboratory # 8 - Host-based firewall (Linux)

I. Objectives

Set up a virtual environment in your own system.
Use host-based Microsoft Windows Firewall.

II. Material Required

Desktop Virtualization Software (VMware Workstation/Fusion), CentOS, and Microsoft Windows 10.

III. Activity

1. Make sure CentOS has 2 network adapters, one connected to the Internet Through NAT, and the other one connected to VMnet2 in VMware Workstation. If you are using MacOS and VMware Fusion you have two options to enable communication among your VMs: *Private to my Network* and *vmnet2*.
2. Make sure Windows 10 has only one network adapter connected to *VMnet2 or Private to my Network.*
3. Create a clone of the Windows 10 VM, the network adapter should be also connected to *VMnet2 or Private to my Network.*
4. To enable communication among all the three systems, configure CentOS with the IP address 172.16.1.1/16, Windows 10 with the IP address 172.16.1.2/16 and Windows 10 Clone with the IP address 172.16.1.3/16.

IV. Review Questions

Add screenshots for each question to **clearly** demonstrate your work.

1. Use the `ping` command to successfully send 4 ICMP packets among all the three VMs in order to demonstrate that you completed steps in *III. Activity.*
2. In CentOS list the services **enabled** by default for *public*, *dmz*, *home* and *internal* firewall zones.
3. In CentOS add a firewall rule to open the 2222/tcp port for the *dmz* zone **permanently**. After that show that the port 2222/tcp was added correctly in the *dmz* zone.
4. In CentOS assign the *public* zone to the network adapter connected to the internet, and the *home* zone to the network adapter connected to VMnet o

Private to my Network. Do not forget to restart the network service to apply configuration.

5. Install and start a web server in CentOS and open the corresponding port in the *home* zone.
6. In Windows 10 and Windows 10 clone open a web browser and access to the web site located in Centos.