INFOTC 3001 - Computer Network Security
Laboratory # 7 - Host-based firewall

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. Download and install VMware Workstation or Fusion from http://e5.onthehub.com/d.ashx?s=d1l8jhxjyz
2. Download and install CentOS from https://www.centos.org/download/
3. Download and install Microsoft Windows 10 Education from https://aka.ms/devtoolsforteaching
4. Have CentOS and Windows 10 VMs connected to the VMnet2 for VMware Workstation. If you are using MacOS and VMware Fusion you have two options to enable communication among your VMs:

   Option 1.

   Select 'Private to my MAC'

   Steps: Click on 'Virtual Machine' -> 'Network Adapter' -> 'Network Adapter Settings', Select 'Private to my MAC' and restart your network service or your VM before assigning an IP address.

   Option 2.

   Enable 'vmnet2' option in the network setting.

   Steps: Click on 'VMWare Fusion' -> 'Preferences' -> 'Network' -> '+' option, Make sure you select the 'vmnet2' and uncheck the option 'Provide addresses on this network via DHCP', click on 'Apply'. After that, you should be able to select 'vmnet2' by following Option 1 steps.

5. Use the 172.16.1.1/16 and the 172.16.1.2/16 for the CentOS and Windows 10 VMs respectively.

IV. Review Questions

Add screenshots for each question to clearly demonstrate your work.

1. Use the `ping` command to successfully send 4 ICMP packets from Windows to CentOS VM.
2. In Windows 10 install third party firewall Windows Firewall Control (WFC), in the new firewall add a rule to enable ICMP packets from remote systems.
3. Use the `ping` command to successfully send 4 ICMP packets from CentOS to Windows VM.
4. Uninstall WFC and use the native Windows Firewall to add a rule to enable ICMP packets from remote systems.