**CMSC 491/791 Active Cyber Defense HW 5**

**Name:**

**Due: October 9th, 2019 at 7:00PM** **EDT**

**Summary:**

In this lab, you will be learning how to manipulate availability to improve security. Through this lab, you will gain experience setting up services on both Windows Server and Linux(Ubuntu) while learning how to configure the default firewalls of both systems.

**Instructions:**

MAKE SURE YOUR VIRTUALBOX (if you’re using it) VMs ARE IN HOST-ONLY MODE, NOT NAT WHEN TESTING (but you’ll still have to download everything in NAT mode).

Linux - iptables

1. Set up ssh on your Ubuntu VM by running

sudo apt-get install openssh-server

sudo service ssh start

1. Set up a basic webserver on your Ubuntu VM

sudo apt-get install apache2

sudo service apache2 start

Test to make sure it’s working

curl localhost or visit localhost in browser

1) Create a new webpage to replace the Apache2 Ubuntu default page. **What is the full path of the file you changed? Provide a screenshot of your new webpage in the browser of your Ubuntu VM. (10 points)**

1. Find your ip address. Ensure you can use this address to see the website on your host machine.

2) **What is the IP address of your Ubuntu VM? (4 points)**

3) **What command did you use to find it? (4 points)**

1. Start up the Windows VM and verify that you can reach the website from your Windows VM.
2. Use iptables to blacklist the Windows VM from accessing the website

4) **Find the ip address of your Windows VM. What is it? (4 points)**

5) **How did you do this? (4 points)**

6) **What rule(s) did you add to your iptables to blacklist http to your Windows VM? (10 points)**

1. Test the blacklist rule(s). This is the easiest rule(s) to test, so it will help you with the rest.
2. Add an iptables to allow only your host to connect to your Ubuntu VM via ssh.

7) **Find the ip address of your host machine. What is it? (4 points)**

8) **How did you do this? (4 points)**

9) **What rule(s) did you add to your iptables to whitelist ssh to your host? (10 points)**

1. Test the whitelist rule(s).
   1. Download PuTTY on your Windows VM and try to ssh into the Ubuntu VM.

10) **Provide a screenshot of the error do you get when you try to ssh from your Windows VM with the rule(s) enabled (5 points)**

Windows - Windows Firewall

1. Set up an FTP server on your Windows VM.
   1. Options:
      1. Default System guide:

<https://www.atlantic.net/hipaa-compliant-cloud-storage/how-to-install-ftp-windows-server-2008-r2/> (not perfect, go into IIS, then FTP manager, then start the FTP Site)

* + 1. Dan’s Quick ‘n Easy FTP: <https://www.pablosoftwaresolutions.com/html/quick__n_easy_ftp_server_pro.html> (worse than not perfect. barely works.)
  1. Access the FTP server from other hosts. Run ftp <>.<>.<>.<> from your host and the Ubuntu VM to verify that this works.

11) **Provide a screenshot showing that you can access the Windows FTP server from your Linux VM. (10 points)**

1. Whitelist your host
   1. Configure the allow rule(s) on the Windows VM’s firewall to only allow access to the FTP server from your host.  
      12) **What does this firewall rule(s) look like? (10 points)**
2. Test your whitelist rule(s)

13) **Provide a screenshot of the error you get from your Ubuntu VM when you try to run the ftp client command to your Windows 2008 server (5 points)**

14) **Run the nmap command from the Ubuntu VM to detect the services running on the Windows VM as well as their versions. What is the full command that you used to do this? (10 points)**

15) **List three services that are listening on the Windows 2008 VM. What are their versions? (6 points)**