

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

**Name:** Daniel Roh

**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**

A. Set up ssh on your Ubuntu VM by running

```
sudo apt-get install openssh-server  
sudo service ssh start
```

B. Set up a basic webserver on your Ubuntu VM

```
sudo apt-get install apache2  
sudo service apache2 start
```

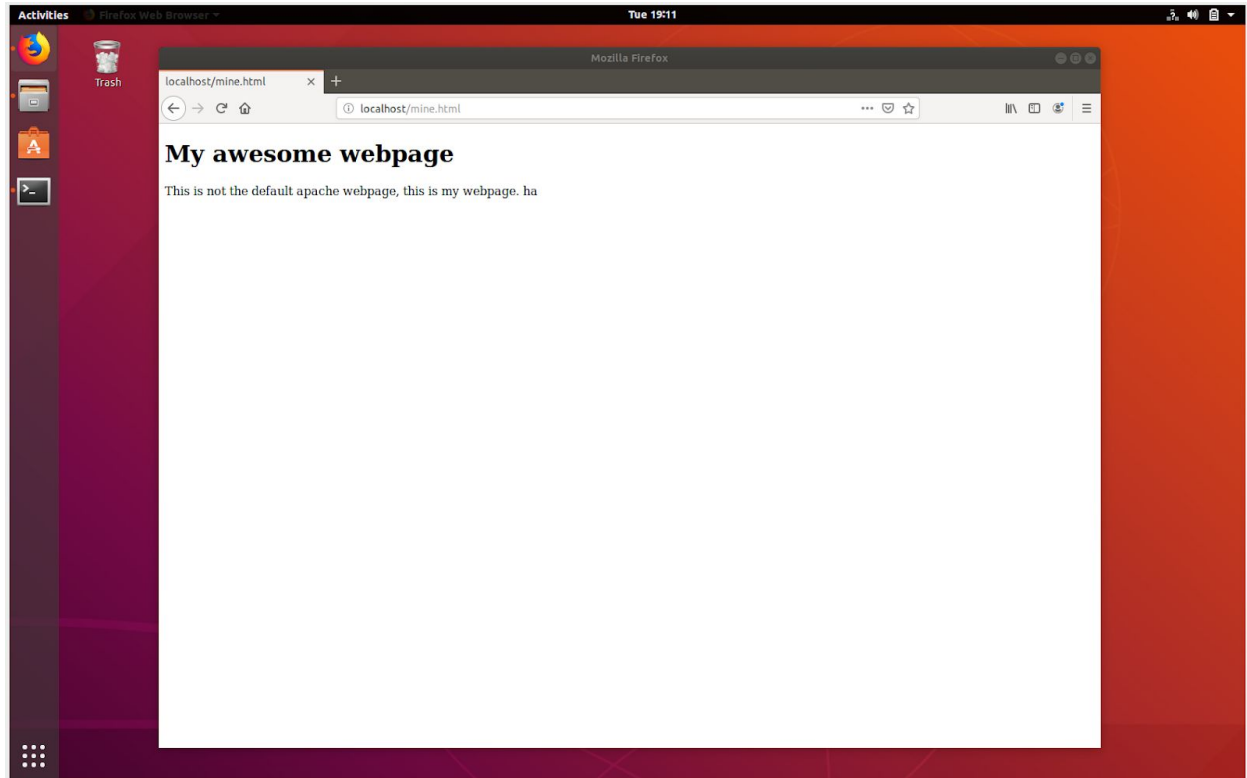
Test to make sure it's working

```
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)**

Path: /etc/apache2/sites-available/

Path of html: /var/www/



C. 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)**

IP: 192.168.56.101

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

Command: `ip addr show`

D. Start up the Windows VM and verify that you can reach the website from your Windows VM.

E. 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)**

Windows ip: 192.168.56.102

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

I just opened the network adapter and found the ip address inside the network connection details

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

The rule I added to blacklist http is by blocking port 80 in the ip tables. This can be done in two ways, by blocking the input from port 80 or blocking the output from port 80. So what I did was block both the output and input with the commands "iptables -A OUTPUT -p tcp --dport http -j REJECT" and "iptables -A INPUT -p tcp --sport -j REJECT"

F. Test the blacklist rule(s). This is the easiest rule(s) to test, so it will help you with the rest.

G. 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)**

Ip of host machine: 192.168.2.48

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

I went into the settings of my machine and went into the network adapter settings to find the ip address of my machine

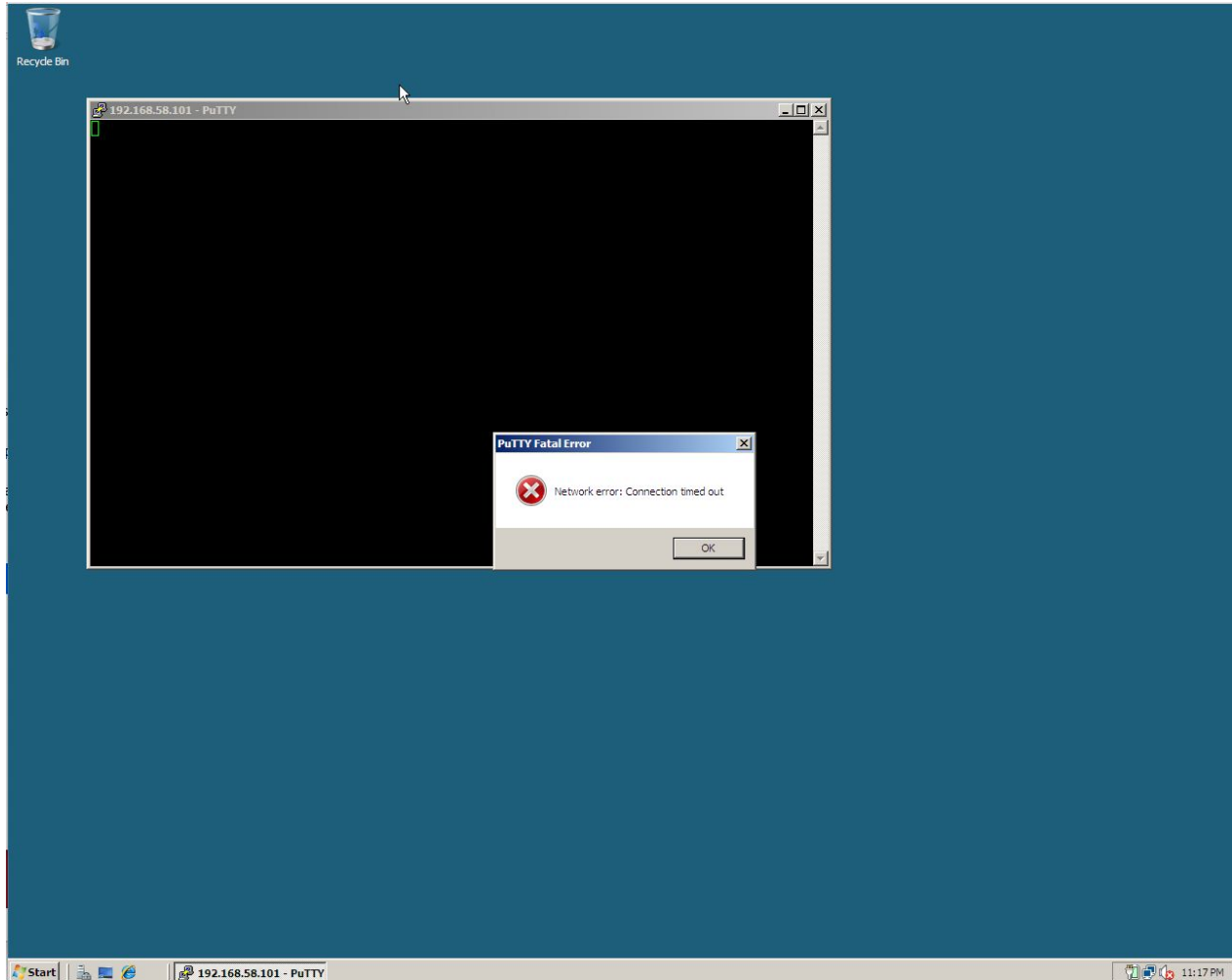
**9) What rule(s) did you add to your iptables to whitelist ssh to your host? (10 points)**

To whitelist the host machine for ssh'ing, ssh uses port 22. So to allow the host computer to only access the server via ssh, I used the command "iptables -A INPUT -p tcp -s 192.168.2.48 --dport 22 -j ACCEPT"

H. Test the whitelist rule(s).

a. 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

### I. Set up an FTP server on your Windows VM.

#### a. Options:

##### i. Default System guide:

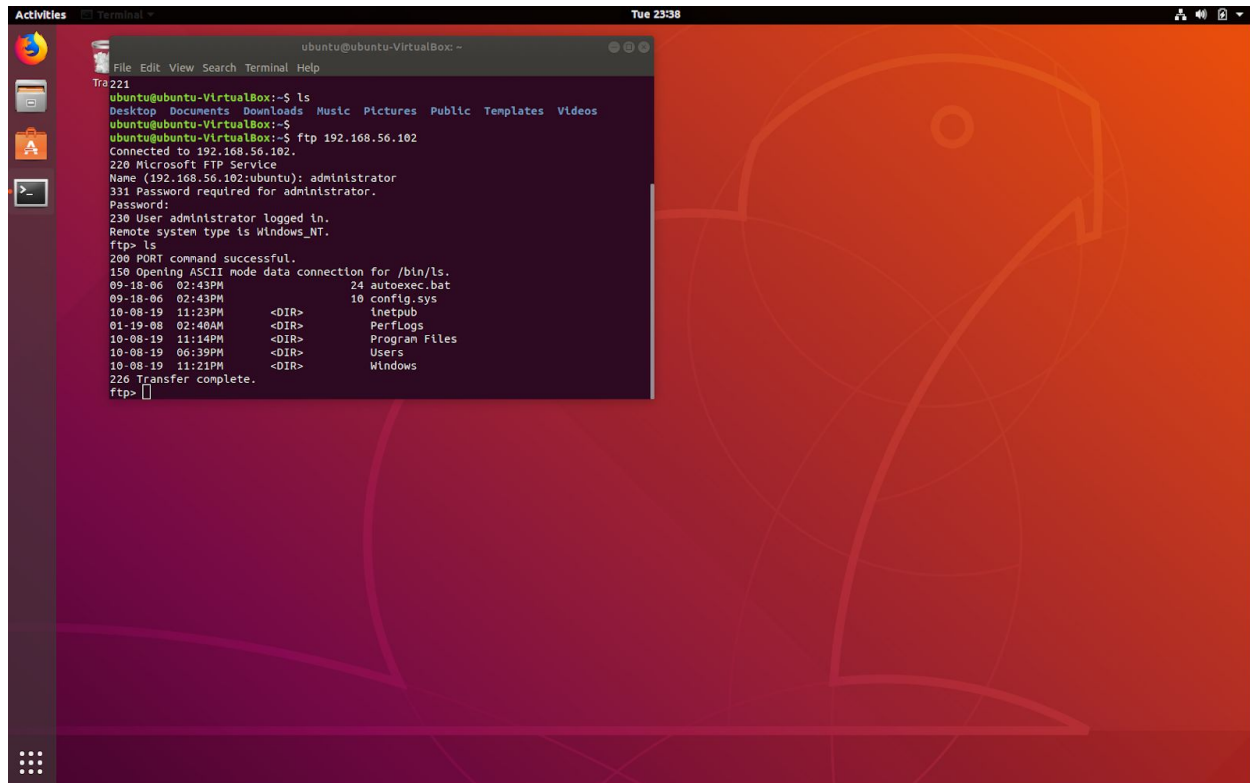
<https://www.atlantic.net/hipaa-compliant-cloud-storage/how-to-install-ftp-windows-server-2008-r2/> (not perfect, go into IIS, then FTP manager, then start the FTP Site)

##### ii. Dan's Quick 'n Easy FTP:

[https://www.pablosoftwaresolutions.com/html/quick\\_n\\_easy\\_ftp\\_server\\_pro.html](https://www.pablosoftwaresolutions.com/html/quick_n_easy_ftp_server_pro.html) (worse than not perfect. barely works.)

#### b. 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)



```
ubuntu@ubuntu-VirtualBox: ~  
File Edit View Search Terminal Help  
Tue 23:38  
Tr221  
ubuntu@ubuntu-VirtualBox:~$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
ubuntu@ubuntu-VirtualBox:~$  
ubuntu@ubuntu-VirtualBox:~$ ftp 192.168.56.102  
Connected to 192.168.56.102.  
220 Microsoft FTP Service  
Name (192.168.56.102:ubuntu): administrator  
331 Password required for administrator.  
Password:  
230 User administrator logged in.  
Remote system type is Windows_NT.  
ftp> ls  
200 PORT command successful.  
150 Opening ASCII mode data connection for /bin/ls.  
09-18-06 02:43PM 24 autoexec.bat  
09-18-06 02:43PM 10 config.sys  
10-08-19 11:23PM <DIR> inetpub  
01-19-08 02:40AM <DIR> PerfLogs  
10-08-19 11:14PM <DIR> Program Files  
10-08-19 06:39PM <DIR> Users  
10-08-19 11:21PM <DIR> Windows  
226 Transfer complete.  
ftp>
```

J. Whitelist your host

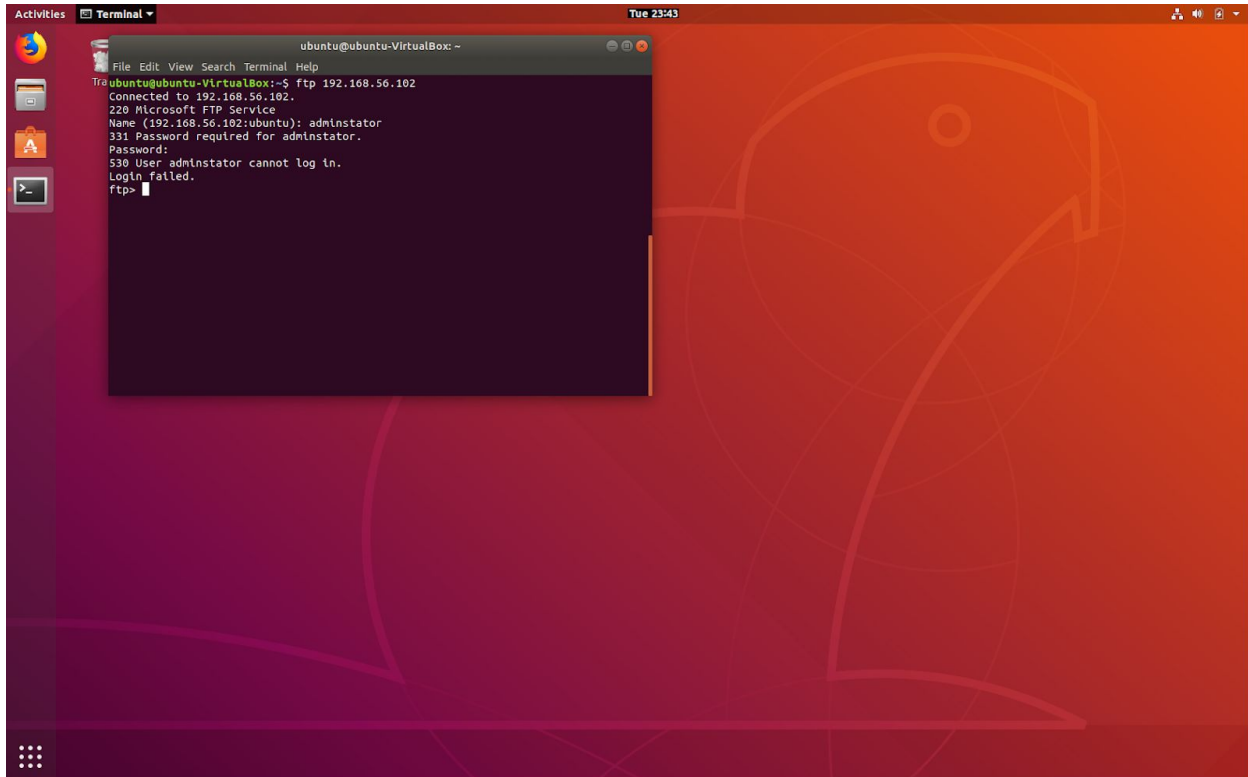
- a. Configure the allow rule(s) on the Windows VM's firewall to only allow access to the FTP server from your host.

12) What does this firewall rule(s) look like? (10 points)

By going into windows firewall, a new rule was created which was placed on port 21 connections. The scope tab was set such that only the host machine's ip address can connect through port 21 and any other ip address will be blocked.

K. 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)

Command: `nmap -sV --version-intensity 5 192.168.56.102`

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

Service	Version
netbios-ssn	Microsoft Windows netbios-ssn
microsoft-ds	Microsoft Windwos Server 2008 R2 microsoft-ds (workgroup: WORKGROUP)
msrpc	Microsoft Windows RPC