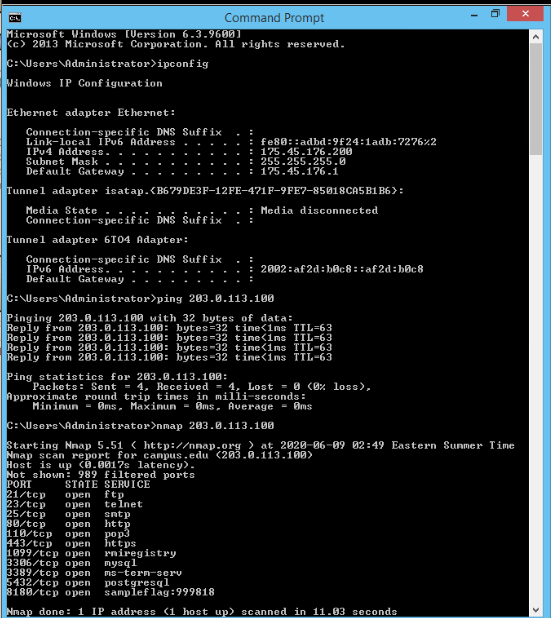
**ISEC 500 - Information Security Overview**

**Assignment 9 - Lab 7: Securing the pfSense Firewall**

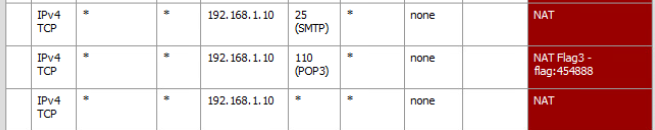
The requirements for this lab are to capture the screenshot of the below steps from given sections and submit in the word document.

**Part 1**

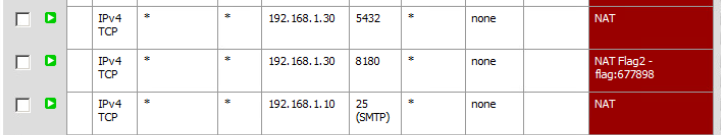
**challenge #1**



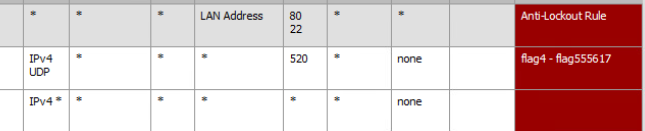
**challenge #2**



**challenge #3**



**challenge #4**



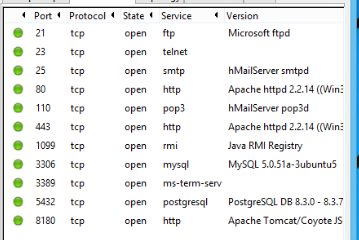
**challenge #5**

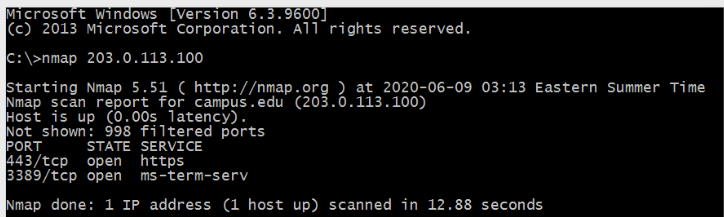


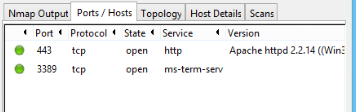
**challenge #6**

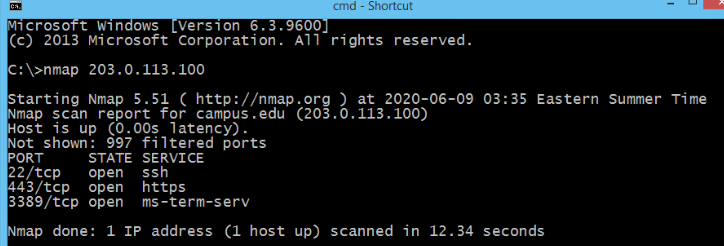


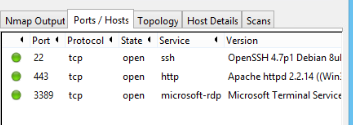
**Screenshots**











**PART 2**

As always, these virtual labs are very informative and very related to real world.

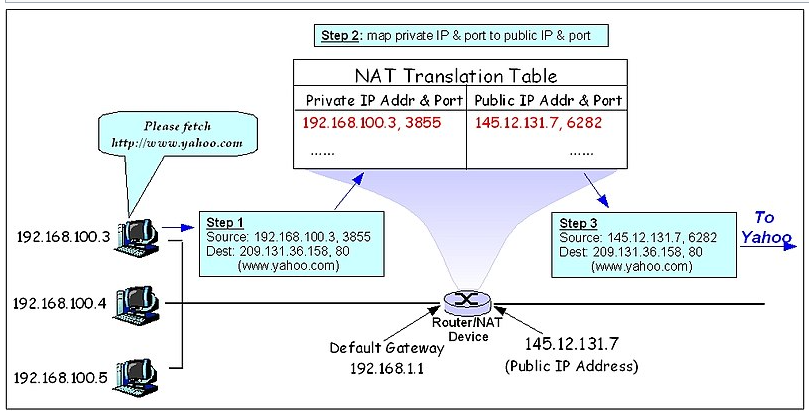
First we use ipconfig to see our own network info. A useful command.

Then we use the ping command on the server (203.0.113.100). This command is also a useful command that I use from time to time. It can be used to see ping time (RTT). When we ping further servers such as European servers, RTT increases. I also realized that TTL(time to live of the packet) is higher when we ping further servers. Ping command is also a nice command to tell whether a server is up and running.

Nmap is another ver useful tool that shows us open ports of a server. I actually just downloaded and installed nmap. It is a good tool that I can use when I do web app development to scan the server I upload application to. I also have this program claled postman that can do http request response to test a server. I also have EditThisCookie browser extension. Again, useful while doing web app development.

Then we use zenmap on the same server. Zenmap is the gui version of nmap.

The VL talks about different ports being directed to different hosts in that same public ip. I actually learned about this while I was doing my bachelors degree. It was very interesting to me back then too. Because when I was taking my computer networking class during my bachelors degree, I learned that ipv4 is not enough for all the hosts on the planet. And then I learned NAT allows us to use more hosts than ipv4 allows because NAT allows us to use multiple hosts with one public ip address. Packets are directed to different hosts in the local network based on port numbers.



Then we went to the windows server and logged into the firewall. On the NAT page, we can see that plenty of ports are open. We can see their destination address and destination port. We can also see their NAT IP and NAT port. We closed all but two of these.

We then went back to the client. And did another nmap scan of the server. We were only able to see the two ports.

We also repeated the zenmap scan. Again, we saw the two ports.

Then we went back to the windows server. Logged in to the firewall again. Went into the Nat section and added another port. We basically said, packets coming to the SSH port of this public ip should be redirected to windows server’s local ip (192.168.1.30) at port 22.

We logged back into the client to do another nmap and zenmap scan. We were able to see the port 22 open.

We then used putty to SSH into the windows server. Lastly we used WinSCP to SCP into the windows server and copy a file.