DOCUMENTATION:

DESIGN & IMPLEMENTATION OF A COMPREHENSIVE CYBERSECURITY LAB

To begin my Phase 1 final project of creating this lab, I needed to start with Topography. Illustrating all components and visually mapping out everything I needed helped tremendously. I wish this had been my very first step, however I initially made the mistake of jumping right in and then backtracking to piece it all together. Once I backtracked and had my Topography in place, I was ready to get going.

I have chosen to use VirtualBox for this project as I am already familiar with it and enjoy the interface. I used my host machine to download the latest version of pfSense available, choose the type as BSD and Version as FreeBSD 64 bit. I had never used pfSense previously, so wrapping my mind around the install proved a bit tricky. I gave pfSense 2040 MB and 1 CPU in my machine. Though the download and install was straightforward, I had not yet configured my network so when it came to accessing the dashboard, that was a no go. I also encountered an error where the set up portion looped, looped, and looped. Only after reading and watching several videos did I realize what kept me in this loop was the fact that I had to remove it from the disk drive to successfully wrap up the setup.

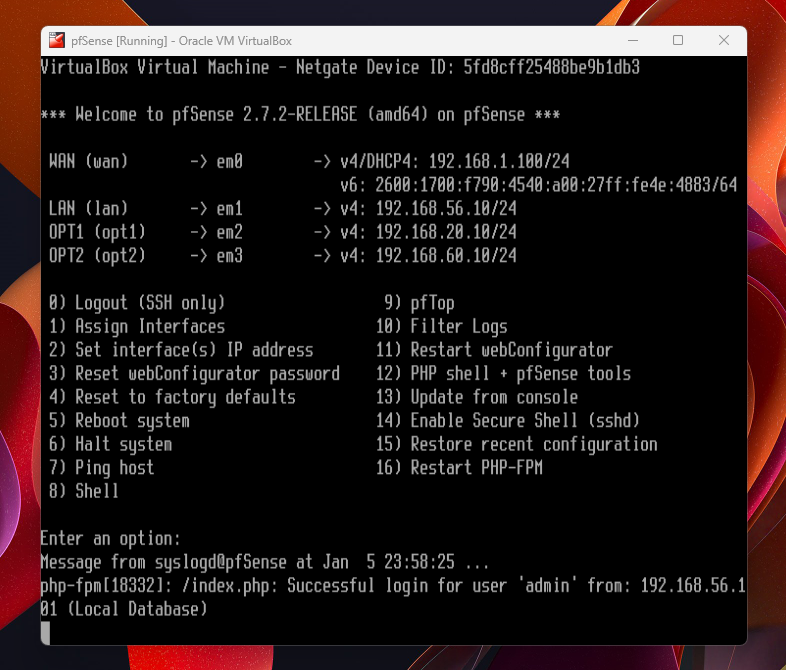
I set my pfSense Network adapters as follows:

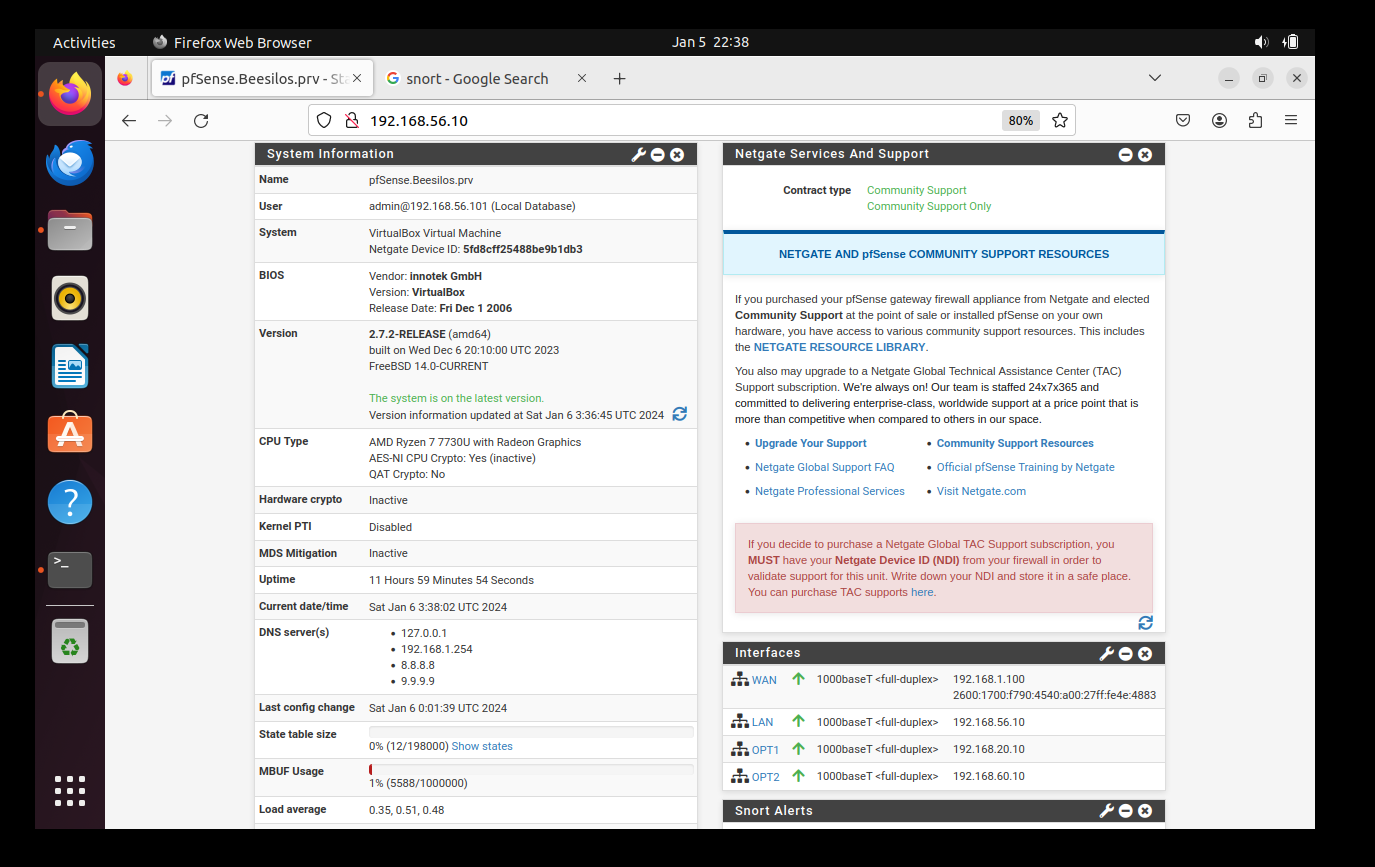
Adapter 1: Bridged Adapter

Adapter 2: Host-only Adapter 192.168.56.1

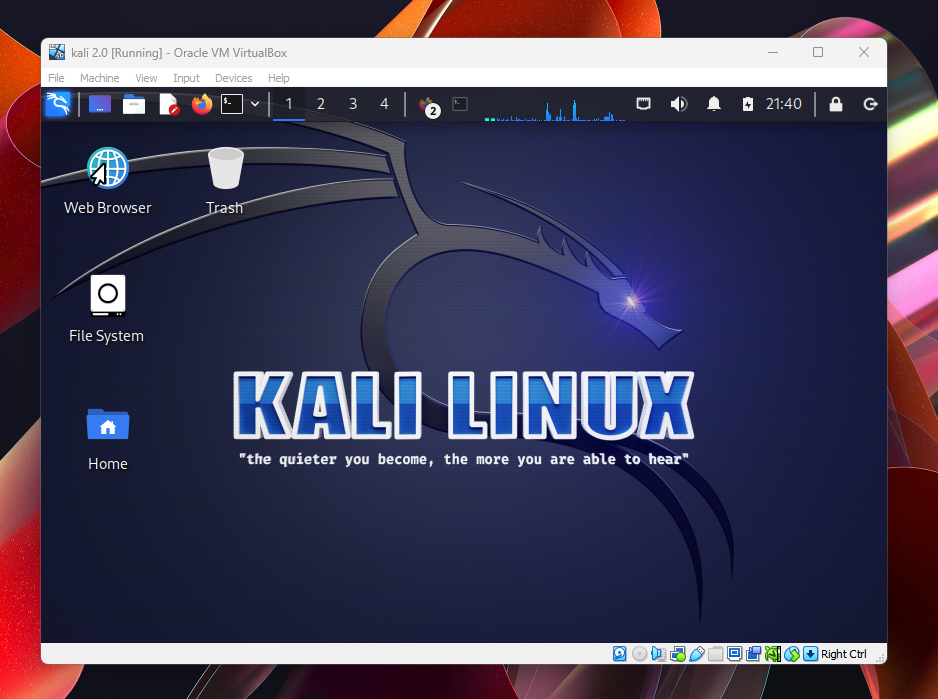
Adapter 3: NAT network 192.168.20.0/24

Adapter 4: Internal Network 192.168.60.0/2





Once pfSense was running, I continued by downloading my Kali 2023.4 64 bit. Kali is super user-friendly and by far the easiest of all the VM’s I worked with. I like having a visually pleasing interface and a mouse! I gave Kali 2048 MB and 2 CPU during the install.



I set my Kali Network adapters as follows:

Adapter 1: Bridged Adapter

Adapter 2: Internal Network 192.168.60.0/2

Next, I moved towards creating my Management VM. This Management VM includes both Snort and Splunk for time-saving purposes. I used the Ubuntu 22.04.3 64 bit download for this. I gave my Management VM 2048 MB and 2 CPUs.

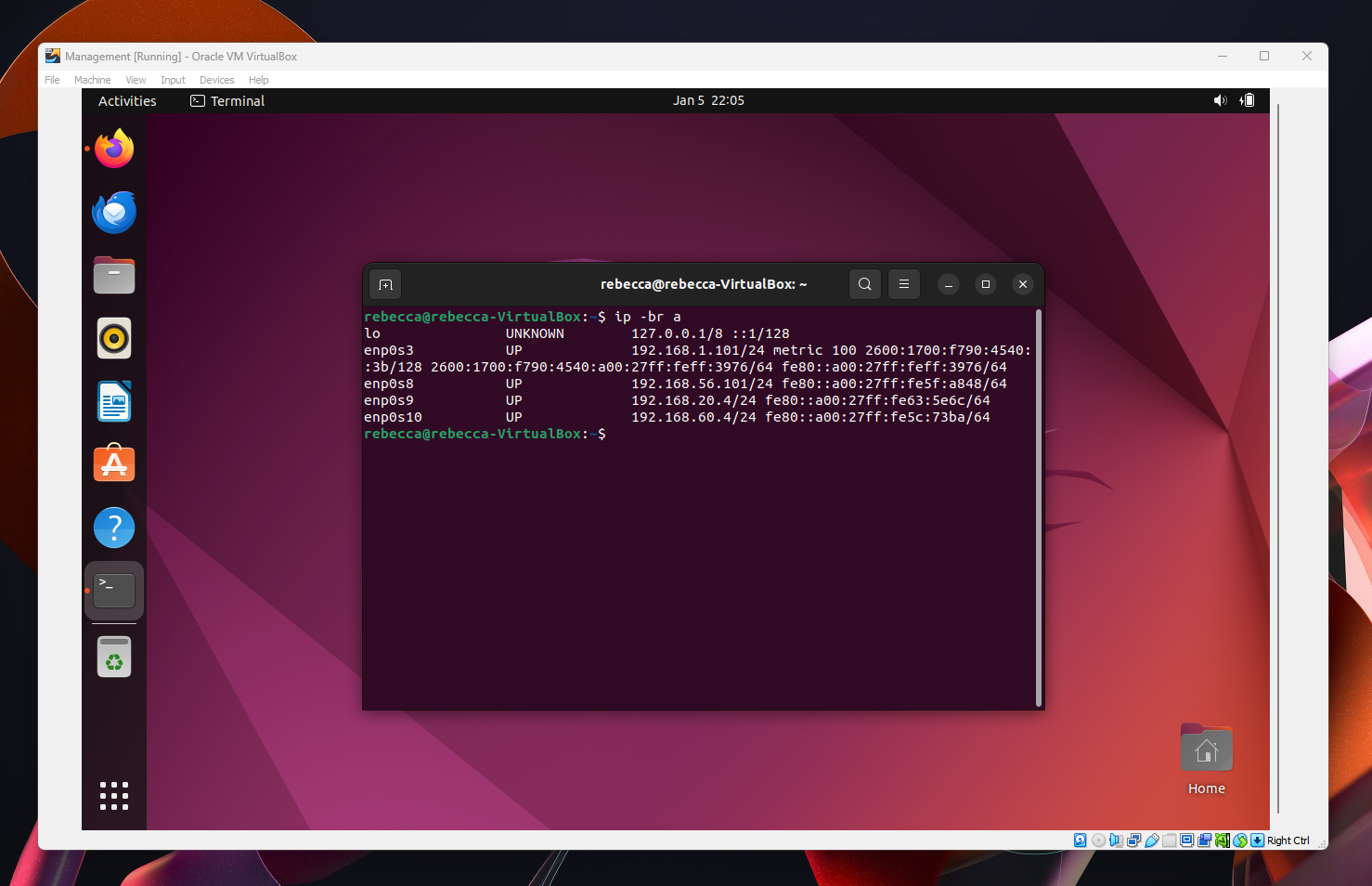
My Management Network adapters are as follows:

Adapter 1: Bridged Adapter

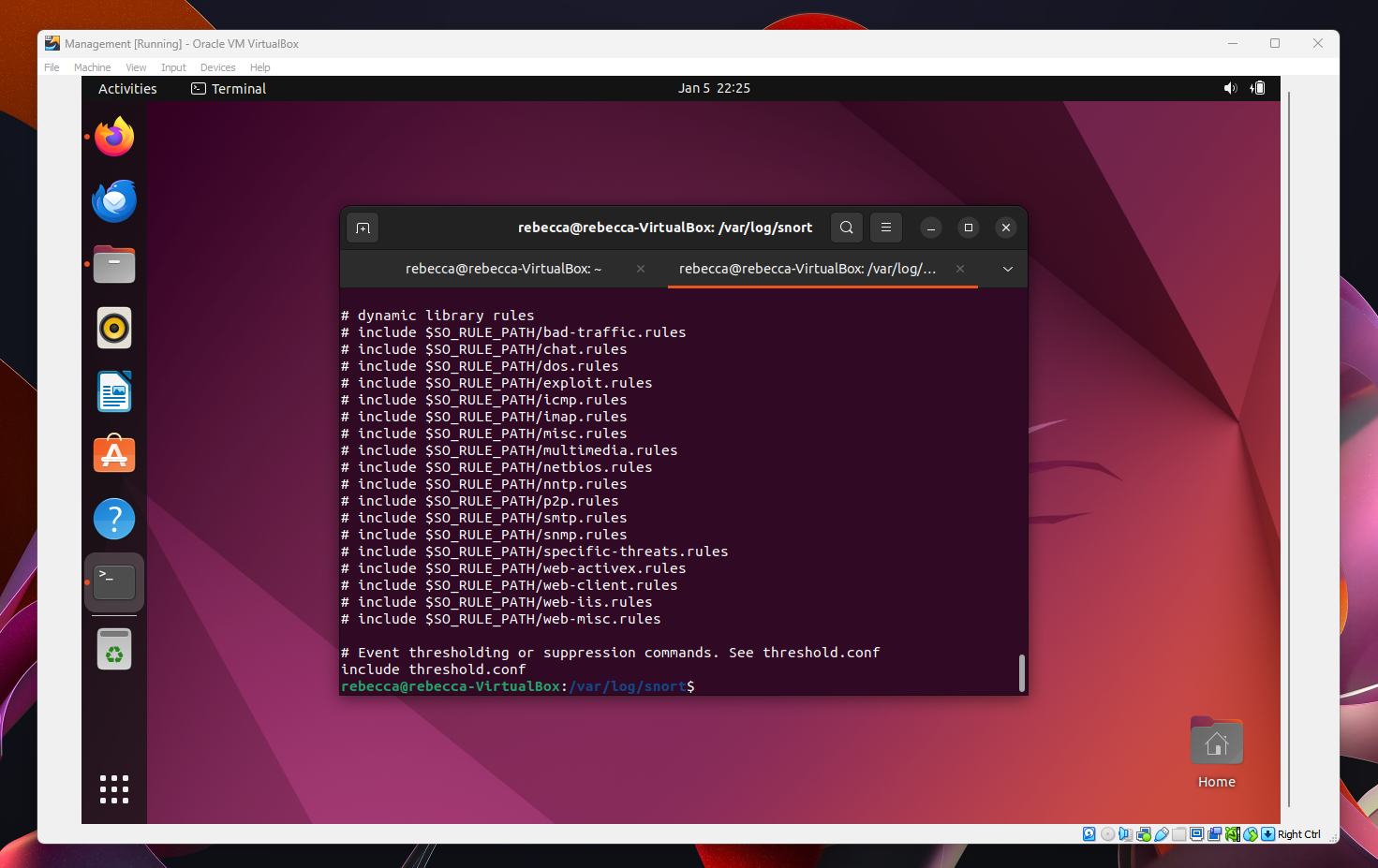
Adapter 2: Host-Only

Adapter 3: NAT network

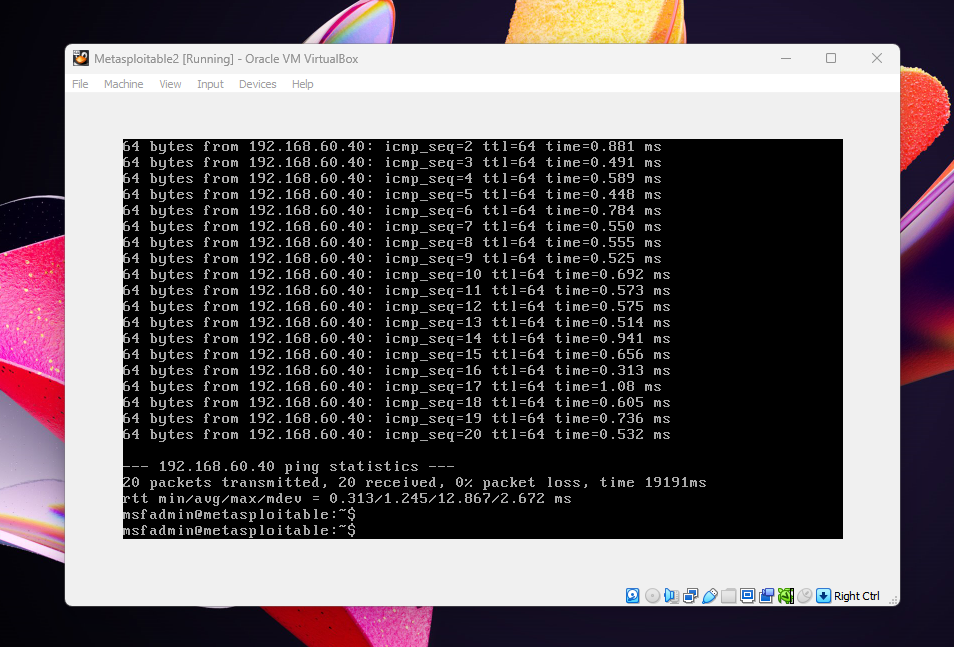
Adapter 4: Internal network



Next, I made sure that Management had a connection and ran sudo apt update as well as sudo apt upgrade before tackling Snort. I used sudo apt install snort -y to install. After I configured Short, it installed successfully for me. I was also able to install Splunk but I have not been able to tinker with either of them to simulate traffic and rules, I hope to keep playing with it to have my lab be fully functional.



Lastly, I set up my Metasploitable2. I downloaded it from Rapid7, gave it 2048MB and 2 CPU. For this, the install and configuration was straightforward. I was able to get it set up and confirm it’s “talking” to the rest of my VMs. Unfortunately I have not been able to properly use it, I am hoping to delve into it more as we continue with our labs. For now it has been installed and properly configured. My Network Adapters for Metasploitable2 is just 1 adapter, NAT network.



Phase 1 Final Project was a FEAT. I am happy and thankful for Emilie’s help throughout creating my lab. Though I am not at the finish line when it comes to being able to simulate/launch attacks from my Kali, I am confident that with the bones of my lab I will continue to be able to learn and grow.