NETWORK SECURITY SOLUTION

This project is based on the network security solution of Ubuntu and other Linux systems.

There are total of 4 VM's used.

1. Ubuntu OS (Victim)
2. Kali Linux (Attacker)
3. Security Onion (NIDS) (Network Intrusion Detection System)
4. Network Firewall (pfsense)

Setting Up:

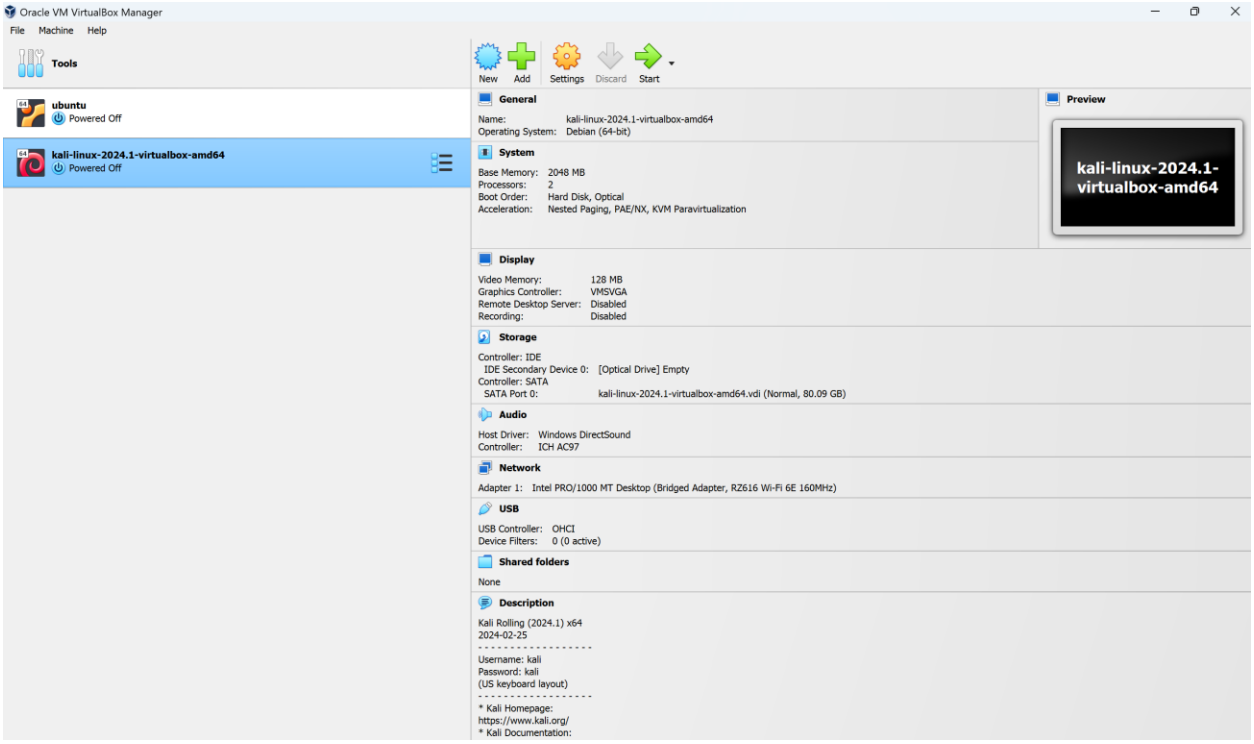
We will first launch our victim and attacker operating systems. These include Ubuntu OS and Kali Linux respectively.

For this purpose, we will be using the concept of virtual machines. The hypervisor that we will be using is VirtualBox.

First, we create 2 VM's. One is of Ubuntu and other is of Kali Linux. Then after setting them up we will start our machines.

Images are attached below for a better understanding,

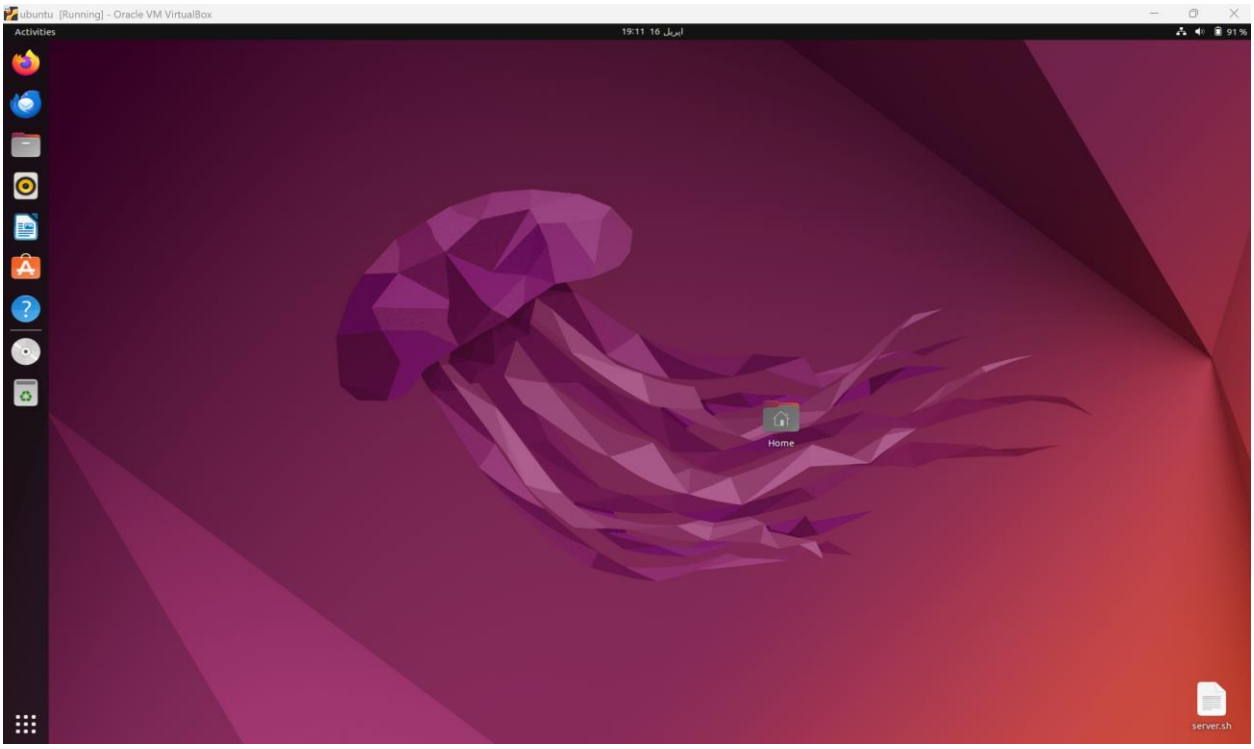
Virtual Box:



This is the main window of Virtual Box. As you can see that we have already set up our two machines.

Now, lets start them one by one to proceed further.

Ubuntu:



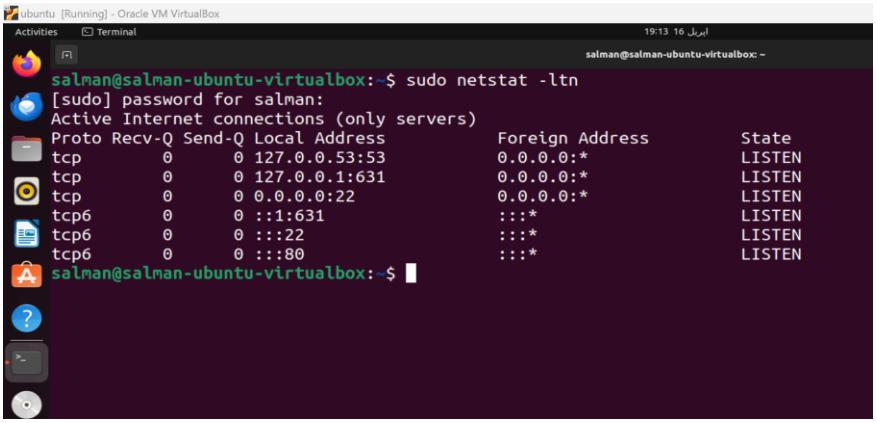
This is the main window of Ubuntu OS.

I have started some services on this machine in order for our attacks to work.

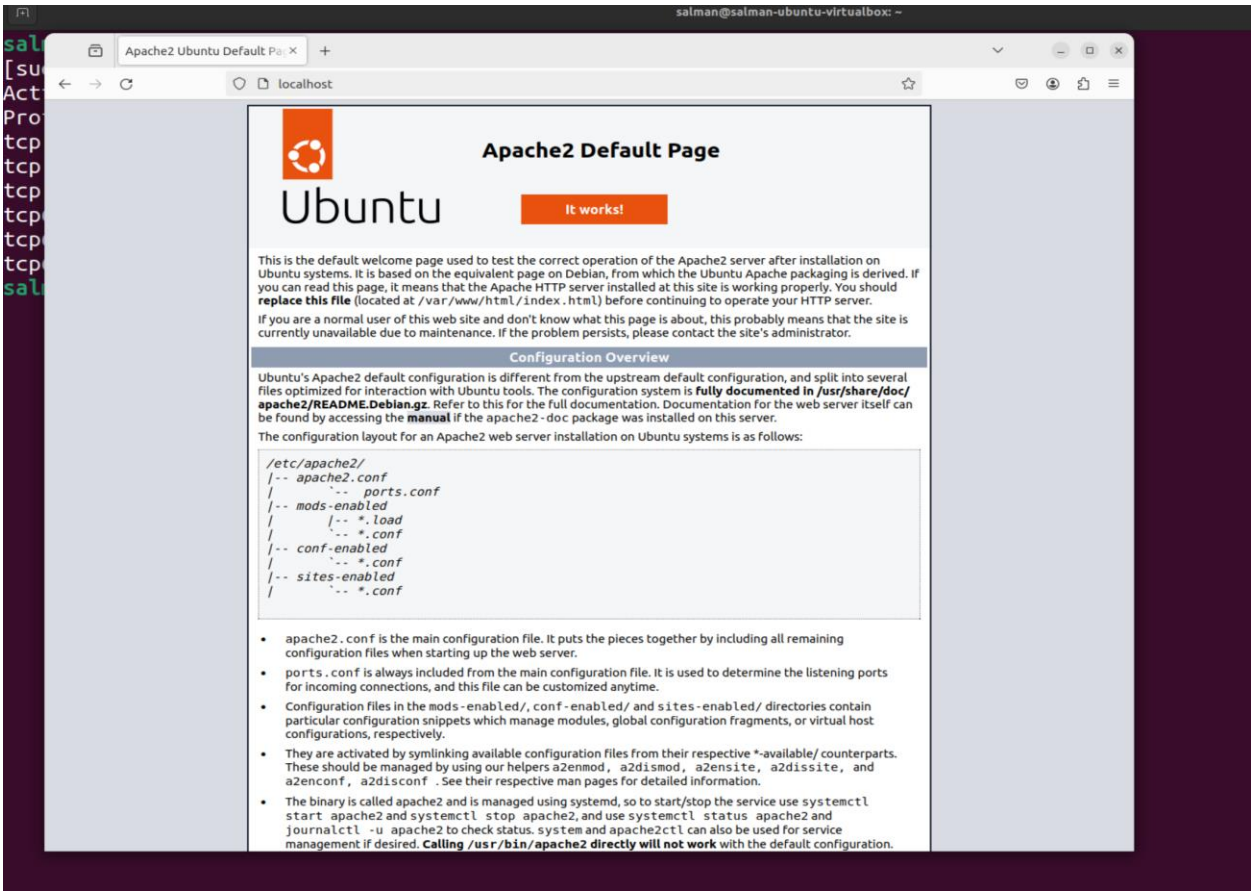
These services are:

1. Open SSH (22)
2. Apache2 (80, 443)

We can confirm this by listing the open listening ports of this machine,



As it clearly shows that we have been listening on these ports. Furthermore, we can also check the apache2 by opening the localhost webpage.



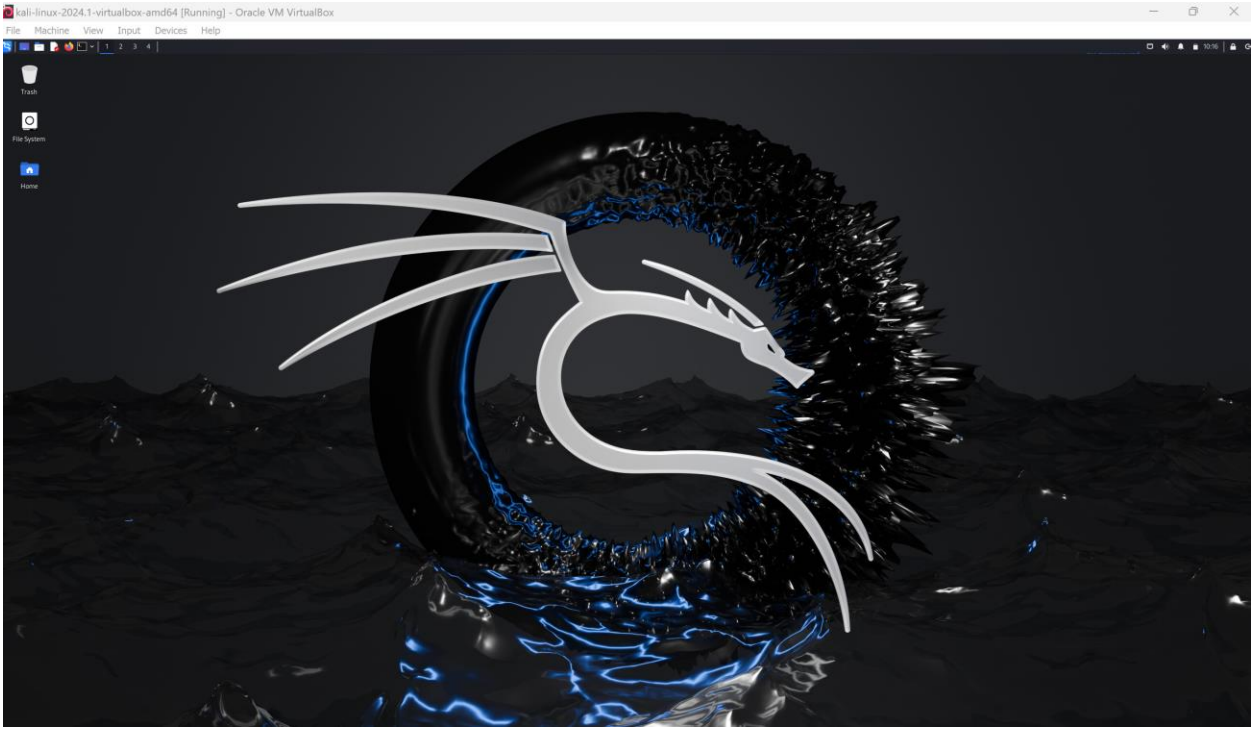
This picture clearly demonstrates and confirm that our apache2 daemon is running successfully in background.

NOTE: I didn't start it, it started automatically when the system boots up.

Checking the internet address on our Ubuntu machine.

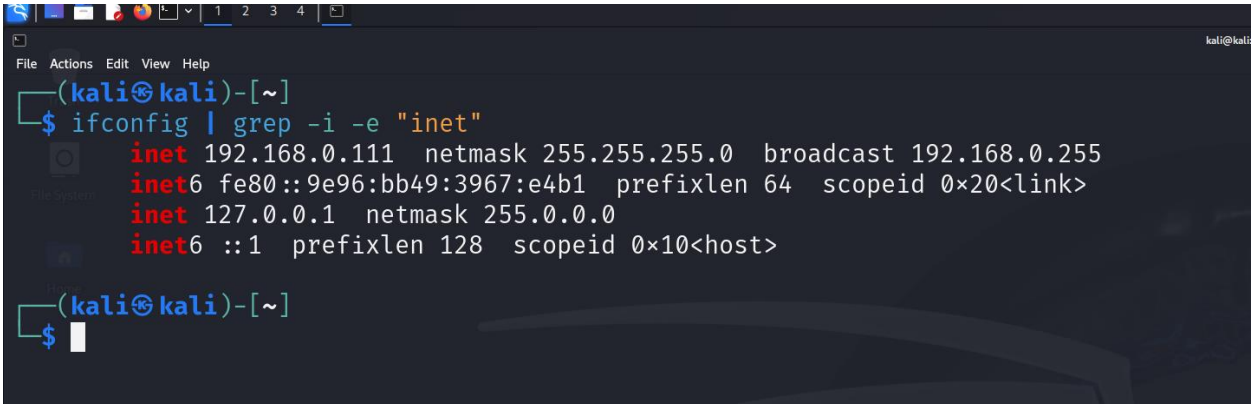
```
salman@salman-ubuntu-virtualbox:~$ ifconfig | grep -i -e "inet"
        inet 192.168.0.108  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::e2f5:c785:376d:f55b  prefixlen 64  scopeid 0x20<link>
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
salman@salman-ubuntu-virtualbox:~$
```

Kali Linux:



This is the main window of Kali Linux operating system. We can now check for its IP.

IP,



Now as we know IP(s) of both of our attacker and victim machine, we can proceed further to scanning ports.

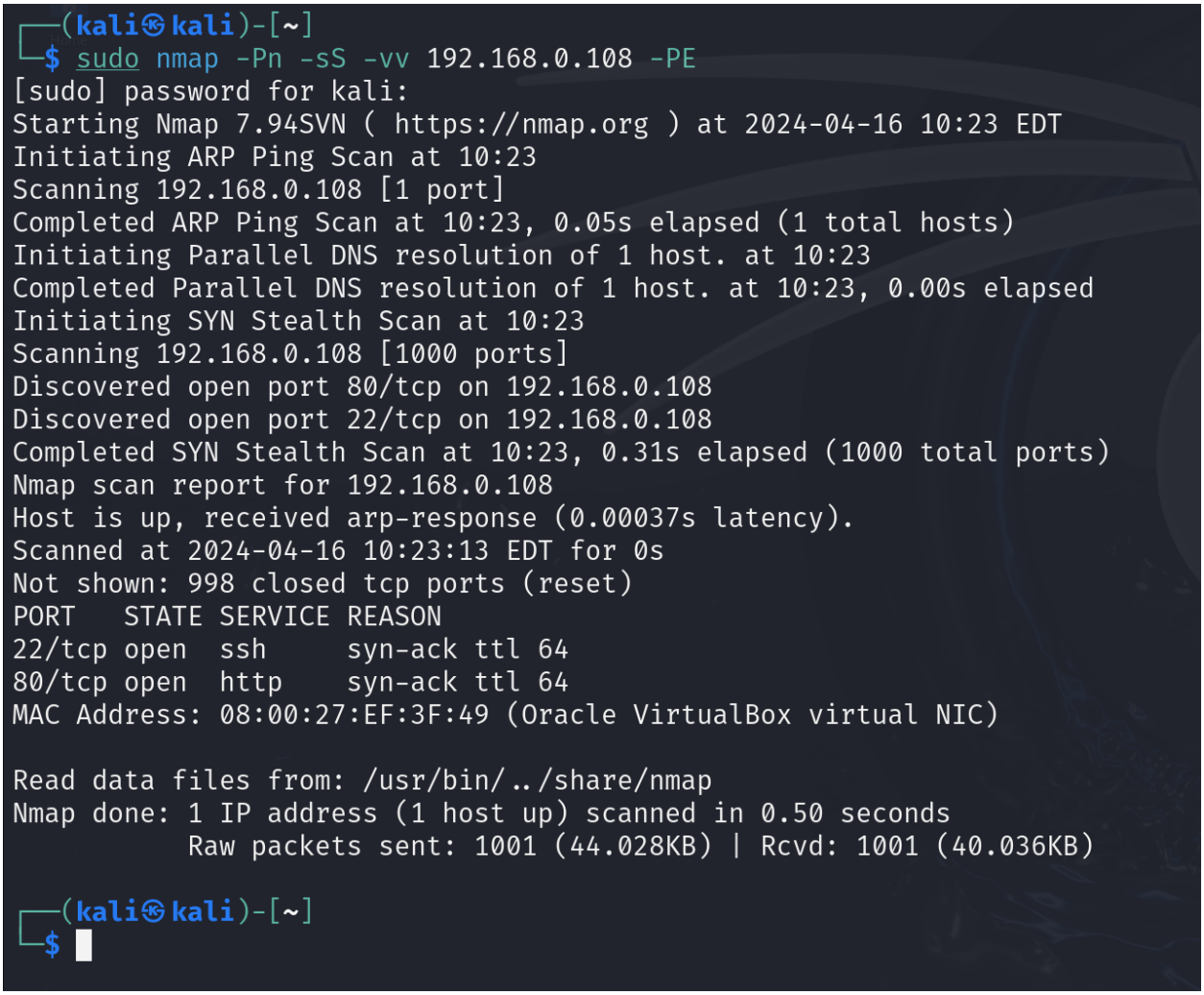
Scanning Ports:

For this purpose, we will be using NMAP. This is almost the best networking tool that comes pre-installed in Kali Linux. This tool is very powerful and can scan an IP for open ports and much more.

As a demo, we can scan for open ports on our Ubuntu machine. The command that we will be using is,

This image shows that our host is up. As a good practice it is very OK to check either the host is up or not. It can be possible that we may be scanning for a machine that doesn't exists or is not active at the moment.

Now, scanning for ports on this,



This result shows that there are currently two open ports. One of them is port 22 which is being used for ssh connections and other is port 80 which is our active apache2 daemon on Ubuntu machine.

Now we can try initiating DDOS on this IP.

DDOS:

DDOS stands for distributed denial of service attack. In this attack an IP is flooded with hundreds and thousands of requests and that system eventually slows down.

In order to demonstrate this attack, we can use a tool that also comes pre-installed in Kali Linux just like NMAP. This tool is known as hping3.

As a demo, we can test DDOS on Ubuntu machine. The command that we will be using is as follows:

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.0.111 -a 192.168.0.108 -p 80 --flood
```

Before executing this command, network and CPU usage on Ubuntu is attached below,

After executing the command we can see the following results,

The results on Kali Linux are,

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.0.111 -a 192.168.0.108 -p 80 --flood
HPING 192.168.0.111 (eth0 192.168.0.111): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

But we need to confirm it on our victim OS.

To confirm, we can see the system resources app on Ubuntu OS.

These are the graphs of system resources after initiating the attack. As it clearly shows that, our network card is very busy in receiving data.

The attack has been launched for almost less than 2 mins and our downloaded/received packets in MB are:

21.7mb. This confirms the DDOS attack on Ubuntu OS.