Portfolio Project

Packet Analysis and Simple DoS using Wireshark And Hping

Ranilo John M. Delos Angeles
University of the East - Caloocan

I. Introduction

From learning the topology creations in Cisco Packet Tracer, I wanted to use a more complicated network simulator and so in this scenario, I simulated topology where I can access the computers through Virtual Machines and this was made possible by GNS3 and Virtual Box.

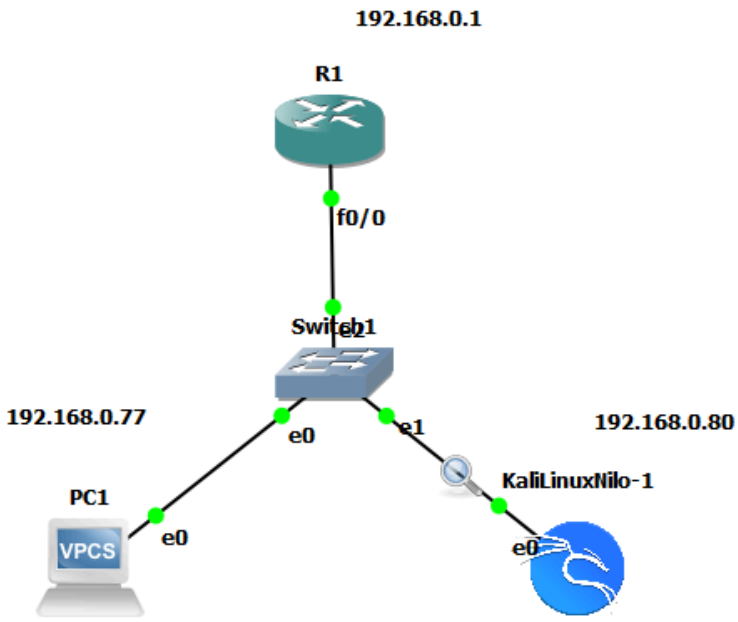

Figure 1.1 GNS3 Simple Topology

The devices I used was a Cisco Router C3745, a Simple Virtual PC, Ethernet Switch, and a Kali Linux simulated using VirtualBox.

II. Configuration

I first started configuring the router, giving the switch its IP Address of 192.168.0.1 255.255.255.0. It is an IP Address because I wanted to check first how I can properly configure and simulate the network. I also went to configure the PC1 with the IP Address of 192.168.0.77 and Kali Linux VM IP Address of 192.168.0.77

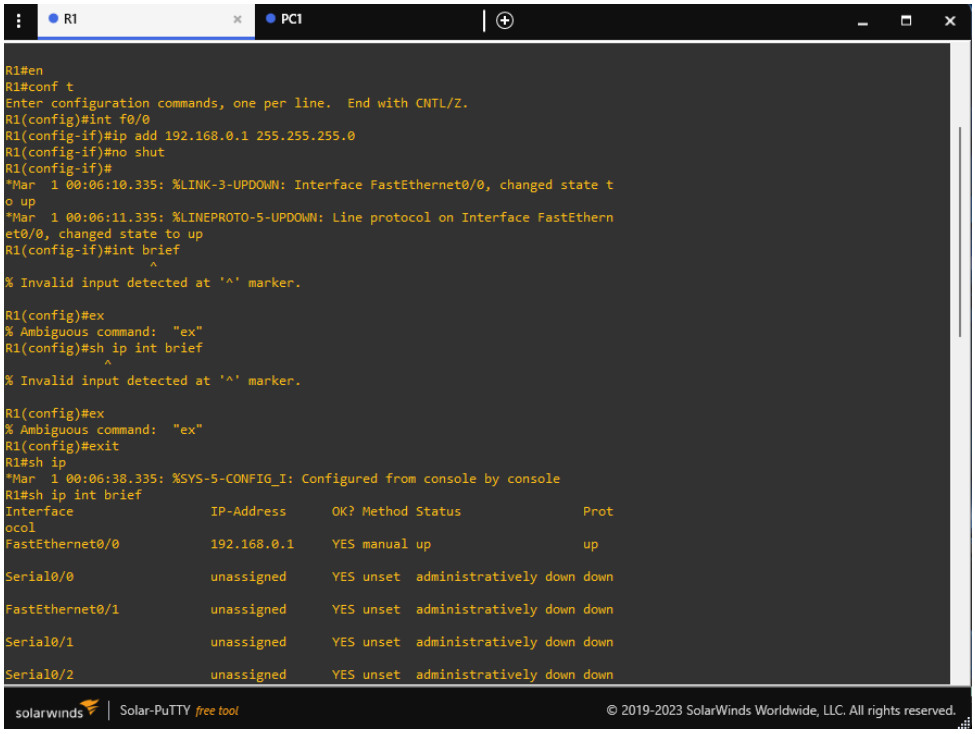

Figure 2.1 Router IP Address

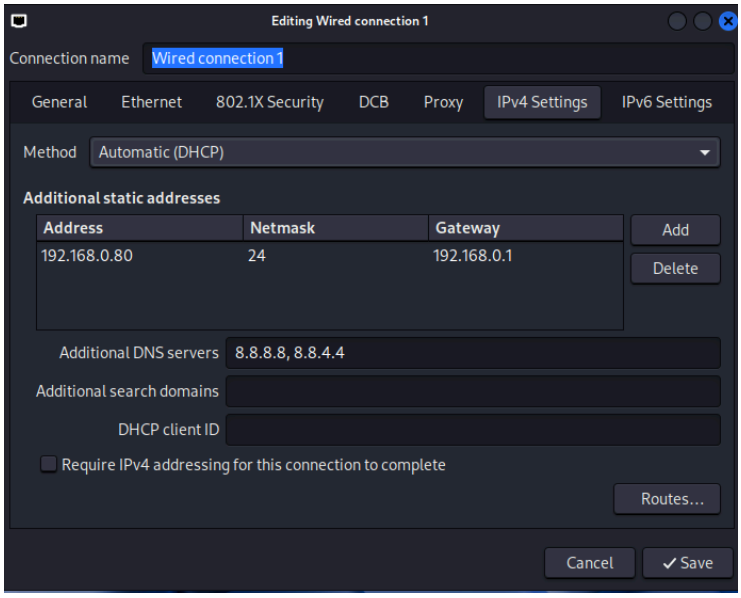

Figure 2.2 Kali Linux IP Address

III. Simulation

So first from the VPCS, I went to ICMP ping the destination IP of 192.168.0.80 (Kali Linux PC) for error checking (to see if it works or not)

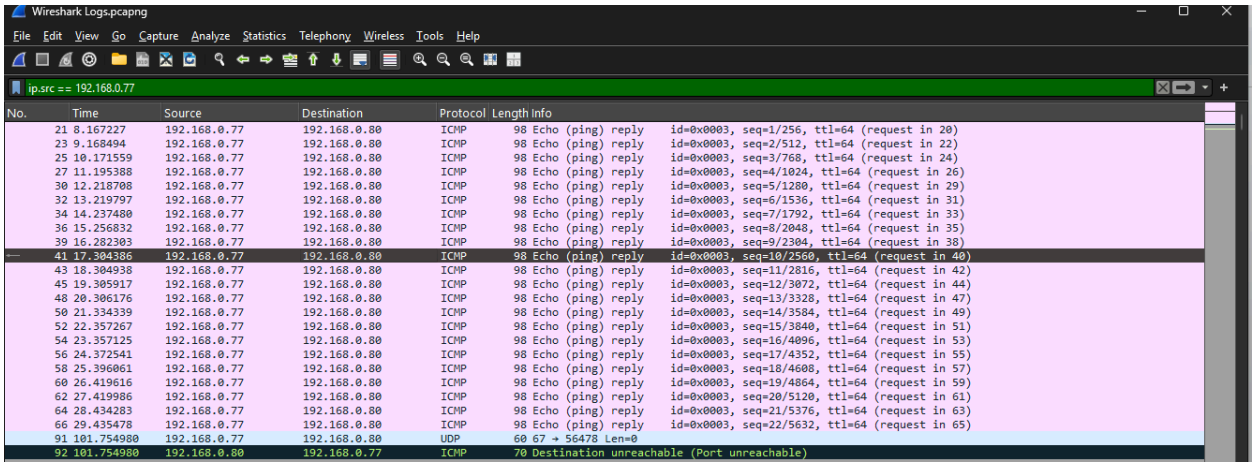

Figure 3.1 ICMPing VPCS to Kali Linux

I also did the same for Kali, I ICMP ping from Kali with IP Address of 192.168.0.80 to VPCS 192.168.0.77.

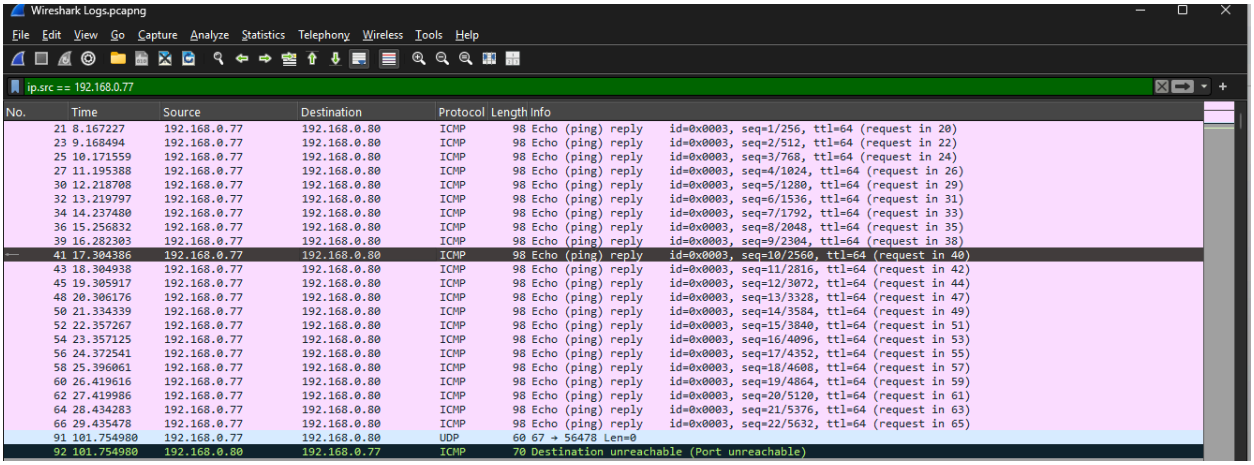

Figure 3.2 ICMPing Kali to VPCS

After that, I started doing nbtscan (netbios scan) on the network to check the ip addresses.

```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan -r 192.168.0.1/24
Doing NBT name scan for addresses from 192.168.0.1/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.0.80     <unknown>                  <unknown>
192.168.0.77     <unknown>                  <unknown>
^C
```

Figure 3.3 NBT scan in the network.

Finishing the nbtscan, I went ahead and used the NMAP command for the scanning of the VPCS, the report below shows the open ports (All ports are open because the PC is unsecured) the -sS does this by getting a SYN/ACK reply and then gets to RST to not complete the three way handshake.

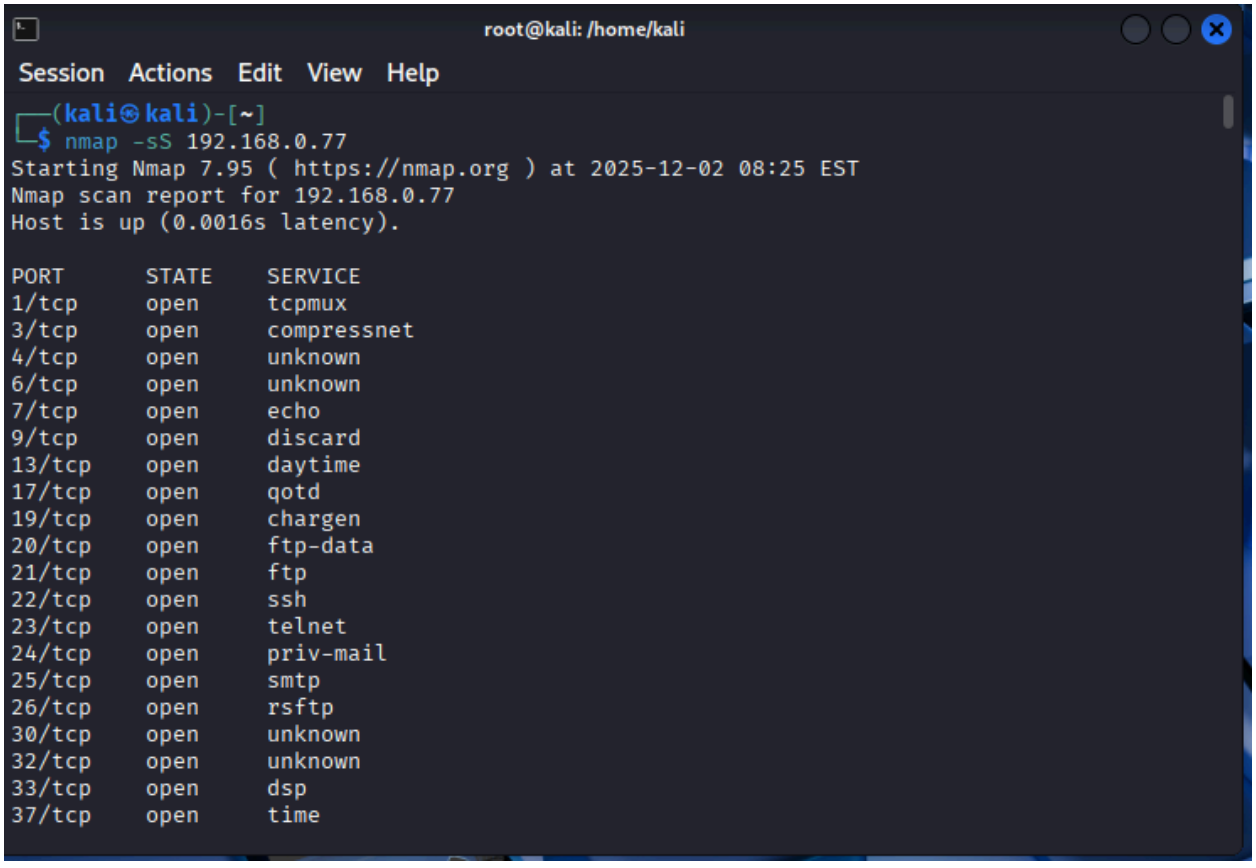

Figure 3.4 NMAP the ports to check which is open.

Here below, shows all the captured packet from the attacker's machine (Kali) the displayed packet are 2018. It shows all the ports from 1 to 65389. It also shows the MAC Address of the VPCS, 00:50:79:66:68:00.

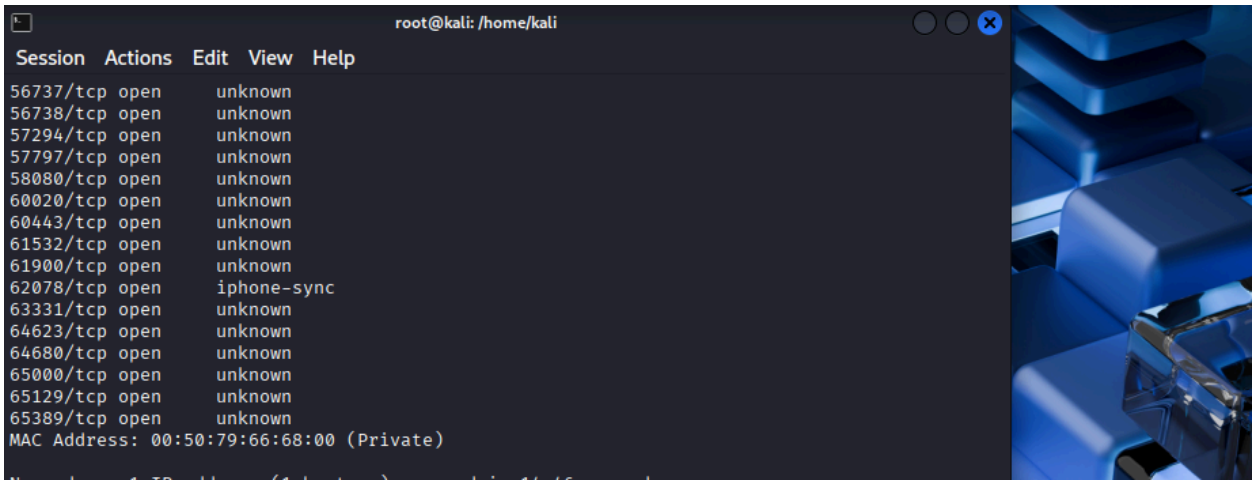

Figure 3.5 NMAP scan finished.

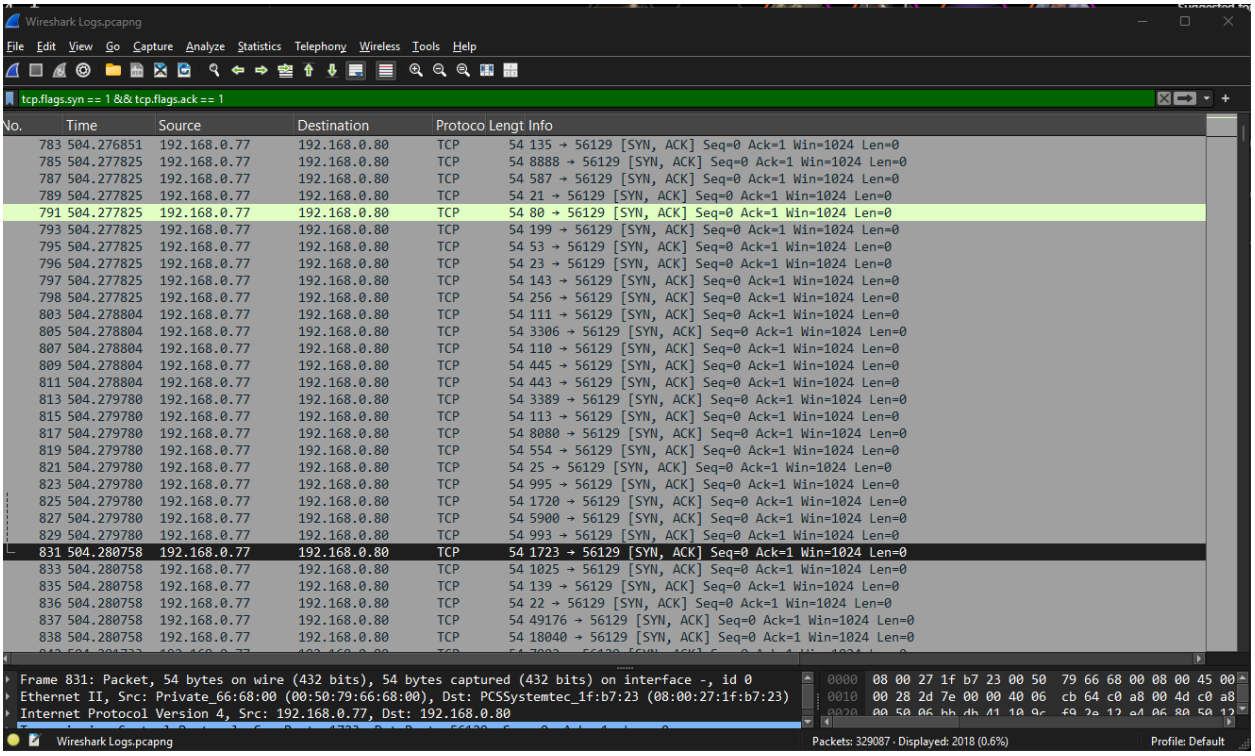

Figure 3.6 Packets captured from NMAP scanning from Port 1 to 65389.

Now since I'm curious about Denial of Service, I tried flooding the VPCS with command hping3 –icmp –flood 192.168.0.77, As shown below, there's about 245665 packets transmitted to the other end device it also did put the PC into a session timeout due to overwhelming amounts of ICMP.

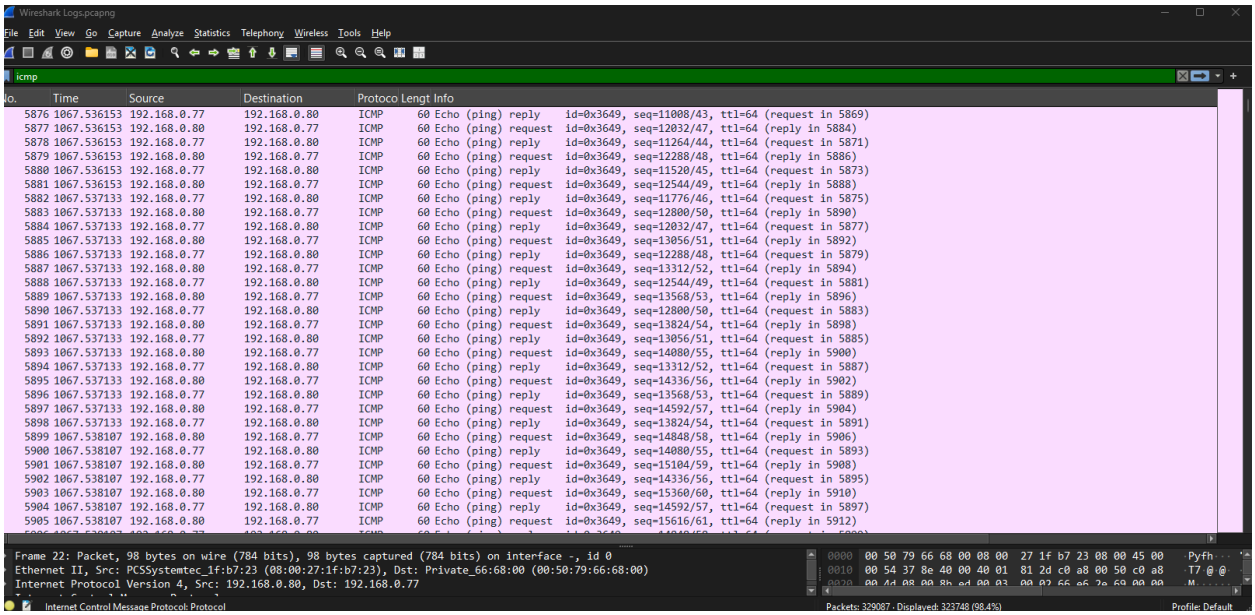

Figure 3.7 Packet Capture of DoS ICMP Flooding

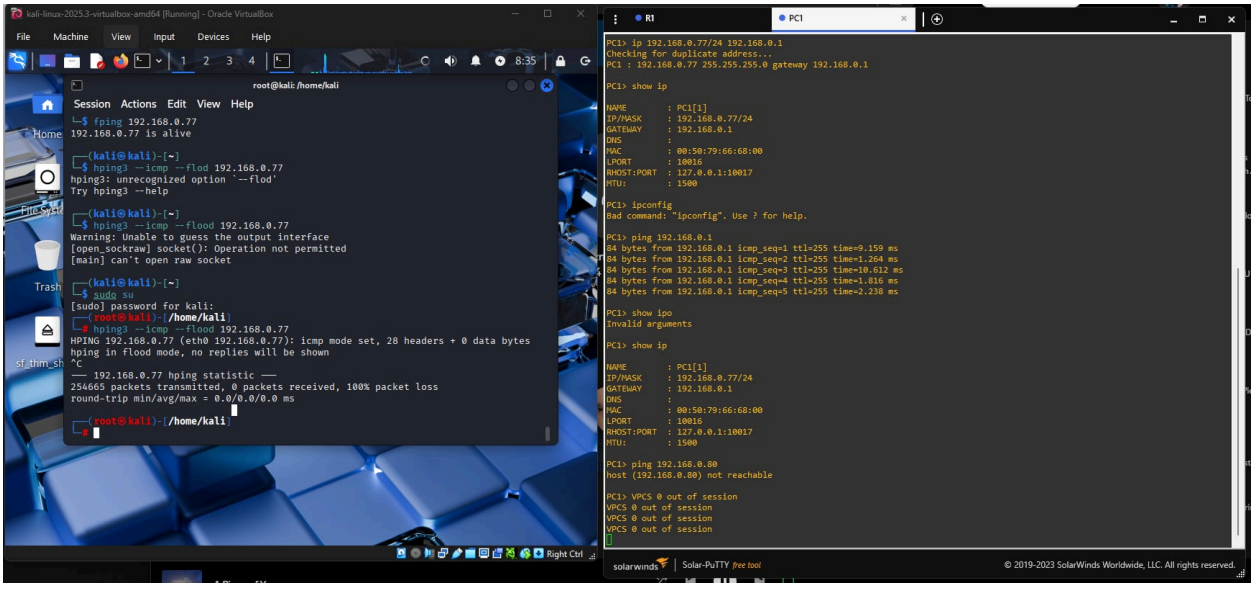

Figure 3.8 Kali command and transmitted packets and putting VPCS down.

IV. Conclusion

This has been a fun experiment to play with, because now I can finally simulate penetration testing via Kali Linux, but for this kind of simulation I want to explore more on how I will defend organizations via IDS and IPS.