Module 3

Firewall/IDS Evasion and Spoofing

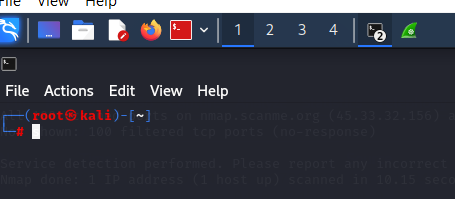
Introduction

Firewalls are an essential part of almost every IT infrastructure. Firewalls are found in any number of shapes and forms. They are usually found on layers 3 and 4 of the OSI Model (and occasionally layer2). Next generation firewalls can be found on layers 5, 6, and 7. This module will discuss a few scenarios where nmap can be used to assess and evade the firewalls encountered.

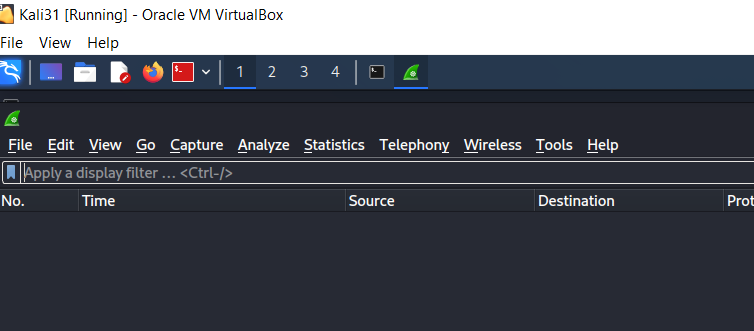
The mission of firewalls is to detect and block our scan, so many different tactics need to be used to circumvent them. Tactics include evasion by control of the IP or MAC address or the source port. Evasion via fragmentation (MTU and data length), or evasion by modifying the header fields can also be used. Below, are examples of ways to deal with firewalls.

**Evasion via source spoofing (Stealth scan)**

1. Start you Kali Linux VM as admin and open the terminal in the root directory. (Figure 1)
2. Start Wireshark (Figure 2)

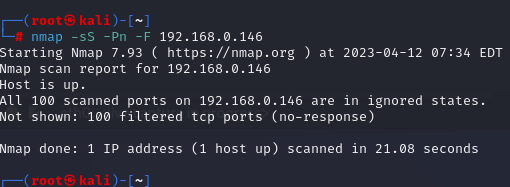


**Figure 1 Kali Linux VM**



**Figure 2 Wireshark**

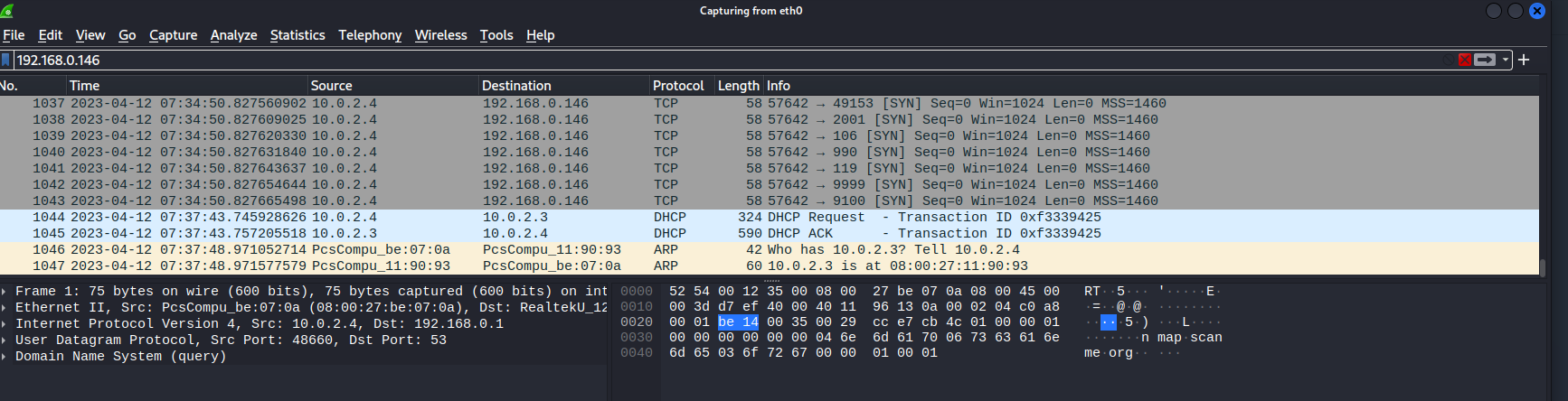
1. Go back to Kali Linux VM and type the following command: **nmap -sS -Pn -F <Ip address>** (Figure 3)



**Figure 3**

1. Go back to Wireshark (Figure 4) to view the results

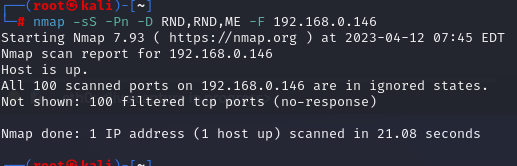
From the wireshark scan, one can see the source port, how big the ip packet was, and time to live.



**Figure 4**

**Decoy –** In order to hide our scans, we can use decoys. When we do so, we mix our IP address with other decoy IP’s. This makes it hard for the firewall and the target host to figure out the source of the port scan.

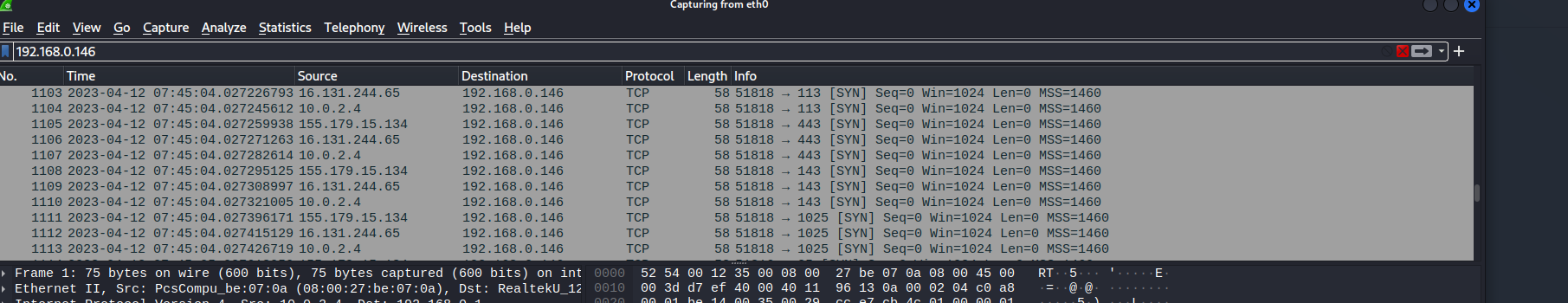
1. Go to Kali VM and type the following command: **nmap -sS -Pn -D RND,RND,ME -F <IP address>** (Figure 5)



**Figure 5**

1. Go to Wireshark to view the results. (Figure 6)

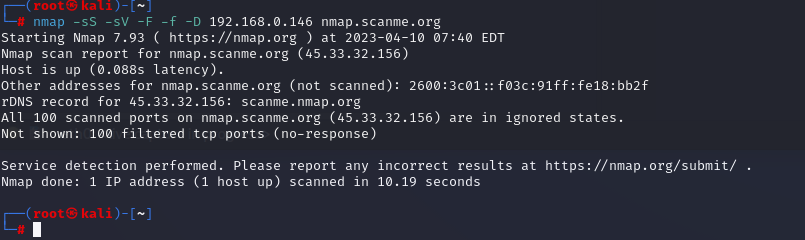
The host 192.168.0.146 sees the scans coming from two IP addresses, 155.179.15.134 and 16.131.244.65 even though one source IP (ME) is actually running the scan.



**Figure 6**

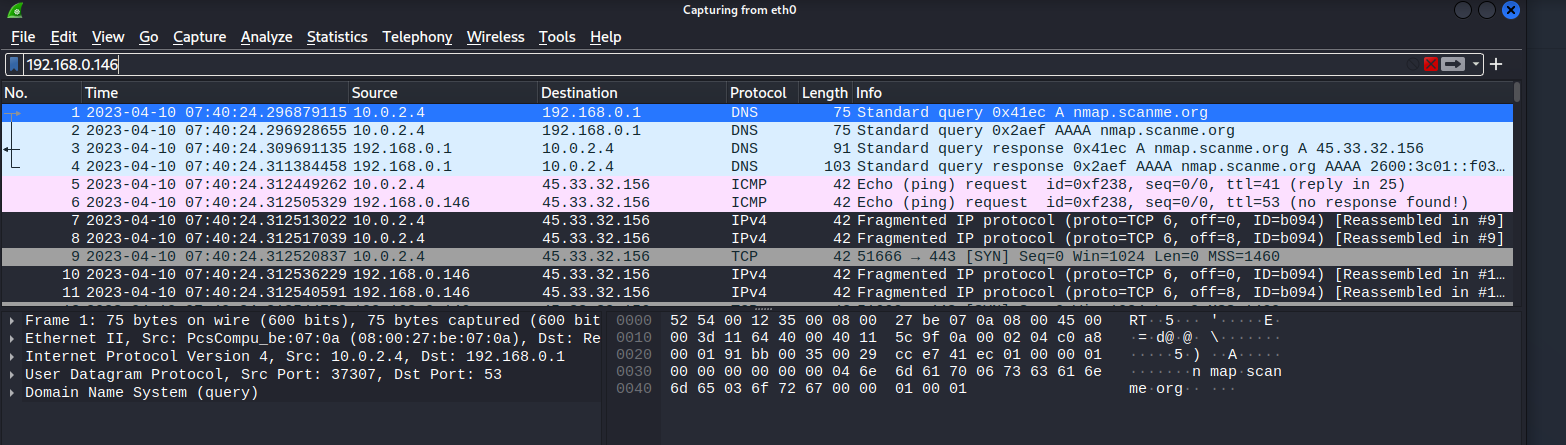
**Fragment packets-** Fragmentation fragments the packets.

1. Go to Kali VM and type the following command: **nmap -sS -sV -F -f <IP address> nmap.scanme.org** (Figure 7)



**Figure7**

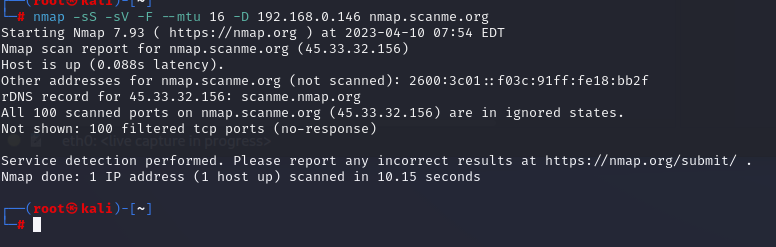
The results can be seen in Wireshark. (Figure 8)



**Figure 8**

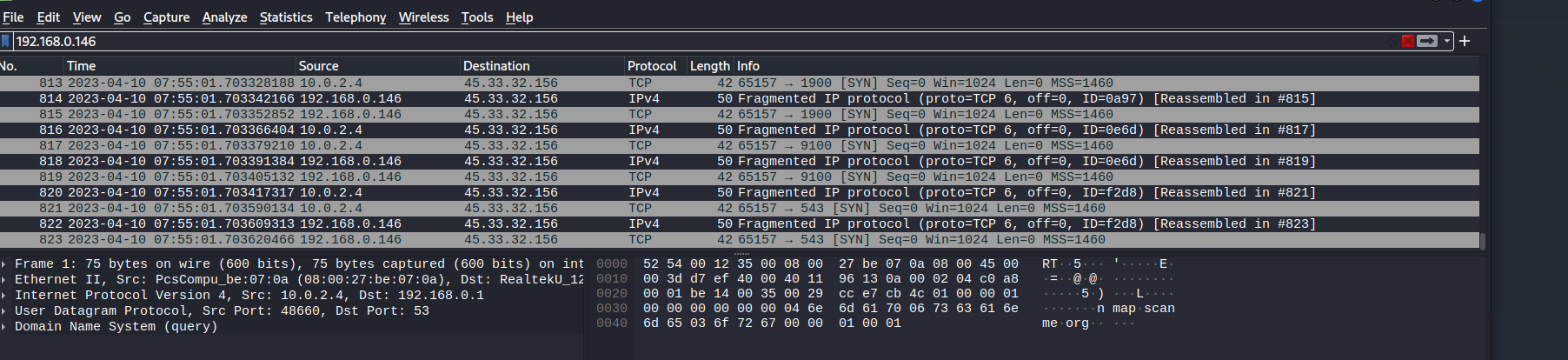
**MTU**- this will set a number of bytes per one IP packet. The value of the value set for an MTU is always a multiple of 8.

1. Go to Kali VM and type the following command: **nmap -sS -sV -F –mtu16 -D <IP address> nmap.scanme.org** (Figure 9)



**Figure 9**

Wireshark shows the results in Figure 10



**Figure 10**

**Spoofed IP Address**

1. Go to Kali VM and type the following command: **nmap -sS -Pn -F -S <IP address>**

IP Spoofing is useful in hiding the true source of IP packets to make it difficult to know where they came from. This is only useful when on the same subnet as your target, if you’re not, the replies from your target will be unreadable. In some cases, nmap may not be able to determine your source address, in this case nmap will tell you. This can be seen in figure 11.

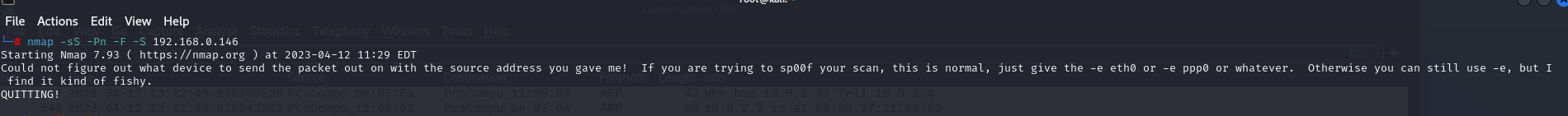


Figure 11

**Spoofed MAC Address**

1. Go to Kali VM and type the following command: **nmap -sS Pn -F –spoof-mac <Mac\_Address>.** Thiswill only work if your machine is on the same network segment as your target. If not, just as with the IP spoofing, you will not be able to read or capture the responses.

Reference

Vicarius. (2022). Nmap Advanced Uses Pt.3: Firewall Evasion. Retrieved from https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion