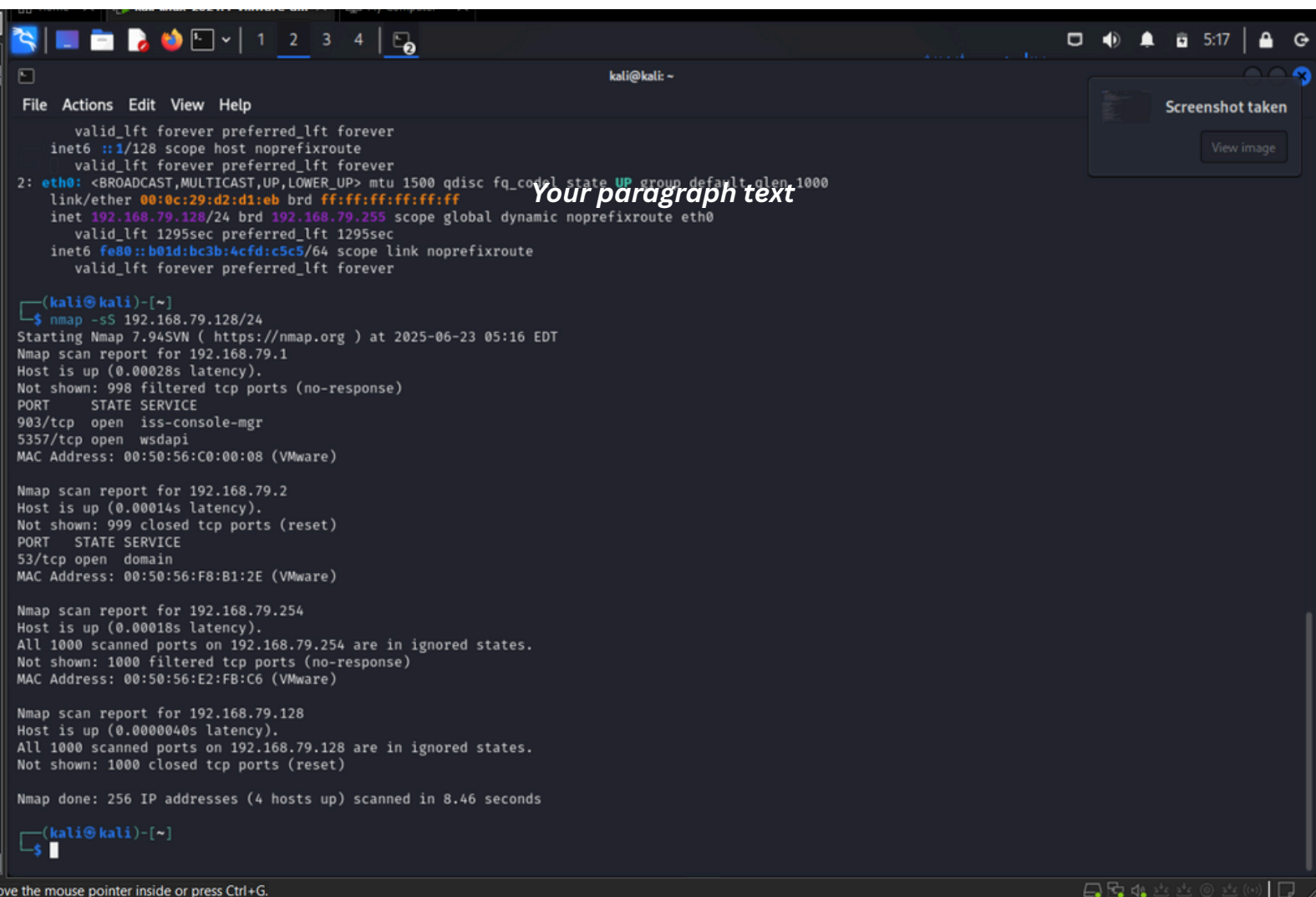


Nmap (Network Mapping)

Finding Local Ip address :



```

kali@kali: ~
File Actions Edit View Help
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d2:d1:eb brd ff:ff:ff:ff:ff:ff
    inet 192.168.79.128/24 brd 192.168.79.255 scope global dynamic noprefixroute eth0
    valid_lft 1295sec preferred_lft 1295sec
    inet6 fe80::b01d:bc3b:4cfd:c5c5/64 scope link noprefixroute
    valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ nmap -sS 192.168.79.128/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 05:16 EDT
Nmap scan report for 192.168.79.1
Host is up (0.00028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
903/tcp    open  iss-console-mgr
5357/tcp   open  wsddapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.79.2
Host is up (0.00014s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp     open  domain
MAC Address: 00:50:56:F8:B1:2E (VMware)

Nmap scan report for 192.168.79.254
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.79.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:FB:C6 (VMware)

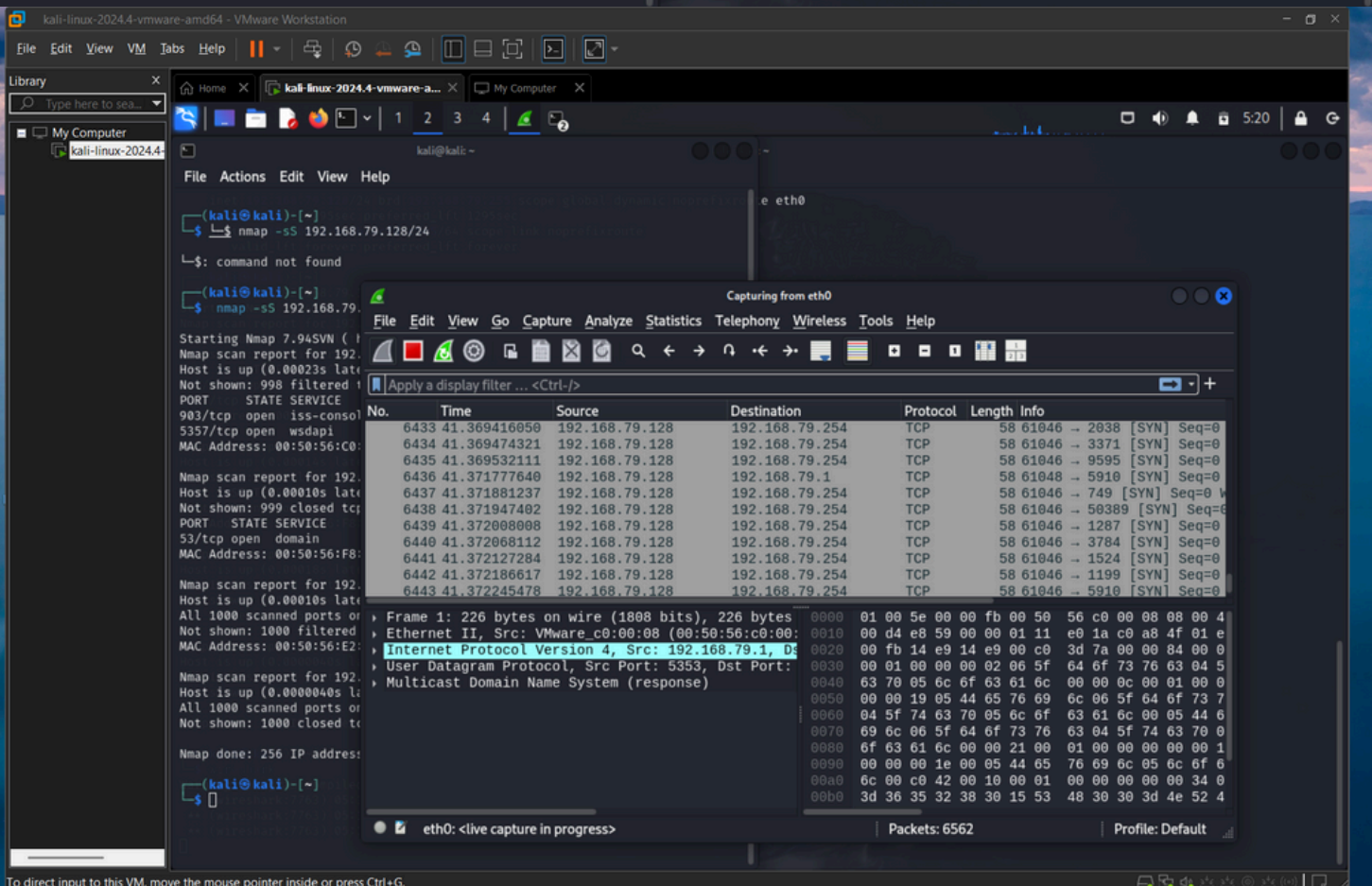
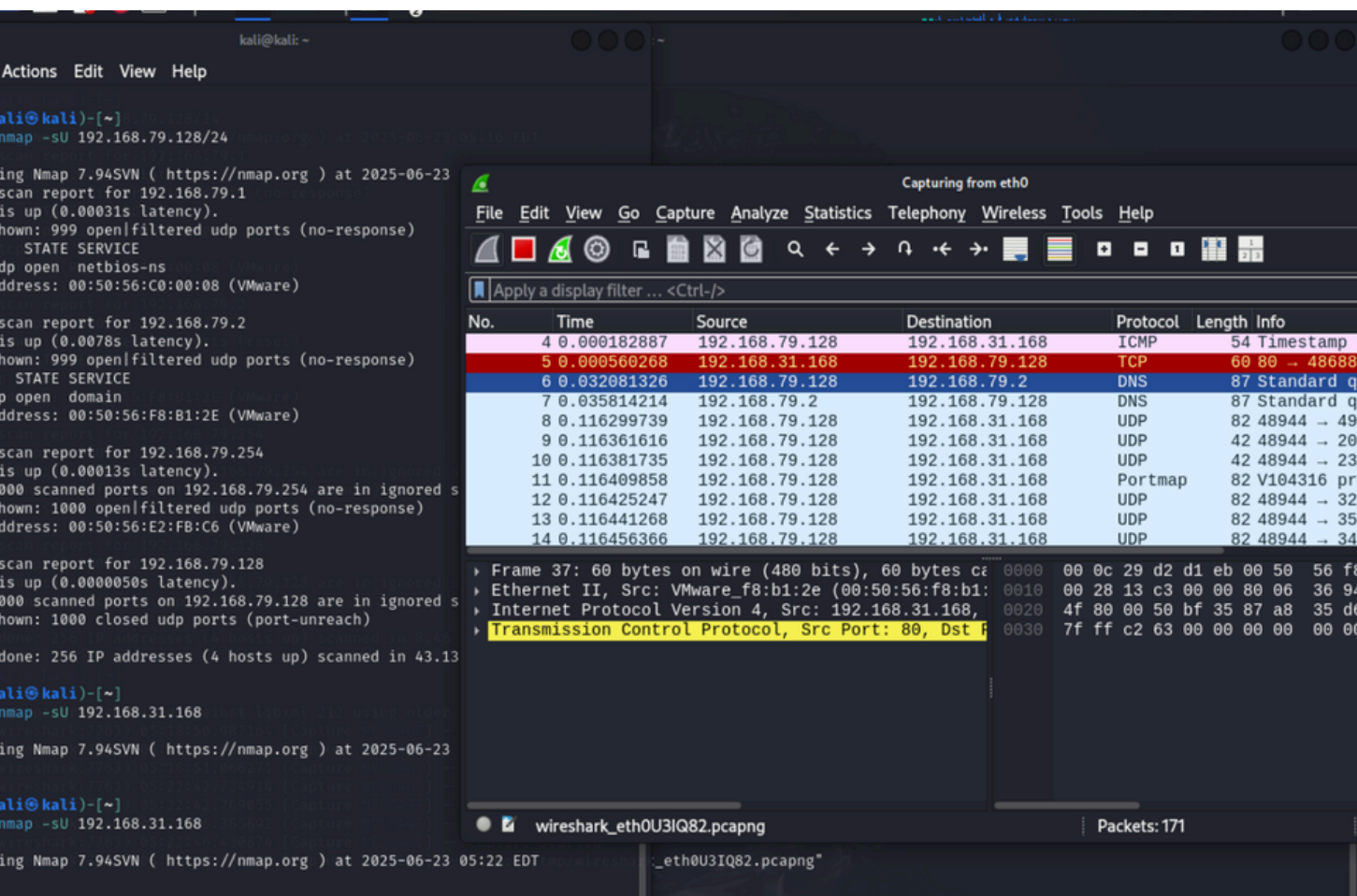
Nmap scan report for 192.168.79.128
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.79.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.46 seconds

(kali@kali)-[~]
$
  
```

used local Ip address of my kali machine and used Stealth scan which is (-sS) stealth scan in nmap and also find my local ip address using in kali terminal by using (ifconfig) and windows (ipconfig).while scanning in nmap filtered port shows that the scan has been detected by firewall and got ignored .

Wireshark



Wireshark

In wireshark we can see the scan made by the nmap can be seen in the above image . The scan from the source and destination are from same ip destination shows the subnet -address of the ip.

In first image I made a Tcp scan and the wireshark protocol shows Tcp and again made the scan with Udp the protocol shows Udp

Ports Running on my machine

- Port -903(Tcp)-Vmware Remote console
- Port-5357(Tcp)-Web service on Device Api

Identify potential security risks from open ports.

Threat actors use open ports to carry out attacks and exploit vulnerabilities. Below, we share some common exploits and attacks that malicious actors leverage, and then detail two famous attacks via open port vulnerabilities.