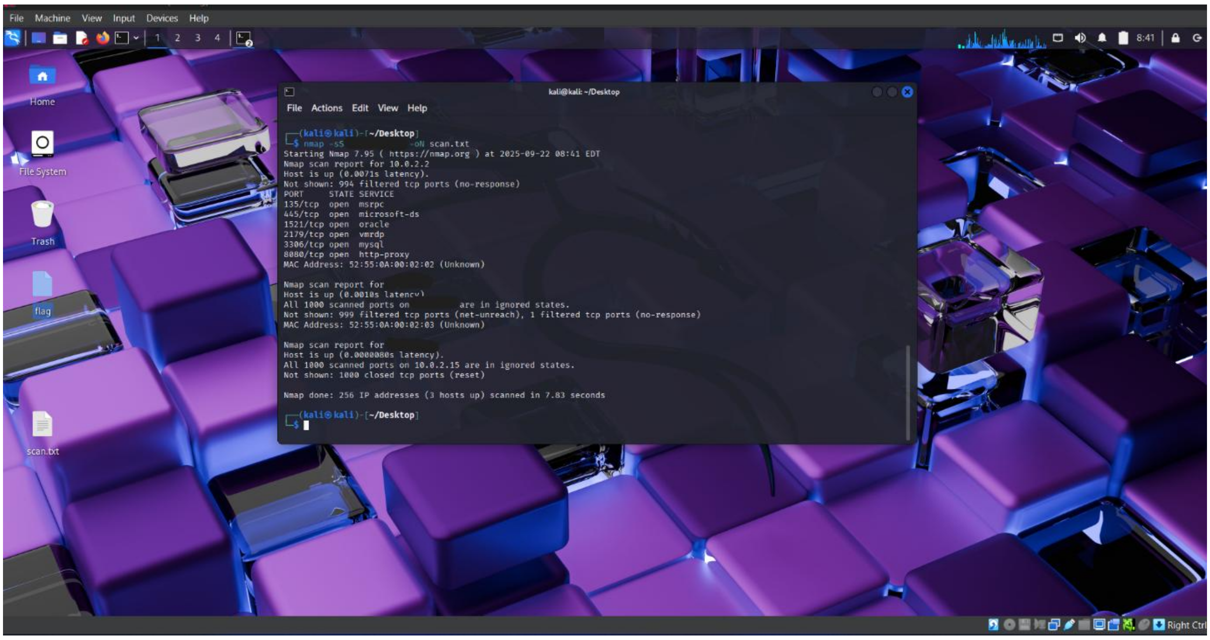
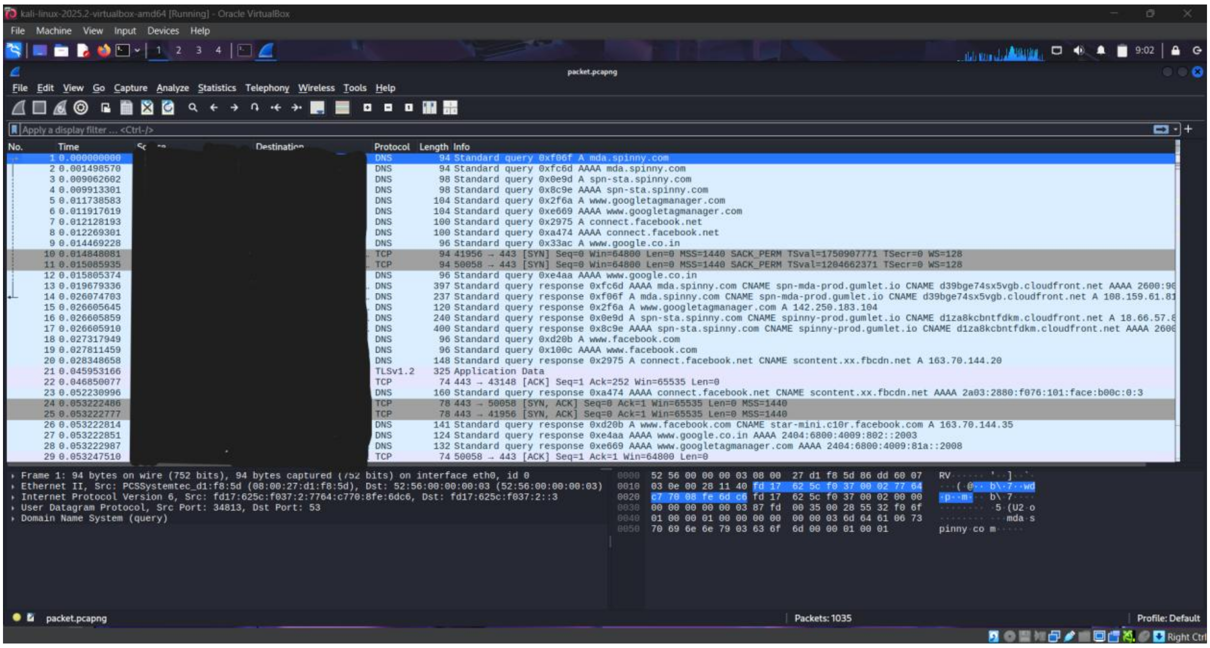
- ***This is the screenshot of the network scanning using nmap in kali machine.***



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sS [redacted] -oN scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 08:41 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0071s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
2179/tcp open  vmrdp
3306/tcp open  mysql
8080/tcp open  http-proxy
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for [redacted]
Host is up (0.0010s latency)
All 1000 scanned ports on [redacted] are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for [redacted]
Host is up (0.0000080s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.83 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

This is the screenshot of scanning the packet of the local network and there packets.



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
9:02
packet.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
packet.pcapng
Packets: 1035
Profile: Default
Right Ctrl

No.	Time	Sc [redacted]	Destination	Protocol	Length	Info
1	0.000000000	[redacted]	[redacted]	DNS	94	Standard query 0xf06f A mda.spinny.com
2	0.001498570	[redacted]	[redacted]	DNS	94	Standard query 0xfc6d AAAA mda.spinny.com
3	0.009062602	[redacted]	[redacted]	DNS	98	Standard query 0x0e9d A spn-sta.spinny.com
4	0.009913301	[redacted]	[redacted]	DNS	98	Standard query 0x8c9e AAAA spn-sta.spinny.com
5	0.011738583	[redacted]	[redacted]	DNS	104	Standard query 0x2f6a A www.googletagmanager.com
6	0.011917619	[redacted]	[redacted]	DNS	104	Standard query 0xe669 AAAA www.googletagmanager.com
7	0.012128193	[redacted]	[redacted]	DNS	100	Standard query 0x2975 A connect.facebook.net
8	0.012269301	[redacted]	[redacted]	DNS	100	Standard query 0xa474 AAAA connect.facebook.net
9	0.014469228	[redacted]	[redacted]	DNS	96	Standard query 0x33ac A www.google.co.in
10	0.014848081	[redacted]	[redacted]	TCP	94	41956 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=1750907771 TSecr=0 WS=128
11	0.015085935	[redacted]	[redacted]	TCP	94	50058 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=1204662371 TSecr=0 WS=128
12	0.015805374	[redacted]	[redacted]	DNS	96	Standard query 0xe4aa AAAA www.google.co.in
13	0.019679336	[redacted]	[redacted]	DNS	397	Standard query response 0xfc6d AAAA mda.spinny.com CNAME spn-mda-prod.gumlet.io CNAME d39bge74sx5vgb.cloudfront.net AAAA 2600:9
14	0.026074703	[redacted]	[redacted]	DNS	237	Standard query response 0xf06f A mda.spinny.com CNAME spn-mda-prod.gumlet.io CNAME d39bge74sx5vgb.cloudfront.net A 108.159.61.81
15	0.026605645	[redacted]	[redacted]	DNS	120	Standard query response 0x2f6a A www.googletagmanager.com A 142.250.183.104
16	0.026605859	[redacted]	[redacted]	DNS	240	Standard query response 0x0e9d A spn-sta.spinny.com CNAME spinny-prod.gumlet.io CNAME d1za8kcbntfdkm.cloudfront.net A 18.66.57.8
17	0.026605910	[redacted]	[redacted]	DNS	400	Standard query response 0x8c9e AAAA spn-sta.spinny.com CNAME spinny-prod.gumlet.io CNAME d1za8kcbntfdkm.cloudfront.net AAAA 260
18	0.027317949	[redacted]	[redacted]	DNS	96	Standard query 0xd20b A www.facebook.com
19	0.027811459	[redacted]	[redacted]	DNS	96	Standard query 0x100c AAAA www.facebook.com
20	0.028348658	[redacted]	[redacted]	DNS	148	Standard query response 0x2975 A connect.facebook.net CNAME scontent.xx.fbcdn.net A 163.70.144.20
21	0.045953166	[redacted]	[redacted]	TLSv1.2	325	Application Data
22	0.046850077	[redacted]	[redacted]	TCP	74	443 → 43148 [ACK] Seq=1 Ack=252 Win=65535 Len=0
23	0.052230996	[redacted]	[redacted]	DNS	160	Standard query response 0xa474 AAAA connect.facebook.net CNAME scontent.xx.fbcdn.net AAAA 2a03:2880:f076:101:face:b00c:0:3
24	0.053222486	[redacted]	[redacted]	TCP	78	443 → 50058 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
25	0.053222777	[redacted]	[redacted]	TCP	78	443 → 41956 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440
26	0.053222814	[redacted]	[redacted]	DNS	141	Standard query response 0xd20b A www.facebook.com CNAME star-mini.c10r.facebook.com A 163.70.144.35
27	0.053222851	[redacted]	[redacted]	DNS	124	Standard query response 0xe4aa AAAA www.google.co.in AAAA 2404:6800:4009:802::2003
28	0.053222987	[redacted]	[redacted]	DNS	132	Standard query response 0xe669 AAAA www.googletagmanager.com AAAA 2404:6800:4009:81a::2008
29	0.053247510	[redacted]	[redacted]	TCP	74	50058 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0

```
▸ Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:56:00:00:00:03 (52:56:00:00:00:03)
▸ Internet Protocol Version 6, Src: fd17:625c:f037:2:7764:c770:8fe:6dc6, Dst: fd17:625c:f037:2::3
▸ User Datagram Protocol, Src Port: 34813, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  52 56 00 00 00 03 08 00  27 d1 f8 5d 86 dd 60 07   RV······'··]··`·
0010  03 0e 00 28 11 40 fd 17  62 5c f0 37 00 02 77 64   ···(·@··b\·7··wd
0020  c7 70 08 fe 6d c6 fd 17  62 5c f0 37 00 02 00 00   ·p··m···b\·7····
0030  00 00 00 00 00 03 87 fd  00 35 00 28 55 32 f0 6f   ·········5·(U2·o
0040  01 00 00 01 00 00 00 00  00 00 03 6d 64 61 06 73   ···········mda·s
0050  70 69 6e 6e 79 03 63 6f  6d 00 00 01 00 01         pinny·co m····
```

Some most common ports like as follow:-

- **135/tcp (msrpc - Microsoft Remote Procedure Call)**
  Port 135 is used in Windows environments for Microsoft RPC services. It allows programs on one computer to communicate and execute functions on another, mainly supporting remote management and services like Active Directory and Windows Management Instrumentation (WMI).
- **445/tcp (microsoft-ds)**
  This port is used for Microsoft Directory Services and Server Message Block (SMB). It handles file sharing, printer sharing, and network resource access primarily on Windows networks.

- **1521/tcp (oracle)**
  Port 1521 is the default port for Oracle Database listeners. It enables clients to connect to an Oracle database for querying and managing data.
- **2179/tcp (vmrdp)**
  This port is used by VMware Remote Desktop Protocol, allowing remote access to virtual machines hosted on VMware infrastructure.
- **3306/tcp (mysql)**
  Port 3306 is the default port for MySQL databases. It is used by client applications to connect and interact with MySQL database servers.
- **8080/tcp (http-proxy)**
  Port 8080 is commonly used as an alternative HTTP port, often for web proxies or web servers running HTTP services that do not use the default port 80.

These ports facilitate important services such as remote management, file sharing, database access, and web traffic handling in typical networked environments.

And this are the some potential security risk form this open ports :-

- **135/tcp (msrpc)**
  This port enables remote procedure calls on Windows but is often targeted for remote code execution or privilege escalation attacks if vulnerabilities exist. Attackers exploit it to control systems remotely.
- **445/tcp (microsoft-ds)**
  Used for file sharing in Windows, this port is highly vulnerable to exploits like EternalBlue, which was used in the massive WannaCry ransomware attack. It can allow attackers to spread malware or gain unauthorized access.
- **1521/tcp (oracle)**
  This port is the Oracle database listener, and if misconfigured or unpatched, attackers can exploit it to access or corrupt database information remotely.
- **2179/tcp (vmrdp)**
  VMware Remote Desktop Protocol port can be targeted for unauthorized remote access, allowing attackers to control virtual machines if weak authentication or vulnerabilities exist.
- **3306/tcp (mysql)**
  Default port for MySQL databases, often targeted for SQL injection, brute force attacks, or unauthorized data access, especially if default passwords or poor configurations are used.
- **8080/tcp (http-proxy)**
  Typically used by web proxies or alternative web servers, this port can be exploited via web-based attacks such as cross-site scripting, SQL injection, or denial of service if the web service is vulnerable.

Open ports increase the attack surface of a network and must be monitored, secured with firewalls, and regularly updated to close known vulnerabilities