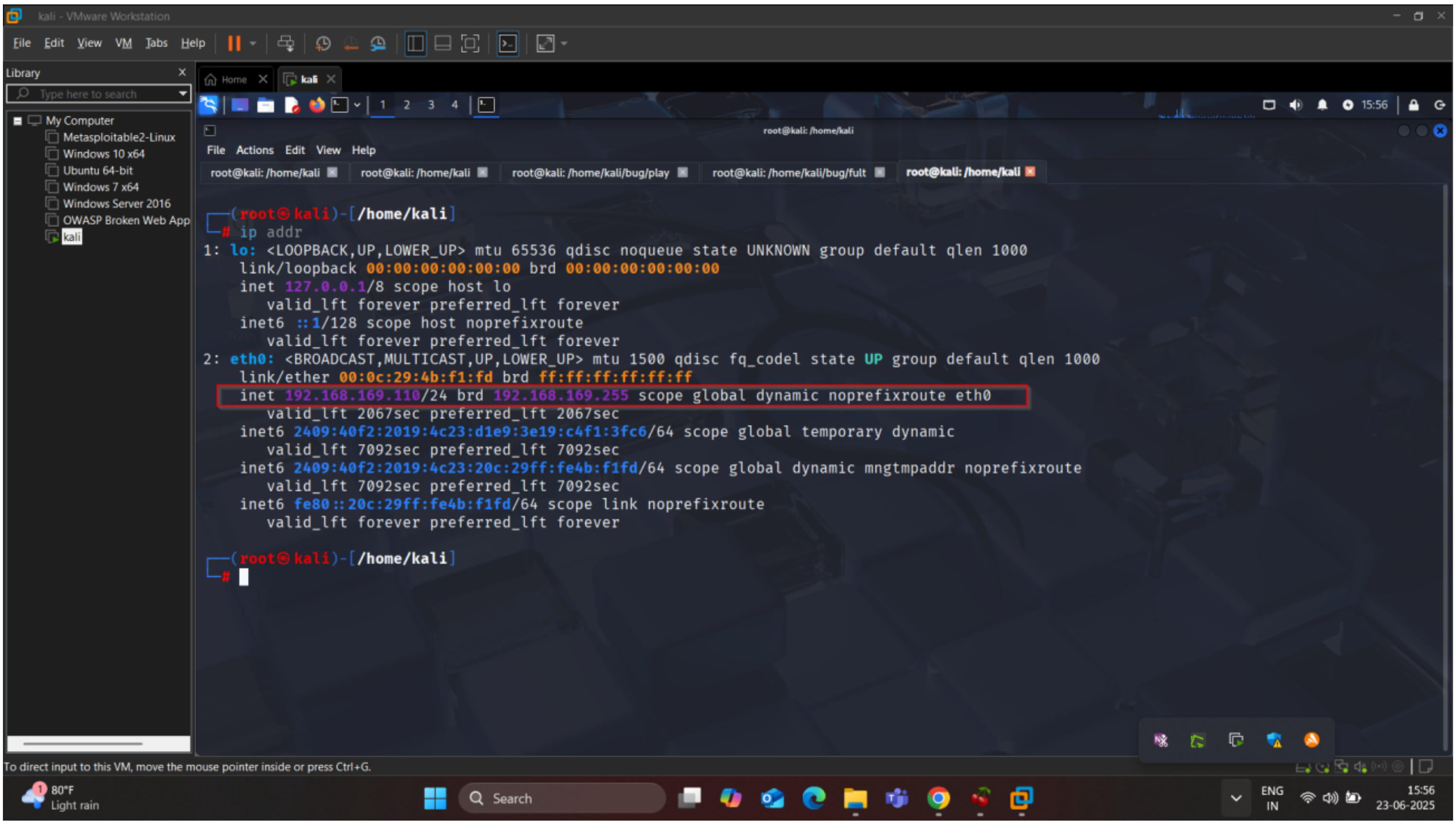
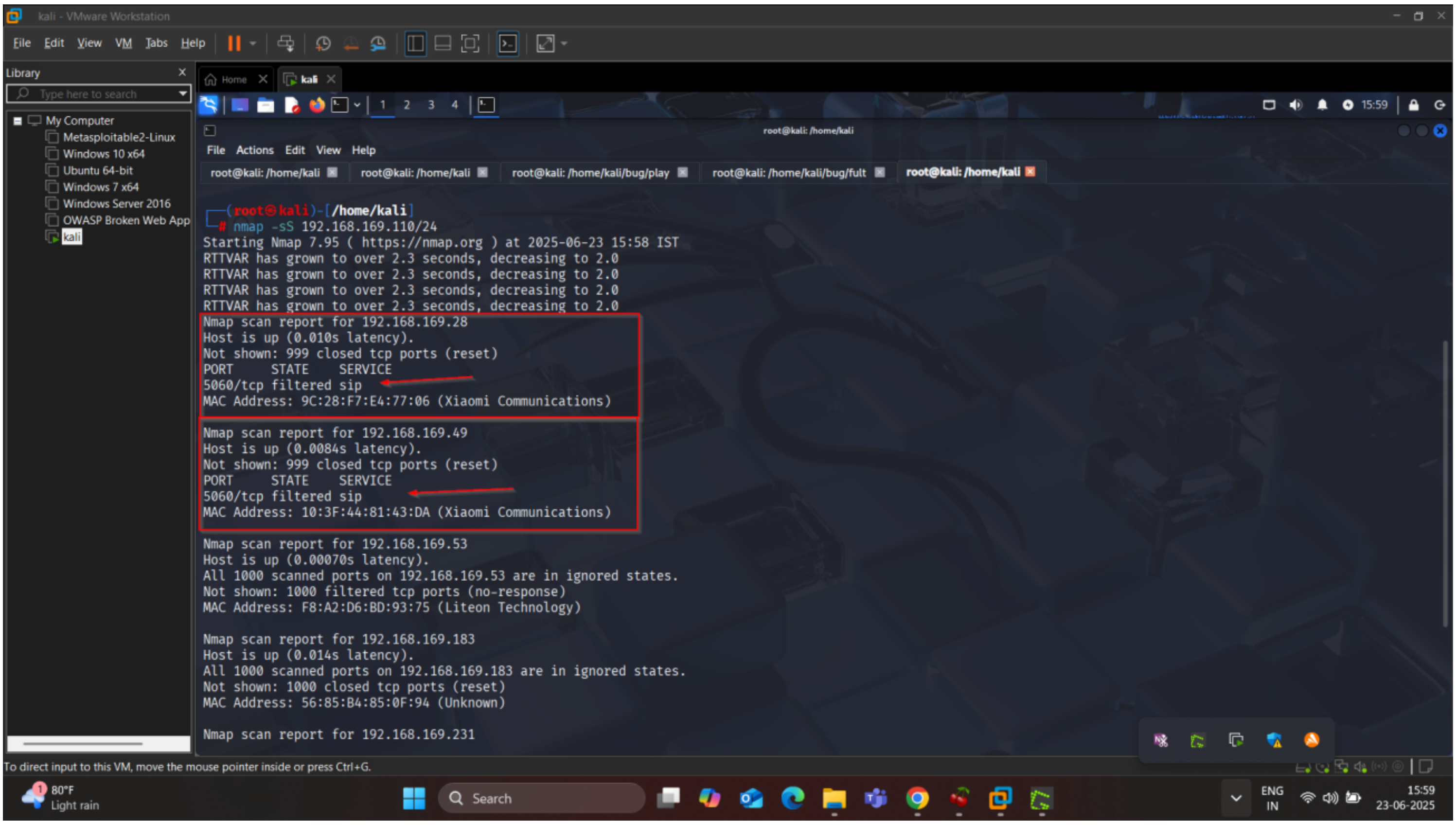
task1

ip addr to know my network range

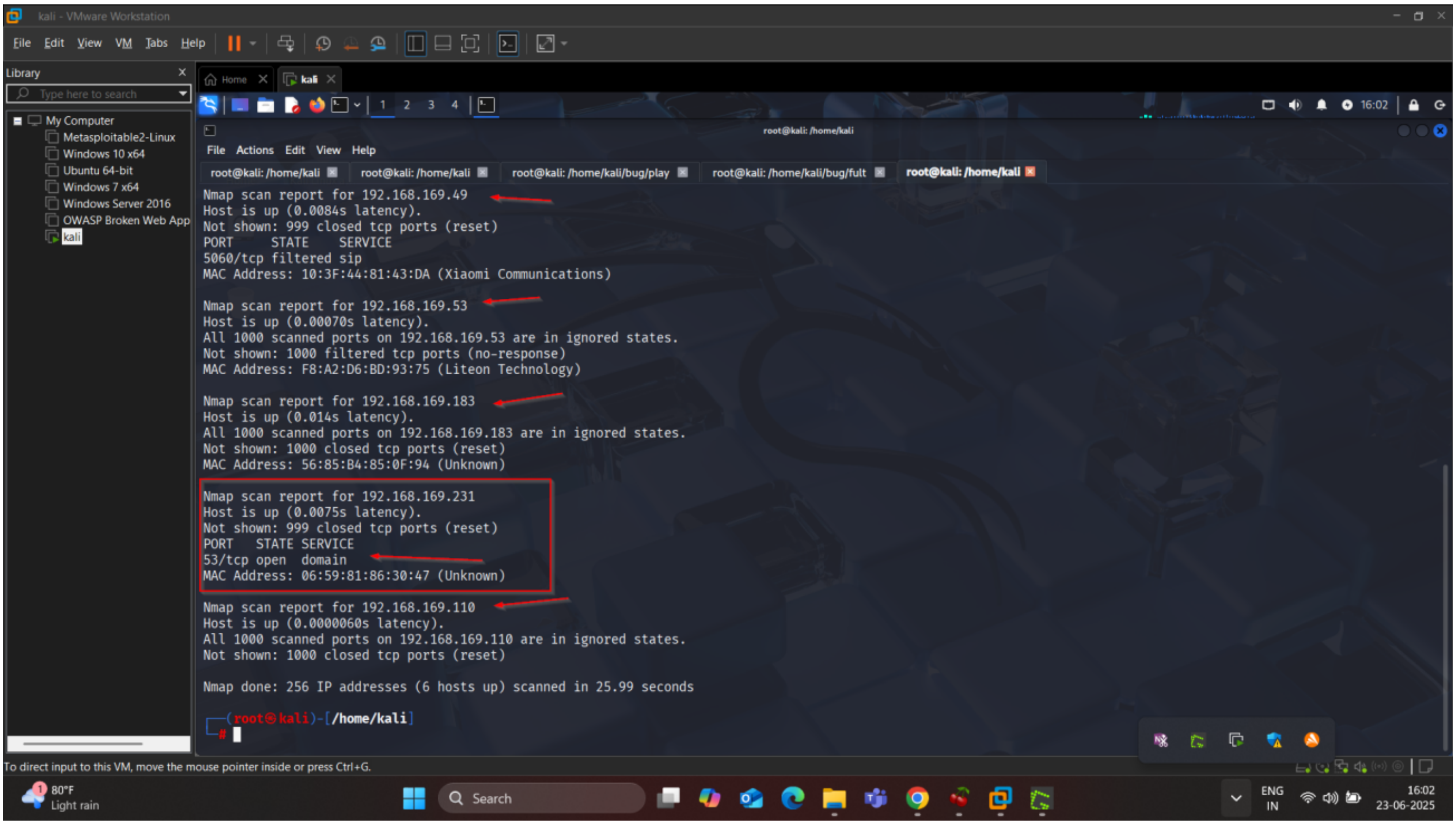


```
┌──(root㉿kali)-[/home/kali]
└─# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host 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:29:4b:f1:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.169.110/24 brd 192.168.169.255 scope global dynamic noprefixroute eth0
       valid_lft 2067sec preferred_lft 2067sec
    inet6 2409:40f2:2019:4c23:d1e9:3e19:c4f1:3fc6/64 scope global temporary dynamic
       valid_lft 7092sec preferred_lft 7092sec
    inet6 2409:40f2:2019:4c23:20c:29ff:fe4b:f1fd/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 7092sec preferred_lft 7092sec
    inet6 fe80::20c:29ff:fe4b:f1fd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali]
└─# 
```

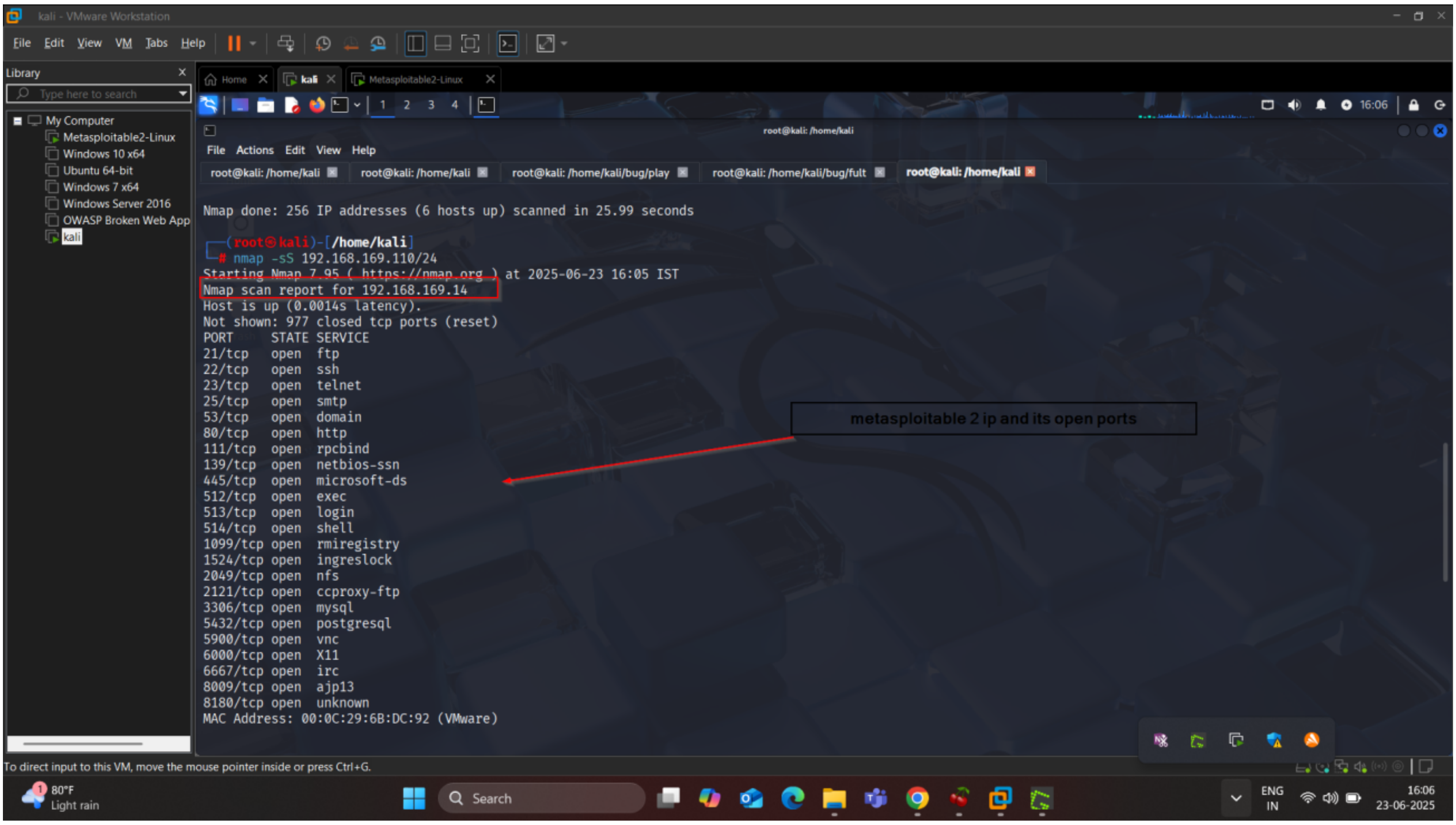
nmap scanned sub nets of system ip



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.169.110/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 15:58 IST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.169.28
Host is up (0.010s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: 9C:28:F7:E4:77:06 (Xiaomi Communications)

Nmap scan report for 192.168.169.49
Host is up (0.0084s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: 10:3F:44:81:43:DA (Xiaomi Communications)

Nmap scan report for 192.168.169.53
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.169.53 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:A2:D6:BD:93:75 (Liteon Technology)

Nmap scan report for 192.168.169.183
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.169.183 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 56:85:B4:85:0F:94 (Unknown)

Nmap scan report for 192.168.169.231
```



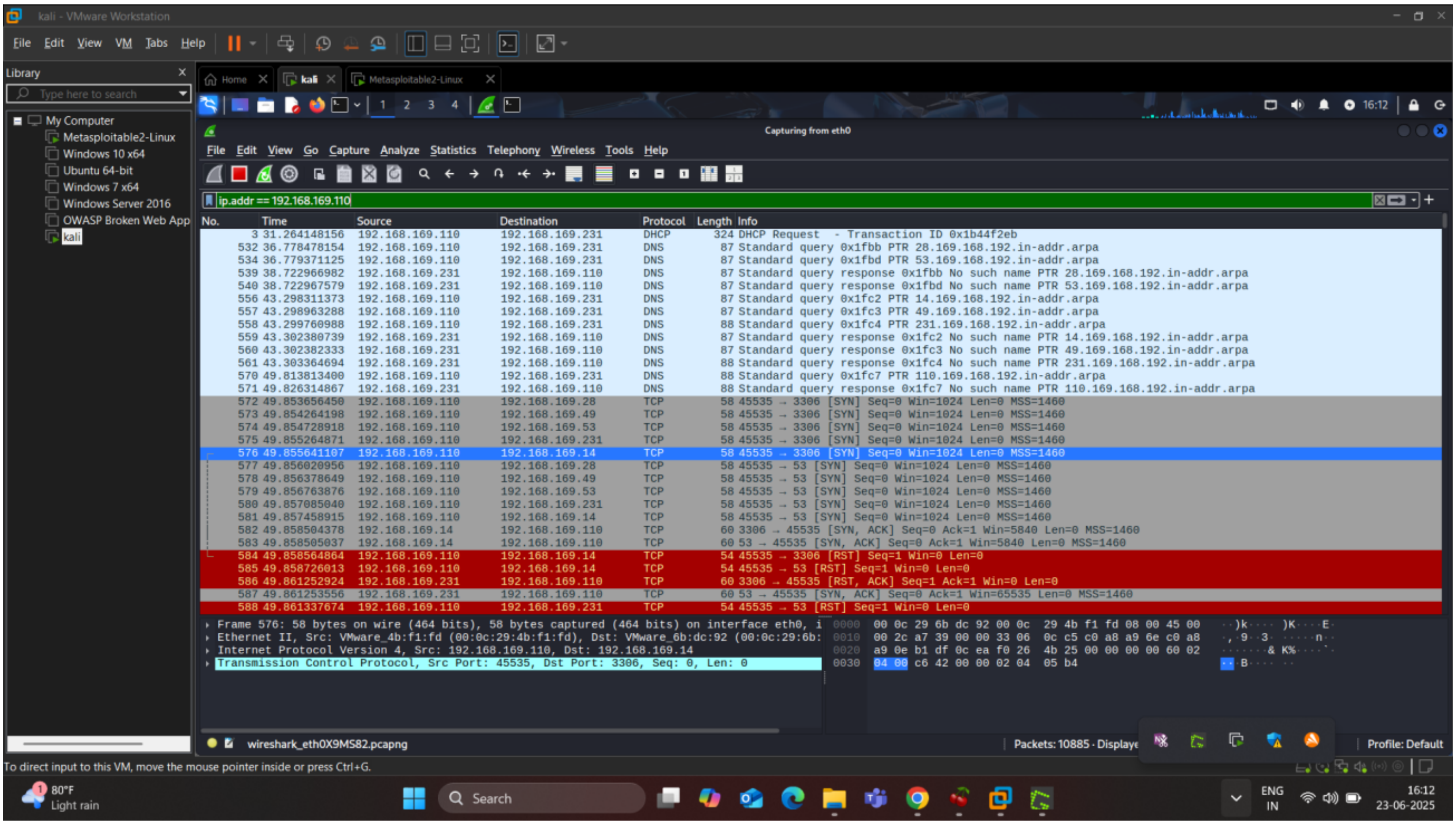
```
Nmap scan report for 192.168.169.49
Host is up (0.0084s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: 10:3F:44:81:43:DA (Xiaomi Communications)

Nmap scan report for 192.168.169.53
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.169.53 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:A2:D6:BD:93:75 (Liteon Technology)

Nmap scan report for 192.168.169.183
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.169.183 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 56:85:B4:85:0F:94 (Unknown)

Nmap scan report for 192.168.169.231
Host is up (0.0075s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 06:59:81:86:30:47 (Unknown)

Nmap scan report for 192.168.169.110
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.169.110 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 25.99 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```



```
Nmap done: 256 IP addresses (6 hosts up) scanned in 25.99 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.169.110/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 16:05 IST
Nmap scan report for 192.168.169.14
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:6B:DC:92 (VMware)
```

metasploitable 2 ip and its open ports

wireshark network packet capture



ip.addr == 192.168.169.110

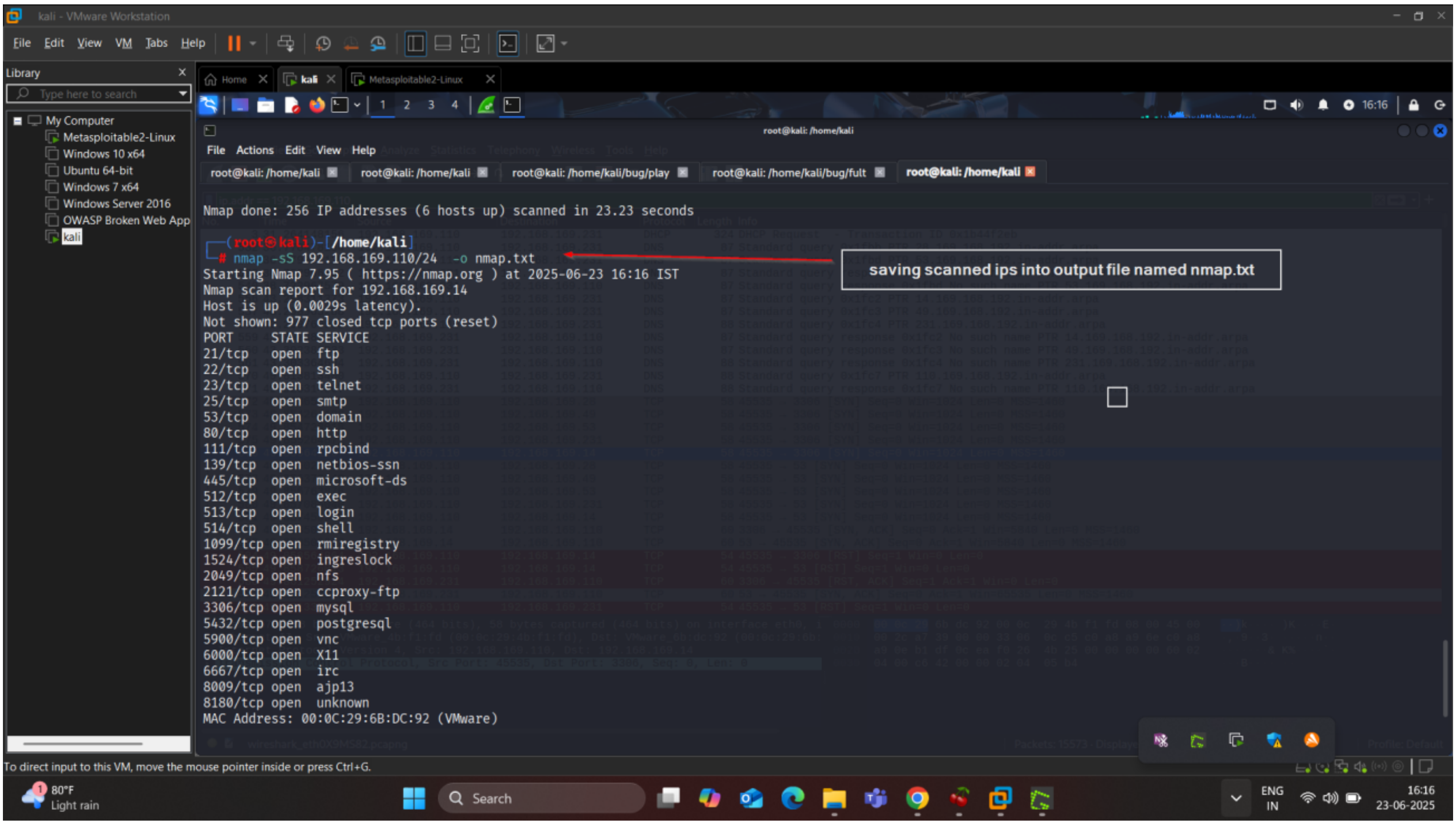
```
No.  Time           Source           Destination      Protocol Length Info
   3 31.264148156   192.168.169.110  192.168.169.231  DHCP     324 DHCP Request  - Transaction ID 0x1b44f2eb
 532 36.778478154   192.168.169.110  192.168.169.231  DNS       87 Standard query 0x1fbb PTR 28.169.168.192.in-addr.arpa
 534 36.779371125   192.168.169.110  192.168.169.231  DNS       87 Standard query 0x1fbd PTR 53.169.168.192.in-addr.arpa
 539 38.722966982   192.168.169.231  192.168.169.110  DNS       87 Standard query response 0x1fbb No such name PTR 28.169.168.192.in-addr.arpa
 540 38.722967579   192.168.169.231  192.168.169.110  DNS       87 Standard query response 0x1fbd No such name PTR 53.169.168.192.in-addr.arpa
 556 43.298311373   192.168.169.110  192.168.169.231  DNS       87 Standard query 0x1fc2 PTR 14.169.168.192.in-addr.arpa
 557 43.298963288   192.168.169.110  192.168.169.231  DNS       87 Standard query 0x1fc3 PTR 49.169.168.192.in-addr.arpa
 558 43.299760988   192.168.169.110  192.168.169.231  DNS       88 Standard query 0x1fc4 PTR 231.169.168.192.in-addr.arpa
 559 43.302380739   192.168.169.231  192.168.169.110  DNS       87 Standard query response 0x1fc2 No such name PTR 14.169.168.192.in-addr.arpa
 560 43.302382333   192.168.169.231  192.168.169.110  DNS       87 Standard query response 0x1fc3 No such name PTR 49.169.168.192.in-addr.arpa
 561 43.303364694   192.168.169.231  192.168.169.110  DNS       88 Standard query response 0x1fc4 No such name PTR 231.169.168.192.in-addr.arpa
 570 49.813813400   192.168.169.110  192.168.169.231  DNS       88 Standard query 0x1fc7 PTR 110.169.168.192.in-addr.arpa
 571 49.826314867   192.168.169.231  192.168.169.110  DNS       88 Standard query response 0x1fc7 No such name PTR 110.169.168.192.in-addr.arpa
 572 49.853656450   192.168.169.110  192.168.169.28   TCP       58 45535 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 573 49.854264198   192.168.169.110  192.168.169.49   TCP       58 45535 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 574 49.854728918   192.168.169.110  192.168.169.53   TCP       58 45535 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 575 49.855264871   192.168.169.110  192.168.169.231  TCP       58 45535 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 576 49.855641107   192.168.169.110  192.168.169.14   TCP       58 45535 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 577 49.856020956   192.168.169.110  192.168.169.28   TCP       58 45535 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 578 49.856378649   192.168.169.110  192.168.169.49   TCP       58 45535 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 579 49.856763876   192.168.169.110  192.168.169.53   TCP       58 45535 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 580 49.857085040   192.168.169.110  192.168.169.231  TCP       58 45535 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 581 49.857458915   192.168.169.110  192.168.169.14   TCP       58 45535 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 582 49.858504378   192.168.169.14   192.168.169.110  TCP       60 3306 → 45535 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 583 49.858505037   192.168.169.14   192.168.169.110  TCP       60 53 → 45535 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 584 49.858564864   192.168.169.110  192.168.169.14   TCP       54 45535 → 3306 [RST] Seq=1 Win=0 Len=0
 585 49.858726013   192.168.169.110  192.168.169.14   TCP       54 45535 → 53 [RST] Seq=1 Win=0 Len=0
 586 49.861252924   192.168.169.231  192.168.169.110  TCP       60 3306 → 45535 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 587 49.861253556   192.168.169.231  192.168.169.110  TCP       60 53 → 45535 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 588 49.861337674   192.168.169.110  192.168.169.231  TCP       54 45535 → 53 [RST] Seq=1 Win=0 Len=0
```

```
› Frame 576: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, i
› Ethernet II, Src: VMware_4b:f1:fd (00:0c:29:4b:f1:fd), Dst: VMware_6b:dc:92 (00:0c:29:6b:
› Internet Protocol Version 4, Src: 192.168.169.110, Dst: 192.168.169.14
› Transmission Control Protocol, Src Port: 45535, Dst Port: 3306, Seq: 0, Len: 0
```

```
0000  00 0c 29 6b dc 92 00 0c  29 4b f1 fd 08 00 45 00   ··)k····)K····E·
0010  00 2c a7 39 00 00 33 06  0c c5 c0 a8 a9 6e c0 a8   ·,·9··3······n··
0020  a9 0e b1 df 0c ea f0 26  4b 25 00 00 00 00 60 02   ·······&K%····`·
0030  04 00 c6 42 00 00 02 04  05 b4                     ···B······
```

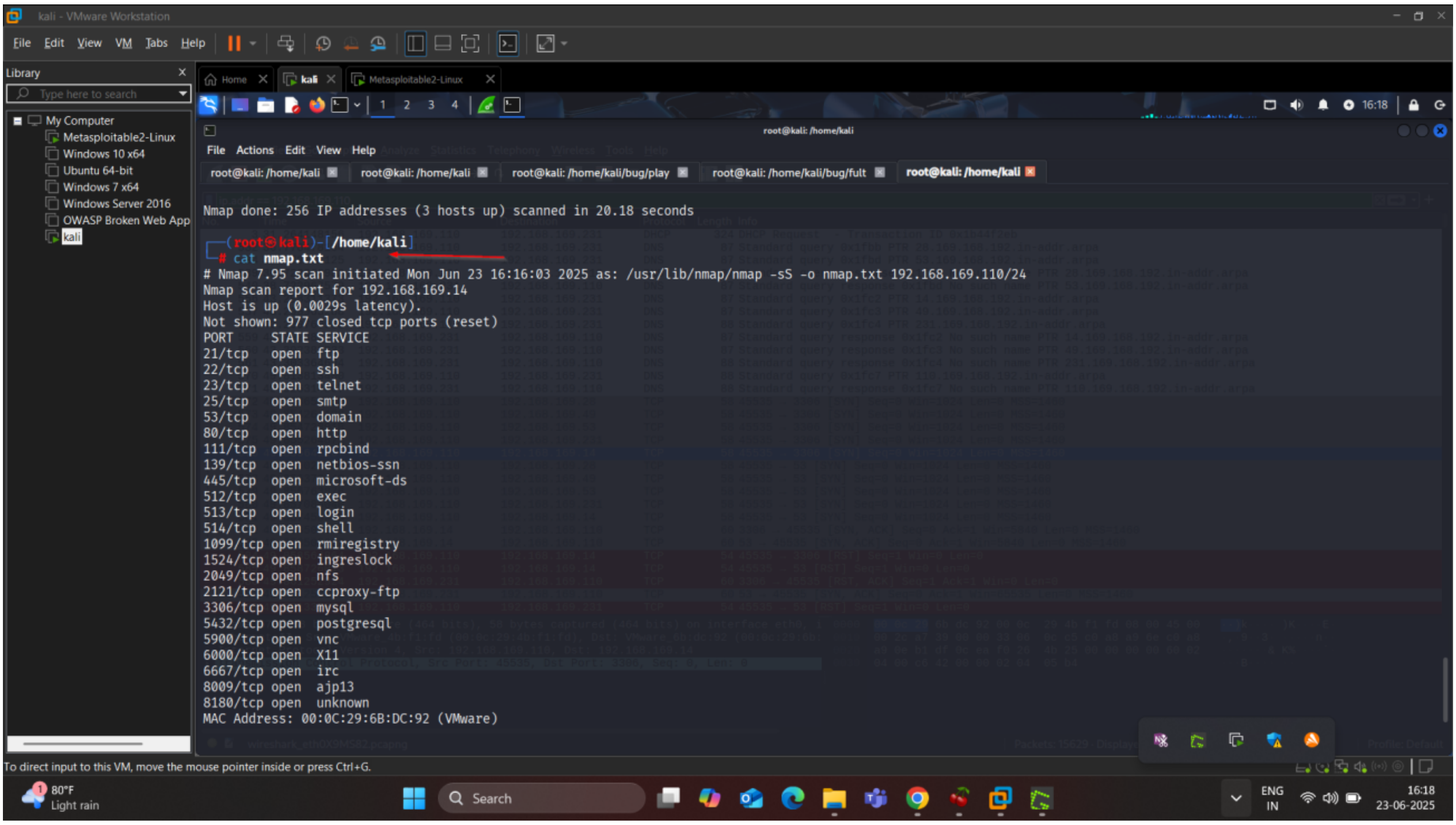
wireshark_eth0X9MS82.pcapng   Packets: 10885 · Displaye

kali - VMware Workstation
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
80°F Light rain
16:12 23-06-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Home
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/bug/play
root@kali: /home/kali/bug/fult
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
80°F
Light rain
Search
ENG
IN
16:16
23-06-2025

```
Nmap done: 256 IP addresses (6 hosts up) scanned in 23.23 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.169.110/24  -o nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 16:16 IST
Nmap scan report for 192.168.169.14
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:6B:DC:92 (VMware)
```

saving scanned ips into output file named nmap.txt


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Home
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/bug/play
root@kali: /home/kali/bug/fult
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
80°F
Light rain
Search
ENG
IN
16:18
23-06-2025

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 20.18 seconds

┌──(root㉿kali)-[/home/kali]
└─# cat nmap.txt
# Nmap 7.95 scan initiated Mon Jun 23 16:16:03 2025 as: /usr/lib/nmap/nmap -sS -o nmap.txt 192.168.169.110/24
Nmap scan report for 192.168.169.14
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:6B:DC:92 (VMware)
```

Port	Service	Potential Risks / Vulnerabilities
21/tcp	FTP	- Unencrypted credentials- Anonymous login- Vulnerable to brute force
22/tcp	SSH	- Weak passwords- Outdated versions (remote code execution)- Credential reuse
23/tcp	Telnet	- Plaintext login (very insecure)- Often replaced with SSH
25/tcp	SMTP	- Open relay (used for spam)- Command injection if misconfigured
53/tcp	DNS	- DNS amplification attacks- Zone transfer (info disclosure)

Port	Service	Potential Risks / Vulnerabilities
80/tcp	HTTP	- Web vulnerabilities (XSS, SQLi, LFI)- Banner leaks, outdated software
111/tcp	rpcbind	- Info leakage- Used with NFS — can lead to file exposure
139/tcp	NetBIOS	- Sensitive file shares- Null sessions- Info disclosure
445/tcp	SMB (Microsoft-DS)	- EternalBlue (MS17-010)- Unauthenticated file access- RCE vulnerabilities
512-514/tcp	r* services (exec, login, shell)	- Legacy, insecure- Trust-based auth (rhosts)- Often exploited in privilege escalation

Port	Service	Potential Risks / Vulnerabilities
1099/tcp	RMI Registry	- Remote code execution if exposed- Often exploited via Java deserialization
1524/tcp	Ingreslock	- Backdoor often left by attackers- Should not be open
2049/tcp	NFS	- File access over network- Misconfigurations can lead to full file system access
2121/tcp	ccproxy-ftp	- Same risks as FTP- May allow anonymous access
3306/tcp	MySQL	- SQL injection- Weak DB credentials- DB exposed over internet
5432/tcp	PostgreSQL	- Same as above — weak credentials or SQLi if accessible

Port	Service	Potential Risks / Vulnerabilities
5900/tcp	VNC	- Unencrypted screen sharing- Default/weak passwords- Exposed desktop sessions
6000/tcp	X11	- Input/output hijacking- Can read GUI keystrokes remotely
6667/tcp	IRC	- Botnet C2 channel- DDoS coordination- Sensitive chat leaks
8009/tcp	AJP13 (Apache JServ)	- GhostCat vulnerability (CVE-2020-1938)- File disclosure / RCE
8180/tcp	Unknown	- Often used for web admin panels (Tomcat, etc.)- Check for web apps or consoles