Network Mapping (NMAP)

List of Content:

1. ARP: ARP (Address Resolution Protocol) is a network protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) within a local network (LAN).

ARP Features:

Host wants to communicate with another device on the same network.

Checks ARP cache: If the MAC address of the target IP is already known, it uses it.

If not found, sends an ARP Request (Broadcast):

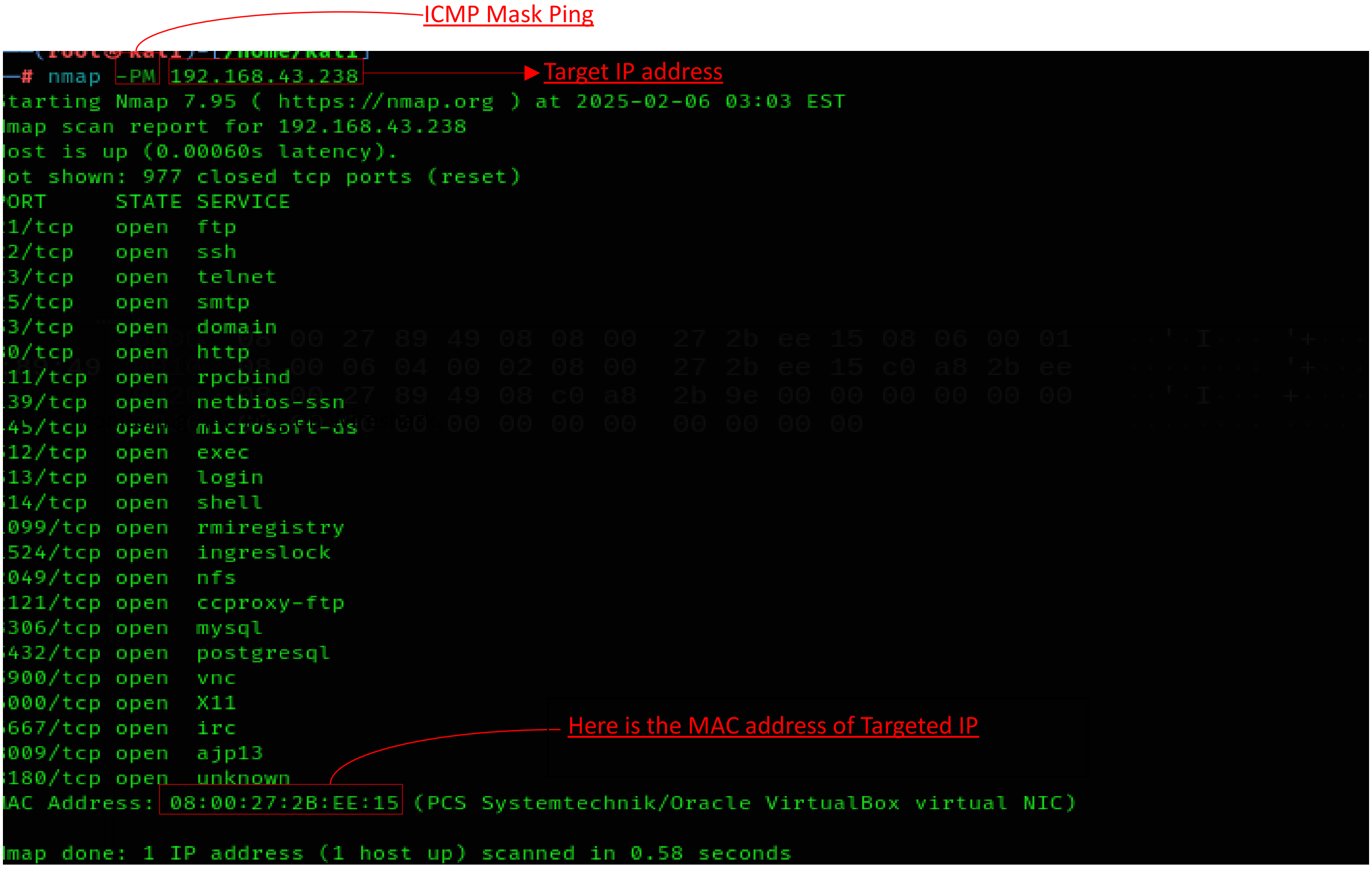
- The sender device asks, "Who has IP 192.168.1.1? Tell me your MAC address."

The target device responds with an ARP Reply (Unicast):

- The target replies, "I am 192.168.1.1, and my MAC address is AA:BB:CC:DD:EE:FF."

The sender updates its ARP table and sends the actual data.

- Performing ARP (Address Resolution Protocol) Ping on KALI.



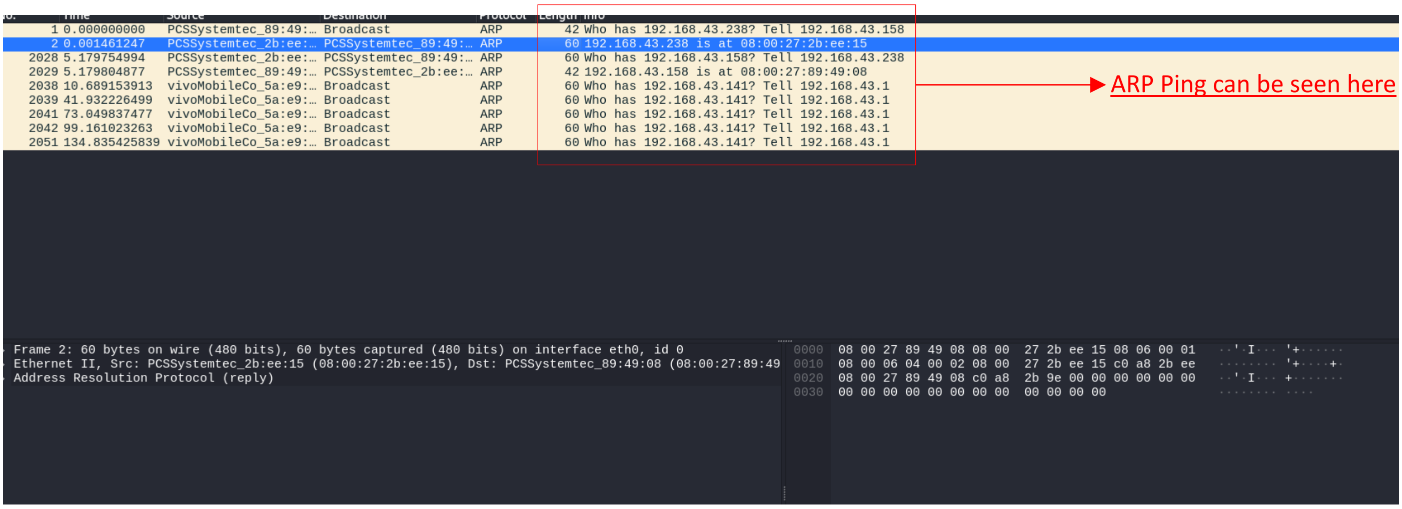
ICMP Mask Ping

Target IP address

```
──(root㉿kali)-[/home/kali]
─# nmap -PM 192.168.43.238
tarting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 03:03 EST
map scan report for 192.168.43.238
ost is up (0.00060s latency).
ot shown: 977 closed tcp ports (reset)
ORT     STATE SERVICE
1/tcp   open  ftp
2/tcp   open  ssh
3/tcp   open  telnet
5/tcp   open  smtp
3/tcp   open  domain
0/tcp   open  http
11/tcp  open  rpcbind
39/tcp  open  netbios-ssn
45/tcp  open  microsoft-ds
12/tcp  open  exec
13/tcp  open  login
14/tcp  open  shell
099/tcp open  rmiregistry
524/tcp open  ingreslock
049/tcp open  nfs
121/tcp open  ccproxy-ftp
306/tcp open  mysql
432/tcp open  postgresql
900/tcp open  vnc
000/tcp open  X11
667/tcp open  irc
009/tcp open  ajp13
180/tcp open  unknown
AC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 0.58 seconds
```

Here is the MAC address of Targeted IP



```
No.   Time            Source                 Destination            Protocol Length Info
    1 0.000000000     PCSSystemtec_89:49:… Broadcast              ARP      42 Who has 192.168.43.238? Tell 192.168.43.158
    2 0.001461247     PCSSystemtec_2b:ee:… PCSSystemtec_89:49:… ARP      60 192.168.43.238 is at 08:00:27:2b:ee:15
 2028 5.179754994     PCSSystemtec_2b:ee:… PCSSystemtec_89:49:… ARP      60 Who has 192.168.43.158? Tell 192.168.43.238
 2029 5.179804877     PCSSystemtec_89:49:… PCSSystemtec_2b:ee:… ARP      42 192.168.43.158 is at 08:00:27:89:49:08
 2038 10.689153913    vivoMobileCo_5a:e9:… Broadcast              ARP      60 Who has 192.168.43.141? Tell 192.168.43.1
 2039 41.932226499    vivoMobileCo_5a:e9:… Broadcast              ARP      60 Who has 192.168.43.141? Tell 192.168.43.1
 2041 73.049837477    vivoMobileCo_5a:e9:… Broadcast              ARP      60 Who has 192.168.43.141? Tell 192.168.43.1
 2042 99.161023263    vivoMobileCo_5a:e9:… Broadcast              ARP      60 Who has 192.168.43.141? Tell 192.168.43.1
 2051 134.835425839   vivoMobileCo_5a:e9:… Broadcast              ARP      60 Who has 192.168.43.141? Tell 192.168.43.1
```

ARP Ping can be seen here

```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_2b:ee:15 (08:00:27:2b:ee:15), Dst: PCSSystemtec_89:49:08 (08:00:27:89:49
Address Resolution Protocol (reply)
```

```
0000  08 00 27 89 49 08 08 00  27 2b ee 15 08 06 00 01   ··'·I···  '+······
0010  08 00 06 04 00 02 08 00  27 2b ee 15 c0 a8 2b ee   ········  '+····+·
0020  08 00 27 89 49 08 c0 a8  2b 9e 00 00 00 00 00 00   ··'·I···  +·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········  ····
```