Network Mapping (NMAP)

List of Content:

1. ARP Ping
2. ICMP Address Mask Ping
3. ICMP Echo Ping
4. ICMP Timestamp Ping
5. Ping Scan
6. TCP ACK Ping
7. TCP Scan Ping
8. UDP Ping

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):

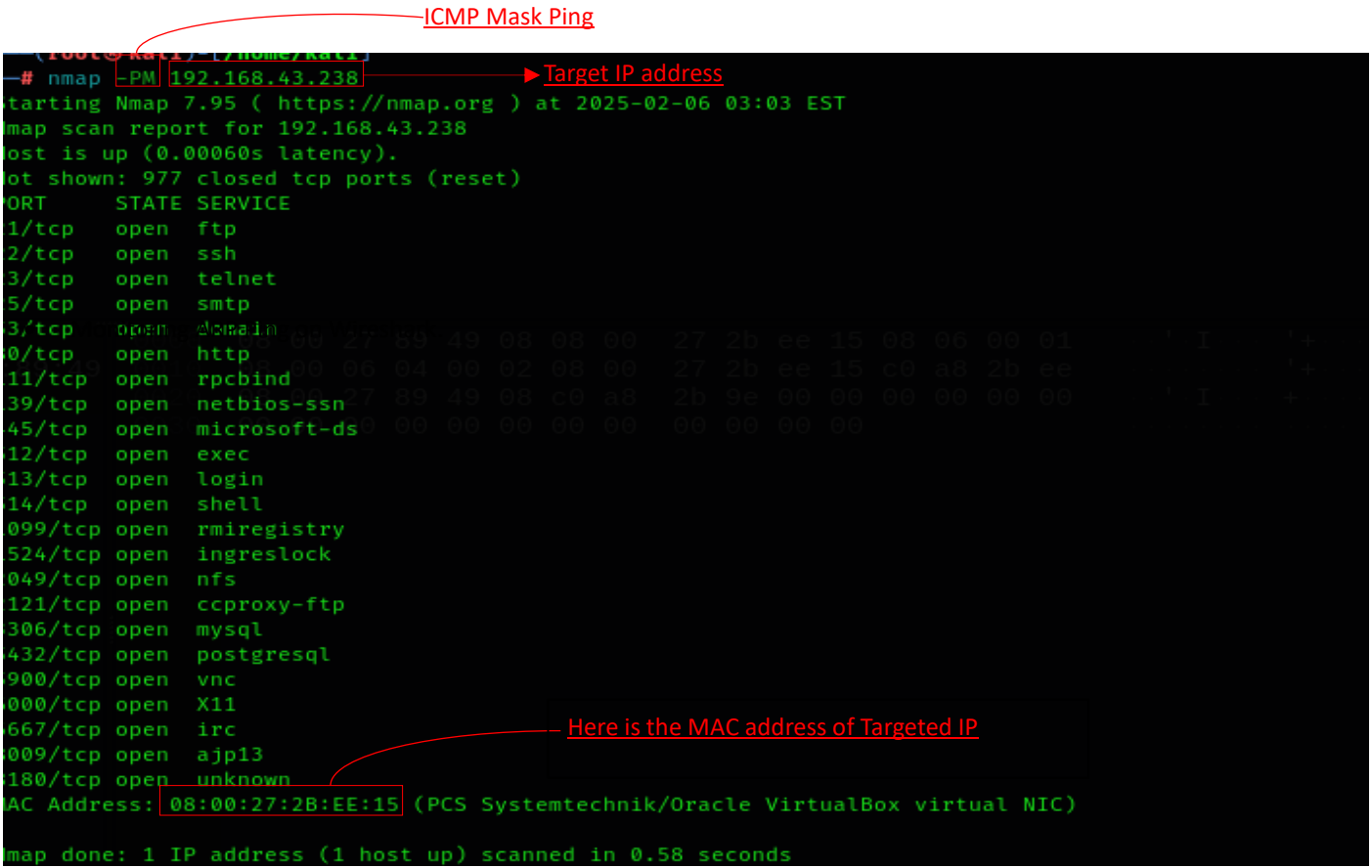
- The sender device asks, "Who has IP 192.168.43.238? Tell me your MAC address."

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

- The target replies, "I am 192.168.43.238, and my MAC address is 08:00:27:2B:EE:15."

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

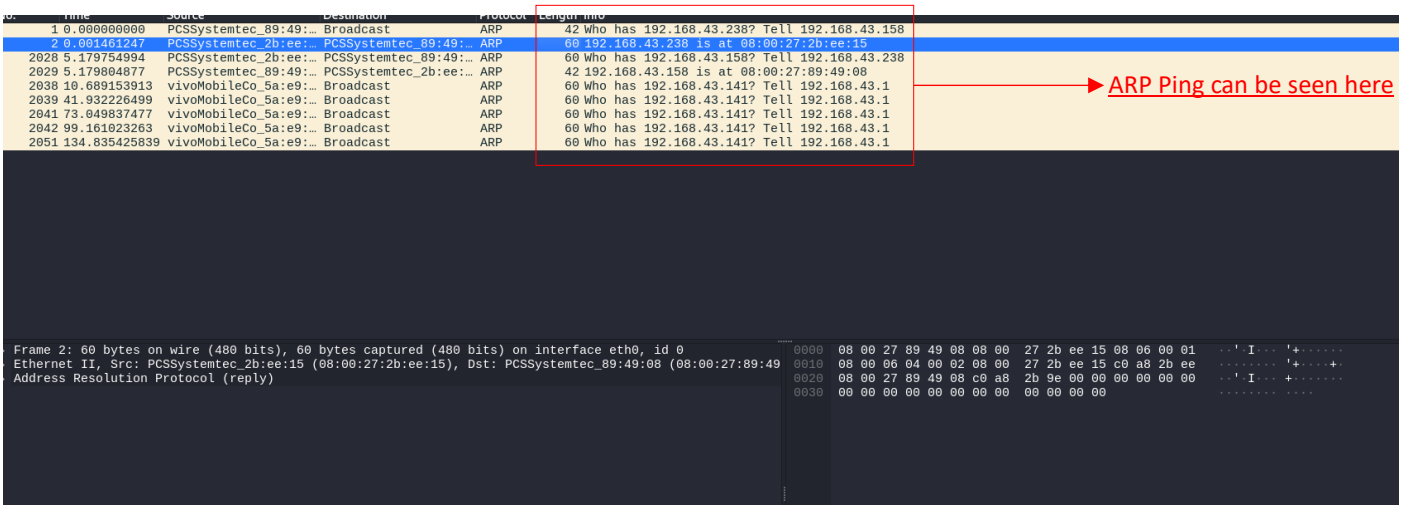
- Performing ARP (Address Resolution Protocol) Ping on KALI.



Nmap – This is the **Network Mapper** tool, used for network discovery and security auditing.

PM – It is used for ICMP Mask Ping.

192.168.43.238 – This is the **target IP address** in a private network.



2. ICMP Address Mask Ping:

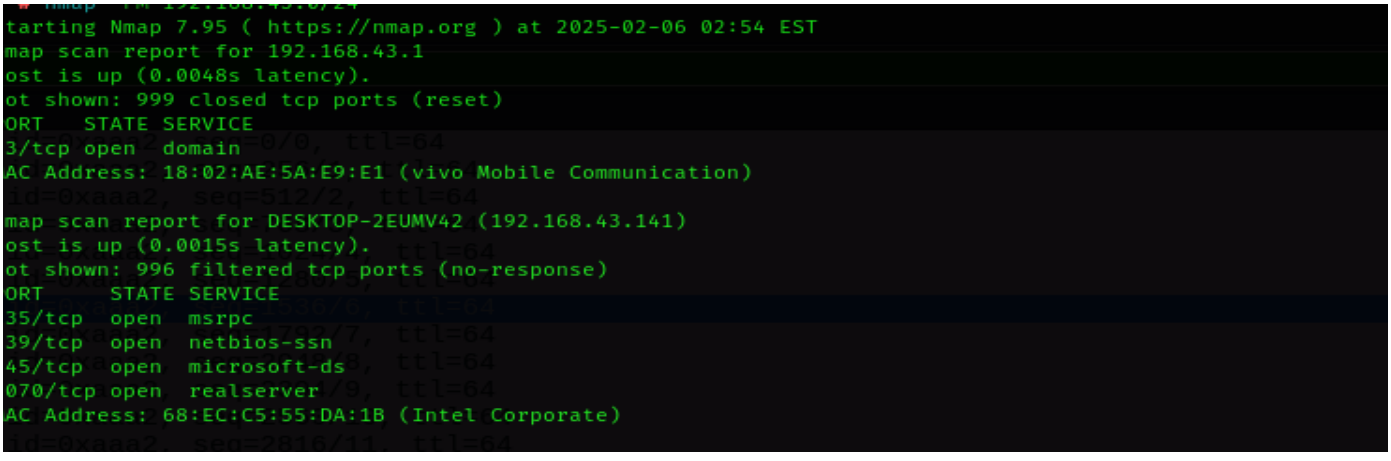
An ICMP Address Mask Request is used to query a host for its subnet mask. The expected response is an ICMP Address Mask Reply, which contains the subnet mask of the target device.

-PM:

The -PM option sends an ICMP Address Mask Request packet to the target.

It is used to request the subnet mask of the target device.

This type of ICMP request was mainly used in older network devices, but most modern systems ignore or block this request for security reasons.



```
map scan report for 192.168.43.238
ost is up (0.0018s 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 scan report for kali (192.168.43.158)
ost is up (0.000017s latency).
ll 1000 scanned ports on kali (192.168.43.158) are in ignored states.
ot shown: 1000 closed tcp ports (reset)

map done: 256 IP addresses (4 hosts up) scanned in 7.11 seconds
```