

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.

```
(root@kali: ~)
# nmap -PM 192.168.43.238
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 03:03 EST
Nmap scan report for 192.168.43.238
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
1/tcp     open  ftp
2/tcp     open  ssh
3/tcp     open  telnet
5/tcp     open  smtp
37/tcp    open  domain
80/tcp    open  http
11/tcp    open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
12/tcp    open  exec
13/tcp    open  login
14/tcp    open  shell
5999/tcp  open  rmiregistry
524/tcp   open  ingreslock
2049/tcp  open  nfs
121/tcp   open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

ICMP Mask Ping

Target IP address

Here is the MAC address of Targeted IP

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.

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	99.161923263	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 (08:00:27:89:49:08)
Address Resolution Protocol (reply)

0000 08 00 27 89 49 08 00 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 ... I ... + ...
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 00 00 00

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.

```
nmap -i 192.168.43.238
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:54 EST
map scan report for 192.168.43.1
Host is up (0.0048s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3/tcp     open  domain 0/0, ttl=64
AC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)
id=0xaaa2, seq=512/2, ttl=64
map scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
35/tcp    open  msrpc
39/tcp    open  netbios-ssn
45/tcp    open  microsoft-ds
070/tcp   open  realserver
AC Address: 68:EC:C5:55:DA:1B (Intel Corporate)
id=0xaaa2, seq=2816/11, ttl=64
```

```

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

```

ICMP Protocol					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=0/0, ttl=64
2	1.000002691	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=256/1, ttl=64
3	2.000552522	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=512/2, ttl=64
4	3.007334423	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=768/3, ttl=64
5	4.008304322	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1024/4, ttl=64
6	5.009808833	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1280/5, ttl=64
9	6.011269016	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1536/6, ttl=64
10	7.012421784	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1792/7, ttl=64
11	8.013022212	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2048/8, ttl=64
13	9.015959794	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2304/9, ttl=64
14	10.016222102	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2560/10, ttl=64
15	11.017106804	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2816/11, ttl=64
16	12.018044250	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=3072/12, ttl=64
17	13.019139010	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=3328/13, ttl=64
18	14.021554877	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=3584/14, ttl=64
19	15.022927241	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=3840/15, ttl=64
20	16.023857831	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=4096/16, ttl=64
21	17.025715433	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=4352/17, ttl=64
22	18.026613039	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=4608/18, ttl=64
23	19.027669565	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=4864/19, ttl=64
24	20.028261036	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=5120/20, ttl=64
25	21.029189021	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=5376/21, ttl=64
Frame 9: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface eth0, id 0 Ethernet II, Src: PCSSystemtec 89:40:08 (08:00:27:89:40:08), Dst: PCSSystemtec 2b:ee:15 (08:00:27:2b:ee:15) Internet Protocol Version 4, Src: 192.168.43.158, Dst: 192.168.43.238 Internet Control Message Protocol					
0000 08 00 27 2b ee 15 08 00 27 89 49 08 08 00 45 00 ...+...I...E 0010 08 29 04 e2 00 00 40 01 9d 1e c0 a8 2b 9e c0 a8 ...@...+... 0020 2b ee 11 00 3e 5d aa a2 06 00 00 00 00 00 00 ...+...>]					