

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 SYN 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).

Works:

Sending ARP Request:

- The ARP Ping tool sends an ARP request to a specific IP address.
 - This request asks: "Who has IP 192.168.1.104? Tell me your MAC address."

Receiving ARP Reply:

- If the target device is active, it replies with its MAC address.
 - If the target device is offline, there will be no response.

Command for ARP ping

```
nmap -PR 192.168.1.104
```

where, nmap denotes network mapping

PR denotes **ARP Ping** (Address Resolution Protocol) to check if the target is alive.

192.168.1.104 is the target ip address.

Example:

```
[root@kali: ~]
# nmap -PR 192.168.1.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 19:30 IST
Nmap scan report for 192.168.1.104
Host is up (0.00044s 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

Target ip address
Use for ARP ping
```

```

512/tcp open exec      192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
513/tcp open login     192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
514/tcp open shell     192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
1099/tcp open rmiregistry 192.168.1.102      192.168.0.1, Dst: 239.255.255.250
1524/tcp open ingreslock 192.168.1.102      51816, Dst Port: 1900
2049/tcp open nfs       192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
2121/tcp open ccproxy-ftp 192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
3306/tcp open mysql     192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
5432/tcp open postgresql 192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
5900/tcp open vnc       192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
6000/tcp open X11       192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
6667/tcp open irc       192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
8009/tcp open ajp13    192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
8180/tcp open unknown   192.168.1.102      224.0.0.22      IGMPv3      54 Membership Report / Join group
MAC Address: 08:00:27:DD:64:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds

```

Result:

No.	Time	Source	Destination	Protocol	Length	Info
21	5.187472934	PCSSystemtec_27:1b:.. Broadcast	ARP	42 Who has 192.168.1.104? Tell 192.168.1.102		
22	5.188349890	PCSSystemtec_27:1b:.. Broadcast	ARP	42 Who has 192.168.1.104? Tell 192.168.1.102		
25	5.338113933	PCSSystemtec_27:1b:.. Broadcast	ARP	42 Who has 192.168.1.104? Tell 192.168.1.102		
26	5.338785986	PCSSystemtec_dd:64:.. PCSSystemtec_27:1b:.. Broadcast	ARP	60 Who has 192.168.1.104 is at 08:00:27:dd:64:c3		
2657	10.333995511	PCSSystemtec_dd:64:.. PCSSystemtec_27:1b:.. Broadcast	ARP	60 Who has 192.168.1.102? Tell 192.168.1.104		
2058	10.334010727	PCSSystemtec_27:1b:.. PCSSystemtec_dd:64:.. Broadcast	ARP	42 192.168.1.102 is at 08:00:27:27:1b:c7		
2059	10.455701980	PCSSystemtec_27:1b:.. MercusysTech_95:c2:.. Broadcast	ARP	42 Who has 192.168.1.102? Tell 192.168.1.104		
2060	10.459487038	PCSSystemtec_95:c2:.. PCSSystemtec_27:1b:.. Broadcast	ARP	60 Who has 192.168.1.104? Tell 192.168.1.102		
2066	18.745760837	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2068	18.745760837	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2069	46.715869682	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2071	58.703559485	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2073	59.727493139	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2100	87.700525608	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2129	120.790733224	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2130	121.712763545	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2136	142.818551673	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2139	154.805568601	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2140	166.792849442	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		
2141	167.817427634	MercusysTech_95:c2:.. Broadcast	ARP	60 Who has 192.168.1.108? Tell 192.168.1.102		

Send and Receive information →

ARP Ping →

Hex Code ←

2. ICMP Address Mask Ping

ICMP (Internet Control Message Protocol) operates at Layer 3 (Network Layer) of the OSI model and is primarily used for network troubleshooting and communication.

ICMP Address Mask Ping (ICMP Type 17 & 18)

ICMP “Address Mask Request” (Type 17) asks a router for its subnet mask. If allowed, the router replies with “Address Mask Reply” (Type 18) containing the subnet mask.

How it Works?

1 Host sends an ICMP Type 17 request (Address Mask Request).

2 If the router allows it, it replies with ICMP Type 18 (Address Mask Reply) containing the subnet mask (e.g., 255.255.255.0).

Command in Linux:

nmap -PM 192.168.1.1

Where, nmap is network mapping.

-PM stands for ICMP Address Mask Ping.

Example:

```

root@Kali: /home/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
33/tcp     open  domain
40/tcp     open  http
111/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
2000/tcp   open  X11
667/tcp    open  irc
009/tcp    open  ajp13
180/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

```

Result:

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000000	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=0/0, ttl=64
2	0.000002691	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=250/1, ttl=64
3	0.000555522	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=532/2, ttl=64
4	3.00733423	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=768/3, ttl=64
5	4.00830432	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1024/4, ttl=64
6	5.009880832	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1280/5, ttl=64
9	6.01242178	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=1536/6, ttl=64
10	7.01242178	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	9.01559794	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2304/9, ttl=64
14	10.016222202	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2560/10, ttl=64
15	11.016222204	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=2816/11, ttl=64
16	12.018844250	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=3072/12, ttl=64
17	13.019339819	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	18.026613839	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=4608/18, ttl=64
23	19.027666665	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=4864/19, ttl=64
24	20.028261638	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=5120/20, ttl=64
25	21.028169821	192.168.43.158	192.168.43.238	ICMP	46 Address mask request id=0xaaa2, seq=5376/21, ttl=64

Frame 9: 0 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface eth0, id 0 0000: 08 00 27 2b ee 15 00 00 27 89 49 08 08 00 45 00 ...+... I E
 Ethernet II, Src: PCSSystemtec_09:49:08 (08:00:27:2b:ee:15), 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

3. ICMP Address Echo Ping:

Purpose: Checks if a device is online and measures response time.

How It Works:

1 Sender sends ICMP Echo Request (Type 8) to the target.

2 Target replies with ICMP Echo Reply (Type 0) if it's reachable.

3 Round-Trip Time (RTT) is measured for latency analysis.

Command in Kali Linux:

```
nmap -PE 192.168.43.0
```

Where, nmap is network mapping.

-PE stands for ICMP echo ping.

192.168.43.0 is a targeted ip address.

```
(root㉿kali)-[~/home/kali]
# nmap -PE 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:33 EST
Nmap scan report for 192.168.43.1
Host is up (0.0020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
2404/tcp  open  domain
53/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

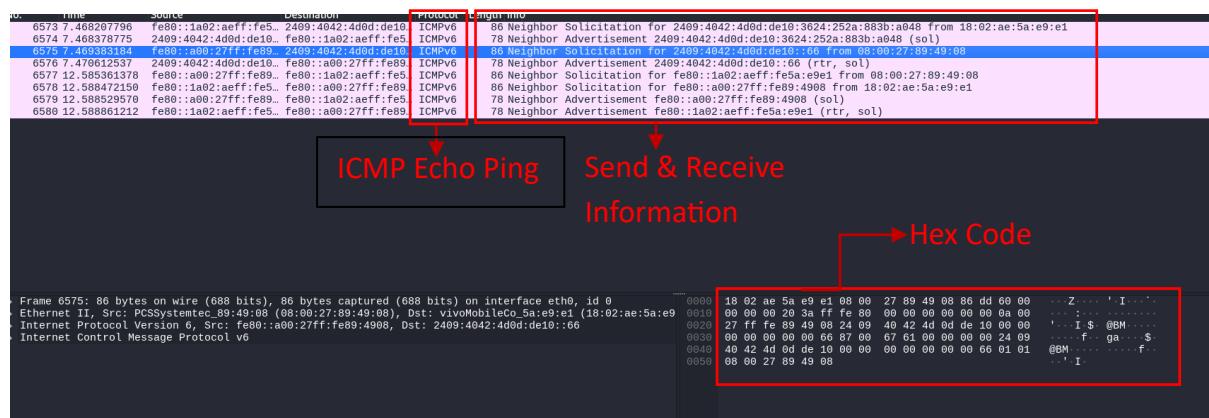
Nmap scan report for fe80::1a02:aeff:feba:e9e1
Host is up (0.00068s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0081s 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
5000/tcp  open  X11
5667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for kali (192.168.43.158)
Host is up (0.000022s latency).
All 1000 scanned ports on kali (192.168.43.158) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.03 seconds
          Packets: 6580 · Displayed: 8 (0.1%) · Dropped: 0
```

Result:



4. ICMP Timestamp Ping:

ICMP Timestamp Request (Type 13) asks a device for the current time. If allowed, the device responds with Type 14 (Timestamp Reply) containing the time in milliseconds since midnight UTC.

How it Works?

1 Host sends an ICMP Type 13 request (Timestamp Request).

2 If the target allows it, it replies with ICMP Type 14 (Timestamp Reply) containing the system timestamp.

Command in Kali Linux:

nmap -PP 192.168.43.0

where, nmap is network mapping.

-PP stands for Timestamp Ping.

192.168.43.0 is targeted ip address.

Example:

```
# nmap -PP 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:42 EST
Nmap scan report for 192.168.43.1
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE          TTL=64
3/tcp      open  domain          -> 192.168.43.16  TTL=64
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE          TTL=64
35/tcp    open  msrpc           192.168.43.19  TTL=64
39/tcp    open  netbios-ssn     20  TTL=64
45/tcp    open  microsoft-ds    20  TTL=64
070/tcp   open  realserver     /> 192.168.43.141  TTL=64
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          TTL=64
1/tcp      open  ftp             192.168.43.244  TTL=64
2/tcp      open  ssh             192.168.43.244  TTL=64
3/tcp      open  telnet          192.168.43.244  TTL=64
5/tcp      open  smtp            192.168.43.244  TTL=64
3/tcp      open  domain          192.168.43.244  TTL=64
0/tcp      open  http            192.168.43.244  TTL=64
11/tcp     open  rpcbind         192.168.43.244  TTL=64
39/tcp     open  netbios-ssn     192.168.43.244  TTL=64
45/tcp     open  microsoft-ds    192.168.43.244  TTL=64
12/tcp     open  exec            192.168.43.244  TTL=64
13/tcp     open  login           192.168.43.244  TTL=64
14/tcp     open  shell            192.168.43.244  TTL=64
099/tcp    open  rmiregistry     192.168.43.244  TTL=64
524/tcp    open  ingreslock      192.168.43.244  TTL=64
049/tcp    open  nfs              192.168.43.244  TTL=64
121/tcp    open  ccproxy-ftp     192.168.43.244  TTL=64
306/tcp    open  mysql            192.168.43.244  TTL=64
432/tcp    open  postgresql      192.168.43.244  TTL=64
900/tcp    open  vnc              192.168.43.244  TTL=64
000/tcp    open  X11              192.168.43.244  TTL=64
667/tcp    open  irc              192.168.43.244  TTL=64
009/tcp    open  ajp13           192.168.43.244  TTL=64
180/tcp    open  unknown          192.168.43.244  TTL=64
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for kali (192.168.43.158)
Host is up (0.000071s latency).
All 1000 scanned ports on kali (192.168.43.158) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Result:

No.	Time	Source	Destination	Protocol	Length Info	Raw Data
11.5	0.09678459	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=3849/15, ttl=64
12.5	0.12843348	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=3849/15, ttl=64
13.6	0.16983164	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4096/16, ttl=64
14.6	0.172732219	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=4096/16, ttl=64
15.7	0.1269057	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4347/17, ttl=64
16.8	0.14850556	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=4347/17, ttl=64
17.8	0.12439748	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4689/18, ttl=64
18.8	0.14177263	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=4689/18, ttl=64
19.9	0.14151838	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4864/19, ttl=64
20.9	0.15616426	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=4864/19, ttl=64
21.10	0.1453577	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5120/20, ttl=64
22.10	0.1453577	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=5120/20, ttl=64
23.11	0.15667193	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5376/21, ttl=64
24.11	0.17177427	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=5376/21, ttl=64
25.12	0.174933199	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5632/22, ttl=64
26.12	0.18955766	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=5632/22, ttl=64
27.13	0.18454948	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5888/23, ttl=64
28.13	0.18454948	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=5888/23, ttl=64
29.14	0.17765729	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=6144/24, ttl=64
30.14	0.23895977	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=6144/24, ttl=64
31.15	0.23955682	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=6409/25, ttl=64
32.15	0.252586316	192.168.43.238	192.168.43.158	ICMP	68	Timestamp reply id=0x5494, seq=6409/25, ttl=64

5. Perform a Ping Scan Only:

A ping scan is used to find live (online) hosts in a network without scanning ports.

Works:

1 Sends ICMP Echo Requests (Ping) to target hosts.

2 Waits for ICMP Echo Replies from active devices.

3 Lists only live hosts (ignores unresponsive ones).

Command in Kali Linux:

nmap -sP 192.168.43.0

where, nmap is network mapping.

-sP stands for Pin Scan.

192.168.43.0 is a targeted ip address.**Example:**

```
(root㉿kali)-[~/home/kali]
# nmap -sP 192.168.43.0/24 ➔ Target ip address
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:39 EST
Nmap scan report for 192.168.43.1
Host is up (0.0031s latency).
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)
Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0017s latency).
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)
Nmap scan report for 192.168.43.238
Host is up (0.0020s latency).
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.43.158)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.35 seconds
```

Result:

Send & Receive Information

Index	Source	Destination	Protocol	Length (bytes)	Info	Hex
i51	51, 275863988	192.168.43.1	MDNS	183	Standard query 0x0005 PTR _23337DE_sub_googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question	
i52	52, 225294312	vivoMobileCo.Sa:e9:1	Broadcast	ARP	60 Who has 192.168.43.158? Tell 192.168.43.1	
i53	52, 225294312	PCSystemec.89:49:08	vivoMobileCo.Sa:e9:1	ARP	42 192.168.43.158 is at 08:02:ae:5a:e9:08	
i54	52, 225293186	fe80::1a02:aeff:fef5:	ICMPv6	86 Neighbor Solicitation for 2409:4042:4d0d:de10:3624:252a:883b:a048 from 10:02:ae:5a:e9:08		
i55	55, 611019058	192.168.43.238	ARP	78 Router Advertisement 2409:4042:4d0d:de10:3624:252a:883b:a048 (sol)		
i56	56, 611019058	192.168.43.141	ICMPv6	243 Host Announcement DESKTOP-2EUMV42, Workstation, Server, NY Workstation		
i57	54, 609106667	192.168.43.238	ARP	239 Browser Election Request		
i58	56, 6099880025	192.168.43.238	ICMPv6	239 Browser Election Request		
i59	57, 267393819	fe80::a00:27ff:fe89:	ICMPv6	86 Neighbor Solicitation for fe80::1a02:aeff:fe91 from 08:00:27:89:49:08		
i60	59, 829117026	fe80::a00:27ff:fe89:	ICMPv6	78 Router Advertisement fe80::1a02:aeff:fe91 (rtr, sol)		
i61	59, 829117026	192.168.43.238	ARP	209 Browser Election Request		
i62	59, 829117026	vivoMobileCo.Sa:e9:1	Broadcast	60 Who has 192.168.43.141? Tell 192.168.43.1		
i63	66, 610466358	192.168.43.238	ARP	239 Browser Election Request		
i64	62, 310264297	fe80::1a02:aeff:fef5:	ICMPv6	86 Neighbor Solicitation for fe80::a00:27ff:fe89:4908 from 10:02:ae:5a:e9:08		
i65	62, 310264297	fe80::a00:27ff:fe89:	ICMPv6	78 Neighbor Advertisement fe80::a00:27ff:fe89:4908 (sol)		
i66	62, 612915449	192.168.43.238	ICMPv6	209 Router Advertisement fe80::a00:27ff:fe89:4908 (sol)		
i67	62, 612915449	192.168.43.238	NBNS	110 Registration NB <01><02>- MSBROWSE <02><01>		
i68	64, 612413199	192.168.43.238	NBNS	110 Registration NB <01><02>- MSBROWSE <02><01>		
i69	64, 612789233	192.168.43.238	NBNS	110 Registration NB <01><02>- MSBROWSE <02><01>		
i70	66, 612915449	192.168.43.238	NBNS	110 Registration NB <01><02>- MSBROWSE <02><01>		
i71	66, 613098284	192.168.43.238	NBNS	110 Registration NB WORKGROUPC1id		
i72	68, 613469078	192.168.43.238	NBNS	110 Registration NB WORKGROUPC1id		

Frame 565: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
Ethernet II, Src: PCSystemec.89:49:08 (08:00:27:89:49:08), Dst: vivoMobileCo.Sa:e9:1 (10:02:ae:5a:e9:08)
Internet Protocol Version 6, Src: fe80::a00:27ff:fe89:4908, Dst: fe80::1a02:aeff:fe91
Internet Control Message Protocol v6
Frame 566: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
Ethernet II, Src: vivoMobileCo.Sa:e9:1 (10:02:ae:5a:e9:08), Dst: fe80::1a02:aeff:fe91 (10:02:ae:5a:e9:08)
Internet Protocol Version 6, Src: fe80::a00:27ff:fe89:4908, Dst: fe80::1a02:aeff:fe91
Internet Control Message Protocol v6

Hex Code

6. TCP ACK Ping:

TCP ACK Ping (-PA) is a technique used by Nmap to detect live hosts by sending TCP ACK packets instead of ICMP Echo Requests.

Works:

- Nmap sends a TCP ACK packet to the target.
- If the target is alive, it responds with TCP RST (Reset) (since no connection exists).
- If no response, the target is either offline or blocking packets.
- Bypasses ICMP filtering, useful when ICMP ping is blocked by firewalls.

Command in Kali Linux:

```
nmap -PA 192.168.43.0/24
```

Where, nmap is network mapping

-PA stands for TCP ACK Ping.

Here 192.168.43.0 is a target ip address.

Example:

```
(root㉿kali)-[~/home/kali]
# nmap -PA 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:58 EST
Nmap scan report for 192.168.43.1
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0022s 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
MAC Address: 00:0C:29:0D:00:00 (Unknown)

Packets: 6583 - Displayed: 2007 (30.5%) | Dropped: 0 (0.0%)
```

Result: **TCP ACK Ping**

Send & Receive Information

No.	Time	Source	Destination	Protocol	Length Info	Hex Code
680 2.609967929	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 13 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
680 2.609968194	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 111 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 28 e4 38 40 08 00 7e a7 c0 a8 2b 01 c0 a8 (80 0 - - +
617 2.613890447	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 8888 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
621 2.613890499	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 88 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1466	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
621 2.613890502	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 89 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1466	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
621 2.628965872	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 143 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
621 2.628965875	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 14 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
621 2.628966253	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 53 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1466	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
620 2.628966580	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 8888 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
627 2.628966916	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 88 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
620 2.628967276	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 89 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
620 2.628967279	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 14 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
630 2.629367936	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 53 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=58535 Len=0 MSS=1466	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
649 2.623472786	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 110 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
650 2.623473451	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 110 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
651 2.623473926	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 995 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
651 2.623474527	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 995 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
651 2.623474590	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 995 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
651 2.623474912	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 25 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1466	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
655 2.623475270	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 8888 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
655 2.623475596	192.168.43.238	192.168.43.158	192.168.43.158	TCP	68 21 - 44683 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1466	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
659 2.624962252	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 8888 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E
660 2.624755672	192.168.43.1	192.168.43.158	192.168.43.158	TCP	68 21 - 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	08 00 27 69 08 18 02 0e 5a e9 e1 08 00 45 00 ... I .. Z .. E

Frame 651: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, link layer type Ethernet II (ethernet), source vivoMobileCo_5a:e9:e1 (18:02:a5:e9:e1), destination PCSSystemec_89:49:08 (08:00:27:89:49:08)

Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.158

Transmission Control Protocol, Src Port: 995, Dst Port: 44683, Seq: 1, Ack: 1, Len: 0

7. TCP SYN Ping:

TCP SYN Ping (-PS) is a host discovery technique used by Nmap to check if a system is alive by sending TCP SYN packets instead of ICMP pings.

Works:

Works:

Sends a TCP SYN Packet: Nmap sends a SYN packet to a target port.

Receives a Response: SYN-ACK: Indicates the port is open and the host is alive.

RST (Reset): Indicates the port is closed, but the host is still up.

No Response: May mean the host is down or blocking the probe.

Command I Kali Linux:

nmap -PS 192.168.43.0

Where, nmap is network mapping.

-PS stands for TCP ACK Ping.

Here 192.168.43.0 is a target ip address.

Example:

```
(root㉿kali)-[~/home/kali]
# nmap -PS 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:48 EST
Nmap scan report for 192.168.43.1
Host is up (0.0025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0010s latency).
Not shown: 996 filtered tcp ports (no-response)
```

```

PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0018s 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

```

Packets: 6620 · Dropped: 0 (0.0%)

Result:

4377 2.579761934	192.168.43.238	192.168.43.158	TCP	68 1059 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4378 2.579762044	192.168.43.238	192.168.43.158	TCP	68 2065 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4379 2.579762156	192.168.43.238	192.168.43.158	TCP	68 5919 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4380 2.579921386	192.168.43.238	192.168.43.158	TCP	68 1318 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4381 2.579921587	192.168.43.238	192.168.43.158	TCP	68 7025 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4382 2.5808158269	192.168.43.1	192.168.43.158	TCP	68 7200 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4383 2.5808158544	192.168.43.1	192.168.43.158	TCP	68 6025 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4384 2.5888356439	192.168.43.1	192.168.43.158	TCP	68 1098 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4385 2.5888356440	192.168.43.1	192.168.43.158	TCP	68 4000 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4386 2.5889852937	192.168.43.1	192.168.43.158	TCP	68 2665 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4387 2.588953481	192.168.43.1	192.168.43.158	TCP	68 5919 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
4388 2.581102835	192.168.43.158	192.168.43.238	TCP	58 49088 - 3827 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4389 2.581161833	192.168.43.158	192.168.43.1	TCP	58 49088 - 1310 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4390 2.581310315	192.168.43.158	192.168.43.238	TCP	58 49088 - 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4391 2.581310316	192.168.43.158	192.168.43.238	TCP	58 49088 - 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4392 2.5813103659	192.168.43.158	192.168.43.238	TCP	58 49088 - 42510 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4393 2.581564973	192.168.43.158	192.168.43.1	TCP	58 40000 - 3827 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4394 2.581585746	192.168.43.158	192.168.43.238	TCP	58 49088 - 687 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4395 2.581607751	192.168.43.158	192.168.43.1	TCP	58 49088 - 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4396 2.581781033	192.168.43.158	192.168.43.238	TCP	58 49088 - 3038 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4397 2.581857967	192.168.43.158	192.168.43.1	TCP	58 49088 - 42518 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
4398 2.5819371795	192.168.43.1	192.168.43.158	TCP	68 1319 - 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		

Send & Receive Information

TCP ACK Ping

Hex Code

8. UDP Ping:

UDP Ping is a network scanning technique used to determine if a host is online by sending UDP packets to a target port.

Works:

Sends a UDP Packet: A UDP packet is sent to a specific port on the target host.

Response Received: ICMP "Port Unreachable" reply indicates the host is up if the port is closed.

No Response: Could mean the port is open/filtered or the host is down.

Command in Kali Linux:

Nmap -PU 192.168.43.0

Where, nmap is network mapping

-PU stand for UDP Ping.

192.168.43.0 is a target ip address.

Example:

```
root@kali: /home/kali$ # nmap -PU 192.168.43.0/24
starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:08 EST
nmap scan report for 192.168.43.1
host is up (0.0013s latency).
not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1070/tcp  open  realserver
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication) DESKTOP-2EUMV42
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

nmap scan report for 192.168.43.238
host is up (0.00074s 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
23/tcp    open  domain
20/tcp    open  http
21/tcp    open  rpcbind
39/tcp    open  netbios-ssn
445/tcp   open  microsoft-ds
12/tcp    open  exec
13/tcp    open  login
14/tcp    open  shell
2099/tcp  open  rmiregistry
524/tcp   open  ingreslock
1049/tcp  open  nfs
121/tcp   open  cccproxy-ftp
306/tcp   open  mysql
432/tcp   open  postgresql
1900/tcp  open  vnc
1000/tcp  open  X11
667/tcp   open  irc
1009/tcp  open  ajp13
1180/tcp  open  unknown
MAC Address: 08:00:27:2B:EE:15 PCS Systemtechnik/Oracle VirtualBox virtual NIC

nmap scan report for kali (192.168.43.158)
host is up (0.000015s latency).
all 1000 scanned ports on kali (192.168.43.158) are in ignored states.
not shown: 1000 closed tcp ports (reset)
```

► Target ip address
► UDP Ping

Result:

No.	Time	Source	Destination	Protocol	Length	Info
519	1.912418813	2409:4042:4d0d:de10...	2409:4042:4d0d:de10...	DNS	105	Standard query 0xd631 PTR 1.43.168.192.in-addr.arpa
520	1.913945993	192.168.43.158	192.168.43.158	DNS	87	Standard query 0xd631 PTR 143.168.192.in-addr.arpa
521	1.92237224	2409:4042:4d0d:de10...	2409:4042:4d0d:de10...	DNS	107	Standard query 0xd633 PTR 158.43.168.192.in-addr.arpa
522	1.922370922	2409:4042:4d0d:de10...	2409:4042:4d0d:de10...	DNS	105	Standard query 0xd631 PTR 143.168.192.in-addr.arpa
523	1.922372227	192.168.43.1	192.168.43.158	DNS	116	Standard query response 0xd632 PTR 143.168.192.in-addr.arpa PTR DESKTOP-2EUMV42
524	1.922372784	2409:4042:4d0d:de10...	2409:4042:4d0d:de10...	DNS	107	Standard query response 0xd633 No such name 238.43.168.192.in-addr.arpa
525	1.930842237	2409:4042:4d0d:de10...	2409:4042:4d0d:de10...	DNS	107	Standard query 0xd634 PTR 158.43.168.192.in-addr.arpa
526	1.941949729	2409:4042:4d0d:de10...	2409:4042:4d0d:de10...	DNS	123	Standard query response 0xd634 PTR 143.168.192.in-addr.arpa PTR kali



UDP Ping



Send & Receive
Information

Hex Code

```

Frame 526: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface eth0, id 0
Ethernet II, Src: vivoMobileCo_5a:e9:e1 (18:02:ae:5a:e9:e1), Dst: PCSSysteme_89:49:08 (08:00:27:89:49)
User Datagram Protocol, Src Port: 53, Dst Port: 53727
Domain Name System (response)

0000 08 00 27 89 49 08 18 02 ae 5a e9 e1 86 dd 00 0d ..I...Z...
0010 2d 00 00 47 11 49 24 09 40 42 4d 0d de 10 00 00 ..G@...BM...
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..F@...ES...
0030 25 2a 88 3b a9 48 00 35 83 bf 00 47 fe f3 d6 34 %*;...G...4
0040 85 00 00 01 00 01 00 00 00 00 03 31 35 38 02 34 .....;....158.4
0050 33 03 31 36 38 03 31 39 32 07 69 6e 2d 61 64 64 3 168 19 2 in-add
0060 72 04 61 72 70 61 00 00 0c 00 01 c0 0c 00 0c 00 r-arp...
0070 01 00 00 00 00 00 00 04 6b 61 6c 69 00 .....kali.

```