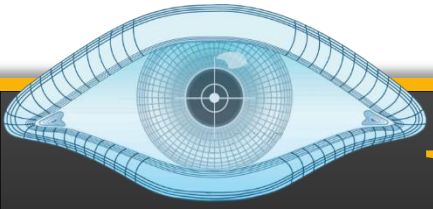


Nmap for Pentester

Host Discovery

Table of Contents

Table of Contents 2
Abstract 3
Ping Sweep 4
Disable-arp-ping 6
Send-ip 8
TCP Flags 8
Types of Scans 9
TCP SYN Ping Scan 10
TCP ACK Ping Scan 11
ICMP Echo Ping Scan 12
ICMP Echo Ping Sweep 13
ICMP Address Mask Scan 14
ICMP ECHO Timestamp Scan 14
UDP Ping Scan 15
IP Protocol Ping Scan 17
No Ping Scan 18
ARP Ping Scan 18
SCTP INIT Ping 20
Traceroute 20
Conclusion 21
References 21

Abstract

Nmap has become one of the most popular tools in network scanning by leaving other scanners behind. Many times, the hosts in some organisations are secured using firewalls or intrusion prevention systems which result in the failure of scanning due to the present set of rules which are used to block network traffic.

In Nmap, a pentester can easily make use of alternate host discovery techniques to prevent this from happening. It consists of certain features that make the network traffic a little less suspicious. Hence, in this report, various techniques of Host Discovery will be explored.

Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.

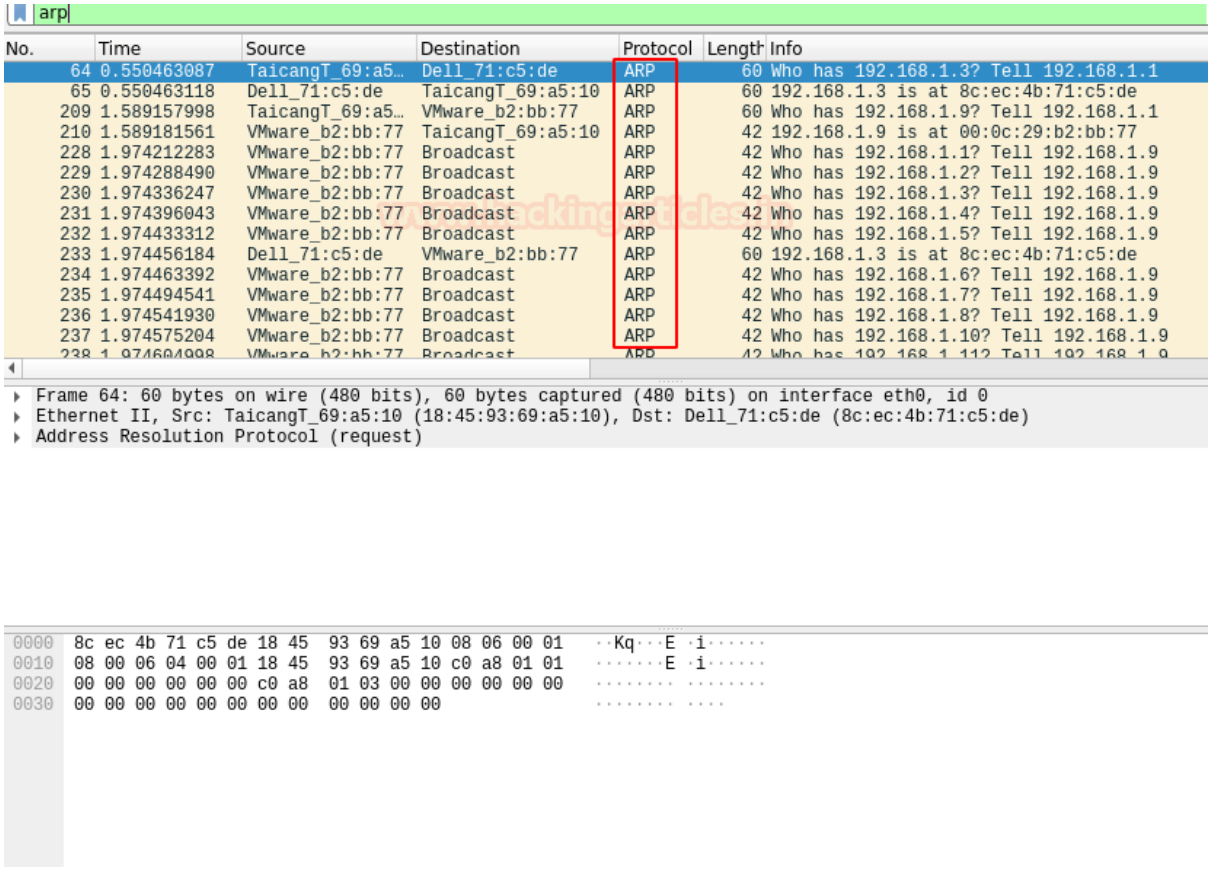
Ping Sweep

Let's begin with scanning the entire network by using the Ping sweep scan (-sP).

```
nmap -sP 192.168.1.0/24
```

```
root@kali:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:43 EST
Nmap scan report for dsldevice.lan (192.168.1.1)
Host is up (0.0012s latency).
MAC Address: 18:45:93:69:A5:10 (Taicang T&W Electronics)
Nmap scan report for 192.168.1.3
Host is up (0.00030s latency).
MAC Address: 8C:EC:4B:71:C5:DE (Dell)
Nmap scan report for 192.168.1.4
Host is up (0.024s latency).
MAC Address: 2A:84:98:9F:E5:5E (Unknown)
Nmap scan report for 192.168.1.5
Host is up (0.012s latency).
MAC Address: 30:24:32:1F:89:AC (Intel Corporate)
Nmap scan report for 192.168.1.8
Host is up (0.0058s latency).
MAC Address: 44:CB:8B:C2:20:DA (LG Innotek)
Nmap scan report for 192.168.1.12
Host is up (0.00027s latency).
MAC Address: 00:0C:29:78:20:90 (VMware)
Nmap scan report for 192.168.1.108
Host is up (0.00017s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap scan report for 192.168.1.9
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 23.67 seconds
root@kali:~#
```

When you closely observe the packets in the Wireshark, you see that here only ARP packets are being sent while scanning the network,



Note: Working of **–sP** and **–sn** is the same.

Let us try the same by using **the no port scanning (-sn)** option. In this option, we are also **using –packet-trace** option which will enable you to see the detailed packet transfer without making use of Wireshark. Here you can observe the ARP packets being received.

```
nmap -sn 192.168.1.0/24 --packet-trace
```

```
root@kali:~# nmap -sn 192.168.1.0/24 --packet-trace
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:48 EST
SENT (0.0687s) ARP who-has 192.168.1.1 tell 192.168.1.9
SENT (0.0688s) ARP who-has 192.168.1.2 tell 192.168.1.9
SENT (0.0689s) ARP who-has 192.168.1.3 tell 192.168.1.9
SENT (0.0690s) ARP who-has 192.168.1.4 tell 192.168.1.9
SENT (0.0691s) ARP who-has 192.168.1.5 tell 192.168.1.9
SENT (0.0692s) ARP who-has 192.168.1.6 tell 192.168.1.9
SENT (0.0692s) ARP who-has 192.168.1.7 tell 192.168.1.9
SENT (0.0693s) ARP who-has 192.168.1.8 tell 192.168.1.9
SENT (0.0694s) ARP who-has 192.168.1.10 tell 192.168.1.9
SENT (0.0695s) ARP who-has 192.168.1.11 tell 192.168.1.9
RCVD (0.0690s) ARP reply 192.168.1.3 is-at 8C:EC:4B:71:C5:DE
RCVD (0.0699s) ARP reply 192.168.1.1 is-at 18:45:93:69:A5:10
SENT (0.0730s) ARP who-has 192.168.1.14 tell 192.168.1.9
SENT (0.0731s) ARP who-has 192.168.1.15 tell 192.168.1.9
SENT (0.0731s) ARP who-has 192.168.1.16 tell 192.168.1.9
SENT (0.0732s) ARP who-has 192.168.1.17 tell 192.168.1.9
RCVD (0.0791s) ARP reply 192.168.1.4 is-at 2A:84:98:9F:E5:5E
RCVD (0.0796s) ARP reply 192.168.1.5 is-at 30:24:32:1F:89:AC
SENT (0.0820s) ARP who-has 192.168.1.20 tell 192.168.1.9
SENT (0.0822s) ARP who-has 192.168.1.21 tell 192.168.1.9
SENT (0.0823s) ARP who-has 192.168.1.22 tell 192.168.1.9
SENT (0.0824s) ARP who-has 192.168.1.23 tell 192.168.1.9
SENT (0.1699s) ARP who-has 192.168.1.26 tell 192.168.1.9
SENT (0.1703s) ARP who-has 192.168.1.27 tell 192.168.1.9
SENT (0.1705s) ARP who-has 192.168.1.28 tell 192.168.1.9
SENT (0.1708s) ARP who-has 192.168.1.29 tell 192.168.1.9
SENT (0.1710s) ARP who-has 192.168.1.30 tell 192.168.1.9
SENT (0.1712s) ARP who-has 192.168.1.31 tell 192.168.1.9
```

Now when we have seen that ARP packets are seen in the network, we will make use of **–disable-arp-ping** option where you can see that there are 4 packets being sent.

Disable-arp-ping

To disable the ARP discovery, Nmap provides this option.

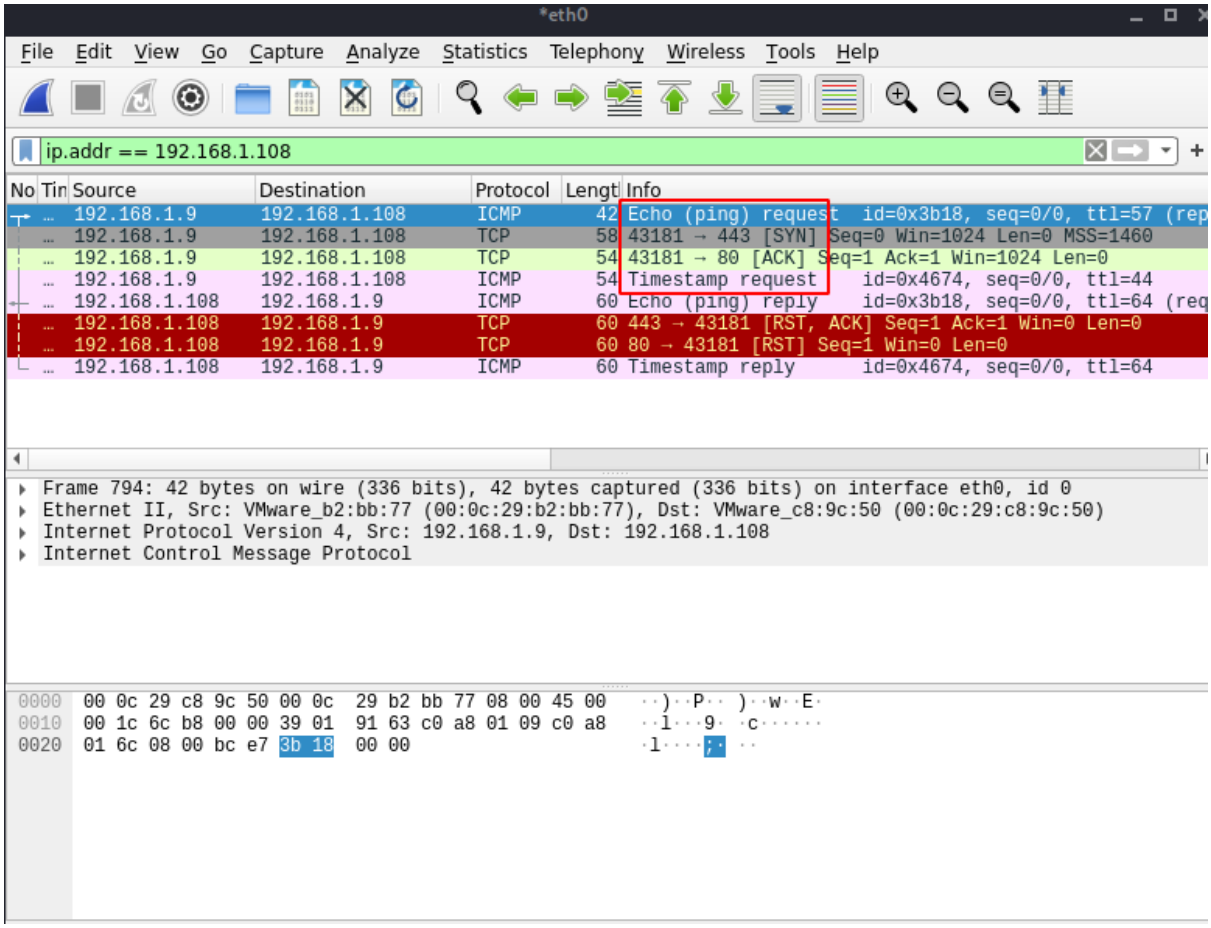
```
nmap -sn 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:58 EST
Nmap scan report for 192.168.1.108
Host is up (0.00027s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#
```

And you will see that the ARP packets are not visible

Note: Scanning Local Network with Nmap where nmap sends an ARP packet with every scan. If an external network is to be scanned; Nmap sends following request packets when –disable-arp-ping is used:

ICMP echo request (Type 8)
ICMP timestamp request(Type 13)
TCP SYN to port 443
TCP ACK to port 80



You can also make use of **–send-ip** option to get the same results as in the step above.

Send-ip

```
nmap -sn 192.168.1.108 --packet-trace --send-ip
```

```
root@kali:~# nmap -sn 192.168.1.108 --packet-trace --send-ip
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:55 EST
SENT (0.0588s) ICMP [192.168.1.9 > 192.168.1.108 Echo request (type=8/code=0) id=297
SENT (0.0589s) TCP 192.168.1.9:43573 > 192.168.1.108:443 S ttl=58 id=30850 iplen=44
SENT (0.0589s) TCP 192.168.1.9:43573 > 192.168.1.108:80 A ttl=55 id=52947 iplen=40
SENT (0.0590s) ICMP [192.168.1.9 > 192.168.1.108 Timestamp request (type=13/code=0)
RCVD (0.0590s) ICMP [192.168.1.108 > 192.168.1.9 Echo reply (type=0/code=0) id=2974
NSOCK INFO [0.1030s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1030s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53
NSOCK INFO [0.1030s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeou
NSOCK INFO [0.1030s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192
NSOCK INFO [0.1030s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for E
NSOCK INFO [0.1030s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID
NSOCK INFO [0.1090s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID
NSOCK INFO [0.1090s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeou
NSOCK INFO [0.1090s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1090s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.1.108
Host is up (0.00024s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Host Discovery is considered to be the most primary step in Information Gathering which provides accurate results on active ports and IP addresses in a network.

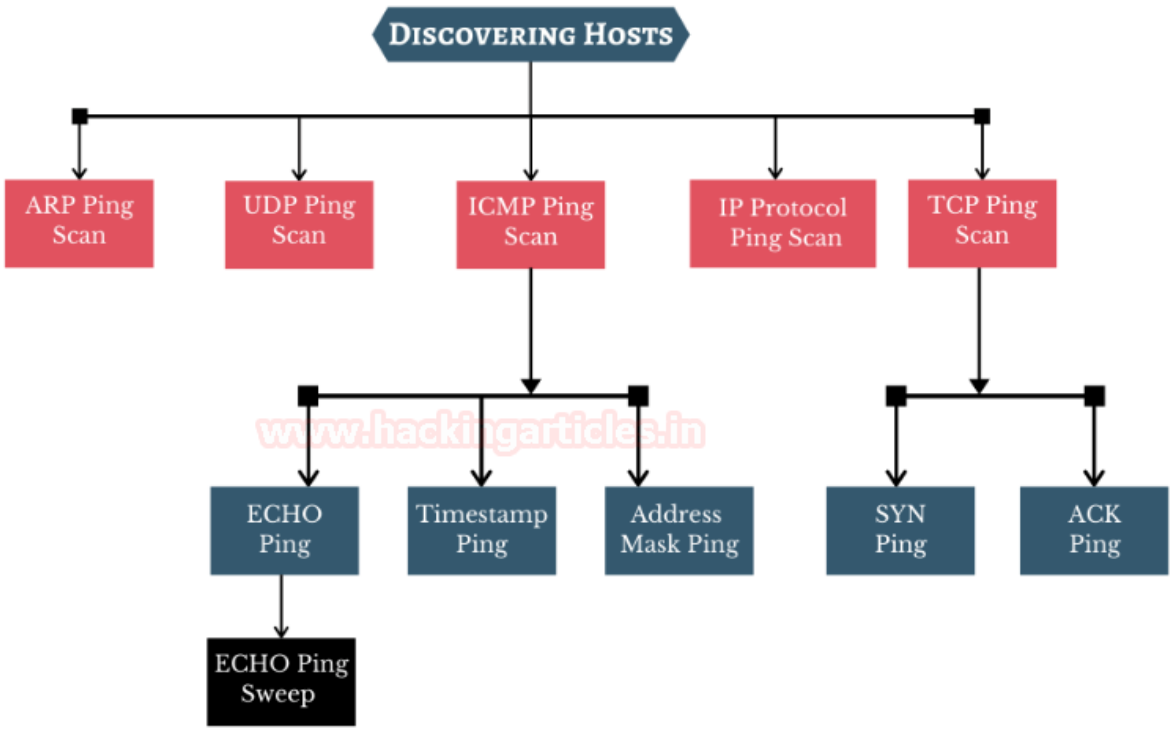
TCP Flags

First, let's get to know the basics about the communication Flags in TCP. The TCP header mainly consists of six flags which manage the connection between the systems and provide instructions to them. Each flag is of 1 bit and hence the size of TCP Flags is 6 bits. Now let us briefly understand each flag.

FLAG	DESCRIPTION
SYN	It stands for Synchronize. It assists in notifying when a new sequence number is transmitted. The SYN flag usually represents the Three-Way Handshake.
ACK	It stands for Acknowledgement. It notifies the status of transmission of packets and also assists in identifying the what sequence number to expect next.
RST	It stands for Reset. This flag shows when there is any error in that connection and sets the flag to 1 and the connection is broken.
URG	It stands for Urgent. This flag usually commands to process the packets as soon as possible.
FIN	It stands for Finish. This flag is set as 1 to indicate no further transmission of packets.
PSH	It stands for Push. It is used to start and end data transfer and prevent occurrence of buffer deadlocks.

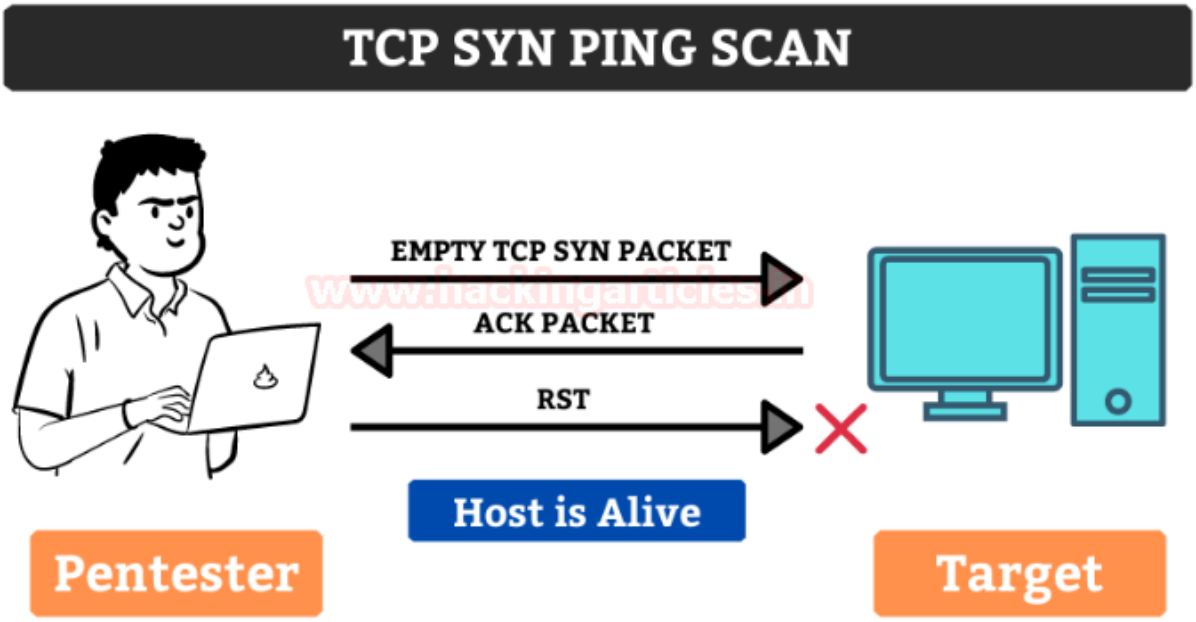
Types of Scans

To discover the hosts in the network, various ping scan methods can be used.



TCP SYN Ping Scan

It is a method of host discovery which helps in looking for discovering if the ports are open and to also make sure if it matches the rules of the firewall. The Pentester can hence, send an empty SYN flag to the target to check where it is alive. Multiple ports can be defined in this scan type.

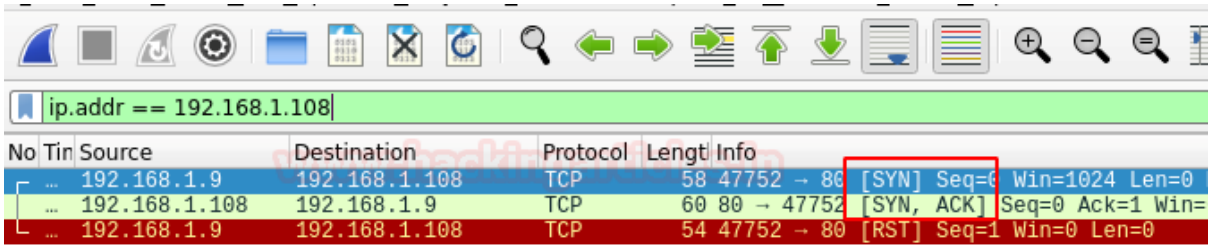


The -sP command in Nmap only allows discovering online hosts. Whereas SYN Ping (-PS) sends a TCP SYN packet to the ports and if it is closed, the host responds with an RST packet. And if the ports requested are open there will be the response of TCP SYN/ACK and there will be a reset packet which will be sent to reset the connection.

```
nmap -sn -PS 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PS 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:13 EST
Nmap scan report for 192.168.1.108
Host is up (0.00030s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

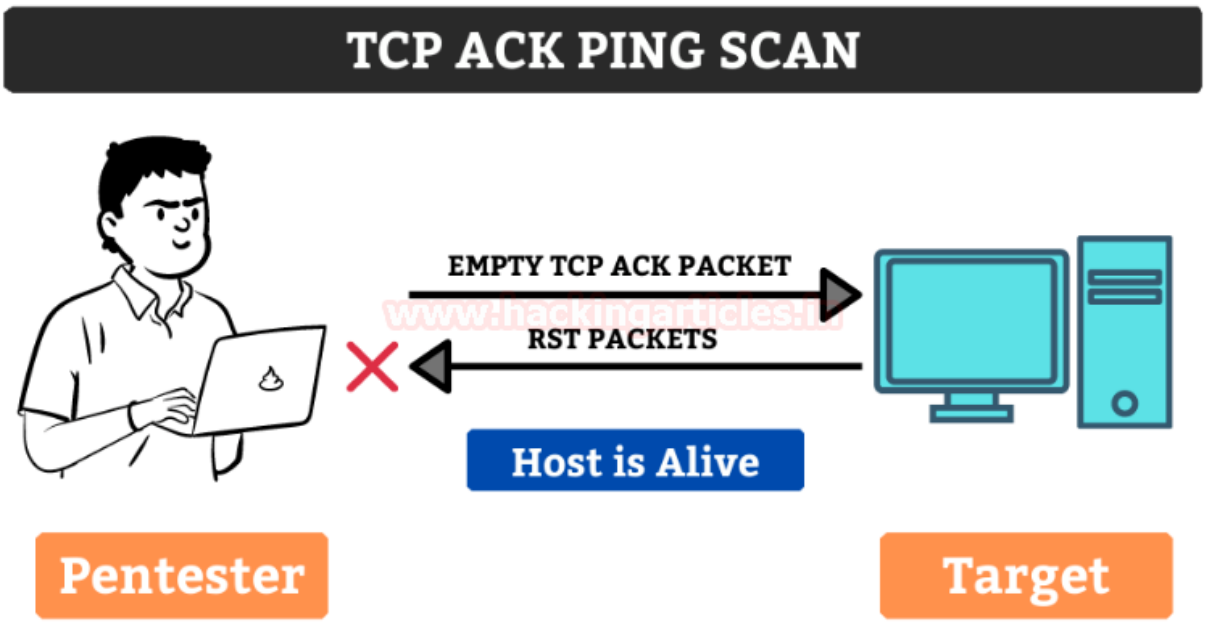
The packets captured using Wireshark can be overserved



The advantage of TCP SYN Ping scan is that the pentester can get the active/inactive status of the host without even creating a connection and hence it does not even create a log in the system or the network.

TCP ACK Ping Scan

It is a method of host discovery which is similar to TCP SYN Ping scan but slightly differs. This scan also makes use of Port 80. The pentester sends an empty TCP packet to the target and as there is no connection between them, it will receive an Acknowledgement packet and will then reset and terminate the request

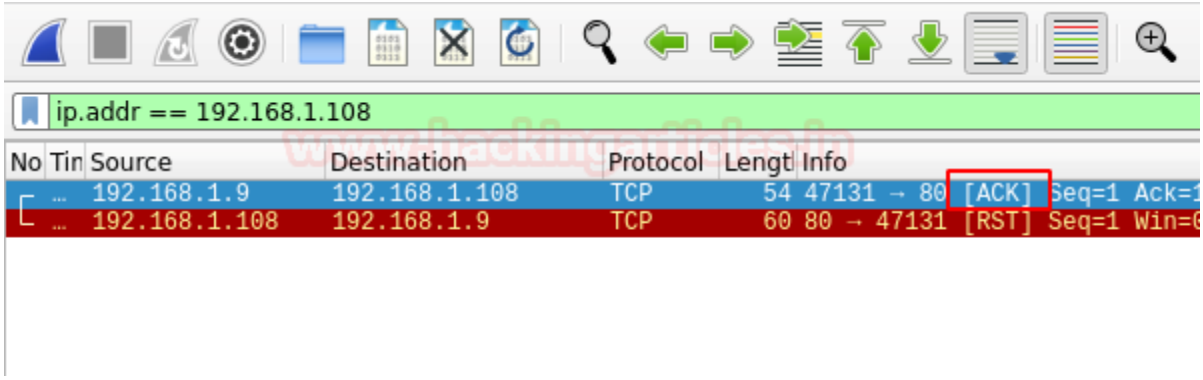


This command is used to determine the target's response and also check if the SYN packets or ICMP echo requests are blocked as of in the latest firewalls

```
nmap -sn -PA 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PA 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:14 EST
Nmap scan report for 192.168.1.108
Host is up (0.00023s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#
```

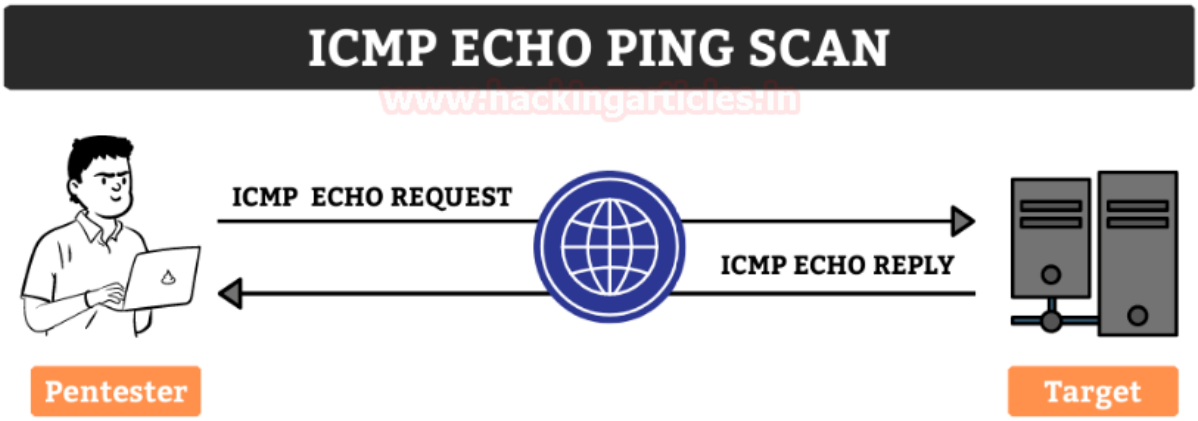
The Packets captured in the Wireshark can be observed here.



Some firewalls are configured to block on SYN ping packets, hence, in this case, this scan would be effective to bypass the firewall easily.

ICMP Echo Ping Scan

The ICMP Ping scan can be used to gather information about the target systems which makes it different from port scanning. The pentester can send an ICMP ECHO request to the target and getting an ICMP Echo reply in return.

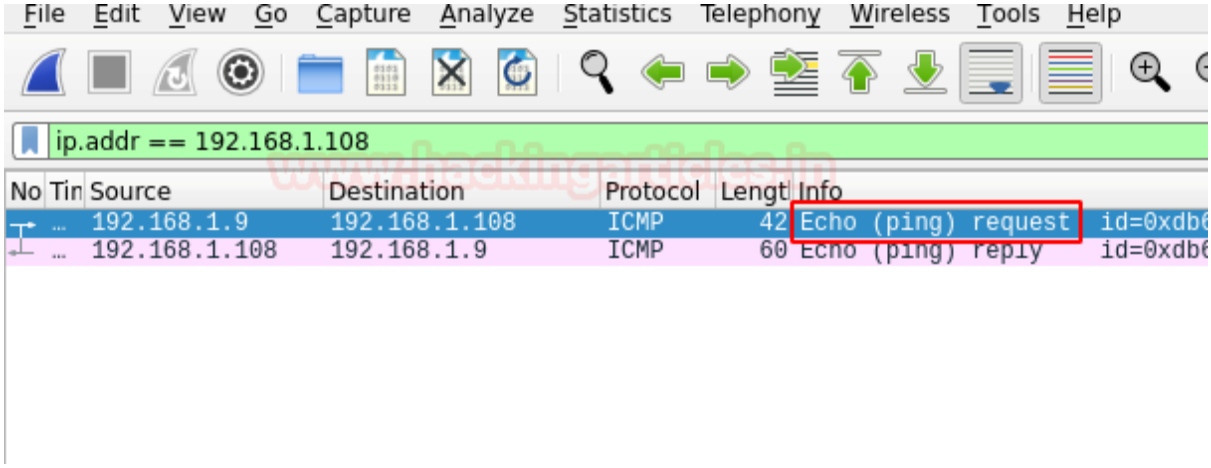


ICMP is now ineffective on remote ICMP packets which have been blocked by admins. It can still be used to monitor local networks.

```
nmap -sn -PE 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PE 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:15 EST
Nmap scan report for 192.168.1.108
Host is up (0.00039s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@kali:~#
```

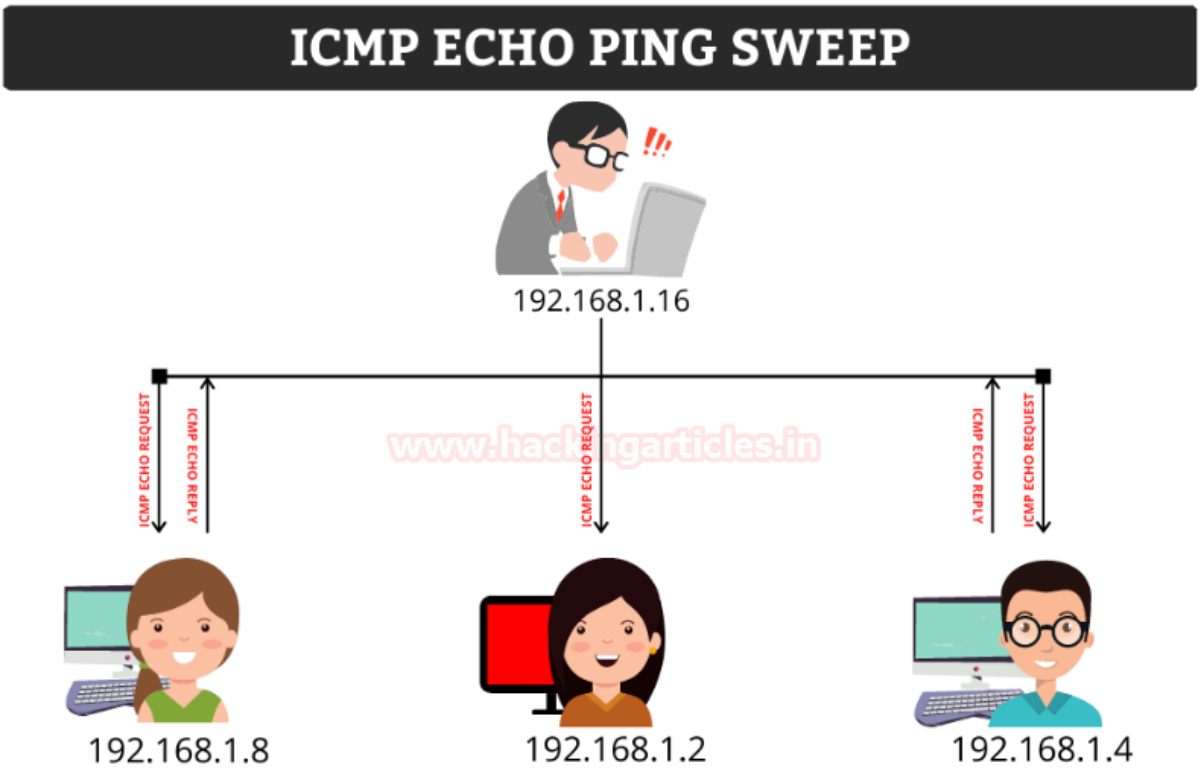
The packets captured in the Wireshark can be observed.



ICMP Echo Ping Sweep

It is similar to Echo Ping Scan and is used to scan the active hosts from a given range of IP addresses. It sends ICMP requests to a huge number of targets and if a particular target is alive then it will return an ICMP reply.

```
nmap -sn -PE 192.168.1-10
```



ICMP Address Mask Scan

It is an older method of ICMP ECHO ping scanning. It gives out the information about the system and its subnet mask.

```
nmap -sn -PM 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PM 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:15 EST
Nmap scan report for 192.168.1.108
Host is up (0.00026s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#
```

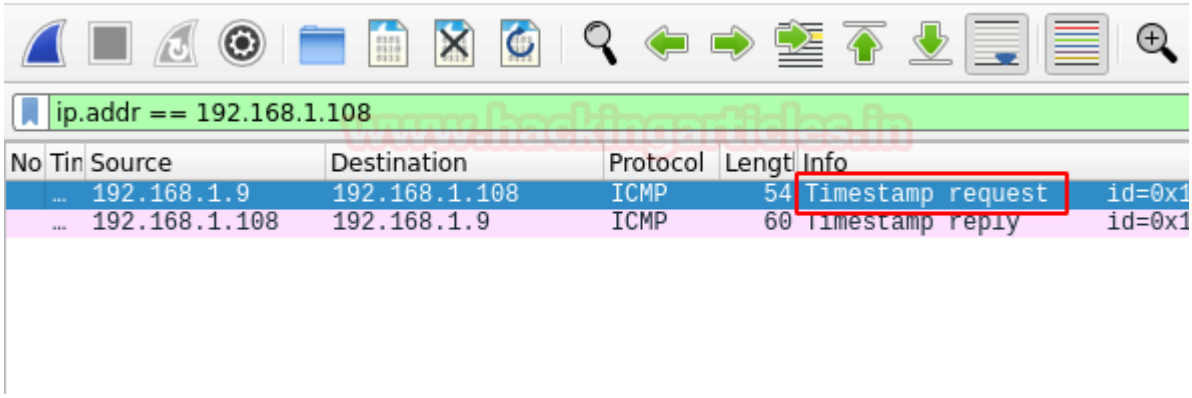
ICMP ECHO Timestamp Scan

The pentester can adopt this technique in a particular condition when the system admin blocks the regular ICMP timestamp. It is usually used in synchronization of time.

```
nmap -sn -PP 192.168.1.108 --disable-arp-ping
```

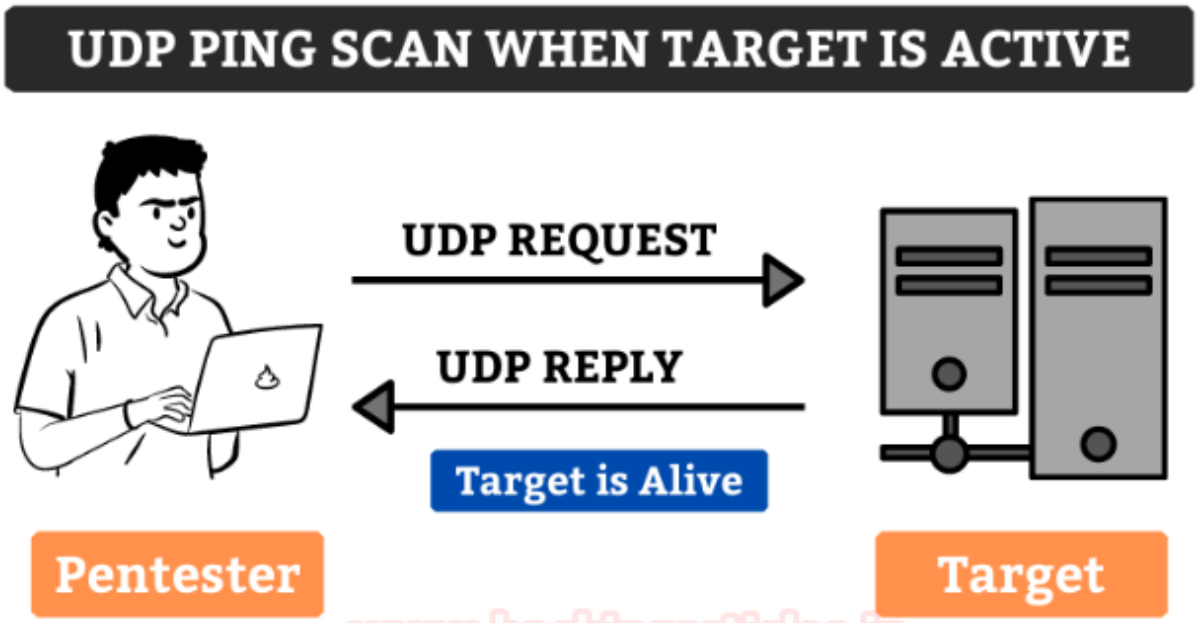
```
root@kali:~# nmap -sn -PP 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:17 EST
Nmap scan report for 192.168.1.108
Host is up (0.00059s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#
```

The packets captured using Wireshark can be observed.

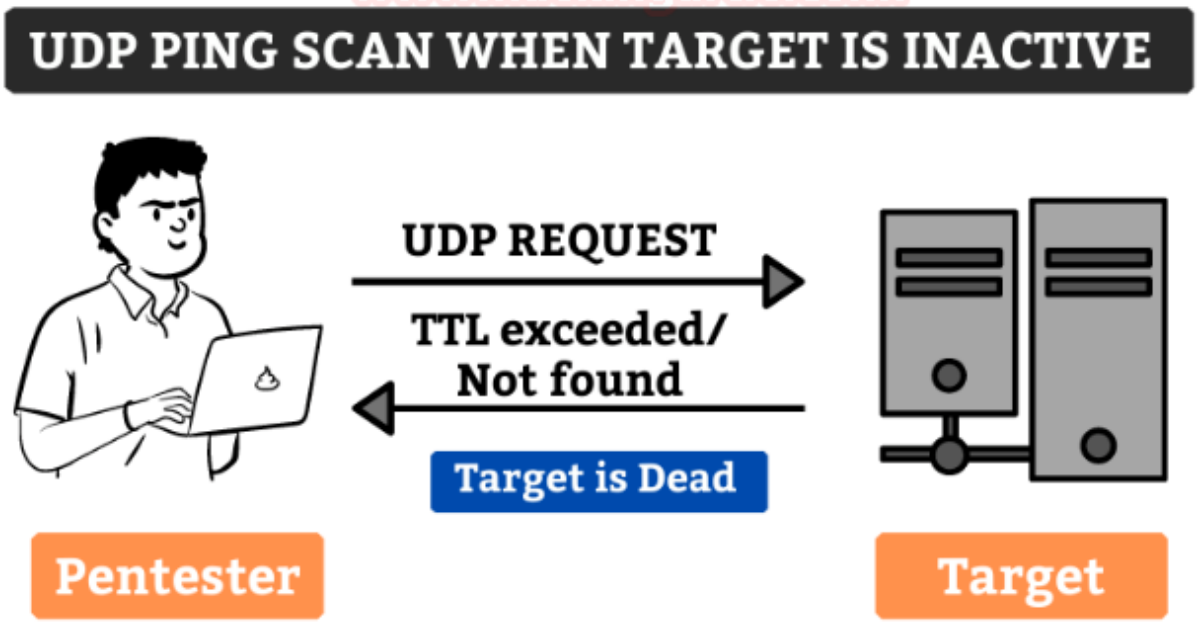


UDP Ping Scan

The UDP Ping Scans uses a highly uncommon default port number 40125 to send packets to the target. It is similar to TCP Ping scan. The Pentester will send the UDP Packets to the target and if there is a response in return which means that the host is alive or else it is offline



www.hackingarticles.in

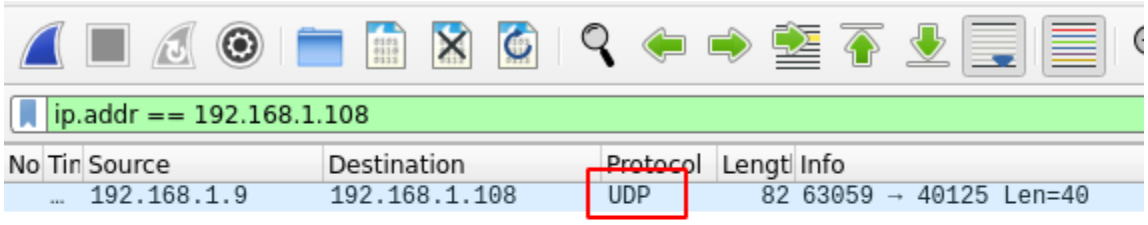


The advantage of UDP scan is that it can detect the systems which have firewalls with strict TCP rules and leaving UDP rules at ease.

```
nmap -sn -PU 192.168.1.108 --disable-arp-ping
```

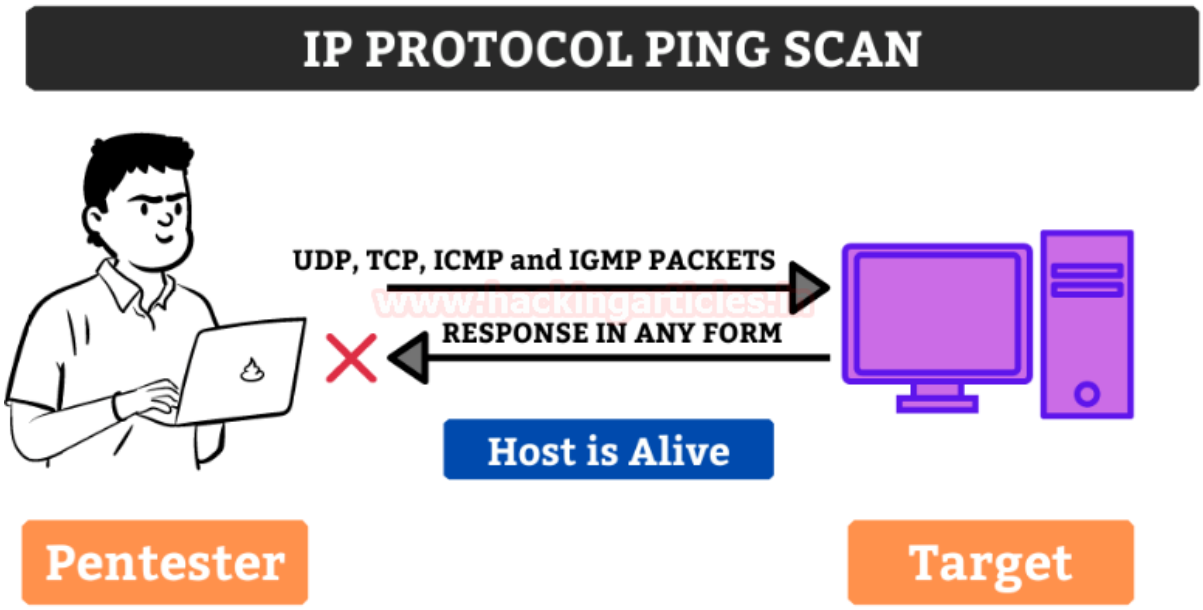
```
root@kali:~# nmap -sn -PU 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:06 EST
Nmap scan report for 192.168.1.108
Host is up (0.00032s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#
```

You can observe the packets sent using Wireshark.



IP Protocol Ping Scan

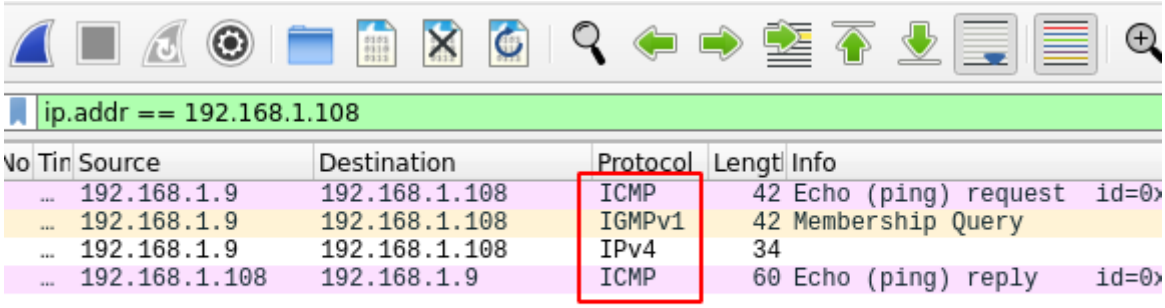
In this method, the pentester sends various packets using different IP protocols and hopes to get a response in return if the target is alive.




```
nmap -sn -PO 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PO 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:07 EST
Nmap scan report for 192.168.1.108
Host is up (0.00040s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

The packets captured can be observed using Wireshark.



No Ping Scan

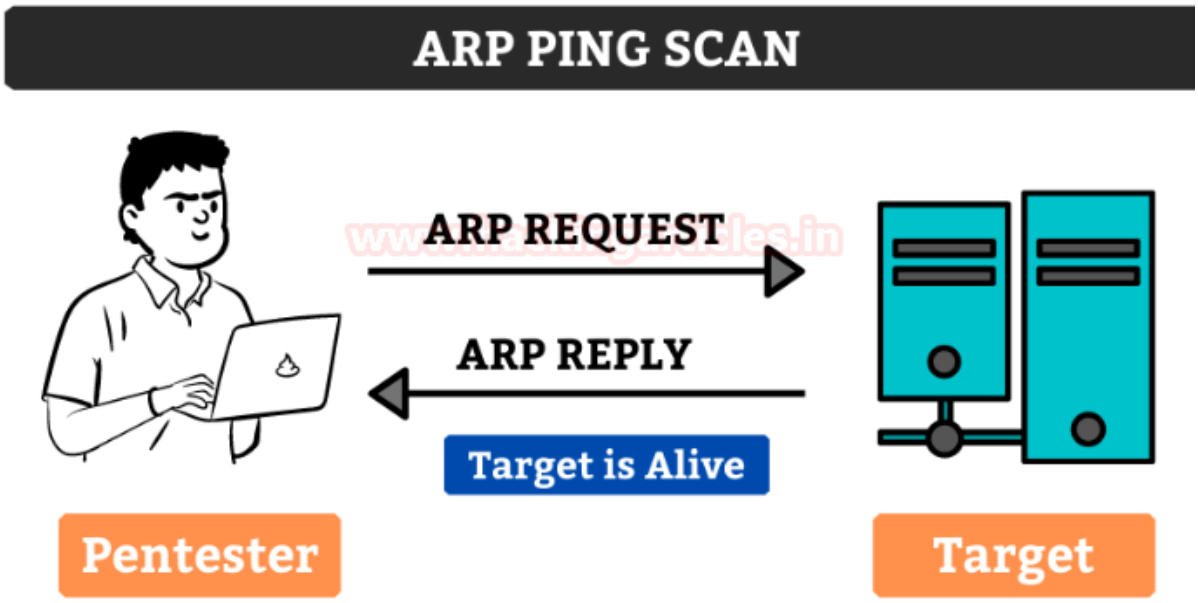
In this method, host discovery is completely skipped. The pentester can use it to determine active machines for heavier scanning and to increase the speed of the network.

```
nmap -sn -PN 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PN 192.168.1.108 --disable-arp-ping
Host discovery disabled (-Pn). All addresses will be marked 'up' and s
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:10 EST
Nmap scan report for 192.168.1.108
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

ARP Ping Scan

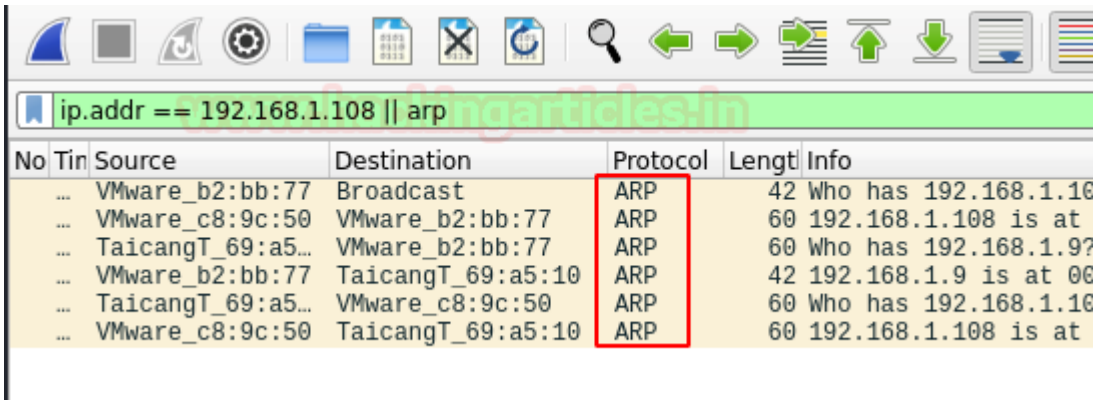
In this method, the ARP packets are sent to all the devices I the network although they are invisible due to the firewall. It is considered to be extremely efficient than other host discovery. It is mainly used for system discovery. It also mentions the latency.




```
nmap -sn -PR 192.168.1.108
```

```
root@kali:~# nmap -sn -PR 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:12 EST
Nmap scan report for 192.168.1.108
Host is up (0.00029s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~#
```

You can see the packets being captured in wireshark.



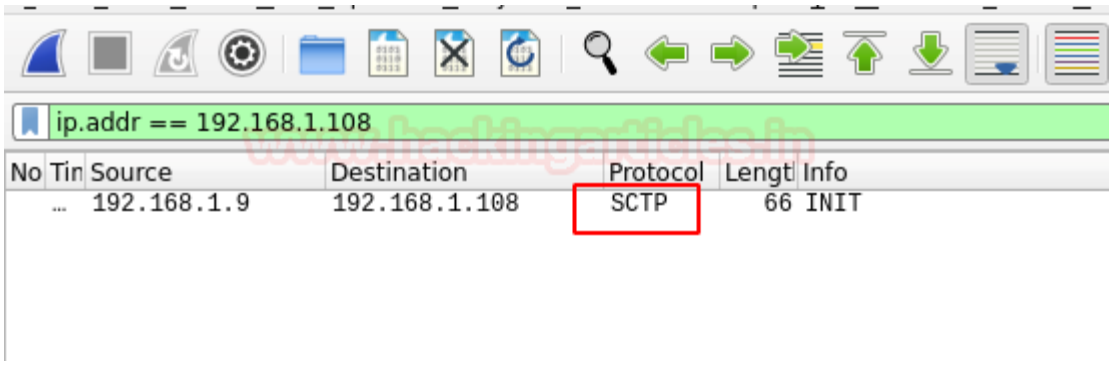
SCTP INIT Ping

It sends SCTP packet containing a minimal INIT chunk. Its default destination port is 80. The INIT chunk provides suggestion to the remote system that the pentester is attempting to establish an association.

```
nmap -sn -PY 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PY 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:13 EST
Nmap scan report for 192.168.1.108
Host is up (0.00030s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#
```

The packets that are captured can be observed.



Traceroute

Traceroutes are used after finishing scanning, by using the information from the scan results and to determine the port and protocol which will reach the target.

```
nmap -sn --traceroute 8.8.8.8
```

```
root@kali:~# nmap -sn --traceroute 8.8.8.8
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 11:38 EST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0014s latency).

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.85 ms dsldevice.lan (192.168.1.1)
2   1.57 ms dns.google (8.8.8.8)
```

Conclusion

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

References

- https://www.hackingarticles.in/nmap-for-pentester-host-discovery/
- https://nmap.org/book/man-host-discovery.html