Host Discovery with Nmap

In nmap we can perform host discovery with various techniques like:

- ARP Ping Scan
- UDP Ping Scan
- ICMP Ping Scan - ICMP Echo Ping, ICMP Timestamp Ping and ICMP Address Mask Ping
- TCP Ping Scan - TCP SYN Ping and TCP ACK Ping
- IP Protocol Scan

ARP Ping Scan

In ARP Ping Scan, we send ARP requests to each IP address and listens for ARP responses to determine which hosts are up. If we got a response that means host is up, otherwise we conclude it as down.

To perform a ARP Ping Scan with nmap, we will use the -PR flag. There is also -sn flag which is to enable only the host discovery mode with port scanning.

```
nmap -sn -PR IP
```

UDP Ping Scan

In UDP Ping Scan, we send UDP packets to the target and if we got a response back from it. Then, we conclude that that the host is up. Otherwise, it is considered as down. We also conclude that the machine is not active if we receive a TTL or Not found error.

To perform UDP scan with nmap, we will use the -PU flag along with -sn.

```
sudo nmap -sn -PU IP
```

ICMP Ping Scan

Now we have ICMP Ping Scan. First we will start off with the normal ICMP ECHO ping scan.

In this, we will send ICMP ECHO request to the server same as we do with the ping command. If the host is live, it will return an ICMP ECHO reply. As i already told you that this technique might not work in Windows machines due to different TCP/IP stack implementation but it does work on Linux Boxes.

To perform the ICMP ECHO Ping Scan, we will use the -PE flag.

```
nmap -sn -PE IP
```

Now, we can also perform a ICMP ping scan on a IP address range like /24. This is called ICMP Ping Sweep. To do this, we just have to provide the subnet mask with the IP address, except this everything will be same like before

```
nmap -sn -PE IP/24
```

ICMP Timestamp Ping Scan

So, the next one we have is ICMP TImestamp ping scan. this is somewhat an interesting one.

Basically, The ICMP timestamp ping scan sends a "what time is it?" message to the target computer. If that computer answers back with the time, it confirms the computer is turned on and connected to the network.

This type of scan can be useful when a firewall or security settings are blocking the standard ICMP echo request packets. The timestamp request may slip through when echo requests are filtered.

However, ICMP timestamp scans are not as widely supported as echo requests. Many systems are configured to ignore or block timestamp requests for security reasons. So while effective in some cases, ICMP timestamp scans are not as reliable as other host discovery methods.

To perform an ICMP Timestamp scan with nmap, we will use the -PP flag.

```
nmap -sn -PP IP
```

ICMP Address Mask Ping Scan

ICMP Address Mask ping scan sends a special ICMP packet to a target system asking for network configuration details. If the target replies, it confirms the system is up and provides useful information to the attacker about the network layout. If it does not responds, that means it is down.

To perform this scan, we use the -PM flag.

```
sudo nmap -sn -PM IP
```

TCP SYN Ping Scan

Now we have TCP SYN Ping Scan.

As we have already learned about the TCP 3 way handshake in our Networking Refresher module. This will be very easy for us to understand. In a TCP SYN Scan, we send a "hello" message or SYN Packet to the target and if the target replies back with "Hello Back" or ACK, then it is confirm that the host is active.

To perform this scan, we will use the -PS flag.

```
sudo nmap -sn -PS IP
```

TCP ACK Ping Scan

In this type of TCP ACK Ping Scan, nmap sends an empty ACK packet to the server and if the server responds with a RST packet then we can conclude that the host is active.

So in simple terms, the TCP ACK ping scan sends a "thank you" message or ACK packet to the target computer on a particular port, even though no conversation has taken place. If that computer answers back with a "huh what do you want man?" or RST packet, then it confirms the computer is turned on.

To perform this scan, we use the -PA Flag.

```
sudo nmap -sn -PA IP
```

IP protocol Scan

In IP protocol ping scan we send packets using different IP protocols like TCP,UDP,ICMP and IGMP to the target computer . If the computer responds with a "I don't understand that protocol" message, it confirms the computer is turned on. If it responds with a protocol-specific message, it indicates the host supports that protocol.

To perform this scan, we will use the -PO flag.

```
sudo nmap -sn -PO IP
```

This concludes our session on host discovery. In this one, we have learned about all the techniques nmap used to discover live hosts. One thing to note is that, if you don't specify any flag related to one of the above techniques. Nmap then by defautl will sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request to the target in order to find out if it alive or not.
