Nmap

Host discovery techniques:

- ARP ping scan
- UDP ping scan
- ICMP Echo scan (?)
- ICMP Timestamp scan (?)
- TCP ping scan (?)
- IP protocol ping scan (?)

What is ARP?

ARP stands for "Address Resolution Protocol" and is used to map dynamic Internet Protocol (IP) addresses to permanent physical machine addresses, also called media access control (MAC) addresses. ARP was designed to let these two systems interoperate by converting 32-bit IPV4 addresses to 48-bit MAC addresses. This conversion protocol lives between layers 2 and 3 of the Open Systems Interconnection (OSI) model — MAC addresses are part of layer 2, the data link layer. In contrast, IP addresses are part of layer 3, the network layer.

Functionally, ARP made it possible for companies to get a more complete picture of their device and network infrastructure at scale — something that's now critical as device use expands, and IT complexity increases. But ARP also offers another benefit: Enhanced security.

ARP Scan:

`nmap -sN (disables port scan) -PR (performs ARP ping scan) <TARGETIP>`

```
┌──(root㉿kali)-[/home/kali/Desktop/Module 2]
└─# nmap -PR 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-20 17:14 EST
Nmap scan report for 192.168.0.1
Host is up (0.0071s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 68:FF:7B:A7:F5:34 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

or

`sudo arp-scan -l` (be careful of duplicates)

```
┌──(root㉿kali)-[/home/kali/Desktop/Module 2]
└─# sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:db:96:6a, IPv4: 192.168.0.106
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     68:ff:7b:a7:f5:34       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.1     68:ff:7b:a7:f5:34       TP-LINK TECHNOLOGIES CO.,LTD. (DUP: 2)
192.168.0.104   d0:37:45:d9:68:76        TP-LINK TECHNOLOGIES CO.,LTD.
```

What is UDP Scan:

UDP scanning is a process in which we scan for the UDP services that are being deployed on the target system or are currently in a running state. UDP is a connectionless protocol, hence it is hard to probe as compared to TCP.

Working of UDP scan:

In UDP scan usually, we take advantage of any UDP service clients like dig or tools like Nmap to send UDP datagrams to the target UDP network services like DNS, SNMP, and DHCP and wait for the response. Besides this, we can also send the UDP datagrams to all the ports and wait for the result.

Some popular services that we look for in UDP scan are:

- DNS
- SNMP
- DHCP

UDP Scan in Nmap:

`nmap -sN -PU <IPADDRESS>`

```
┌──(root㉿kali)-[/home/kali/Desktop/Module 2]
└─# nmap -PU 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-20 17:17 EST
Nmap scan report for 192.168.0.1
Host is up (0.15s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 68:FF:7B:A7:F5:34 (Tp-link Technologies)
```

ICMP Echo Scan

`nmap -PE 192.168.0.1`

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PE 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-22 16:07 EST
Nmap scan report for 192.168.0.1
Host is up (0.011s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 68:FF:7B:A7:F5:34 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

ICMP Timestamp scan

`nmap -PP 192.168.0.1`

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PP 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-22 16:09 EST
Nmap scan report for 192.168.0.1
Host is up (0.0095s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 68:FF:7B:A7:F5:34 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

[Link to full NMAP course]

[David Bombai video]

Evading firewalls using Nmap:

`nmap -f [Target IP Address] - to send fragmented packets`

`nmap -g 80 [Target IP Address] - to send packets from port 80`

`nmap -mtu 9 [Target IP Address] - to specify maximum transmission unit`

`nmap -D RND:10 [Target IP Address] - to send packets from 10 random IPs`

`nmap -sT -Pn --spoof-mac 0 [Target IP Address] - randomize the mac address`

OS Version detection using Nmap:

`nmap -A [IP ADDRESS]`

Where:

`-A`: Enable OS detection, version detection, script scanning, and traceroute

```
nmap -O [IP ADDRESS]
```

Where:

`-O`: Enable OS detection

SMB OS discovery using Nmap:

```
nmap --script=smb-os-discovery.nse [IP ADDRESS]
```

Attempts to determine the operating system, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139). This is done by starting a session with the anonymous account (or with a proper user account, if one is given; it likely doesn't make a difference); in response

to a session starting, the server will send back all this information.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=smb-os-discovery.nse 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-11 08:32 EST
Nmap scan report for 192.168.1.103
Host is up (0.00017s latency).
Not shown: 978 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
6000/tcp open  X11
6667/tcp open  irc
8180/tcp open  unknown
MAC Address: 08:00:27:74:D1:36 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-01-11T08:32:36-05:00

Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
```

Stealth scan in Nmap to bypass firewall:

```
nmap -sS -v [IP ADDRESS]
```