EX.NO.12
16.9.25

Nmap to discover live hosts using ARP scan, ICMP scan.

Aim:

To discover live hosts on a network using different Nmap host-discovery techniques - ARP, ICMP, TCP ping, UDP ping.

Procedure:

1. Identify the target (subnet provided by the room)
2. Open the AttackBox terminal
3. ARP ping scan
4. ICMP Echo scan
5. TCP SYN ping
6. UDP ping
7. combined Discovery scan
8. check results.

Commands:

```
sudo nmap -sn -PR 10.10.24.0/24 -oN arp
sudo nmap -sn -PC 10.10.24.0/24 -oN icmp
sudo nmap -sn -PS 2480,443 100.24.0/24
sudo nmap -sn -PU 53,161 10.10.24.0/24
                          -oN udp-ping.
```

Result:

Thus live host on a network with ARP scan, ICMP scan, TCP ping & UDP ping has been executed & verified successfully.

Output:

ARP Scan

```
Nmap scan repast for 10.0.247
 Host is up (0.00018s latetheracy)
```

ICMP Scan

```
Nmap scan repost for 10.10.24.5
 Host is up (0.12s latency)
```

TCP Ping

```
Nmap scan repost for 10.10.24.5
Host is up (0.02s latency).
```