Host Discovery

@mmar

Host Discovery is the always the first step in any ethical hacking certification exam and in CTFs. It involves enumeration IP addresses of the systems available in the test environment

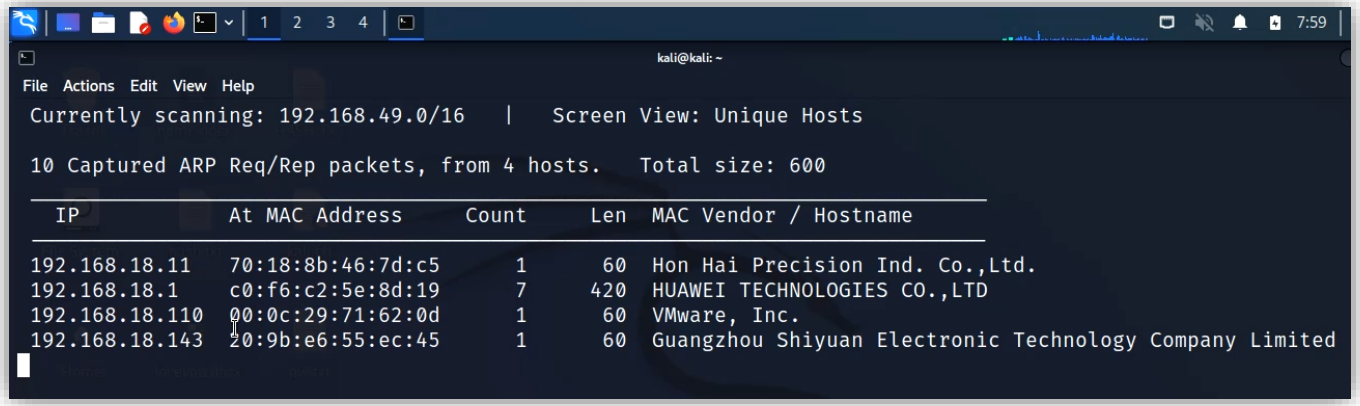
Netdiscover

- Netdiscover can be used to inspect your network ARP traffic, or find network addresses using auto scan mode, which will scan for common local networks.
- Although Not covered in CEH practicals, it’s the most essential tool to deal with any pen testing exam

Netdiscover

- Netdiscover is used to scan for the live hosts on the network

```
netdiscover -i (network interface name)
```

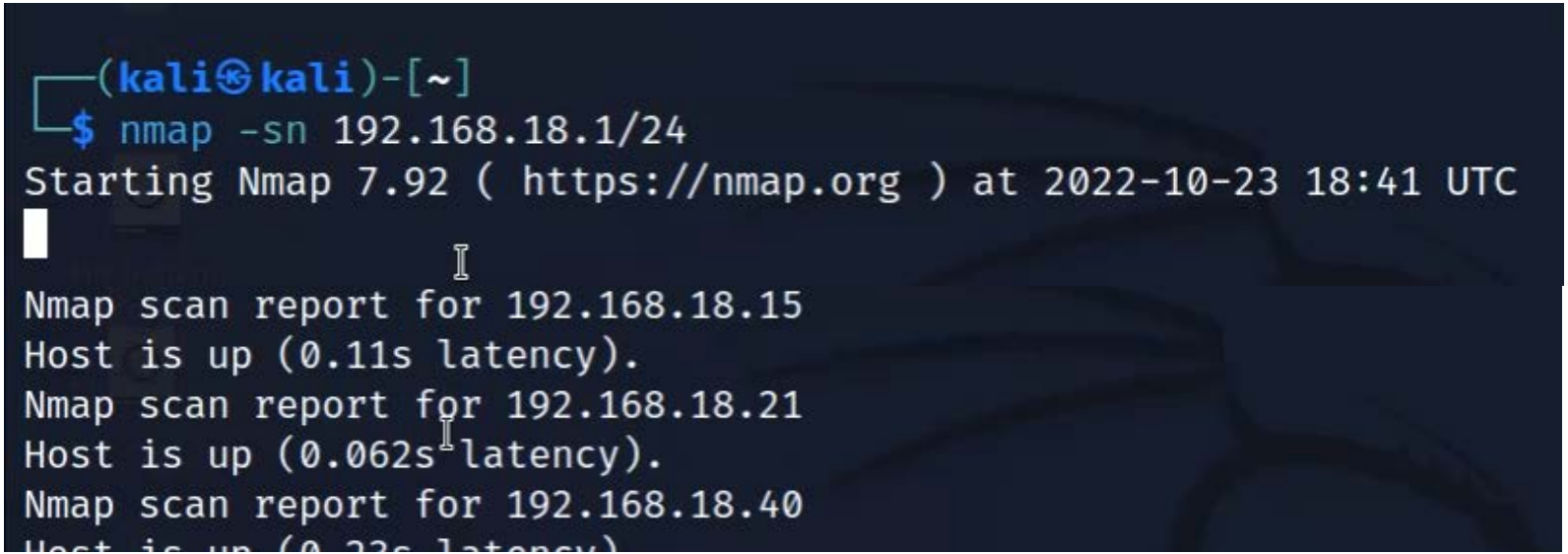


- Nmap is a free and open-source network scanner. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses
- Nmap provides different scanning options to search for live hosts

Ping Scan

- Ping scan is used to scan for the live hosts on the network

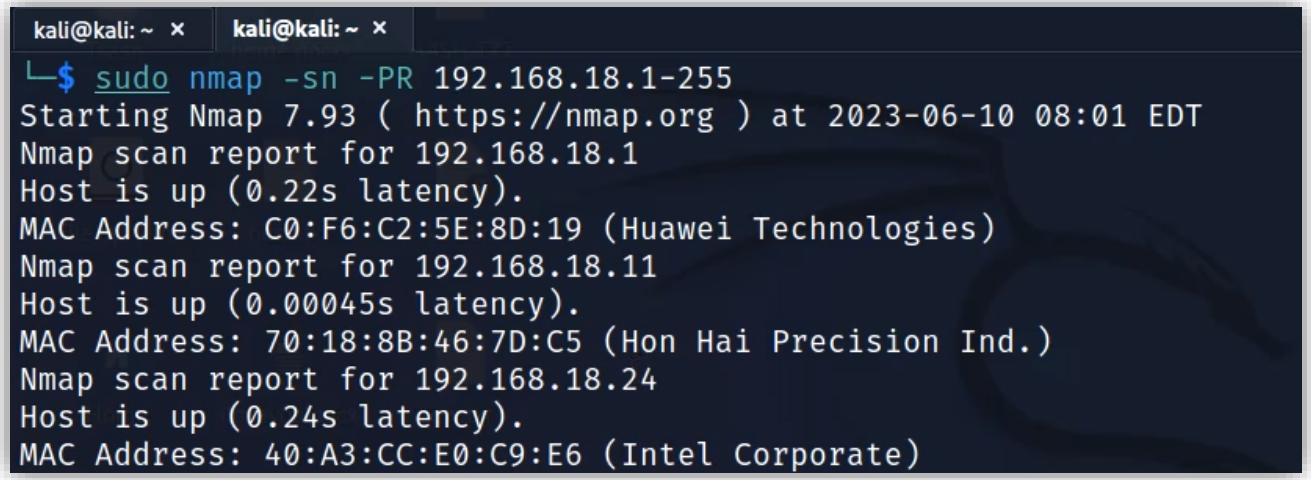
```
>nmap –sn 192.168.18.1/24
```



Arp Scan

- Arp scan is another method to scan for the live hosts on the network

```
nmap -sn -PR 192.168.18.0-255
```



Misc Nmap Scans

- Nmap has a vast variety of scans aval. Some of the most useful scans for host discovery are listed below

```
nmap -sn -PU 192.168.18.110   //UDP ping scan
nmap -sn -PE 192.168.18.1-255   //ICMP Echo Ping scan
nmap -sn -PM 192.168.18.1-255    //Mask Ping scan (use if ICMP is blocked)
nmap -sn -PP 192.168.18.1-255    //ICMP timestamp scan
nmap -sn -PS 192.168.18.1-255    //tcp syn ping scan
nmap -sn -PO 192.168.18.1-255     //IP protocol scan.use different protocols to test the connectivity
```

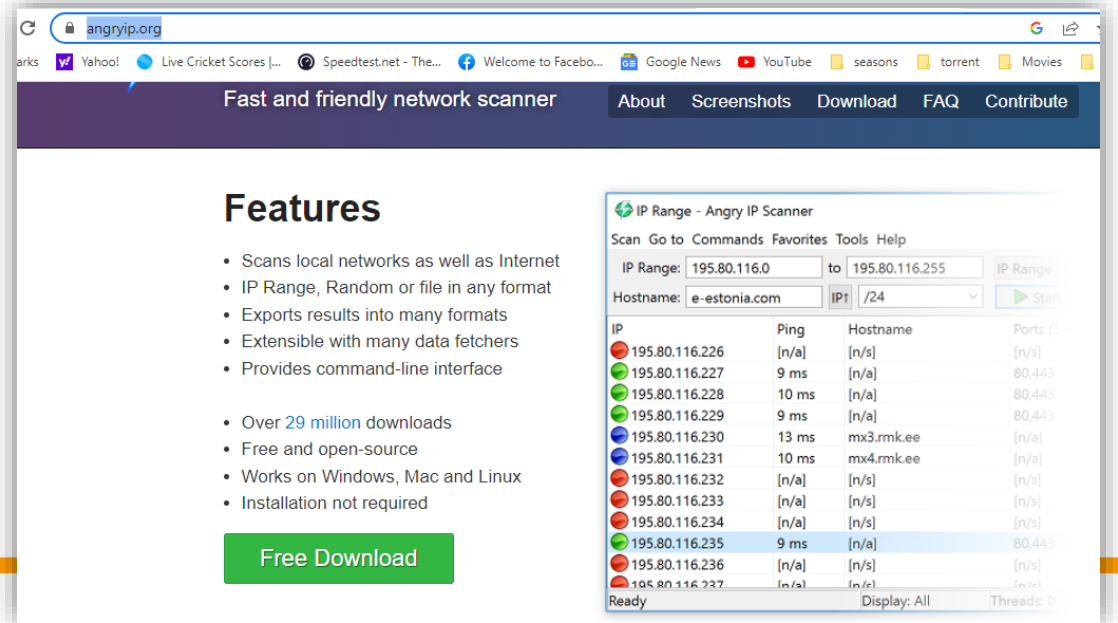
Angry IP Scanner

- Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use

Angry IP Scanner

- You can download and install the tool on Windows from the official website

https://angryip.org/

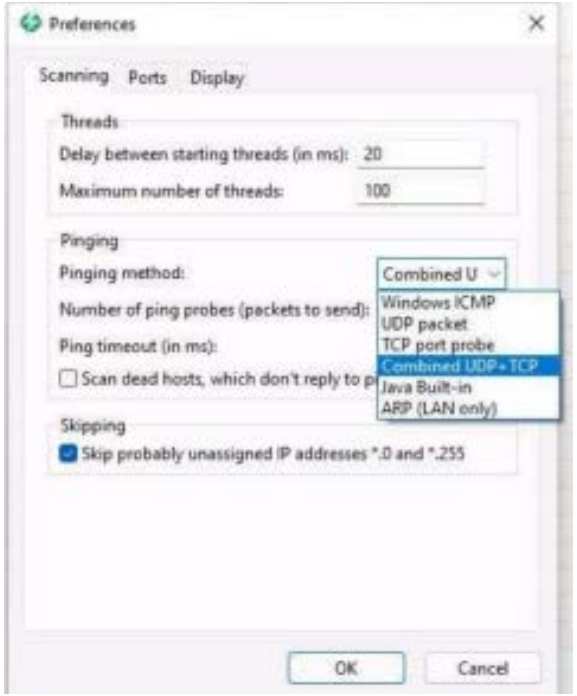


Angry IP Scanner

- Open the Preference and ensure that pinging method is set to UDP+TCP

Angry IP Scanner

- In display tab, change to display only live hosts



Angry IP Scanner

- Now provide the IP range and scan for targets

DEMO

THANKS