

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



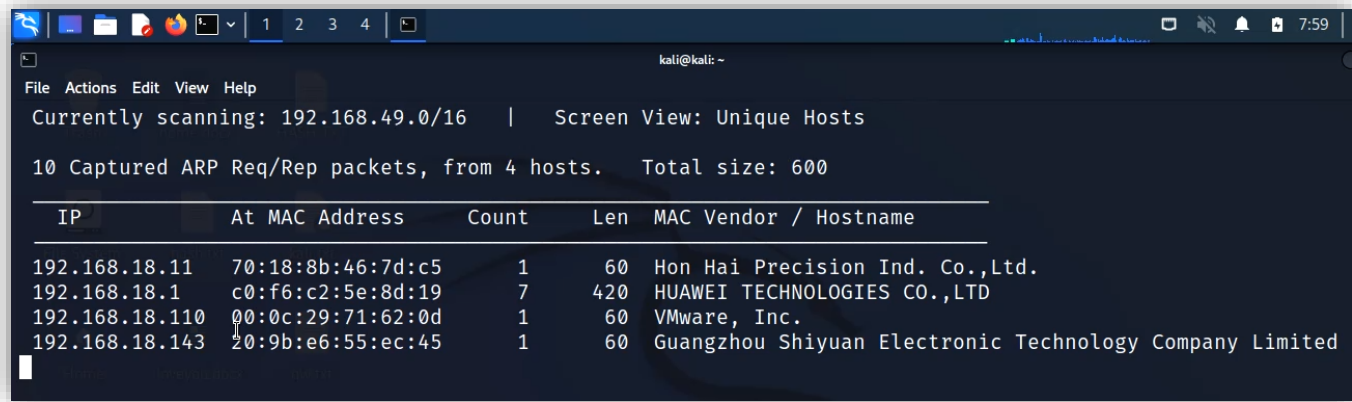
Netdiscover

- 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)
```



```
kali@kali: ~  
File Actions Edit View Help  
Currently scanning: 192.168.49.0/16 | Screen View: Unique Hosts  
10 Captured ARP Req/Rep packets, from 4 hosts. Total size: 600  
-----  
IP                At MAC Address    Count  Len  MAC Vendor / Hostname  
-----  
192.168.18.11     70:18:8b:46:7d:c5  1      60  Hon Hai Precision Ind. Co.,Ltd.  
192.168.18.1      c0:f6:c2:5e:8d:19  7      420 HUAWEI TECHNOLOGIES CO.,LTD  
192.168.18.110    00:0c:29:71:62:0d  1      60  VMware, Inc.  
192.168.18.143    20:9b:e6:55:ec:45  1      60  Guangzhou Shiyuan Electronic Technology Company Limited
```



- 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
```

```
(kali㉿kali)-[~]  
└─$ nmap -sn 192.168.18.1/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 18:41 UTC  
Nmap scan report for 192.168.18.15  
Host is up (0.11s latency).  
Nmap scan report for 192.168.18.21  
Host is up (0.062s latency).  
Nmap scan report for 192.168.18.40  
Host is up (0.22s latency).
```

Arp Scan

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

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

```
kali@kali: ~ × kali@kali: ~ ×
└─$ sudo nmap -sn -PR 192.168.18.1-255
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 08:01 EDT
Nmap scan report for 192.168.18.1
Host is up (0.22s latency).
MAC Address: C0:F6:C2:5E:8D:19 (Huawei Technologies)
Nmap scan report for 192.168.18.11
Host is up (0.00045s latency).
MAC Address: 70:18:8B:46:7D:C5 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.18.24
Host is up (0.24s latency).
MAC Address: 40:A3:CC:E0:C9:E6 (Intel Corporate)
```

Misc Nmap Scans

- ❖ Nmap has a vast variety of scans available. 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/>

The image shows a screenshot of the Angry IP Scanner website and its application interface. The website header reads "Fast and friendly network scanner" with navigation links for "About", "Screenshots", "Download", "FAQ", and "Contribute". The "Features" section lists:

- Scans local networks as well as Internet
- IP Range, Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface
- Over 29 million downloads
- Free and open-source
- Works on Windows, Mac and Linux
- Installation not required

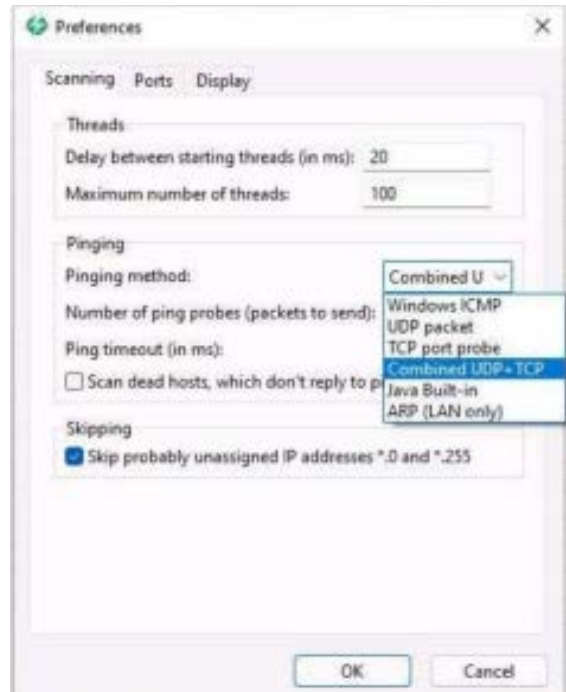
At the bottom of the website, there is a green button labeled "Free Download" with the URL <https://t.me/learningnets>.

The application interface, titled "IP Range - Angry IP Scanner", shows a scan configuration for IP Range: 195.80.116.0 to 195.80.116.255 and Hostname: e-estonia.com. The results table is as follows:

IP	Ping	Hostname	Ports
195.80.116.226	[n/a]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443
195.80.116.228	10 ms	[n/a]	80,443
195.80.116.229	9 ms	[n/a]	80,443
195.80.116.230	13 ms	mx3.rmk.ee	[n/a]
195.80.116.231	10 ms	mx4.rmk.ee	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443
195.80.116.236	[n/a]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]

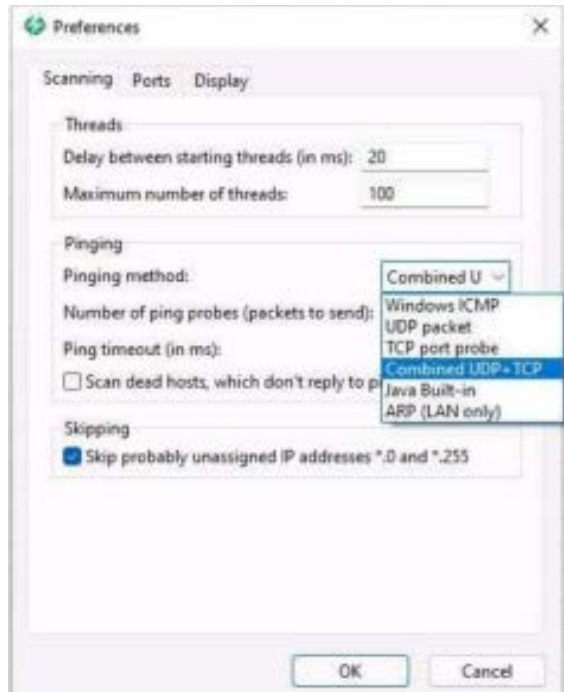
Angry IP Scanner

- ❖ 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