

# Cryptus Security

## Net Discover

**Netdiscover:-** Simple ARP Scanner to scan for live hosts in a network.

Netdiscover is a simple ARP scanner which can be used to scan for live hosts in a network. It can scan for multiple subnets also. It simply produces the output in a live display (ncurses). This can be used in the first phases of a pentest where you have access to a network. Netdiscover is a simple and initial-recon tool which can be very handy.

### Features:-

- Simple Arp Scanner
- Works in both Active & Passive modes
- Produces a live display of identified hosts
- Able to scan multiple subnets
- Timing Options

Commands	Descriptions
-i device	your network device
-r range	scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
-l file	scan the list of ranges contained into the given file
-p passive mode	do not send anything, only sniff
-m file	scan the list of known MACs and host names
-F filter	Customize pcap filter expression (default: "arp")
-s time	time to sleep between each arp request (milliseconds)

Commands	Descriptions
-n node	last ip octet used for scanning (from 2 to 253)
-c count	number of times to send each arp request (for nets with packet loss)
-f	enable fastmode scan saves a lot of time, recommended for auto
-d	ignore home config files for autoscan and fast mode
-S	enable sleep time suppression between each request (hardcore mode)
-P	print results in a format suitable for parsing by another program
-N	Do not print header Only valid when -P is enabled.
-L	in parsable output mode (-P) continue listening after the active scan is completed

## Start Netdiscover in Kali Linux

Netdiscover is a very attractive tool for discovering hosts on wired or wireless network. It can be used in both active and passive mode.

Inactive Mode it send requests to hosts for getting information but in otherhand it is working in silent mode called passive mode or listening mode. To start and check for available options in netdiscover run following command.

## # netdiscover -help

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
(root@kali)-[~]  
# netdiscover -help  
Netdiscover 0.7 [Active/passive ARP reconnaissance tool]  
Written by: Jaime Penalba <jpenalbae@gmail.com>  
  
Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time]  
[-c count] [-n node] [-dfPLNS]  
-i device: your network device  
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8  
-l file: scan the list of ranges contained into the given file  
-p passive mode: do not send anything, only sniff  
-m file: scan a list of known MACs and host names  
-F filter: customize pcap filter expression (default: "arp")  
-s time: time to sleep between each ARP request (milliseconds)  
-c count: number of times to send each ARP request (for nets with packet loss)  
-n node: last source IP octet used for scanning (from 2 to 253)  
-d ignore home config files for autoscan and fast mode  
-f enable fastmode scan, saves a lot of time, recommended for auto  
-P print results in a format suitable for parsing by another program and stop after ac  
tive scan  
-L similar to -P but continue listening after the active scan is completed  
-N Do not print header. Only valid when -P or -L is enabled.
```

lots of switches can be used with different manners for getting desired result. Netdiscover work only in internal network so you must know network you are connecting. use following command to check the IP Address:



## # ifconfig

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
(root@kali)-[~]  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.19 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::20c:29ff:fea9:1f7e prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:a9:1f:7e txqueuelen 1000 (Ethernet)  
    RX packets 78 bytes 9164 (8.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25 bytes 2968 (2.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

So My network is 192.168.1.0/24 and network device is eth0. -r for range of network. So I used following syntax to get result.

```
# netdiscover -i eth0 -r 192.168.1.0/24
```

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x  
(root@kali)~  
# netdiscover -i eth0 -r 192.168.1.0/24
```

When you hit enter the result will display on the screen.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
Currently scanning: Finished! | Screen View: Unique Hosts  
60 Captured ARP Req/Rep packets, from 16 hosts. Total size: 3600  
+-----+-----+-----+-----+-----+  
IP           At MAC Address    Count  Len  MAC Vendor / Hostname  
+-----+-----+-----+-----+-----+  
192.168.1.1   c0:9f:e1:ee:21:ca  37     2220 zte corporation  
192.168.1.3   80:d2:1d:c4:62:23   1       60 AzureWave Technology Inc.  
192.168.1.6   c0:e4:34:ac:1a:a3   1       60 AzureWave Technology Inc.  
192.168.1.4   5e:7f:5c:bd:01:f8   1       60 Unknown vendor  
192.168.1.2   08:11:96:e9:ad:28   1       60 Intel Corporate  
192.168.1.13  38:00:25:e4:eb:4d   1       60 Intel Corporate  
192.168.1.8   34:c9:3d:d7:90:b5   1       60 Intel Corporate  
192.168.1.16  d8:c0:a6:ee:2e:bd   1       60 AzureWave Technology Inc.  
192.168.1.9   08:11:96:e9:ad:28   1       60 Intel Corporate  
192.168.1.12  f8:e4:e3:a9:9b:b5   1       60 Intel Corporate  
192.168.1.24  7e:15:cb:1c:60:ea   1       60 Unknown vendor  
192.168.1.18  d8:3b:bf:5d:e5:e9   1       60 Intel Corporate  
192.168.1.20  9c:29:76:14:c5:67   9       540 Intel Corporate  
192.168.1.33  f8:e4:e3:a9:d7:88   1       60 Intel Corporate  
192.168.1.34  76:da:d6:53:79:60   1       60 Unknown vendor
```