

# R V COLLEGE OF ENGINEERING

Name: HASIFA A S    USN: 1RV18IS016    Dept/Lab: ISE/CSDF    Expt No.: 08 b  
Date: 14/12/2021    Title: INFORMATION GATHERING TOOL

---

## b. NETDISCOVER

### INTRODUCTION

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(ncurse). This can be used in the first phases of a pentest where you have access to a network.

Netdiscover is a tool which is used to gather all the important information about the network. It gathers information about the connected clients and the router. As for the connected clients, we'll be able to know their IP, MAC address and the operating system, as well as the ports that they have open in their devices. As for the router, it will help us to know the manufacturer of the router. Then we'll be able to look for vulnerabilities that we can use against the clients or against the router if we are trying to hack them.

Netdiscover is a quicker and simplest program to use, but it doesn't show very detailed information about the target clients. It'll only show their IP address, their MAC address, and sometimes the hardware manufacturer.

**Objectives** - To use a simple ARP scanner which can be used to enumerate hosts.

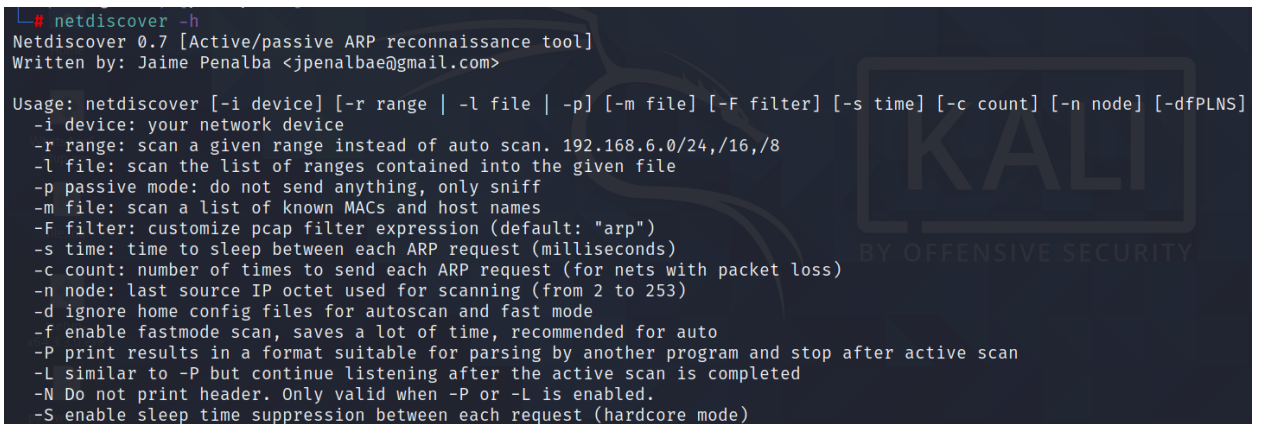
### EXECUTION STEPS

#### 1. Installing Netdiscover from a package

Command - *sudo apt install netdiscover*

#### 2. Basic Usage

Syntax - *netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]*



```
└─$ netdiscover -h
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 active 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.
-S enable sleep time suppression between each request (hardcore mode)
```

## Example cases

### 1. To scan a specific range (-r)

Syntax - `netdiscover -r <range>`

Command - `netdiscover -r 192.168.1.0/24`

```
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	c8:5a:9f:bc:0d:98	3	180	zte corporation
192.168.1.7	14:2d:27:e6:2e:6b	1	60	Hon Hai Precision Ind. Co.,Ltd.
192.168.1.4	a8:34:6a:bd:0c:de	1	60	Samsung Electronics Co.,Ltd
192.168.1.3	70:5e:55:b5:c0:3f	1	60	Realme Chongqing MobileTelecommunications Corp Ltd

### 2. To scan multiple ranges from a file (-l)

Syntax - `netdiscover -l <file containing ranges>`

Command - `netdiscover -l ranges`

```
Currently scanning: Finished! | 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
192.168.1.7	14:2d:27:e6:2e:6b	1	60	Hon Hai Precision Ind. Co.,Ltd.
192.168.1.1	c8:5a:9f:bc:0d:98	7	420	zte corporation
192.168.1.8	86:4b:09:d0:c5:a7	1	60	Unknown vendor
192.168.1.3	70:5e:55:b5:c0:3f	1	60	Realme Chongqing MobileTelecommunications Corp Ltd

```
(root@kali)-[/home/kali]
# cat ranges
192.168.1.0/24
10.0.2.0/24
```

### 3. Passive Scanning (-p)

Syntax - `netdiscover -p -r <range, optional>`

Command - `netdiscover -p -r 192.168.1.0/24`

```
Currently scanning: (passive) | Screen View: Unique Hosts
14 Captured ARP Req/Rep packets, from 1 hosts. Total size: 840
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	c8:5a:9f:bc:0d:98	14	840	zte corporation

#### a. Parsable outputs

A parsable output option can be used to pipe it to a file.

Syntax - `netdiscover -P<parsable> -N<commit headers>`

```
(root@kali)-[/home/kali]
# netdiscover -r 192.168.1.0/24 -PN
-- Active scan completed, 0 Hosts found.
```

## CONCLUSION

1. Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.
2. Netdiscover can also be used to inspect your network ARP traffic, or find network addresses using auto scan mode, which will scan for common local networks.
3. Netdiscover uses the OUI table to show the vendor of the each MAC address discovered and is very useful for security checks or in pentests.

## REFERENCES

1. Netdiscover - <https://www.kali.org/tools/netdiscover/>
2. Netdiscover - Live host Identification - <https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/>
3. Netdiscover - <https://www.javatpoint.com/netdiscover>