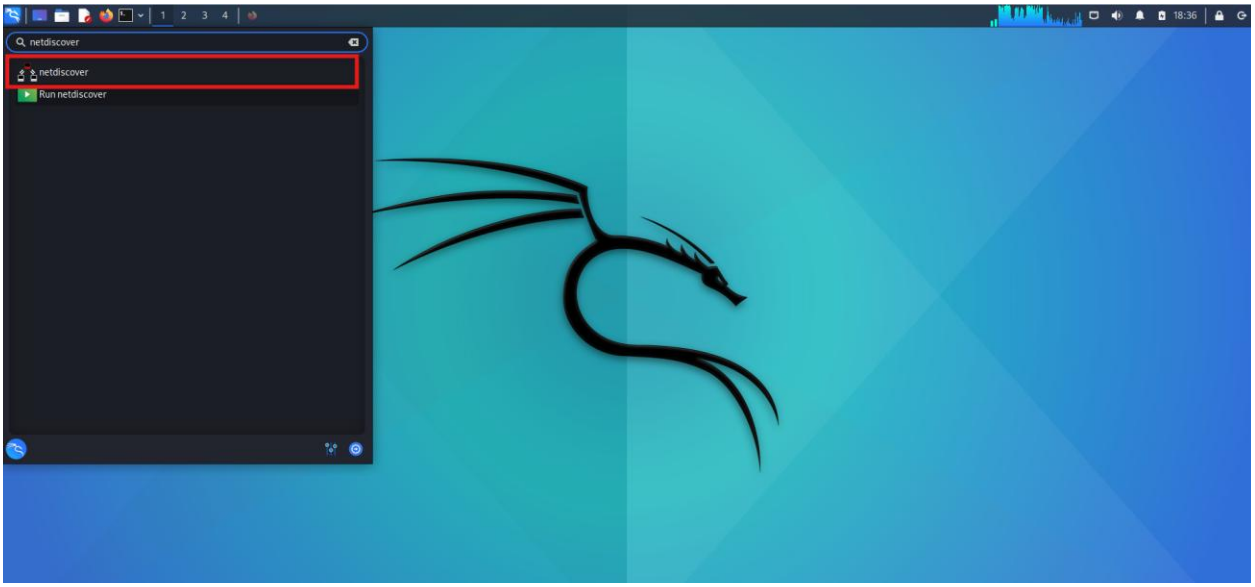
Netdiscover

The 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.

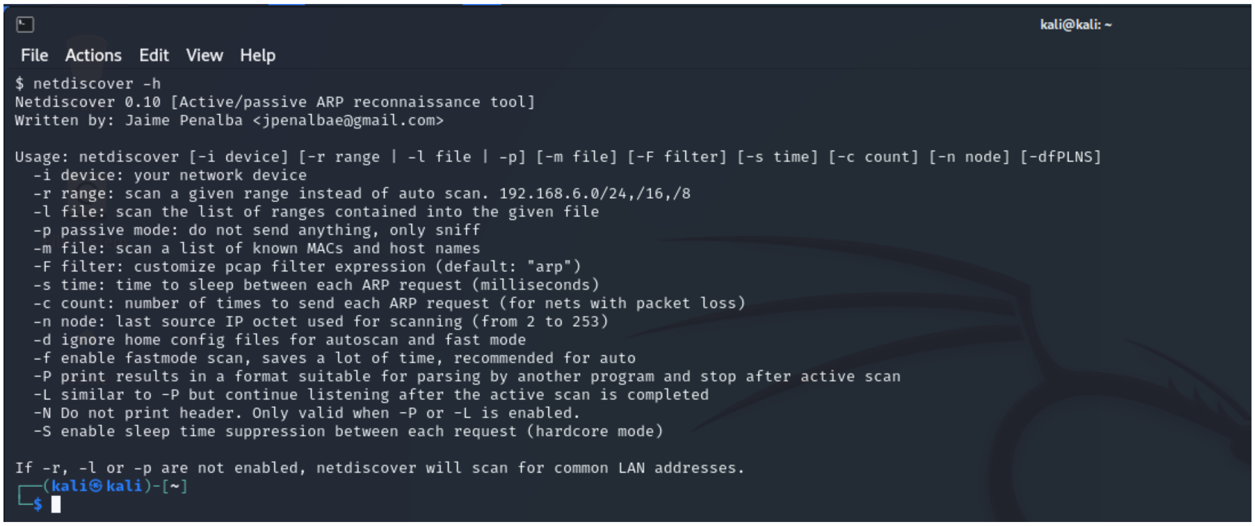
The **netdiscover** is a quicker and simplest program to use, but it doesn't show very detailed information about the target clients. It'll only show us their IP address, their MAC address, and sometimes the hardware manufacturer. We're going to use it by typing netdiscover, then we are going to use -r, and then we are going to specify the range, which can be any range we want. Looking at the IP (which is 10.0.2.1) tells us which network we are in. We want to discover all the clients that are in this network, so we're going to try and see if there is a device in 10.0.2.1. Then we're going to try **12, 13, 14, 15, 16**, up to **254**, that's the end of the range. So, to specify a whole range, we can write /24. That means we want **10.0.2.1**, and then this IP is just going to increase up to **10.0.2.254**, which is the end of the IP range in the network

Commands:-

1. Netdiscover is pre insatlled in Linux distribution we can run it by searching it in the start menu.



2. -h will displays all the flags for the netdiscover command.

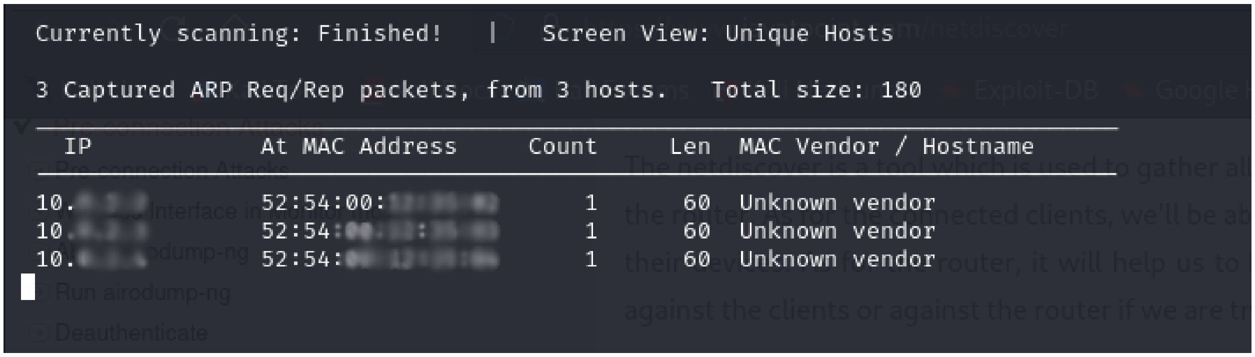


```
$ netdiscover -h
Netdiscover 0.10 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

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)

If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.
┌──(kali㉿kali)-[~]
└─$ 
```

3. Now type your ip with -r in order to find host in your network.



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.[redacted]   52:54:00:[redacted]      1      60  Unknown vendor
 10.[redacted]   52:54:[redacted]         1      60  Unknown vendor
 10.[redacted]   52:54:[redacted]         1      60  Unknown vendor
```