1. Respond to the following questions:

i. Which protocol uses the netdiscover command to find out IP addresses in a network?

ARP protocol

ii. How many UDP, TCP ports exist in total?

65,353 UDP ports and 65,535 TCP ports

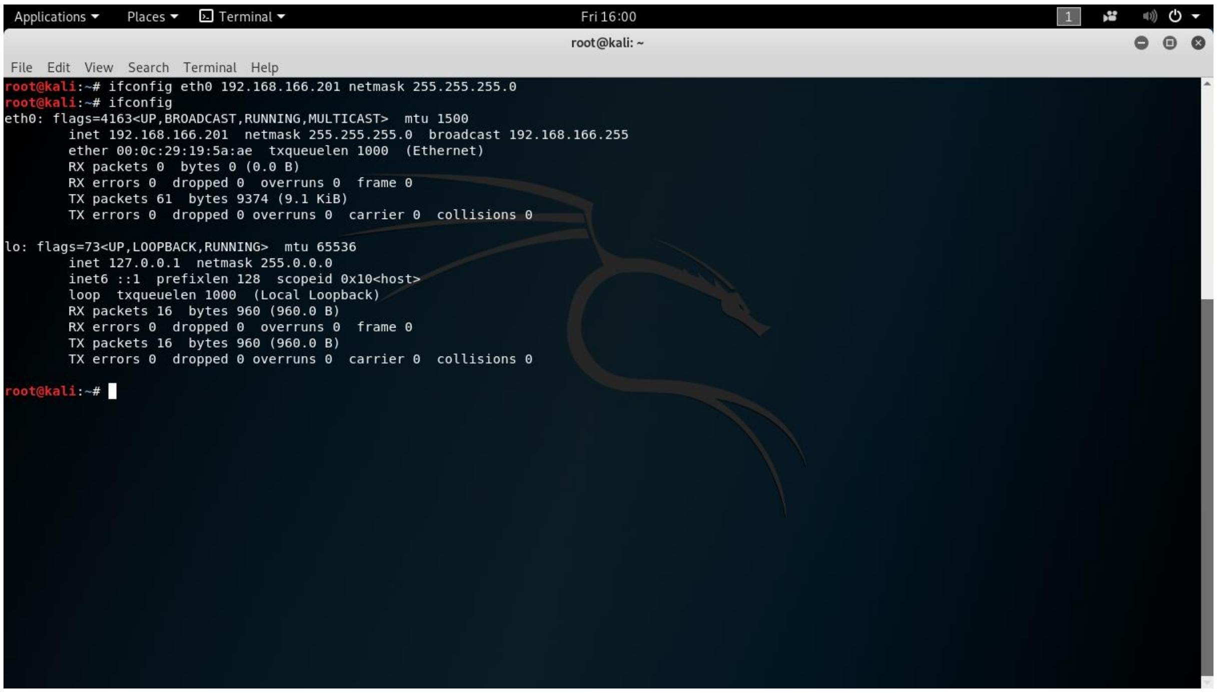
iii. The port 22 is the port assigned to the SSH service, would be possible to assign a different port number to the SSH?

Yes, it is possible to assign a different port number to the SSH service

iv. How many bits has a MAC address?

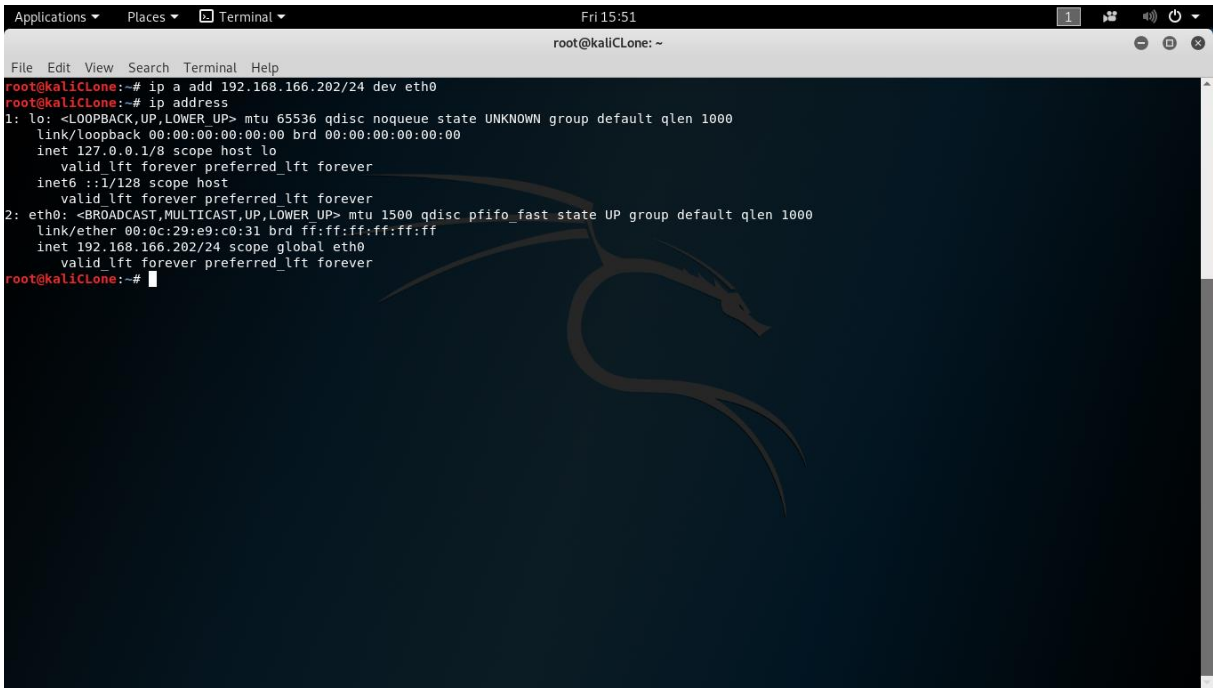
A MAC address is made up of 48 bits

2. Assign the 192.168.166.201/24 to Kali host by using the ifconfig command. Show screenshot.



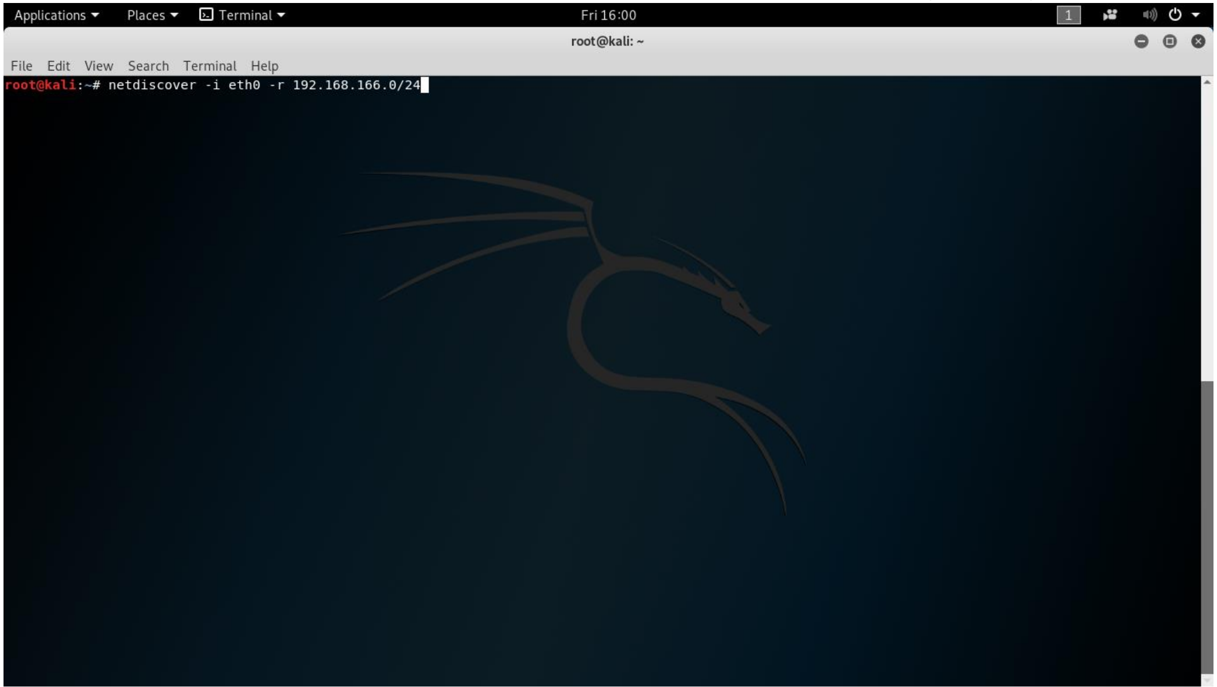
```
root@kali:~# ifconfig eth0 192.168.166.201 netmask 255.255.255.0
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.166.201  netmask 255.255.255.0  broadcast 192.168.166.255
        ether 00:0c:29:19:5a:ae  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 61  bytes 9374 (9.1 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 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

3. Assign the 192.168.166.202/24 to KaliClone host by using the ip command. Show screenshot.

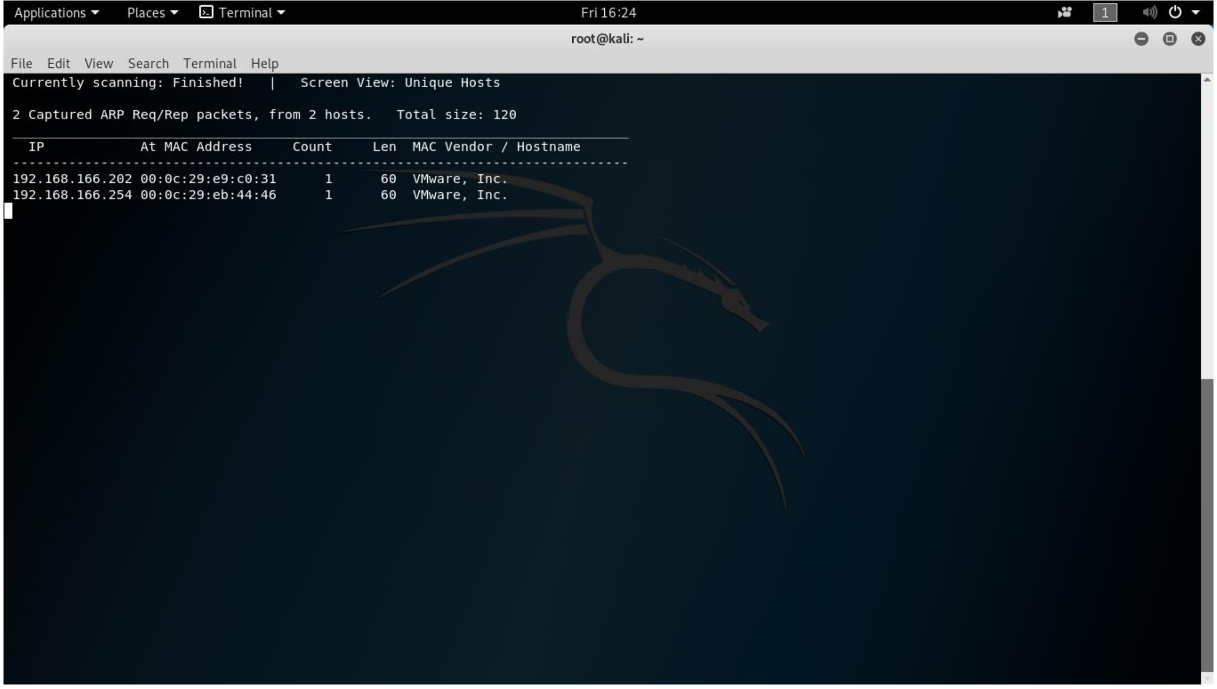


```
root@kaliCLone:~# ip a add 192.168.166.202/24 dev eth0
root@kaliCLone:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:e9:c0:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.166.202/24 scope global eth0
       valid_lft forever preferred_lft forever
root@kaliCLone:~# 
```

4. Attach a screenshot of the netdiscover command specifying the network adapter and the 192.168.166.0 network (make sure all three systems are connected to VMnet2). The screenshot should show the IP addresses of KaliClone and the WS2K3(TW3P0) h



```
root@kali:~# netdiscover -i eth0 -r 192.168.166.0/24
```



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

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.166.202 00:0c:29:e9:c0:31      1      60  VMware, Inc.
192.168.166.254 00:0c:29:eb:44:46      1      60  VMware, Inc.
```

5. Select 5 ports showed with nmap command over the WS2K3(TW3P0) host and explain the purposes.

Port	Service	Purpose
21/tcp	ftp	Allows users to exchange files
25/tcp	smtp	Email transmission used to send and receive mail
42/tcp	nameserver	Translates a host name to an internet address
53/tcp	domain	Naming system for networks
80/tcp	http	Foundation of data communication for the world wide web

6. Is there any way to use nmap on a Windows system or other Linux distributions besides Kali? If so, what would be the installation process in Windows and Linux systems? Check nmap.org for more information.

Yes, for windows there is a self-installer which is typically what most Nmap users choose to do since, as the name states, installs itself. Another option is to do the command-line zip binaries installation in which one would download the zip, uncompress the file and install the Npcap packet capture library, Microsoft Visual C++ 2013 Redistributed Package, and execute the instructions given in the section called "Executing Nmap on Windows", etc.

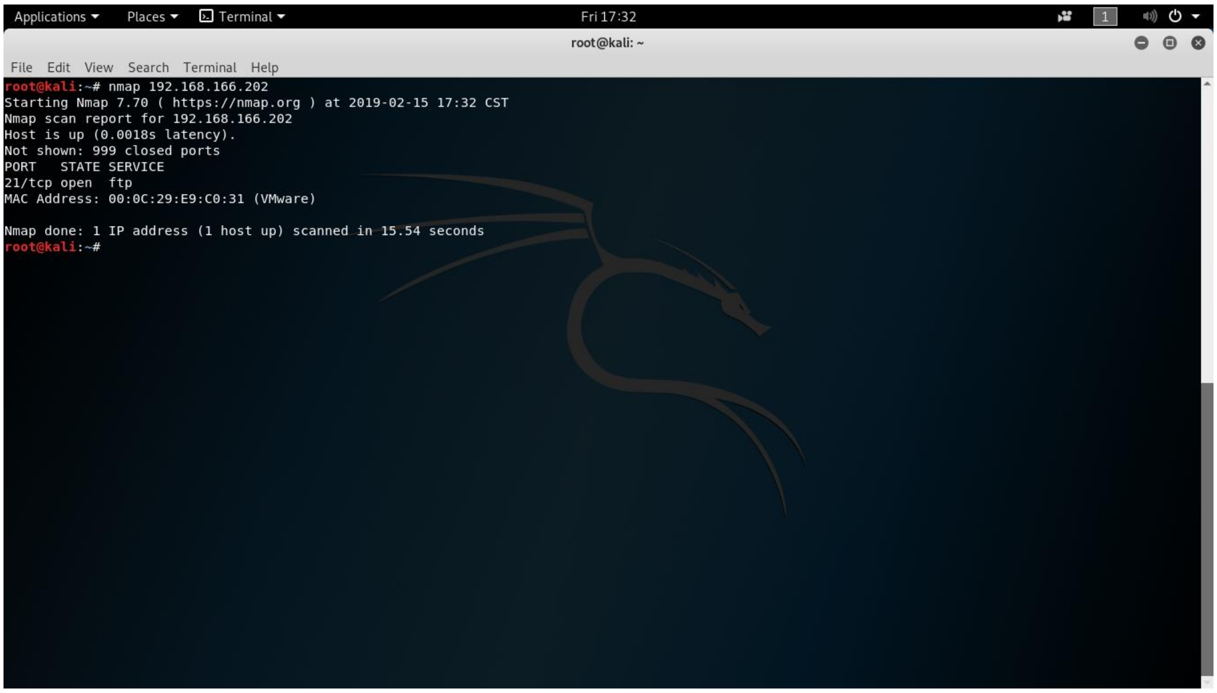
For Linux distributions besides Kali, RPM-based Distribution installation is quite easy, given the proper URL then Nmap will download and install itself.
Example installing Nmap from binary RPMs: # rpm -vhU https://nmap.org/dist/nmap-4.68=1.i386.rpm
Example building and installing Nmap from source RPMs: > rpmbuild –rebuild https://nmap.org/dist/nmap-4.68-1.src.rpm

For Yum based applications, users will use them yum command which manages software installation and updates from central RPM repositories.

For Debian Linux and Derivatives the proper upgrade/install command is apt-get install nmap

etc, etc.

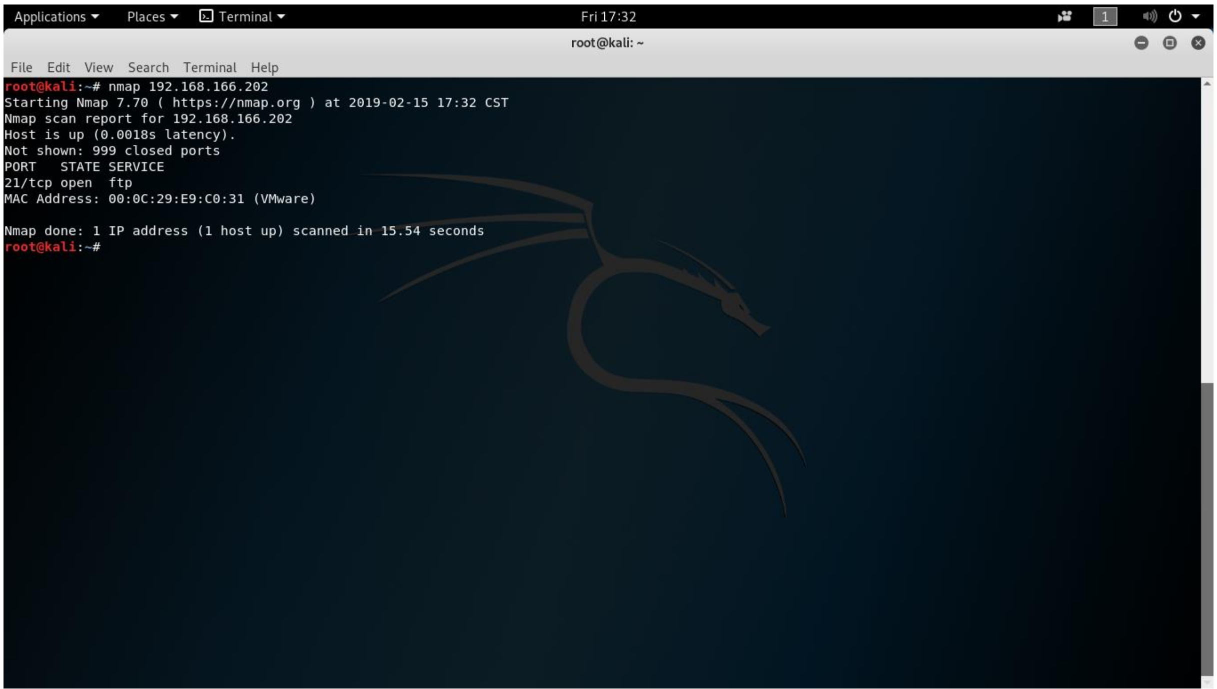
7. Open FTP port on 'Kali Clone' host (you might need to connect to the internet to install the service), from 'Kali' host execute:
# nmap 192.168.166.202
Which port number is assigned to the FTP service? Submit screenshot.



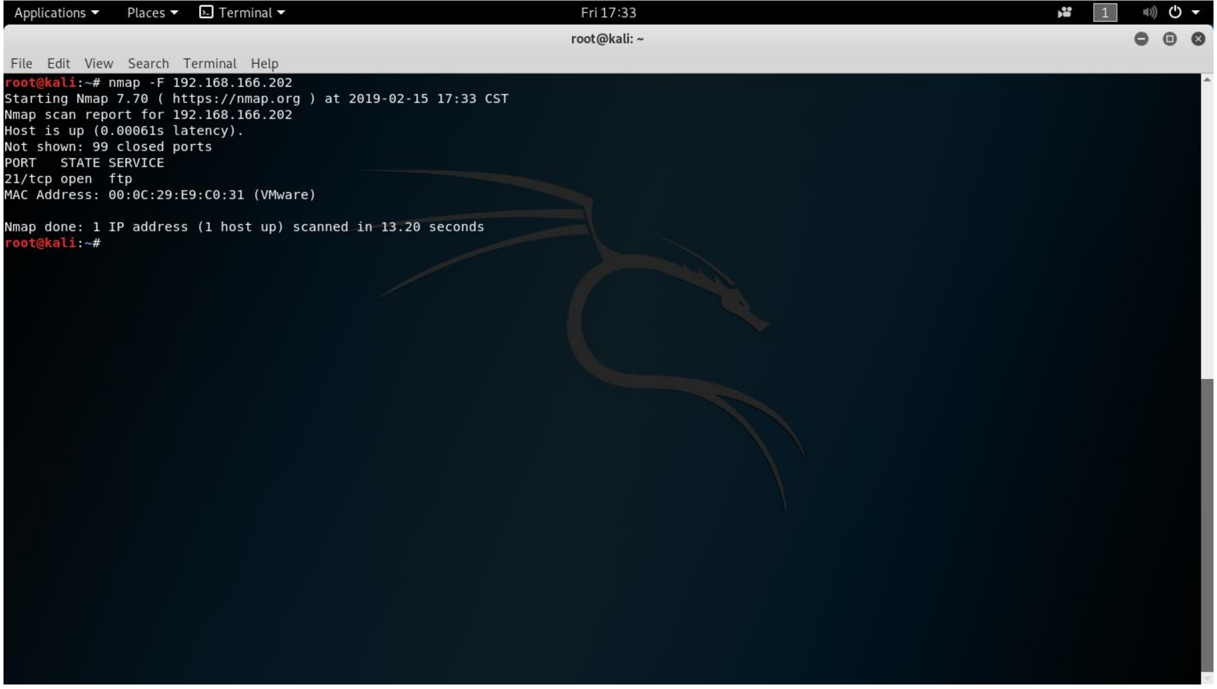
```
root@kali:~# nmap 192.168.166.202
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-15 17:32 CST
Nmap scan report for 192.168.166.202
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:E9:C0:31 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
root@kali:~#
```

Port number 21 is assigned to the FTP service

8. Use the ‘-F’ option to obtain similar results as the previous question. Compare the execution time. Which one was executed faster, why? Provide a screenshot showing clearly the execution time for both commands.



```
root@kali:~# nmap 192.168.166.202
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-15 17:32 CST
Nmap scan report for 192.168.166.202
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:E9:C0:31 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
root@kali:~#
```



```
root@kali:~# nmap -F 192.168.166.202
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-15 17:33 CST
Nmap scan report for 192.168.166.202
Host is up (0.00061s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:E9:C0:31 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
root@kali:~#
```

The nmap -F option executed faster because it scans for 100 ports rather than the nmap which scans for 1000 ports.