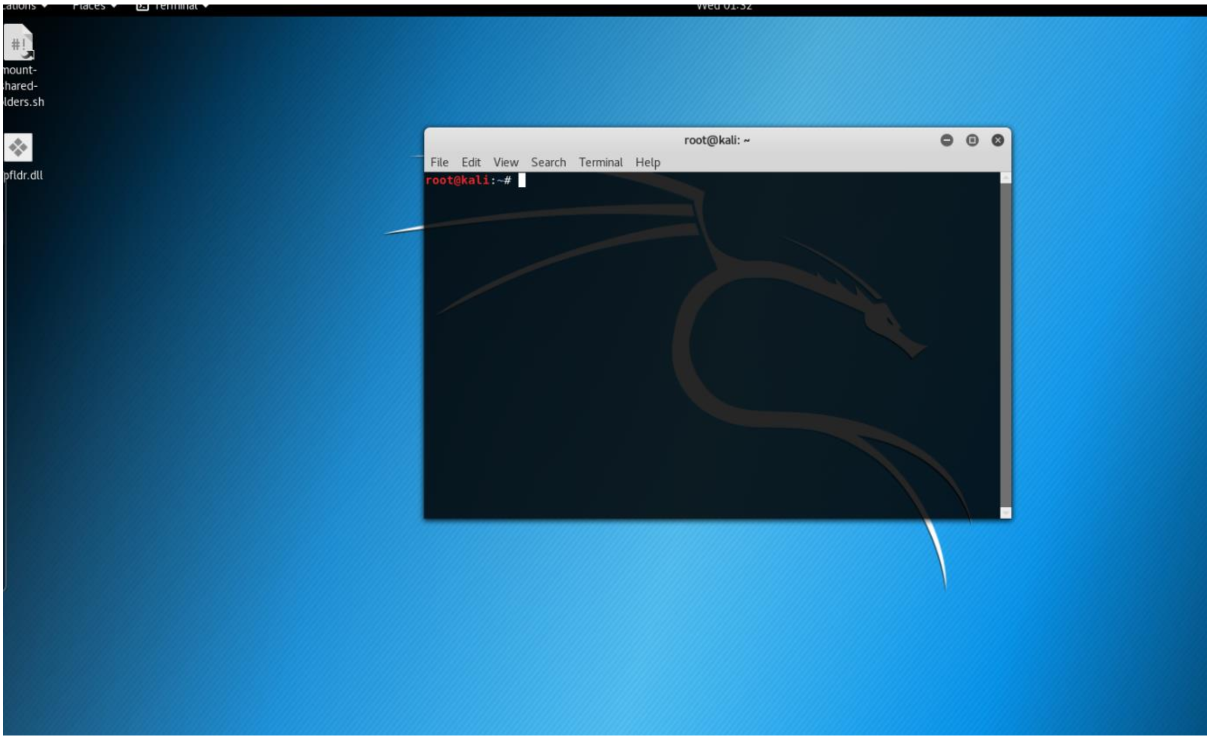
Project -Scanning Network

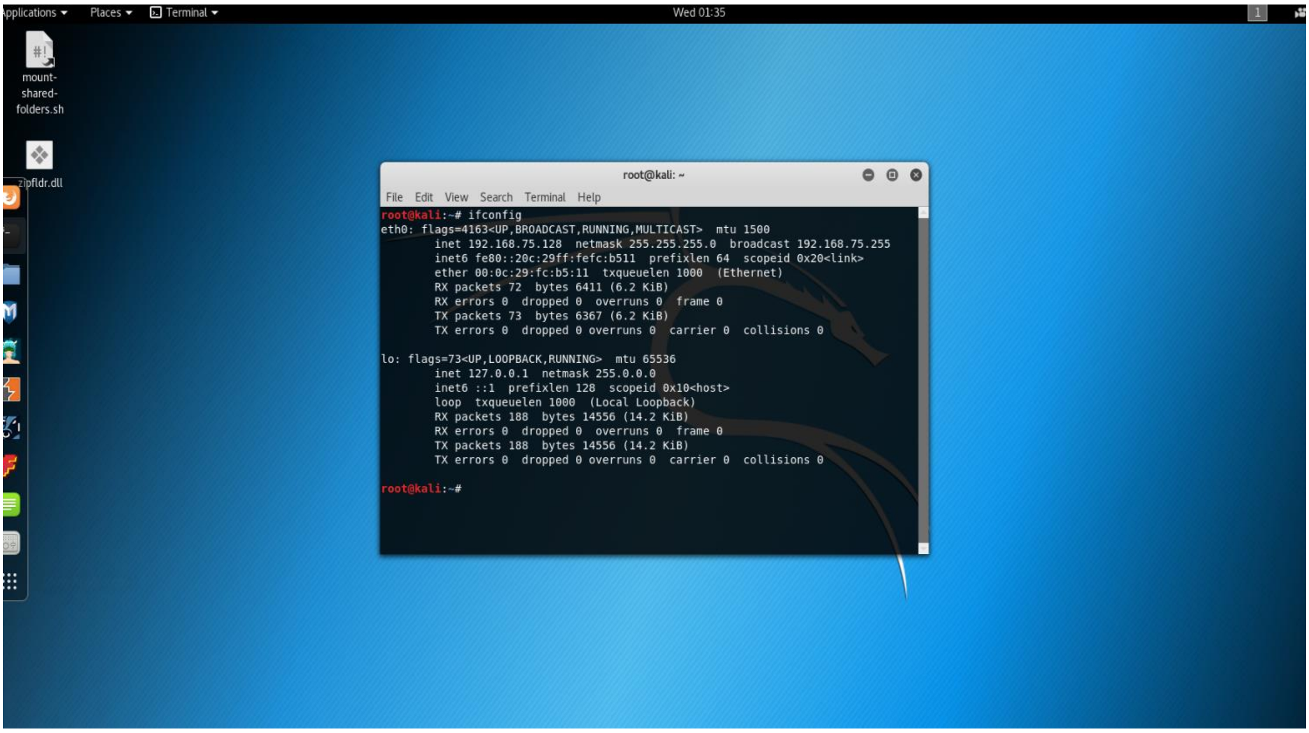
Step-1 Open linux

Step 2- open terminal



```
root@kali:~#
```

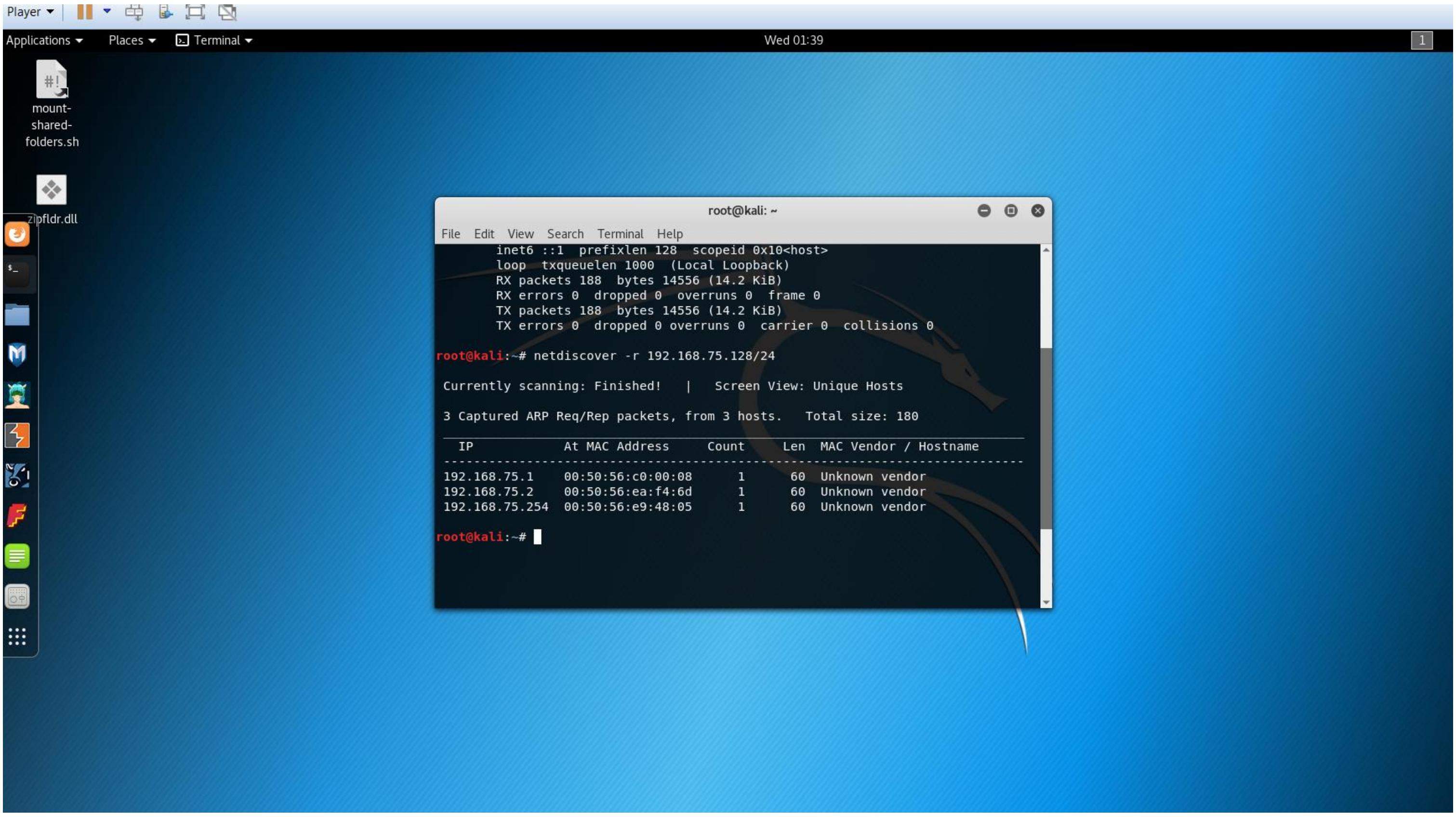
Step-3 type ifconfig to know the ip address



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.75.128  netmask 255.255.255.0  broadcast 192.168.75.255
        inet6 fe80::20c:29ff:fefc:b511  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:fc:b5:11  txqueuelen 1000  (Ethernet)
        RX packets 72  bytes 6411 (6.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 73  bytes 6367 (6.2 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 188  bytes 14556 (14.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 188  bytes 14556 (14.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Step 4- copy the ip address and then type

netdiscover -r ip(copied)/24

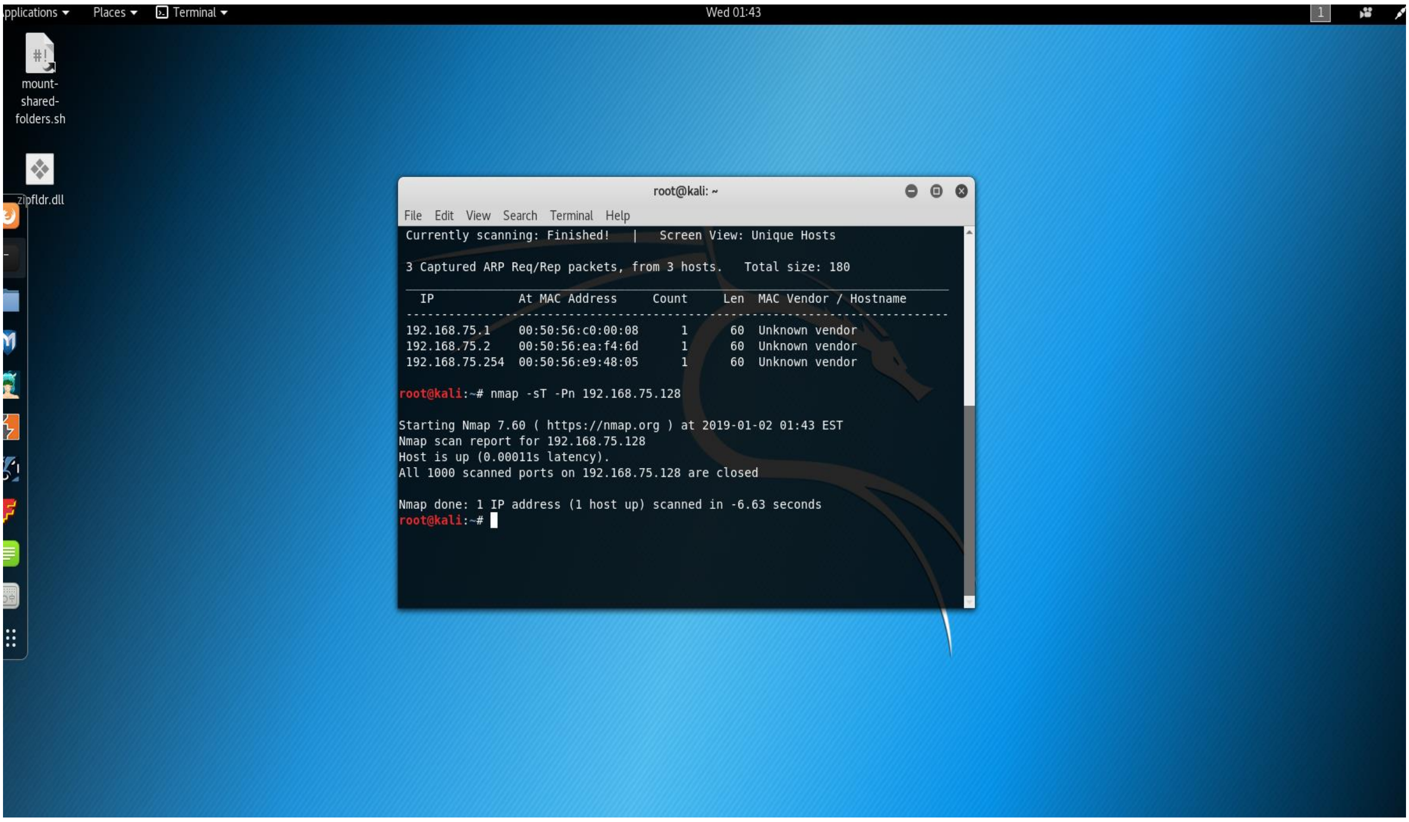


```
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 188  bytes 14556 (14.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 188  bytes 14556 (14.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# netdiscover -r 192.168.75.128/24

 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
 -----------------------------------------------------------------------------
 192.168.75.1    00:50:56:c0:00:08      1      60  Unknown vendor
 192.168.75.2    00:50:56:ea:f4:6d      1      60  Unknown vendor
 192.168.75.254  00:50:56:e9:48:05      1      60  Unknown vendor

root@kali:~# 
```

Step-5 Type the command

nmap -sT -Pn ip address

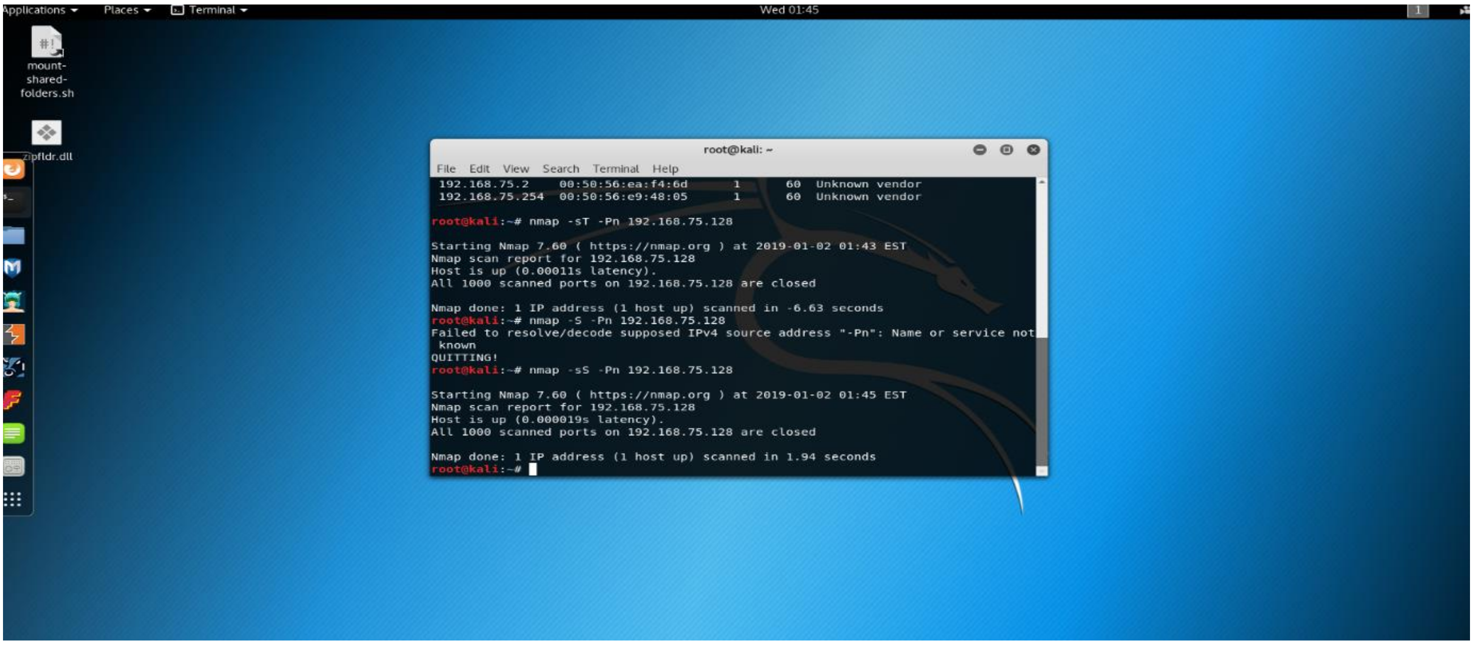
(TCP connect scan)



```
 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
 -----------------------------------------------------------------------------
 192.168.75.1    00:50:56:c0:00:08      1      60  Unknown vendor
 192.168.75.2    00:50:56:ea:f4:6d      1      60  Unknown vendor
 192.168.75.254  00:50:56:e9:48:05      1      60  Unknown vendor

root@kali:~# nmap -sT -Pn 192.168.75.128

Starting Nmap 7.60 ( https://nmap.org ) at 2019-01-02 01:43 EST
Nmap scan report for 192.168.75.128
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.75.128 are closed

Nmap done: 1 IP address (1 host up) scanned in -6.63 seconds
root@kali:~#
```

Step 6- Type command in terminal

nmap -S -Pn ip address

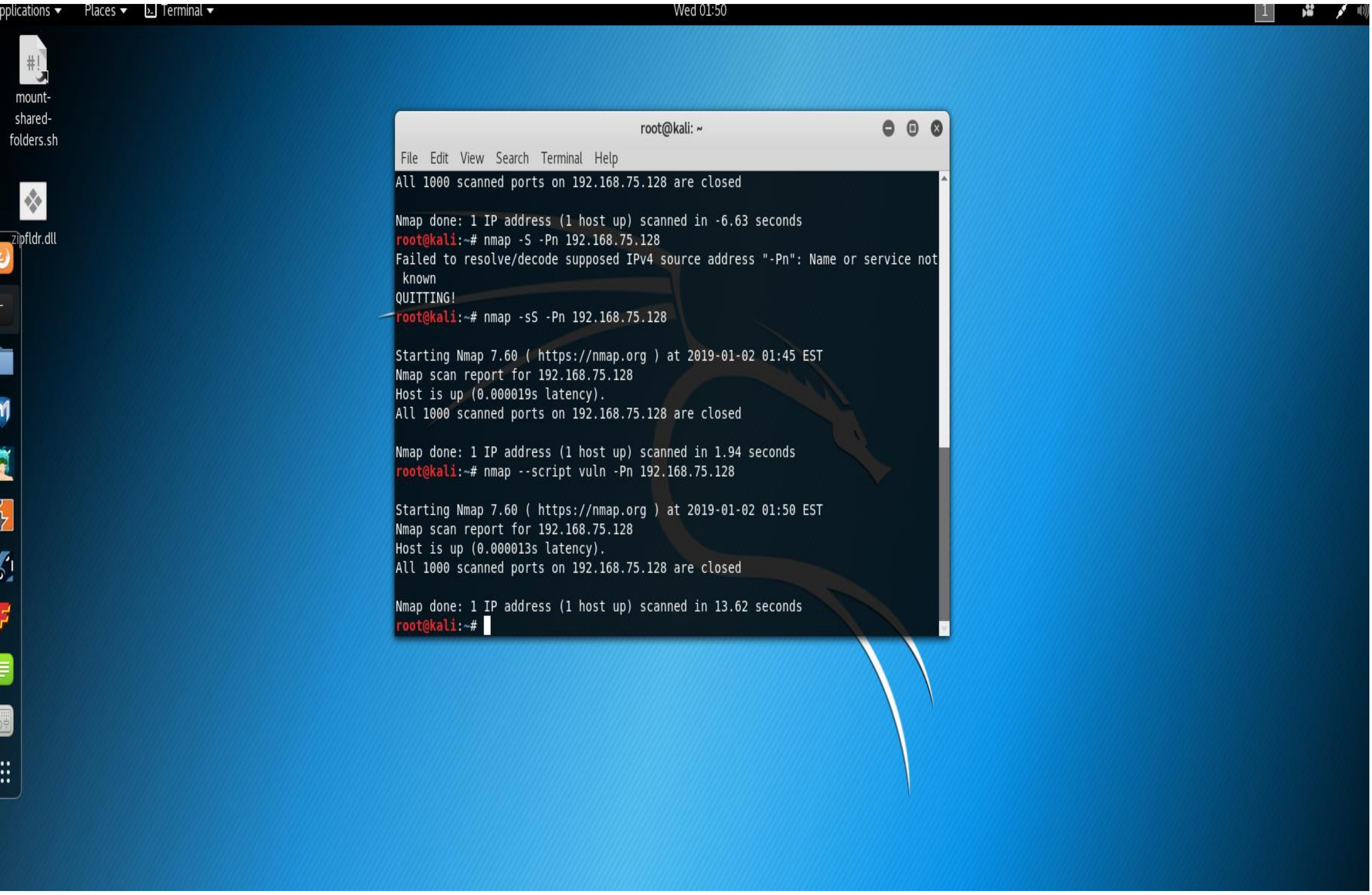


```
 192.168.75.2    00:50:56:ea:f4:6d      1       60  Unknown vendor
 192.168.75.254  00:50:56:e9:48:05      1       60  Unknown vendor

root@kali:~# nmap -sT -Pn 192.168.75.128

Starting Nmap 7.60 ( https://nmap.org ) at 2019-01-02 01:43 EST
Nmap scan report for 192.168.75.128
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.75.128 are closed

Nmap done: 1 IP address (1 host up) scanned in -6.63 seconds
root@kali:~# nmap -S -Pn 192.168.75.128
Failed to resolve/decode supposed IPv4 source address "-Pn": Name or service not
 known
QUITTING!
root@kali:~# nmap -sS -Pn 192.168.75.128

Starting Nmap 7.60 ( https://nmap.org ) at 2019-01-02 01:45 EST
Nmap scan report for 192.168.75.128
Host is up (0.000019s latency).
All 1000 scanned ports on 192.168.75.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
root@kali:~# 
```

Step -7 Vulnerability Scanning

Type the command in terminal

nmap - -script vuln -Pn ip address



```
All 1000 scanned ports on 192.168.75.128 are closed

Nmap done: 1 IP address (1 host up) scanned in -6.63 seconds
root@kali:~# nmap -S -Pn 192.168.75.128
Failed to resolve/decode supposed IPv4 source address "-Pn": Name or service not
 known
QUITTING!
root@kali:~# nmap -sS -Pn 192.168.75.128

Starting Nmap 7.60 ( https://nmap.org ) at 2019-01-02 01:45 EST
Nmap scan report for 192.168.75.128
Host is up (0.000019s latency).
All 1000 scanned ports on 192.168.75.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
root@kali:~# nmap --script vuln -Pn 192.168.75.128

Starting Nmap 7.60 ( https://nmap.org ) at 2019-01-02 01:50 EST
Nmap scan report for 192.168.75.128
Host is up (0.000013s latency).
All 1000 scanned ports on 192.168.75.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
root@kali:~# 
```