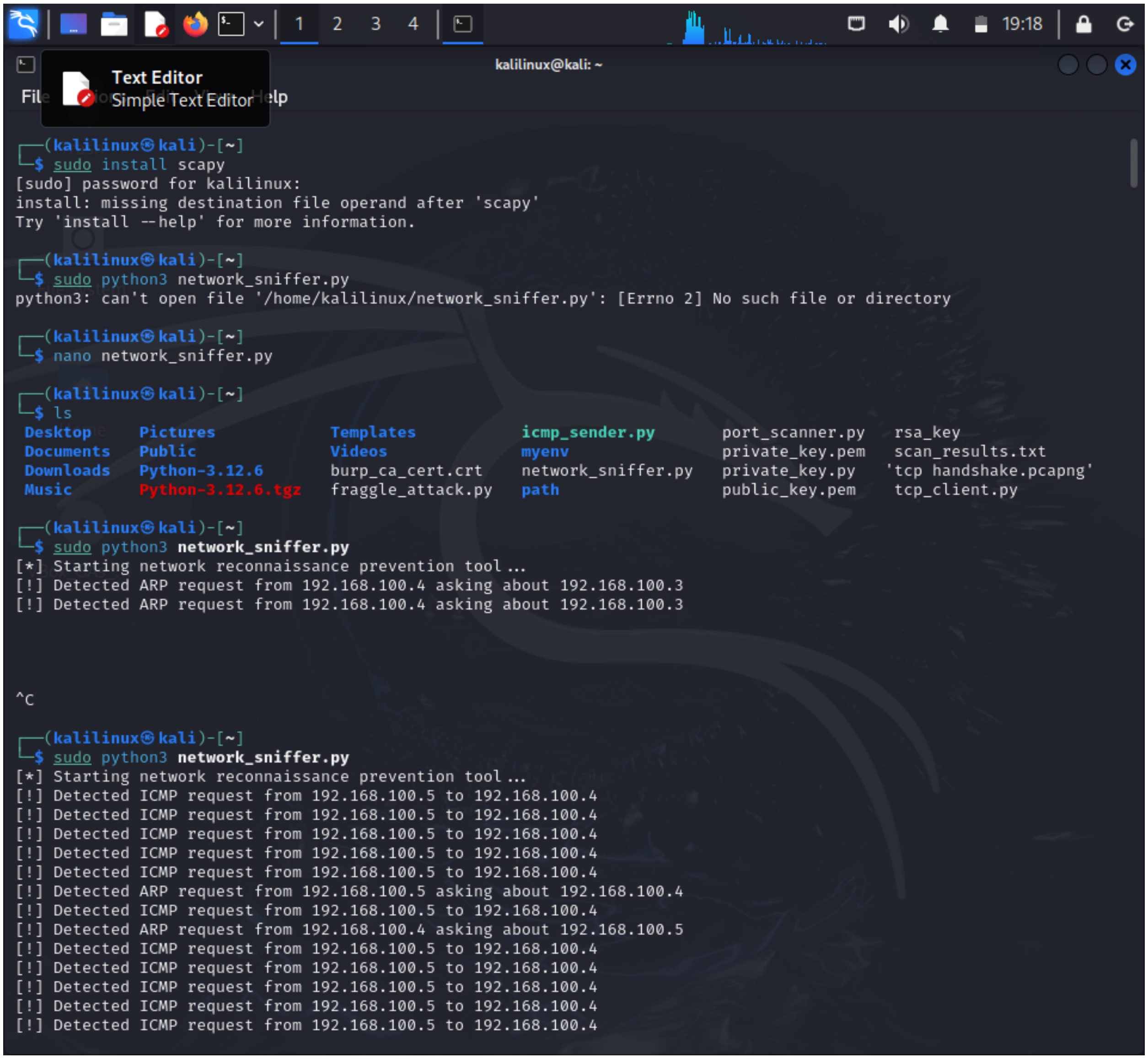
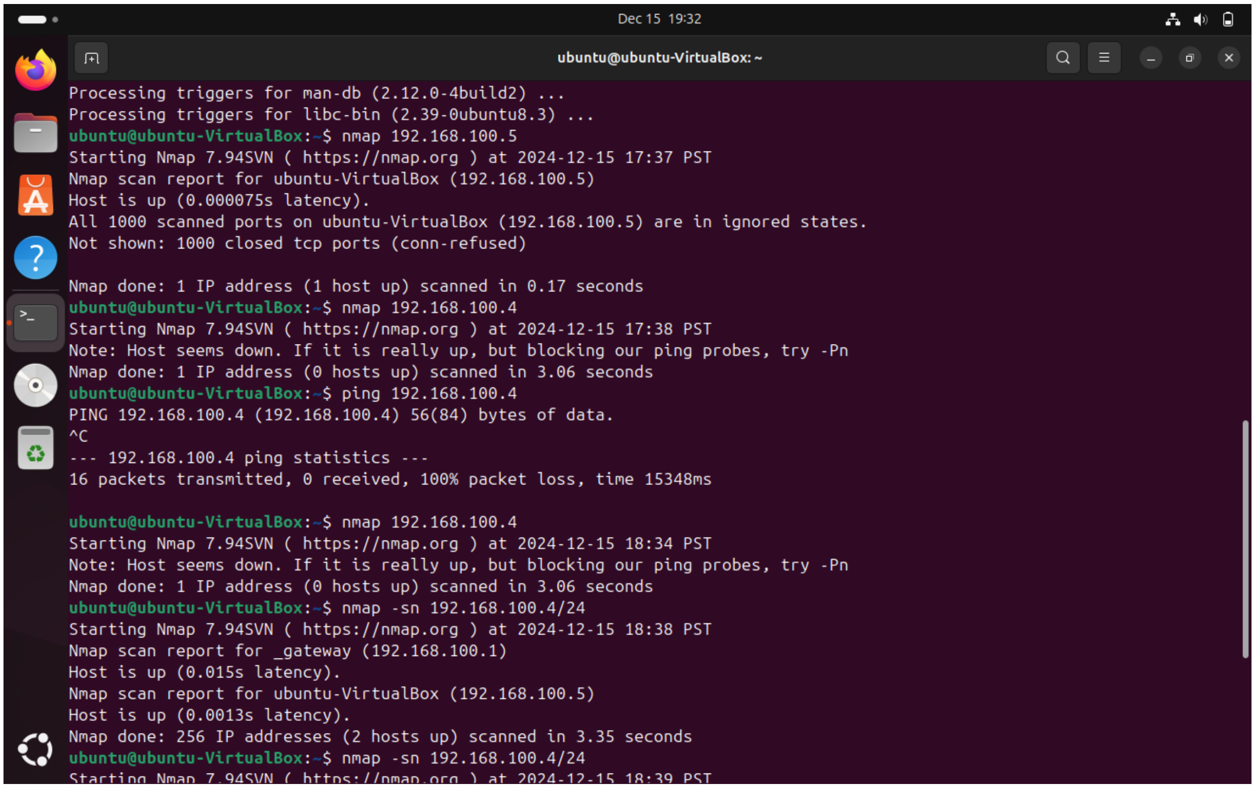
CYB 552 - Detecting and Blocking Network Reconnaissance

Attacker vm- kali Linux , ip address – 192.168.100.4

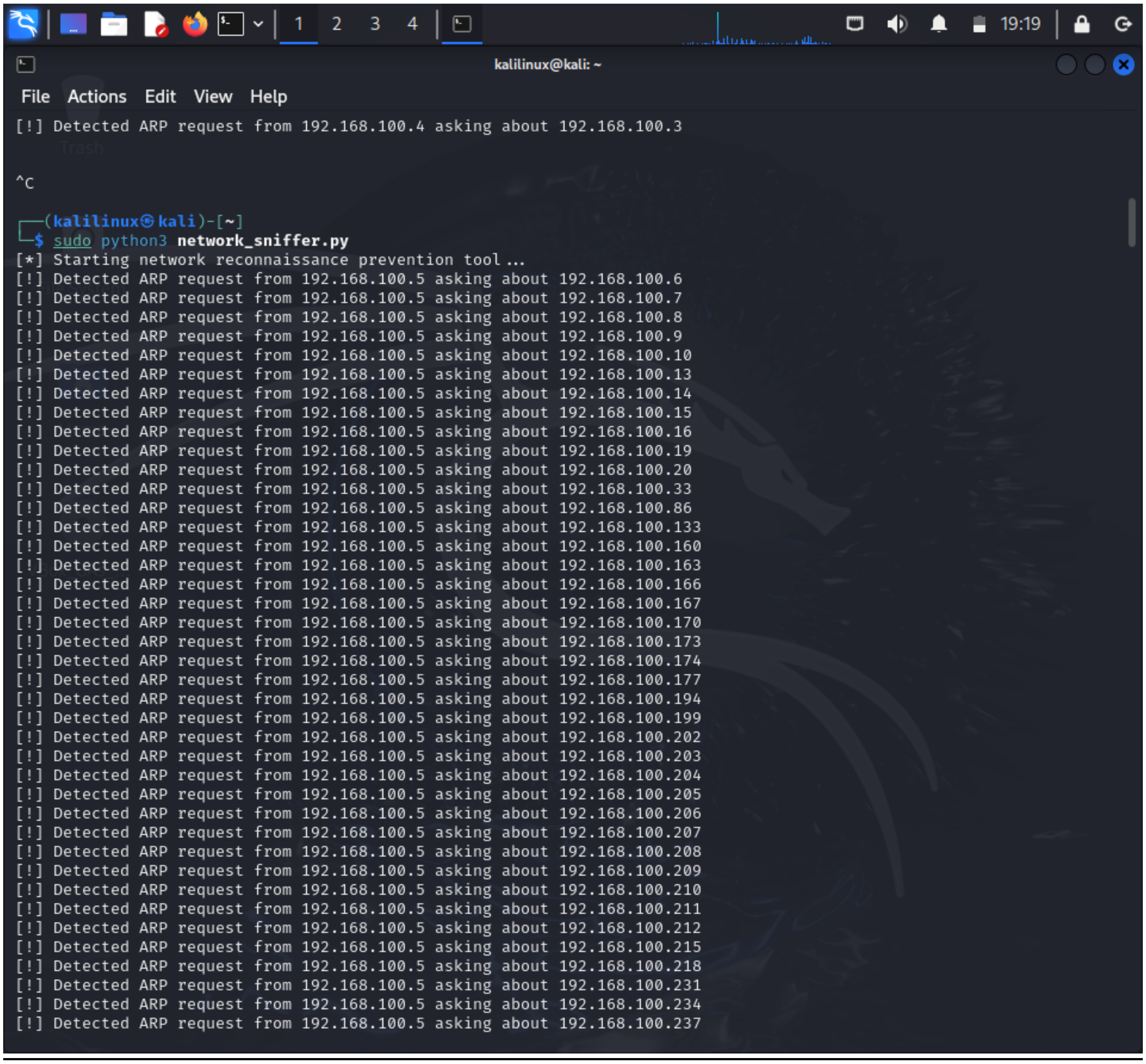
Target vm – Ubuntu , ip address -192.168.100.5



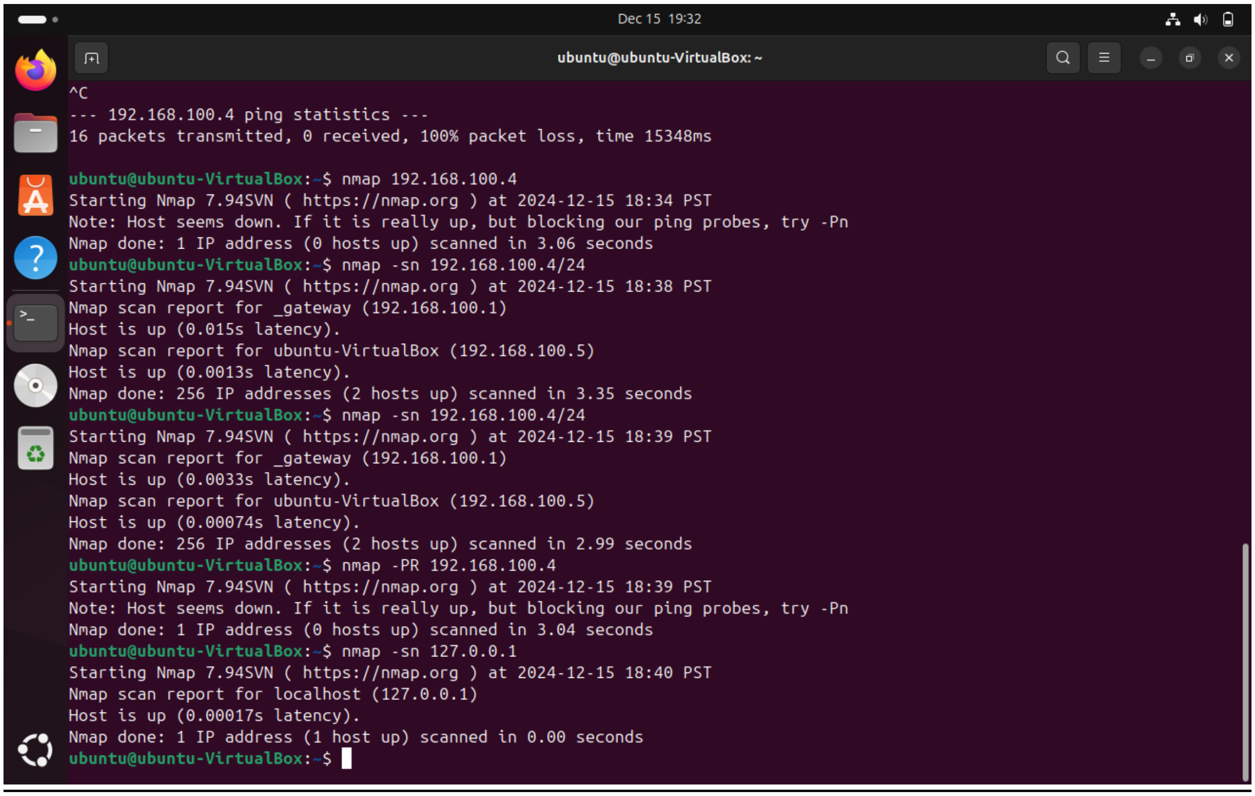
```
┌──(kalilinux㉿kali)-[~]
└─$ sudo install scapy
[sudo] password for kalilinux:
install: missing destination file operand after 'scapy'
Try 'install --help' for more information.

┌──(kalilinux㉿kali)-[~]
└─$ sudo python3 network_sniffer.py
python3: can't open file '/home/kalilinux/network_sniffer.py': [Errno 2] No such file or directory

┌──(kalilinux㉿kali)-[~]
└─$ nano network_sniffer.py

┌──(kalilinux㉿kali)-[~]
└─$ ls
 Desktop     Pictures             Templates          icmp_sender.py      port_scanner.py    rsa_key
 Documents   Public               Videos             myenv               private_key.pem    scan_results.txt
 Downloads   Python-3.12.6        burp_ca_cert.crt   network_sniffer.py  private_key.py    'tcp handshake.pcapng'
 Music       Python-3.12.6.tgz    fraggle_attack.py  path                public_key.pem     tcp_client.py

┌──(kalilinux㉿kali)-[~]
└─$ sudo python3 network_sniffer.py
[*] Starting network reconnaissance prevention tool ...
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3



^C

┌──(kalilinux㉿kali)-[~]
└─$ sudo python3 network_sniffer.py
[*] Starting network reconnaissance prevention tool ...
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.5
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
[!] Detected ICMP request from 192.168.100.5 to 192.168.100.4
```



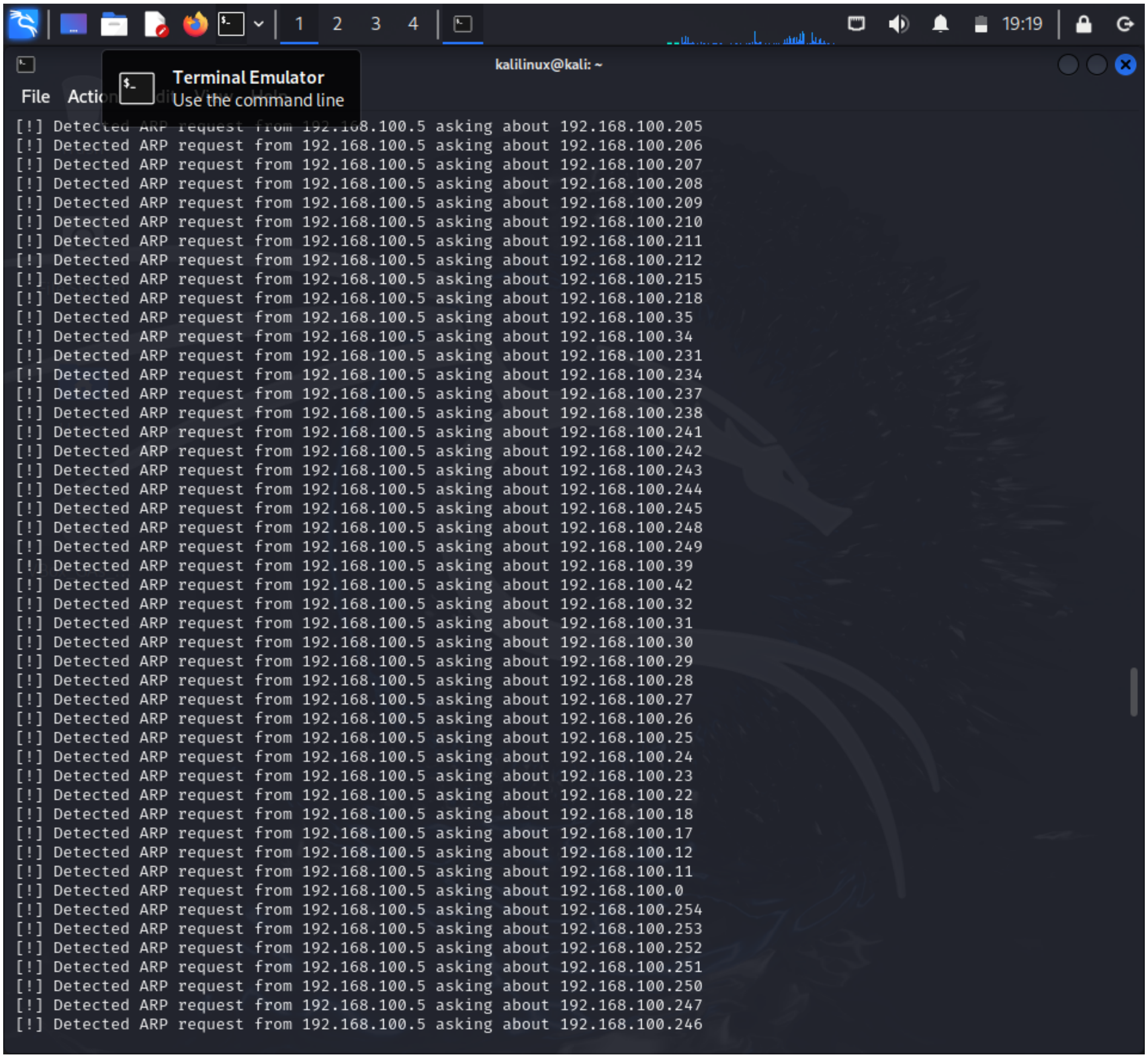
```
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
ubuntu@ubuntu-VirtualBox:~$ nmap 192.168.100.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 17:37 PST
Nmap scan report for ubuntu-VirtualBox (192.168.100.5)
Host is up (0.000075s latency).
All 1000 scanned ports on ubuntu-VirtualBox (192.168.100.5) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 17:38 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
ubuntu@ubuntu-VirtualBox:~$ ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data.
^C
--- 192.168.100.4 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15348ms

ubuntu@ubuntu-VirtualBox:~$ nmap 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:34 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap -sn 192.168.100.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:38 PST
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.015s latency).
Nmap scan report for ubuntu-VirtualBox (192.168.100.5)
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.35 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap -sn 192.168.100.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:39 PST
```



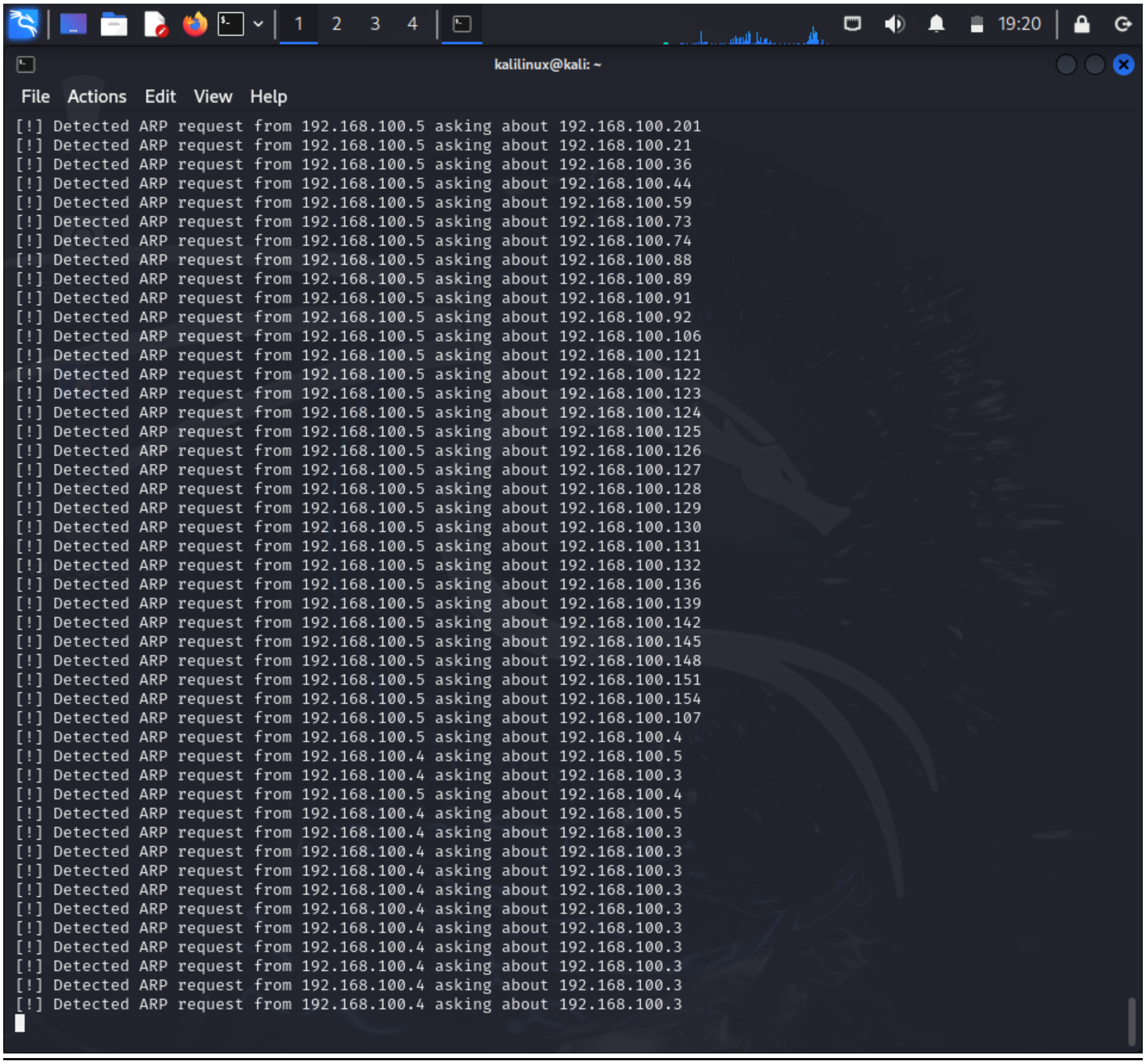
```
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3

^C

┌──(kalilinux㉿kali)-[~]
└─$ sudo python3 network_sniffer.py
[*] Starting network reconnaissance prevention tool ...
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.6
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.7
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.8
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.9
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.10
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.13
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.14
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.15
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.16
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.19
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.20
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.33
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.86
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.133
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.160
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.163
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.166
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.167
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.170
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.173
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.174
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.177
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.194
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.199
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.202
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.203
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.204
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.205
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.206
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.207
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.208
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.209
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.210
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.211
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.212
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.215
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.218
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.231
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.234
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.237
```



```
^C
--- 192.168.100.4 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15348ms

ubuntu@ubuntu-VirtualBox:~$ nmap 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:34 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap -sn 192.168.100.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:38 PST
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.015s latency).
Nmap scan report for ubuntu-VirtualBox (192.168.100.5)
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.35 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap -sn 192.168.100.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:39 PST
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.0033s latency).
Nmap scan report for ubuntu-VirtualBox (192.168.100.5)
Host is up (0.00074s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.99 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap -PR 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:39 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
ubuntu@ubuntu-VirtualBox:~$ nmap -sn 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:40 PST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
ubuntu@ubuntu-VirtualBox:~$
```



```
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.205
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.206
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.207
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.208
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.209
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.210
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.211
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.212
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.215
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.218
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.35
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.34
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.231
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.234
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.237
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.238
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.241
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.242
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.243
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.244
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.245
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.248
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.249
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.39
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.42
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.32
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.31
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.30
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.29
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.28
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.27
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.26
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.25
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.24
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.23
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.22
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.18
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.17
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.12
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.11
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.0
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.254
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.253
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.252
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.251
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.250
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.247
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.246
```



```
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.201
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.21
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.36
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.44
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.59
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.73
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.74
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.88
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.89
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.91
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.92
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.106
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.121
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.122
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.123
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.124
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.125
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.126
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.127
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.128
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.129
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.130
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.131
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.132
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.136
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.139
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.142
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.145
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.148
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.151
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.154
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.107
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.4
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.5
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.5 asking about 192.168.100.4
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.5
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
[!] Detected ARP request from 192.168.100.4 asking about 192.168.100.3
```