NETWORKING AND SYSTEM ADMINISTRATION LAB

ASSIGNMENT

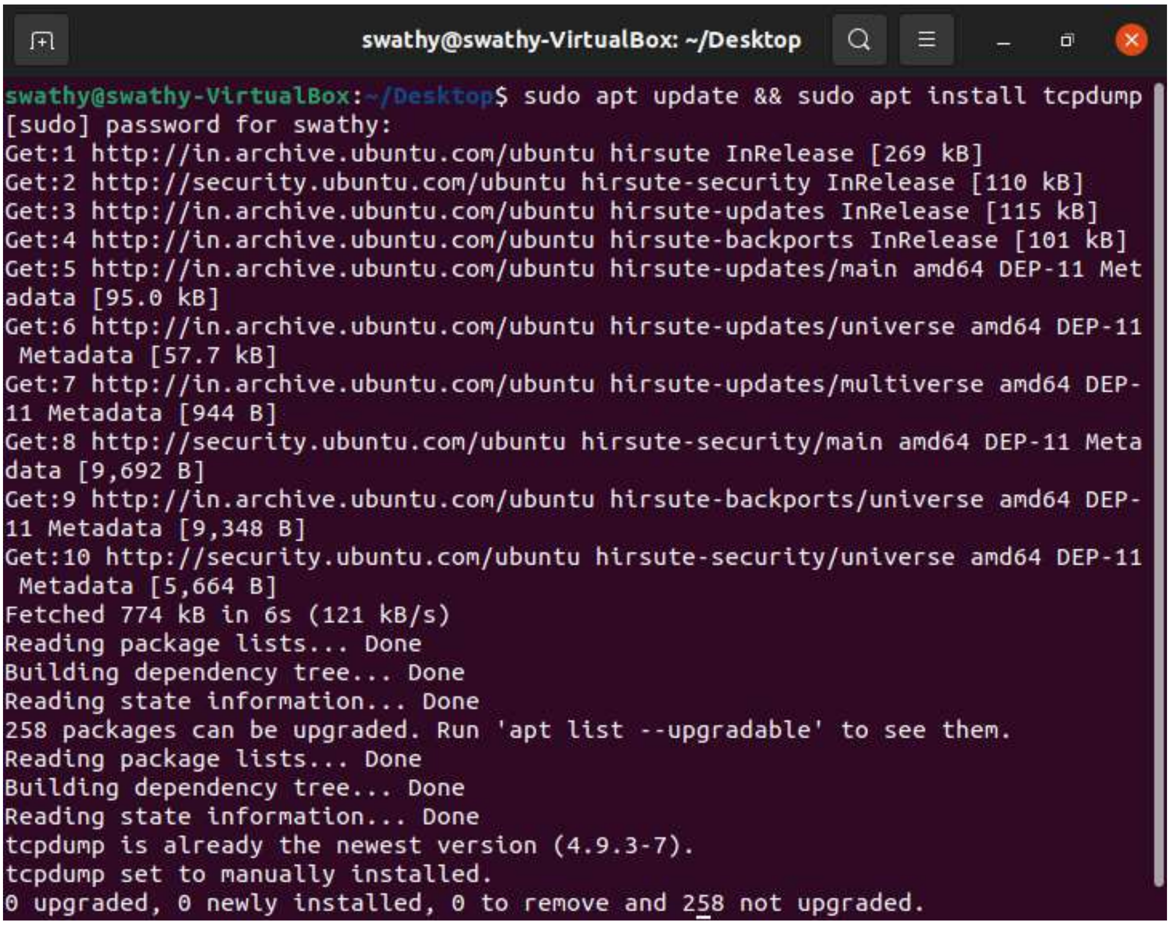
TCPDUMP INSTALLATION

SUBMITTED BY
SWATHY KRISHNA P R
S2 RMCA B
ROLL NO: 31

1. Execute tcpdump and its options on your own system, and submit the output screenshot as a

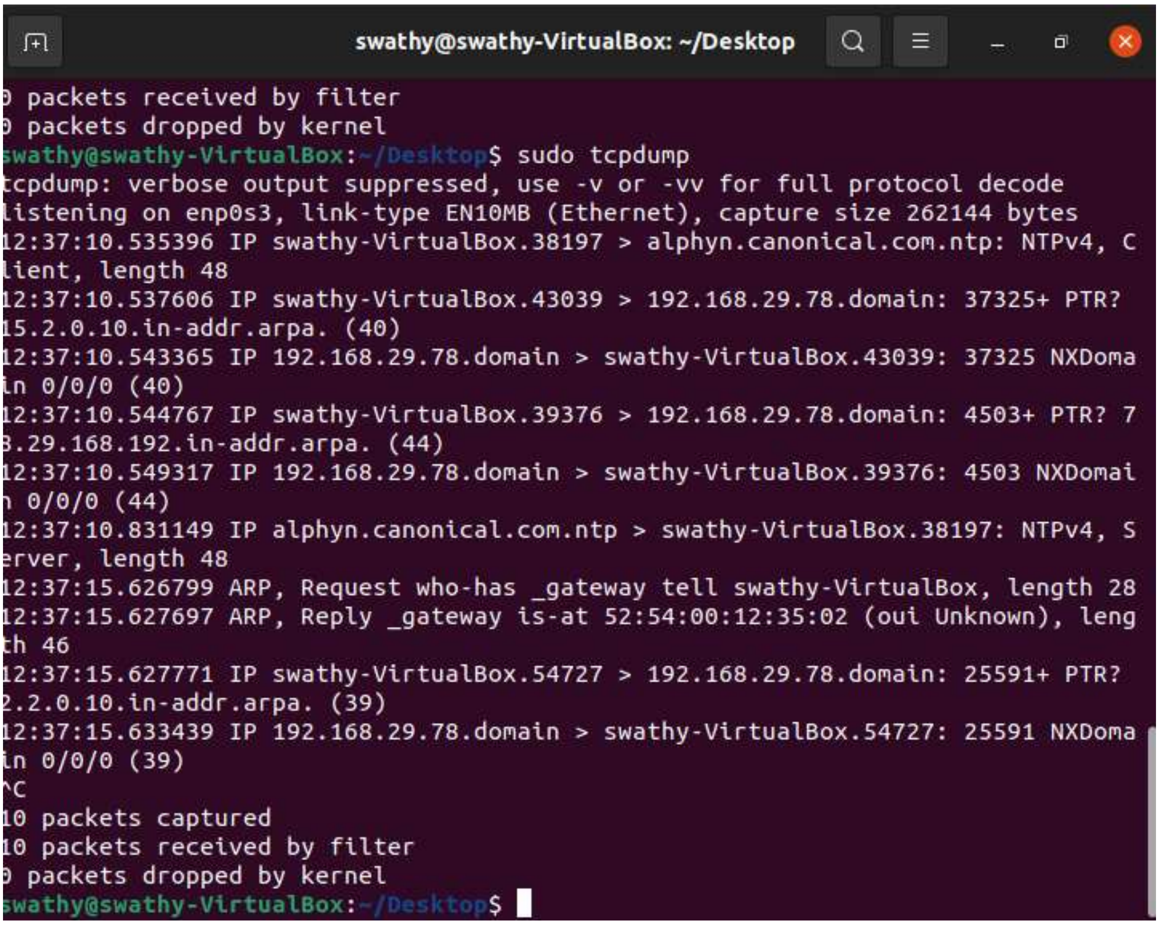
document.

Sudo apt install tcpdump



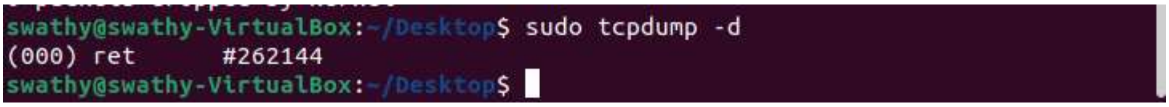
```
swathy@swathy-VirtualBox:~/Desktop$ sudo apt update && sudo apt install tcpdump
[sudo] password for swathy:
Get:1 http://in.archive.ubuntu.com/ubuntu hirsute InRelease [269 kB]
Get:2 http://security.ubuntu.com/ubuntu hirsute-security InRelease [110 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu hirsute-updates InRelease [115 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu hirsute-backports InRelease [101 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 DEP-11 Met
adata [95.0 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu hirsute-updates/universe amd64 DEP-11
 Metadata [57.7 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu hirsute-updates/multiverse amd64 DEP-
11 Metadata [944 B]
Get:8 http://security.ubuntu.com/ubuntu hirsute-security/main amd64 DEP-11 Meta
data [9,692 B]
Get:9 http://in.archive.ubuntu.com/ubuntu hirsute-backports/universe amd64 DEP-
11 Metadata [9,348 B]
Get:10 http://security.ubuntu.com/ubuntu hirsute-security/universe amd64 DEP-11
 Metadata [5,664 B]
Fetched 774 kB in 6s (121 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
258 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpdump is already the newest version (4.9.3-7).
tcpdump set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 258 not upgraded.
```

Sudo tcpdump



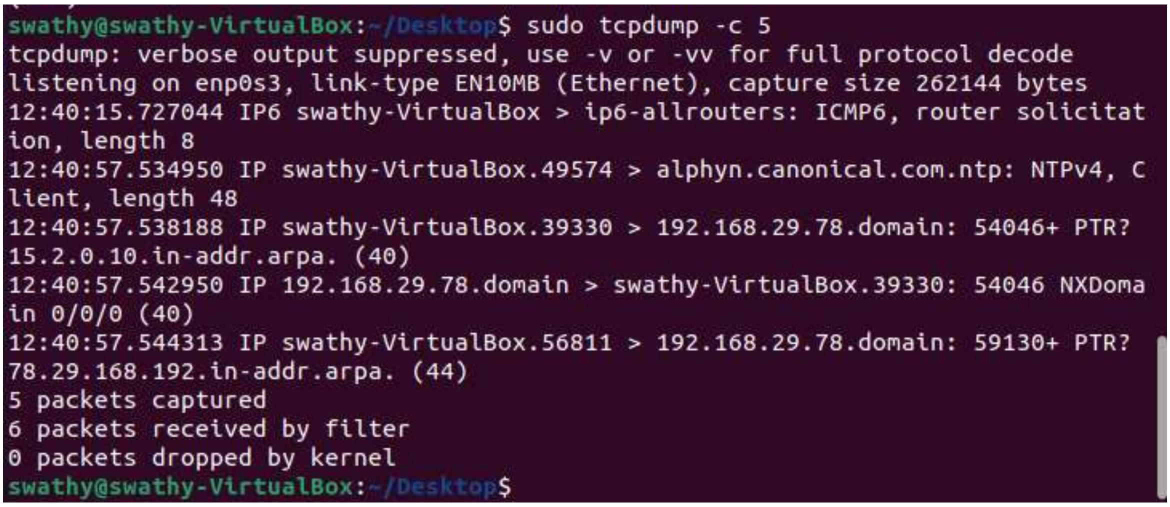
```
0 packets received by filter
0 packets dropped by kernel
swathy@swathy-VirtualBox:~/Desktop$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
12:37:10.535396 IP swathy-VirtualBox.38197 > alphyn.canonical.com.ntp: NTPv4, C
lient, length 48
12:37:10.537606 IP swathy-VirtualBox.43039 > 192.168.29.78.domain: 37325+ PTR?
15.2.0.10.in-addr.arpa. (40)
12:37:10.543365 IP 192.168.29.78.domain > swathy-VirtualBox.43039: 37325 NXDoma
in 0/0/0 (40)
12:37:10.544767 IP swathy-VirtualBox.39376 > 192.168.29.78.domain: 4503+ PTR? 7
8.29.168.192.in-addr.arpa. (44)
12:37:10.549317 IP 192.168.29.78.domain > swathy-VirtualBox.39376: 4503 NXDomai
n 0/0/0 (44)
12:37:10.831149 IP alphyn.canonical.com.ntp > swathy-VirtualBox.38197: NTPv4, S
erver, length 48
12:37:15.626799 ARP, Request who-has _gateway tell swathy-VirtualBox, length 28
12:37:15.627697 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), leng
th 46
12:37:15.627771 IP swathy-VirtualBox.54727 > 192.168.29.78.domain: 25591+ PTR?
2.2.0.10.in-addr.arpa. (39)
12:37:15.633439 IP 192.168.29.78.domain > swathy-VirtualBox.54727: 25591 NXDoma
in 0/0/0 (39)
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
swathy@swathy-VirtualBox:~/Desktop$
```

Sudo tcpdump –d



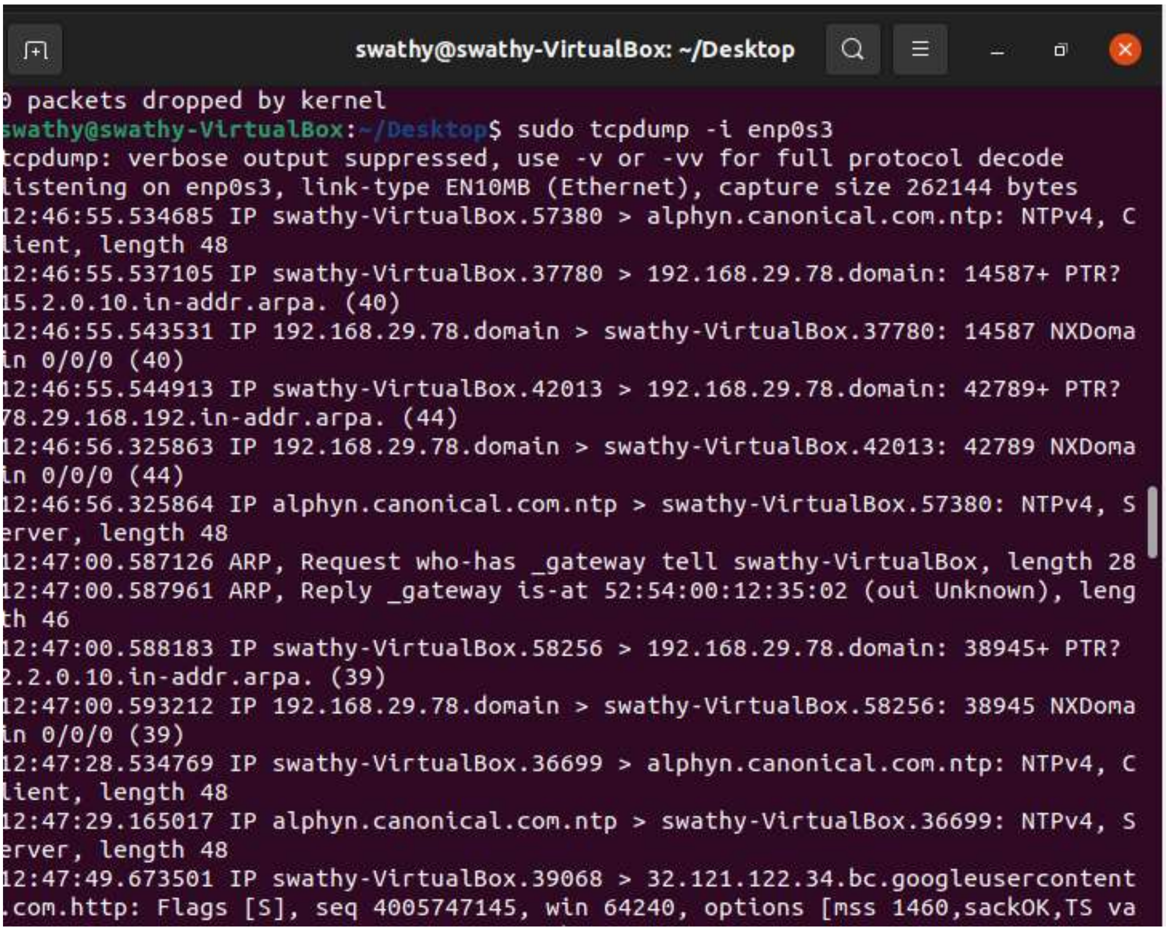
```
swathy@swathy-VirtualBox:~/Desktop$ sudo tcpdump -d
(000) ret      #262144
swathy@swathy-VirtualBox:~/Desktop$
```

Sudo tcpdump -c 5



```
swathy@swathy-VirtualBox:~/Desktop$ sudo tcpdump -c 5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
12:40:15.727044 IP6 swathy-VirtualBox > ip6-allrouters: ICMP6, router solicitat
ion, length 8
12:40:57.534950 IP swathy-VirtualBox.49574 > alphyn.canonical.com.ntp: NTPv4, C
lient, length 48
12:40:57.538188 IP swathy-VirtualBox.39330 > 192.168.29.78.domain: 54046+ PTR?
15.2.0.10.in-addr.arpa. (40)
12:40:57.542950 IP 192.168.29.78.domain > swathy-VirtualBox.39330: 54046 NXDoma
in 0/0/0 (40)
12:40:57.544313 IP swathy-VirtualBox.56811 > 192.168.29.78.domain: 59130+ PTR?
78.29.168.192.in-addr.arpa. (44)
5 packets captured
6 packets received by filter
0 packets dropped by kernel
swathy@swathy-VirtualBox:~/Desktop$
```

Sudo tcpdum -I enp2s0



```
0 packets dropped by kernel
swathy@swathy-VirtualBox:~/Desktop$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
12:46:55.534685 IP swathy-VirtualBox.57380 > alphyn.canonical.com.ntp: NTPv4, C
lient, length 48
12:46:55.537105 IP swathy-VirtualBox.37780 > 192.168.29.78.domain: 14587+ PTR?
15.2.0.10.in-addr.arpa. (40)
12:46:55.543531 IP 192.168.29.78.domain > swathy-VirtualBox.37780: 14587 NXDoma
in 0/0/0 (40)
12:46:55.544913 IP swathy-VirtualBox.42013 > 192.168.29.78.domain: 42789+ PTR?
78.29.168.192.in-addr.arpa. (44)
12:46:56.325863 IP 192.168.29.78.domain > swathy-VirtualBox.42013: 42789 NXDoma
in 0/0/0 (44)
12:46:56.325864 IP alphyn.canonical.com.ntp > swathy-VirtualBox.57380: NTPv4, S
erver, length 48
12:47:00.587126 ARP, Request who-has _gateway tell swathy-VirtualBox, length 28
12:47:00.587961 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), leng
th 46
12:47:00.588183 IP swathy-VirtualBox.58256 > 192.168.29.78.domain: 38945+ PTR?
2.2.0.10.in-addr.arpa. (39)
12:47:00.593212 IP 192.168.29.78.domain > swathy-VirtualBox.58256: 38945 NXDoma
in 0/0/0 (39)
12:47:28.534769 IP swathy-VirtualBox.36699 > alphyn.canonical.com.ntp: NTPv4, C
lient, length 48
12:47:29.165017 IP alphyn.canonical.com.ntp > swathy-VirtualBox.36699: NTPv4, S
erver, length 48
12:47:49.673501 IP swathy-VirtualBox.39068 > 32.121.122.34.bc.googleusercontent
.com.http: Flags [S], seq 4005747145, win 64240, options [mss 1460,sackOK,TS va
```