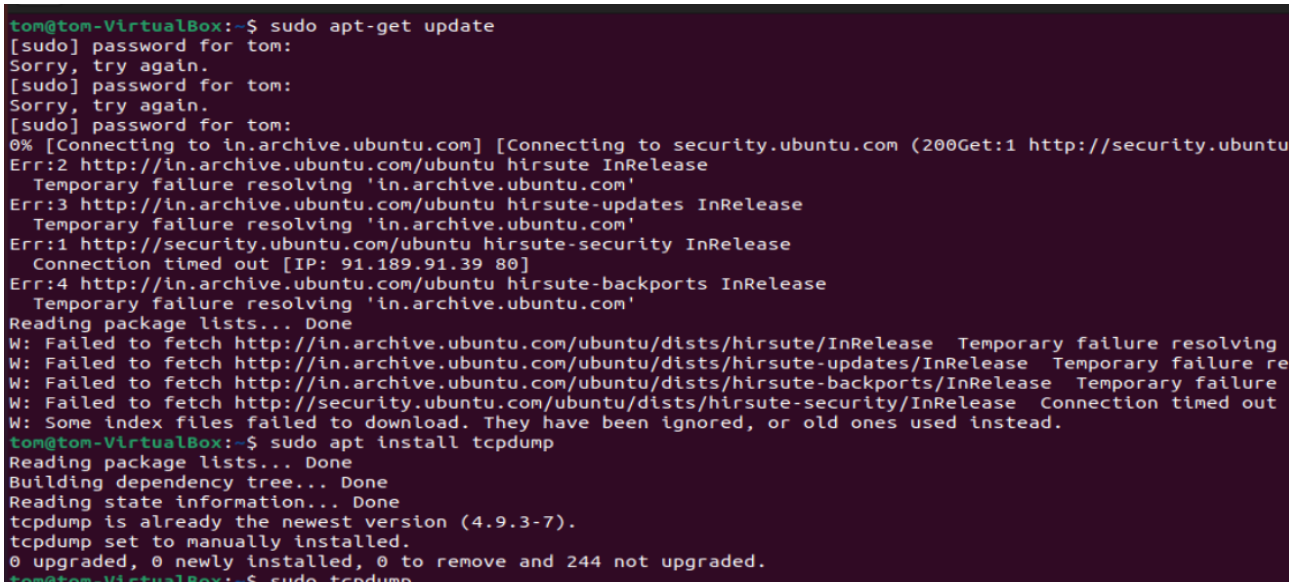
Analyzing network packet stream using tcpdump

Analyzing network packet stream using tcpdump

Tcpdump Installation

command : #sudo apt update && sudo apt install tcpdump



Capturing Packets with tcpdump

command : sudo tcpdump

```
0 upgraded, 0 newly installed, 0 to remove and 244 not upgraded.
tom@tom-VirtualBox:~$ 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
21:14:10.280129 IP tom-VirtualBox.53496 > golem.canonical.com.ntp: NTPv4, Client, length 48
21:14:10.286413 IP tom-VirtualBox.56096 > 192.168.137.1.domain: 61353+ [1au] PTR? 199.89.189.91.in-addr.arpa. (55)
21:14:10.762954 IP golem.canonical.com.ntp > tom-VirtualBox.53496: NTPv4, Server, length 48
21:14:10.763056 IP 192.168.137.1.domain > tom-VirtualBox.56096: 61353 1/0/1 PTR golem.canonical.com. (88)
21:14:10.768888 IP tom-VirtualBox.36852 > 192.168.137.1.domain: 5810+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
21:14:10.887403 IP 192.168.137.1.domain > tom-VirtualBox.36852: 5810 NXDomain 0/0/1 (51)
21:14:10.887554 IP 192.168.137.1.domain > tom-VirtualBox.36852: 5810 NXDomain 0/0/1 (51)
21:14:10.887740 IP tom-VirtualBox.36852 > 192.168.137.1.domain: 5810+ PTR? 15.2.0.10.in-addr.arpa. (40)
21:14:10.889905 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 73+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:10.906060 IP 192.168.137.1.domain > tom-VirtualBox.46656: 73- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:10.906360 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 2294+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:11.798024 IP 192.168.137.1.domain > tom-VirtualBox.46656: 2294- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:11.798151 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 54296+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:13.430006 IP 192.168.137.1.domain > tom-VirtualBox.46656: 54296- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:13.430208 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 10412+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:14.106994 IP 192.168.137.1.domain > tom-VirtualBox.46656: 10412- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:14.107260 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 49724+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:14.614462 IP 192.168.137.1.domain > tom-VirtualBox.46656: 49724- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:14.614698 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 64928+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:14.906285 IP 192.168.137.1.domain > tom-VirtualBox.46656: 64928- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:14.906517 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 41800+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:15.283673 ARP, Request who-has _gateway tell tom-VirtualBox, length 28
21:14:15.284048 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
21:14:15.556366 IP 192.168.137.1.domain > tom-VirtualBox.46656: 41800- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:15.556587 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 41277+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:16.190305 IP 192.168.137.1.domain > tom-VirtualBox.46656: 41277- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:16.190490 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 10851+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:16.649189 IP 192.168.137.1.domain > tom-VirtualBox.46656: 10851- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:16.649384 IP tom-VirtualBox.46656 > 192.168.137.1.domain: 11458+ [1au] PTR? 1.137.168.192.in-addr.arpa. (55)
21:14:17.024400 IP 192.168.137.1.domain > tom-VirtualBox.46656: 11458- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
21:14:17.024417 IP 192.168.137.1.domain > tom-VirtualBox.36852: 5810 NXDomain 0/0/1 (51)
21:14:17.024439 IP tom-VirtualBox > 192.168.137.1: ICMP tom-VirtualBox udp port 36852 unreachable, length 87
21:14:17.024454 IP 192.168.137.1.domain > tom-VirtualBox.36852: 5810 NXDomain 0/0/1 (51)
21:14:20.896357 IP tom-VirtualBox.50422 > 192.168.137.1.domain: 42324+ PTR? 2.2.0.10.in-addr.arpa. (39)
21:14:21.002948 IP 192.168.137.1.domain > tom-VirtualBox.46656: 17634- 1/0/0 PTR LAPTOP-5GEAB7TG.mshome.net. (110)
```

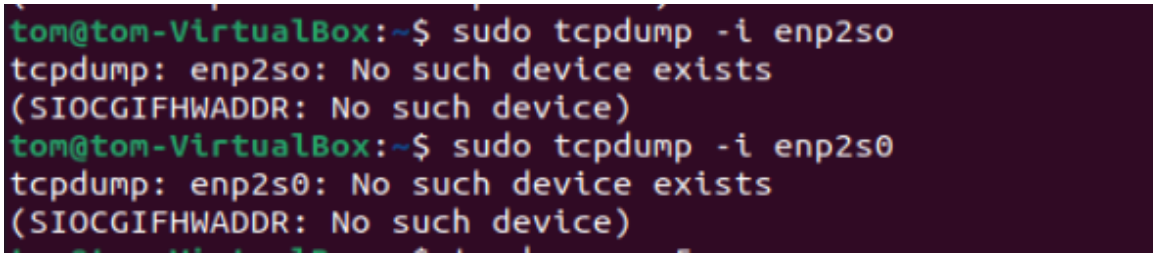
```
21:21:34.323609 IP tom-VirtualBox.38150 > 117.18.237.29.http: Flags [.], ack 1479, win 63554, length 0
21:21:34.324248 IP 117.18.237.29.http > tom-VirtualBox.38150: Flags [.], ack 759, win 65535, length 0
21:21:34.579682 IP tom-VirtualBox.44684 > maa05s13-in-f3.1e100.net.http: Flags [.], ack 703, win 63791, length 0
21:21:34.579750 IP tom-VirtualBox.44648 > maa05s13-in-f3.1e100.net.http: Flags [.], ack 3510, win 63882, length 0
21:21:34.580538 IP maa05s13-in-f3.1e100.net.http > tom-VirtualBox.44684: Flags [.], ack 383, win 65535, length 0
21:21:34.580569 IP maa05s13-in-f3.1e100.net.http > tom-VirtualBox.44648: Flags [.], ack 1909, win 65535, length 0
21:21:36.598243 IP tom-VirtualBox.34400 > 104.18.31.182.http: Flags [F.], seq 1, ack 939, win 63852, length 0
21:21:36.599261 IP 104.18.31.182.http > tom-VirtualBox.34400: Flags [.], ack 2, win 65535, length 0
^C
4777 packets captured
6664 packets received by filter
1887 packets dropped by kernel
tom@tom-VirtualBox:~$
```

tcpdump command option

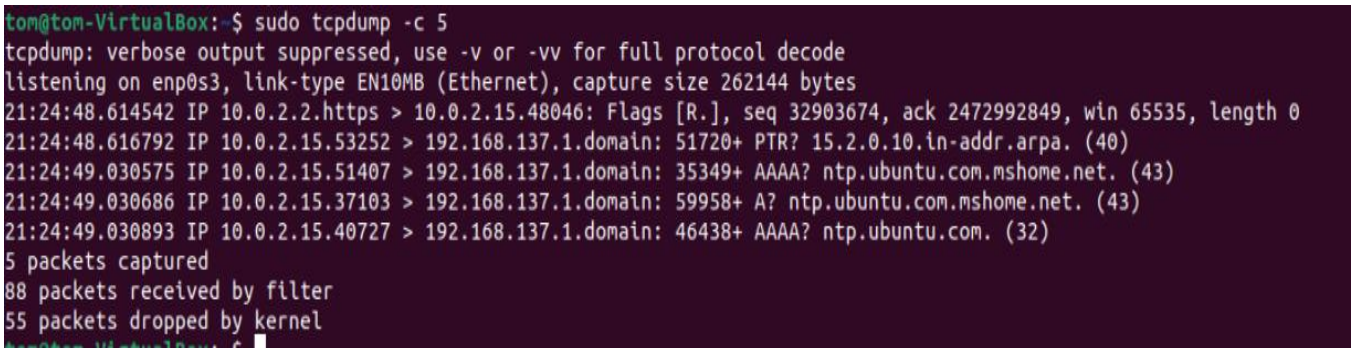
command : # tcpdump –D

```
tom@tom-VirtualBox:~$ tcpdump -D
1.enp0s3 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
tom@tom-VirtualBox:~$
```

command : # tcpdump -i enp2s0

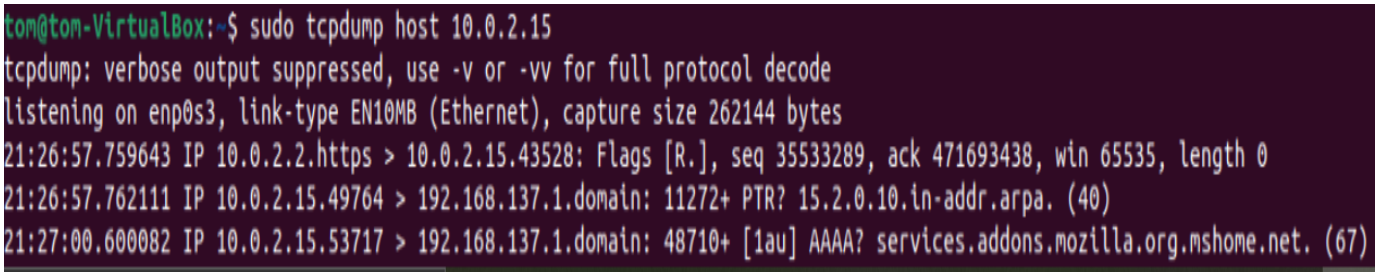


command : #tcpdump -c 5



tcpdump filter expressions

command : # tcpdump host 10.0.2.15



```
21:28:31.031237 IP 10.0.2.15.58987 > 192.168.137.1.
^C
265 packets captured
276 packets received by filter
11 packets dropped by kernel
```

command : # tcpdump -i eth1 icmp

command : # tcpdump -i eth1 not icmp

Saving packet headers to a file

command : # tcpdump -i eth1 -c 10 -w icmp.pcap

command : tcpdump -r icmp.pcap

Viewing packet details

command : # tcpdump -c10 -i eth1 -n -A port 8

```
tom@tom-VirtualBox:~$ sudo tcpdump -i eth 1 not icmp
tcpdump: eth: No such device exists
(SIOCGIFHWADDR: No such device)
tom@tom-VirtualBox:~$ tcpdump -i eth1 -c 10 -w icmp.pcap
tcpdump: eth1: You don't have permission to capture on that device
(socket: Operation not permitted)
tom@tom-VirtualBox:~$ sudo tcpdump -i eth1 -c 10 -w icmp.pcap
tcpdump: eth1: No such device exists
(SIOCGIFHWADDR: No such device)
tom@tom-VirtualBox:~$ tcpdump -c10  -i eth1 -n -A port 80
tcpdump: eth1: You don't have permission to capture on that device
(socket: Operation not permitted)
tom@tom-VirtualBox:~$ sudo tcpdump -c10  -i eth1 -n -A port 80
tcpdump: eth1: No such device exists
(SIOCGIFHWADDR: No such device)
tom@tom-VirtualBox:~$
```