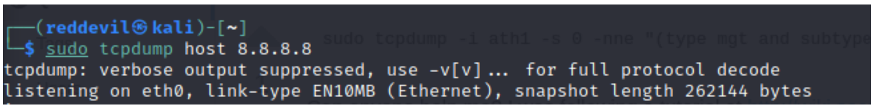
NETWORKING AND SYSTEM ADMINISTRATION LAB

TCPDUMP

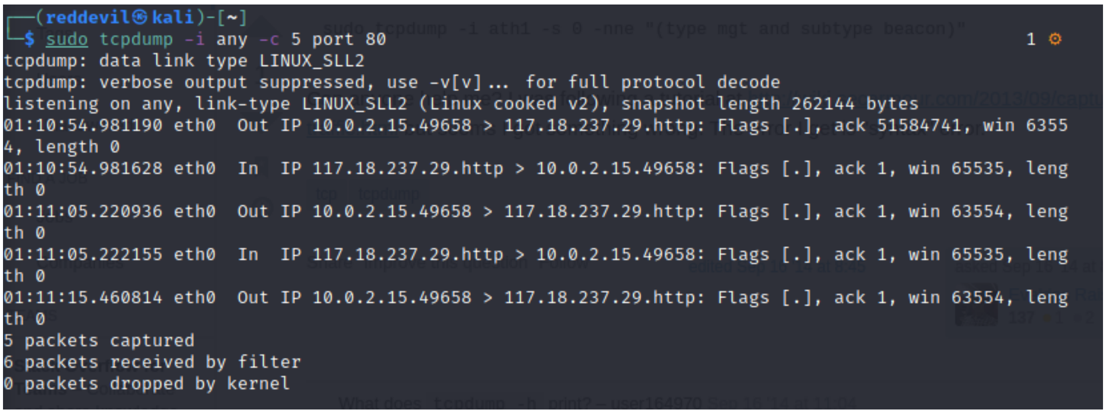
ANTONY SCARIA
MCA A SEM II
ROLL NO 23

Sudo tcpdump host 8.8.8.8



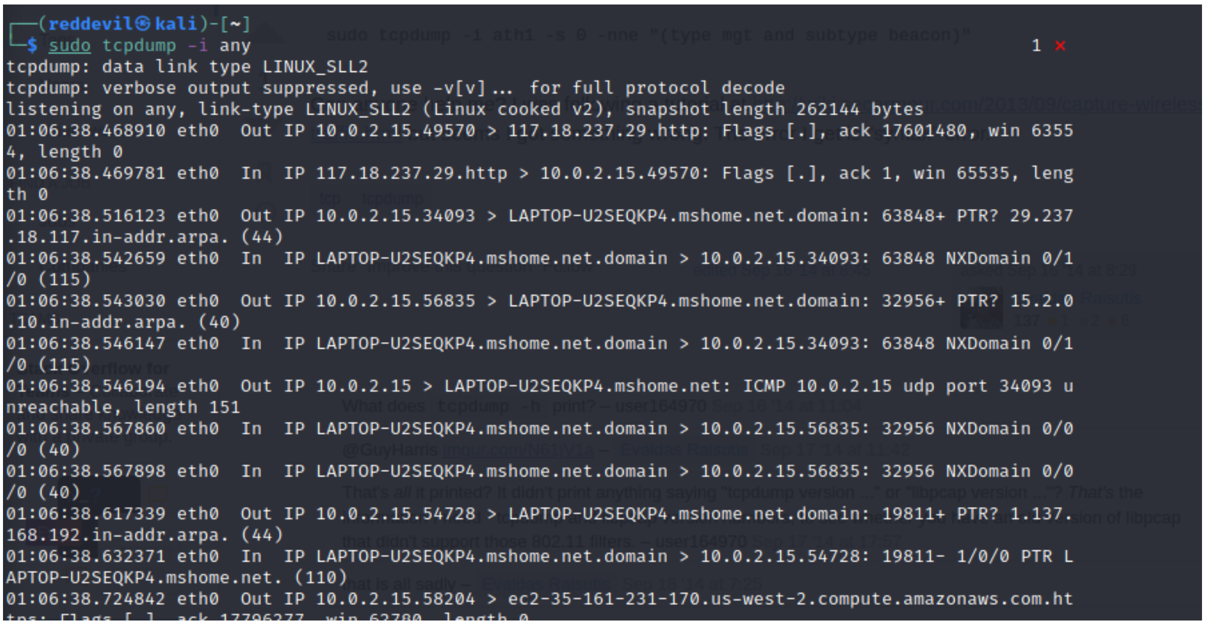
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump host 8.8.8.8
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Sudo tcpdump -i any -c 5 port 80



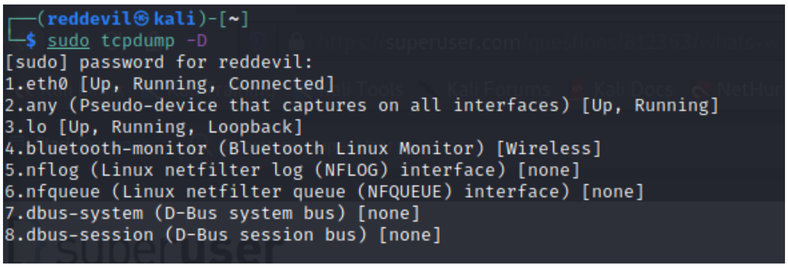
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -i any -c 5 port 80                                      1 ⚙
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
01:10:54.981190 eth0  Out IP 10.0.2.15.49658 > 117.18.237.29.http: Flags [.], ack 51584741, win 6355
4, length 0
01:10:54.981628 eth0  In  IP 117.18.237.29.http > 10.0.2.15.49658: Flags [.], ack 1, win 65535, leng
th 0
01:11:05.220936 eth0  Out IP 10.0.2.15.49658 > 117.18.237.29.http: Flags [.], ack 1, win 63554, leng
th 0
01:11:05.222155 eth0  In  IP 117.18.237.29.http > 10.0.2.15.49658: Flags [.], ack 1, win 65535, leng
th 0
01:11:15.460814 eth0  Out IP 10.0.2.15.49658 > 117.18.237.29.http: Flags [.], ack 1, win 63554, leng
th 0
5 packets captured
6 packets received by filter
0 packets dropped by kernel
```

Sudo tcpdump -i any



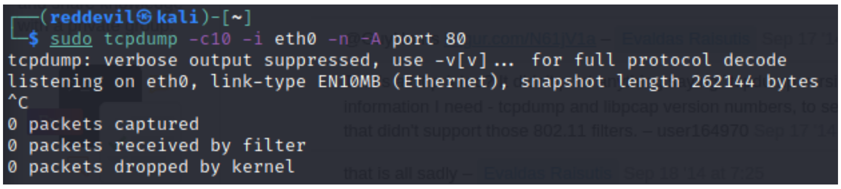
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -i any                                                   1 ×
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
01:06:38.468910 eth0  Out IP 10.0.2.15.49570 > 117.18.237.29.http: Flags [.], ack 17601480, win 6355
4, length 0
01:06:38.469781 eth0  In  IP 117.18.237.29.http > 10.0.2.15.49570: Flags [.], ack 1, win 65535, leng
th 0
01:06:38.516123 eth0  Out IP 10.0.2.15.34093 > LAPTOP-U2SEQKP4.mshome.net.domain: 63848+ PTR? 29.237
.18.117.in-addr.arpa. (44)
01:06:38.542659 eth0  In  IP LAPTOP-U2SEQKP4.mshome.net.domain > 10.0.2.15.34093: 63848 NXDomain 0/1
/0 (115)
01:06:38.543030 eth0  Out IP 10.0.2.15.56835 > LAPTOP-U2SEQKP4.mshome.net.domain: 32956+ PTR? 15.2.0
.10.in-addr.arpa. (40)
01:06:38.546147 eth0  In  IP LAPTOP-U2SEQKP4.mshome.net.domain > 10.0.2.15.34093: 63848 NXDomain 0/1
/0 (115)
01:06:38.546194 eth0  Out IP 10.0.2.15 > LAPTOP-U2SEQKP4.mshome.net: ICMP 10.0.2.15 udp port 34093 u
nreachable, length 151
01:06:38.567860 eth0  In  IP LAPTOP-U2SEQKP4.mshome.net.domain > 10.0.2.15.56835: 32956 NXDomain 0/0
/0 (40)
01:06:38.567898 eth0  In  IP LAPTOP-U2SEQKP4.mshome.net.domain > 10.0.2.15.56835: 32956 NXDomain 0/0
/0 (40)
01:06:38.617339 eth0  Out IP 10.0.2.15.54728 > LAPTOP-U2SEQKP4.mshome.net.domain: 19811+ PTR? 1.137.
168.192.in-addr.arpa. (44)
01:06:38.632371 eth0  In  IP LAPTOP-U2SEQKP4.mshome.net.domain > 10.0.2.15.54728: 19811- 1/0/0 PTR L
APTOP-U2SEQKP4.mshome.net. (110)
01:06:38.724842 eth0  Out IP 10.0.2.15.58204 > ec2-35-161-231-170.us-west-2.compute.amazonaws.com.ht
tps: Flags [.], ack 17796277, win 62780, length 0
```

Sudo tcpdump -D



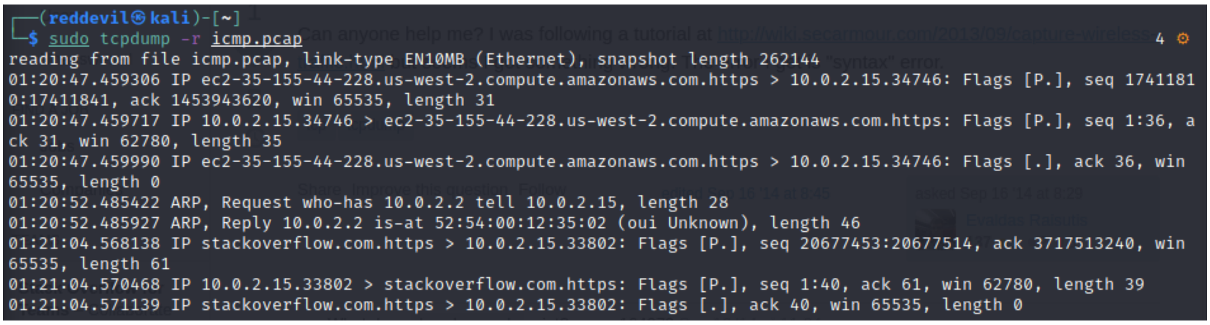
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -D
[sudo] password for reddevil:
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [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]
```

Sudo tcpdump -c 10 -i eth0 -n -A port 80



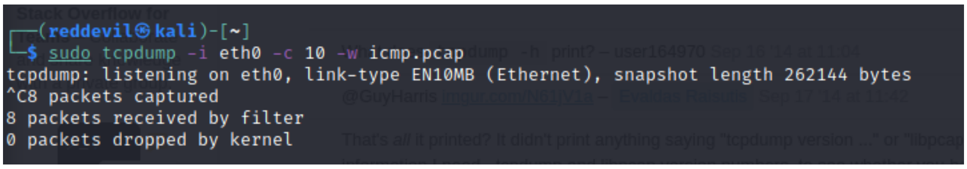
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -c10 -i eth0 -n -A port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

Sudo tcpdump -r icmp.pcap



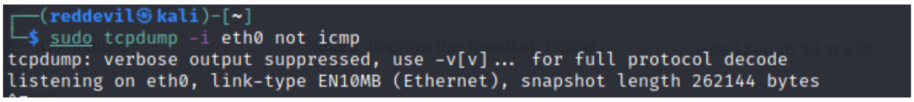
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -r icmp.pcap                                                                    4 ⚙
reading from file icmp.pcap, link-type EN10MB (Ethernet), snapshot length 262144
01:20:47.459306 IP ec2-35-155-44-228.us-west-2.compute.amazonaws.com.https > 10.0.2.15.34746: Flags [P.], seq 1741181
0:17411841, ack 1453943620, win 65535, length 31
01:20:47.459717 IP 10.0.2.15.34746 > ec2-35-155-44-228.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 1:36, a
ck 31, win 62780, length 35
01:20:47.459990 IP ec2-35-155-44-228.us-west-2.compute.amazonaws.com.https > 10.0.2.15.34746: Flags [.], ack 36, win
65535, length 0
01:20:52.485422 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
01:20:52.485927 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02 (oui Unknown), length 46
01:21:04.568138 IP stackoverflow.com.https > 10.0.2.15.33802: Flags [P.], seq 20677453:20677514, ack 3717513240, win
65535, length 61
01:21:04.570468 IP 10.0.2.15.33802 > stackoverflow.com.https: Flags [P.], seq 1:40, ack 61, win 62780, length 39
01:21:04.571139 IP stackoverflow.com.https > 10.0.2.15.33802: Flags [.], ack 40, win 65535, length 0
```

Sudo tcpdump -i eth0 -c 10 -w icmp.pcap



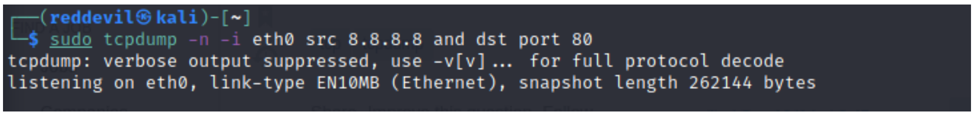
```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -c 10 -w icmp.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

Sudo tcpdump -i eth0 not icmp



```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -i eth0 not icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Sudo tcpdump -n -i eth0 scr 8.8.8.8 and dst port 80



```
┌──(reddevil㉿kali)-[~]
└─$ sudo tcpdump -n -i eth0 src 8.8.8.8 and dst port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```