ASSIGNMENT NO – 1

SIDDHI PAWAR (TI46)

Part A

Installation Scapy -

bcl07@bcl07:~$ sudo apt update

bcl07@bcl07:~$ sudo apt install python3-pip python3-dev libpcap0.8-dev

bcl07@bcl07:~$ sudo pip3 install scapy

bcl07@bcl07:~$ python3 -c "import scapy; print(scapy.__version__)"

bcl07@bcl07:~$ sudo scapy

Installation WireShark -

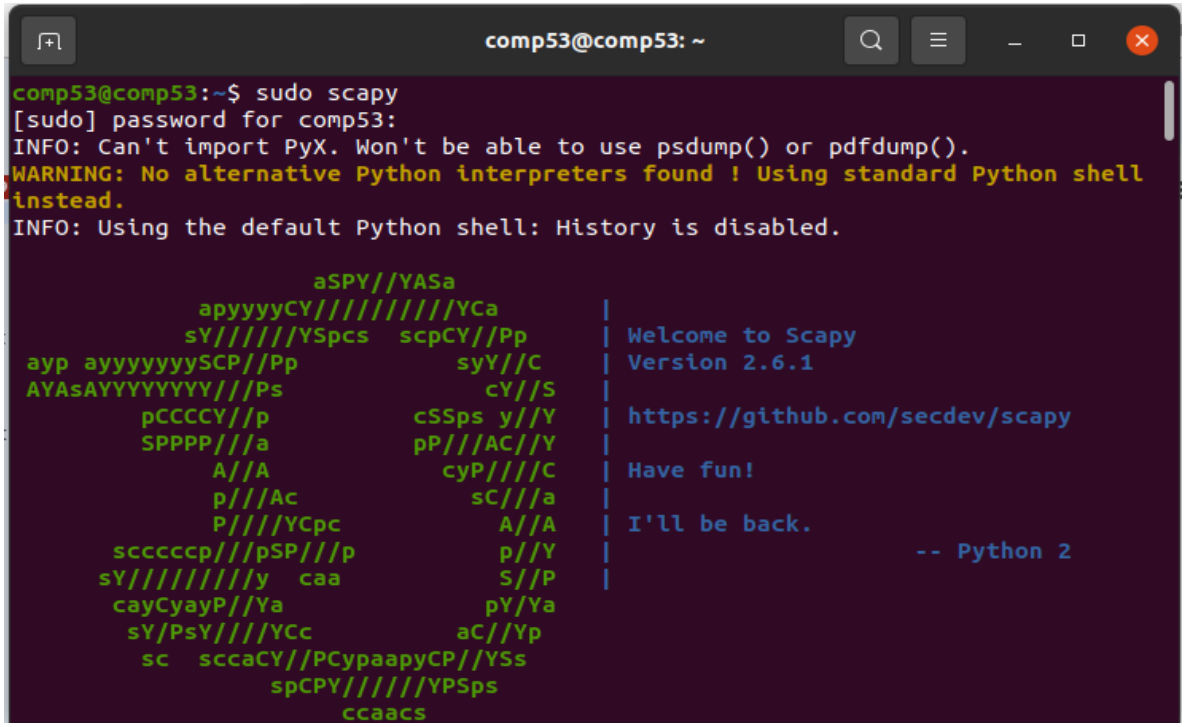
bcl07@bcl07:~$ sudo apt update

bcl07@bcl07:~$ sudo apt install wireshark

bcl07@bcl07:~$ wireshark

Practical –

comp53@comp53:~$ sudo scapy



>>> capture = sniff()

```
comp53@comp53: ~
>>> capture = sniff()
INFO: DNS RR prematured end (ofs=19, len=19)
INFO: DNS RR prematured end (ofs=16, len=16)
INFO: DNS RR TXT prematured end of character-string (size=6, remaining bytes=4)
INFO: DNS RR prematured end (ofs=20, len=5)
INFO: DNS RR prematured end (ofs=20, len=16)
INFO: DNS RR prematured end (ofs=27, len=24)
INFO: DNS RR prematured end (ofs=20, len=8)
INFO: DNS RR TXT prematured end of character-string (size=22, remaining bytes=13
)
INFO: DNS RR TXT prematured end of character-string (size=22, remaining bytes=3)
INFO: DNS RR prematured end (ofs=19, len=19)
INFO: DNS RR prematured end (ofs=20, len=8)
INFO: DNS RR TXT prematured end of character-string (size=6, remaining bytes=4)
INFO: DNS RR prematured end (ofs=20, len=5)
INFO: DNS RR prematured end (ofs=27, len=24)
INFO: DNS RR prematured end (ofs=20, len=16)
INFO: DNS RR prematured end (ofs=20, len=8)
INFO: DNS RR TXT prematured end of character-string (size=6, remaining bytes=4)
INFO: DNS RR prematured end (ofs=20, len=5)
INFO: DNS RR prematured end (ofs=20, len=16)
INFO: DNS RR prematured end (ofs=27, len=24)
INFO: DNS RR prematured end (ofs=10, len=10)
```

^C>>> capture.summary()

```
comp53@comp53: ~
INFO: DNS RR prematured end (ofs=16, len=16)
INFO: DNS RR prematured end (ofs=16, len=16)
^C>>> capture.summary()
Ether / ARP who has 172.16.10.135 says 172.16.11.246 / Padding
Ether / ARP who has 172.16.1.1 says 172.16.20.33 / Padding
Ether / IP / UDP 172.16.11.246:37214 > 235.5.5.5:58581 / Raw
Ether / IP / UDP 172.16.11.246:48704 > 172.16.255.255:58581 / Raw
Ether / ARP who has 172.16.1.4 says 172.16.20.240 / Padding
Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - Source Link-Laye
r Address f8:32:e4:9c:18:0a
Ether / 172.16.4.193 > 224.0.0.113 igmp / Raw / Padding
Ether / fe80::e14:4121:da13:cb0 > ff02::16 (0) / IPv6ExtHdrHopByHop / ICMPv6MLRe
port2
Ether / 172.16.11.246 > 224.0.0.251 igmp / Raw / Padding
Ether / 172.16.11.246 > 224.0.0.251 igmp / Raw / Padding
Ether / ARP who has 192.168.1.1 says 192.168.1.9 / Padding
Ether / IP / UDP / NBTDatagram / SMB_Header / Tran b'\\MAILSLOT\\BROWSE' BecomeB
ackup from b'IMERTLABPC'
Ether / IP / UDP 172.16.11.245:59729 > 172.16.255.255:58581 / Raw
Ether / IP / UDP 172.16.11.245:57753 > 235.5.5.5:58581 / Raw
Ether / 172.30.2.207 > 239.255.255.253 igmp / Raw / Padding
Ether / IP / UDP 172.16.11.250:48517 > 235.5.5.5:58581 / Raw
Ether / IP / UDP 172.16.11.250:38013 > 172.16.255.255:58581 / Raw
Ether / 172.30.2.208 > 224.0.1.60 igmp / Raw / Padding
```

>>> capture = sniff(count = 5)
>>> capture.summary()

```
>>> capture = sniff(count = 5)
>>> capture.summary()
Ether / 172.30.2.207 > 239.255.255.253 igmp / Raw / Padding
Ether / 10.10.1.243 > 224.0.0.251 igmp / Raw / Padding
Ether / 10.10.1.243 > 224.0.0.251 igmp / Raw / Padding
Ether / IP / UDP 192.168.40.159:64625 > 192.168.40.255:3490 / Raw
Ether / IPv6 / UDP fe80::f18c:4737:428a:a372:51974 > ff02::1:3:hostmon / LLMNRQu
ery who has 'https.'
```

>>> sniff(filter = "tcp", count = 5)

```
>>> sniff(filter = "tcp", count = 5)
<Sniffed: TCP:5 UDP:0 ICMP:0 Other:0>
```

>>> show_interfaces()

```
>>> show_interfaces()
Source  Index  Name    MAC                IPv4        IPv6
sys     1      lo      00:00:00:00:00:00  127.0.0.1   ::1
sys     2      enp3s0  58:11:22:b7:4a:70  172.16.7.53 fe80::20:4d18:400b:de5b
```

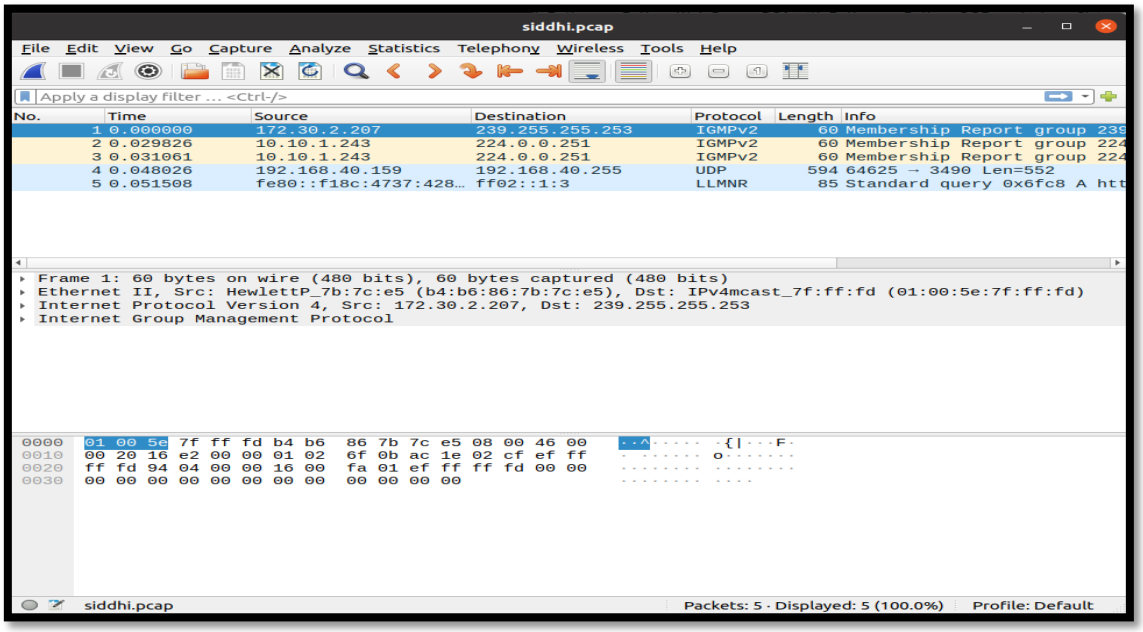
>>> sniff(iface = "enp3s0", count = 5)

```
>>> sniff(iface = "enp3s0", count = 5)
<Sniffed: TCP:0 UDP:3 ICMP:0 Other:2>
```

>>> sniff(prn=lambda x:x.summary(), count = 5)

```
>>> sniff(prn=lambda x:x.summary(), count = 5)
Ether / IP / UDP / mDNS Qry b'Chhomu._dosvc._tcp.local.'
Ether / IPv6 / UDP / mDNS Qry b'Chhomu._dosvc._tcp.local.'
Ether / IP / UDP / NBNSHeader / NBNSQueryRequest who has '\\HTTPS'
Ether / ARP who has 10.10.4.44 says 10.10.10.1 / Padding
Ether / ARP who has 10.10.5.142 says 10.10.10.1 / Padding
<Sniffed: TCP:0 UDP:3 ICMP:0 Other:2>
```

WireShark (Packet Sniffing) -



>>> wrpcap("siddhi.pcap", capture)

>>> sniff(offline = "siddhi.pcap")

```
>>> wrpcap("siddhi.pcap", capture)
>>> sniff(offline = "siddhi.pcap")
<Sniffed: TCP:0 UDP:2 ICMP:0 Other:3>
```

>>> sniff(offline = "siddhi.pcap", prn = lambda x:x.summary())

```
>>> sniff(offline = "siddhi.pcap", prn = lambda x:x.summary())
Ether / 172.30.2.207 > 239.255.255.253 igmp / Raw / Padding
Ether / 10.10.1.243 > 224.0.0.251 igmp / Raw / Padding
Ether / 10.10.1.243 > 224.0.0.251 igmp / Raw / Padding
Ether / IP / UDP 192.168.40.159:64625 > 192.168.40.255:3490 / Raw
Ether / IPv6 / UDP fe80::f18c:4737:428a:a372:51974 > ff02::1:3:hostmon / LLMNRQu
ery who has 'https.'
<Sniffed: TCP:0 UDP:2 ICMP:0 Other:3>
```

>>>