CLASS TEST SHEET

Date of Test

Roll No. Reg. No. Course Code Section Test No.

TCPdump N/W Analyzer tool
Or
Packet Sniffer tool

Windows version - Windump.

✓ To install:- Sudo apt-get install tcpdump

used by pentesters to watch traffic going through the n/w. Also used by Security administators to look for any suspicious activity in the n/w.

We can check each & every packet going to & from one PC to another.

SYNTAX:- tcpdump [options] [protocol] [type]

Options:-

-n	display no. not names of M/C
-nn	IP add. & port no.
-i	Sniff a particular interface eg: eth0
-v	(verbose) More details like TTL, length of packet
-w	Dump packets to a file
-r	Read packets from file.

*To be used for class test purpose only **Strictly not to be used for any other purpose.

-x	hex
-X	hex and ASCII
-A	ASCII
-s	snap these many bytes from each packet. (default 68)

-s 0 → entire packet

Protocol :

~~host~~ ~~net~~ ~~port~~ ether, ip, ip6, arp, rarp, tcp, udp. ✓

Type :

host	–	packets	to	and	from	host
net	–	"	"	"	"	n/w
port	–	"	"	"	"	"
portrange						

src	–	packets	from	this	src only
dst	–	"	"	"	dst "

LOGICAL EXPRESSIONS :- "and" "or"

eg:- tcpdump -nn -X -s 0 tcp and dst 192.198.11.7.

Grab only tcp packets going to dst ______.

(2)

CLASS TEST SHEET

Date of Test

Roll No. Reg. No. Course Code Section Test No.

Windows :

```
nc -l -p 4444
```

Linux :

```
nc -n IP of windows 4444
```

Windows :

```
nc -l -p 4444 < hi.txt    send
```

Linux :

```
nc -n IP of windows 4444 > meee.txt
                           Receive.
```

~~Ist~~

(II) tcpdump -X -n -s 0 dst windows IP ~~[illegible]~~ and port 4444

Grab packets going to windows M/C

AAAA ↵

Ist :- nc -n IP of windows 4444

Entire Packet in Hexadecimal

45 00
↓16 bits

Source IP

32
32
32

S IP

*To be used for class test purpose only **Strictly not to be used for any other purpose.

C 251829

```
tcpdump -D.

    - i  etho0

    -c 5  -i etho

    - A   -i   etho  (ASC7I)

    -XX    -i etho  (ASCII & Hex"

    -i  etho  tcp.
```

```
tcpdump -X -nn -s0 host testphp.
vulnweb. com and port 80.
```