Rollno 63
Batch S13

Assignment 7

Aim:-Analysis of Packet header:TCP,UDP and IP using TCP
Theory:-
What is tcpdump
Tcpdump is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.A powerful and versatile tool that includes many options and filters, tcpdump can be used in a variety of cases. Since it's a command line tool, it is ideal to run in remote servers or devices for which a GUI is not available, to collect data that can be analyzed later. It can also be launched in the background or as a scheduled job using tools like cron.

How to install tcpdump

Installing Tcpdump with APT

If you're using a Debian-based distribution like Ubuntu, you can install 'tcpdump' using the Advanced Package Tool (APT). APT simplifies the process of managing software on Unix-like computer systems by automating the retrieval, configuration, and installation of software packages.

Here's how to install 'tcpdump' with APT:

```
sudo apt-get install tcpdump
```

-D
The `-d` option in `tcpdump` is used to print the compiled packet filter in a human-readable format. This option is particularly useful for debugging and understanding the filter expressions you are using with `tcpdump`.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -D
1.enp4s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```

-i
The `-i` option in `tcpdump` is used to specify the network interface on which you want to capture packets. By default, `tcpdump` captures packets on the first available interface if you do not specify one. Using the `-i` option allows you to target a specific interface, which is particularly useful in systems with multiple network interfaces.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i enp4s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:14:46.098437 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 386
11:14:46.098762 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 395
11:14:46.098945 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 458
11:14:46.099203 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 454
11:14:46.099381 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 434
11:14:46.099580 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 466
11:14:46.099799 IP _gateway.42955 > 239.255.255.250.1900: UDP, length 448
11:14:47.913268 ARP, Request who-has 192.168.0.145 tell _gateway, length 46
11:14:47.913537 IP lab1003-HP-280-G4-MT-Business-PC.39410 > _gateway.domain: 684+ PTR? 145.0.168.192.in-addr.arpa. (44)
11:14:47.919153 IP _gateway.domain > lab1003-HP-280-G4-MT-Business-PC.39410: 684 NXDomain* 0/1/0 (103)
11:14:48.910232 ARP, Request who-has 192.168.0.145 tell _gateway, length 46
^C
11 packets captured
15 packets received by filter
4 packets dropped by kernel
```

Capture packets on all interfaces: If you want to capture packets on all interfaces, you can use the `-i any` option:

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
11:15:16.392249 IP lab1003-HP-280-G4-MT-Business-PC.40644 > ec2-18-143-51-214.ap-southeast-1.compute.amazonaws.com.https: Flags [P.], seq 4020
501095:4020501141, ack 3347666272, win 501, options [nop,nop,TS val 3743781600 ecr 4203336990], length 46
11:15:16.392323 IP lab1003-HP-280-G4-MT-Business-PC.44794 > ec2-3-0-164-222.ap-southeast-1.compute.amazonaws.com.https: Flags [P.], seq 421130
7390:4211307436, ack 685815327, win 501, options [nop,nop,TS val 2184062952 ecr 1848716423], length 46
^C^C^C11:15:16.392404 IP lab1003-HP-280-G4-MT-Business-PC.44714 > 207.65.33.78.https: Flags [P.], seq 2002295904:2002295943, ack 2222011903, w
in 501, options [nop,nop,TS val 629408850 ecr 2728508441], length 39

3 packets captured
78 packets received by filter
69 packets dropped by kernel
```

The command `tcpdump -i lo` is used to capture packets on the loopback interface, which is typically referred to as `lo`. The loopback interface is a virtual network interface that the operating system uses to communicate with itself. It is commonly used for testing and inter-process communication.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
11:16:16.176594 IP localhost.39659 > localhost.domain: 12941+ [1au] A? securepubads.g.doubleclick.net. (59)
11:16:16.176606 IP localhost.39659 > localhost.domain: 42391+ [1au] AAAA? securepubads.g.doubleclick.net. (59)
11:16:16.176968 IP localhost.58607 > localhost.domain: 354+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
11:16:16.177046 IP localhost.domain > localhost.58607: 354 1/0/1 PTR localhost. (75)
11:16:16.180533 IP localhost.domain > localhost.39659: 12941 1/0/1 A 142.250.70.66 (75)
11:16:16.182815 IP localhost.domain > localhost.39659: 42391 1/0/1 AAAA 2404:6800:4009:803::2002 (87)
11:16:17.227360 IP localhost.57028 > localhost.domain: 64458+ [1au] A? connectivity-check.ubuntu.com. (58)
11:16:17.227370 IP localhost.57028 > localhost.domain: 26842+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
11:16:17.229193 IP localhost.domain > localhost.57028: 26842 12/0/1 AAAA 2001:67c:1562::24, AAAA 2620:2d:4002:1::197, AAAA 2620:2d:4000:1::96,
 AAAA 2620:2d:4000:1::98, AAAA 2620:2d:4002:1::198, AAAA 2620:2d:4000:1::97, AAAA 2620:2d:4002:1::196, AAAA 2620:2d:4000:1::22, AAAA 2620:2d:4
000:1::2b, AAAA 2001:67c:1562::23, AAAA 2620:2d:4000:1::23, AAAA 2620:2d:4000:1::2a (394)
11:16:17.370593 IP localhost.domain > localhost.57028: 64458 12/0/1 A 91.189.91.48, A 185.125.190.49, A 91.189.91.96, A 91.189.91.97, A 185.12
5.190.97, A 185.125.190.48, A 185.125.190.17, A 185.125.190.98, A 185.125.190.18, A 185.125.190.96, A 91.189.91.98, A 91.189.91.49 (250)
^C
10 packets captured
20 packets received by filter
0 packets dropped by kernel
```

It seems like there might be a small typo in your command. The correct command should be `tcpdump -i bluetooth0` if you want to capture packets on a Bluetooth interface named `bluetooth0`.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i bluetooth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bluetooth0, link-type BLUETOOTH_HCI_H4_WITH_PHDR (Bluetooth HCI UART transport layer plus pseudo-header), capture size 262144 byt
es
^C
0 packets captured
366 packets received by filter
0 packets dropped by kernel
```

The command `tcpdump -nflog` is used to capture packets from the Linux kernel's netfilter logging subsystem, specifically using the `NFLOG` target. This allows you to capture packets that have been logged by the netfilter framework, which is commonly used for firewall and packet filtering in Linux.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i nflog
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on nflog, link-type NFLOG (Linux netfilter log messages), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

The command `tcpdump -nflog` is used to capture packets from the Linux kernel's netfilter logging subsystem, specifically using the `NFLOG` target. This allows you to capture packets that have been logged by the netfilter framework, which is commonly used for firewall and packet filtering in Linux.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i nfqueue
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on nfqueue, link-type IPV4 (Raw IPv4), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

The command `tcpdump -nflog` is used to capture packets from the Linux kernel's netfilter logging subsystem, specifically using the `NFLOG` target. This allows you to capture packets that have been logged by the netfilter framework, which is commonly used for firewall and packet filtering in Linux.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i usbmon1
tcpdump: Can't open USB bus file /sys/kernel/debug/usbmon/1t: No such file or directory
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i usbmon2
tcpdump: Can't open USB bus file /sys/kernel/debug/usbmon/2t: No such file or directory
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$
```

-c

The `-c` option captures **X** number of packets and then stops. Otherwise, `tcpdump` will keep running indefinitely. So when you want to capture only a small sample set of packets, you can use this option. However, if there is no activity on the interface, `tcpdump` keeps waiting

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -c 5 -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
11:27:32.084755 IP lab1003-HP-280-G4-MT-Business-PC.42462 > server-54-239-216-78.bom52.r.cloudfront.net.https: Flags [P.], seq 1768136190:1768
136229, ack 378833406, win 501, options [nop,nop,TS val 282336652 ecr 2950759432], length 39
11:27:32.084820 IP lab1003-HP-280-G4-MT-Business-PC.54346 > ec2-3-213-1-145.compute-1.amazonaws.com.https: Flags [P.], seq 4132411291:41324113
37, ack 2966476738, win 501, options [nop,nop,TS val 2290645211 ecr 2573809479], length 46
11:27:32.084874 IP lab1003-HP-280-G4-MT-Business-PC.37300 > 104.22.4.69.https: Flags [P.], seq 2989625050:2989625089, ack 484854748, win 501,
options [nop,nop,TS val 3495873170 ecr 633906515], length 39
11:27:32.084884 IP lab1003-HP-280-G4-MT-Business-PC.47952 > server-18-172-64-19.bom78.r.cloudfront.net.https: Flags [P.], seq 378149105:378149
144, ack 4020659694, win 501, options [nop,nop,TS val 4107866154 ecr 90482999], length 39
11:27:32.084938 IP lab1003-HP-280-G4-MT-Business-PC.49356 > server-18-172-78-53.bom78.r.cloudfront.net.https: Flags [P.], seq 4079679951:40796
79990, ack 1633878205, win 2446, options [nop,nop,TS val 3481564717 ecr 4254516682], length 39
11:27:32.084955 IP lab1003-HP-280-G4-MT-Business-PC.38912 > 104.22.52.173.https: Flags [P.], seq 1461723732:1461723771, ack 1221161139, win 50
1, options [nop,nop,TS val 2449945906 ecr 3120446031], length 39
^C
6 packets captured
68 packets received by filter
56 packets dropped by kernel
```

-n

It is usually easier to work if you use IP addresses instead of names, such as **kkulkarni.53013** as shown in the above output. You can use `-n` for this.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:28:35.583151 IP 192.168.0.166.42180 > 15.197.196.10.443: Flags [.], ack 3676510635, win 501, options [nop,nop,TS val 3368229242 ecr 3942693
429], length 0
11:28:35.583263 IP 192.168.0.104.5353 > 224.0.0.251.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)
11:28:35.583354 IP6 fe80::c626:187b:9aca:8498.5353 > ff02::fb.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)
11:28:35.583468 IP 192.168.0.104.5353 > 224.0.0.251.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)
11:28:35.583477 IP6 fe80::c626:187b:9aca:8498.5353 > ff02::fb.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)
11:28:35.600227 IP 192.168.0.166.36806 > 3.219.245.116.443: Flags [P.], seq 3618742924:3618742995, ack 1191399948, win 501, options [nop,nop,T
S val 3174611898 ecr 1250259947], length 71
11:28:35.647339 IP 15.197.196.10.443 > 192.168.0.166.42180: Flags [.], ack 1, win 171, options [nop,nop,TS val 3942703669 ecr 3368198812], len
gth 0
11:28:35.745785 IP 3.216.147.127.443 > 192.168.0.166.51242: Flags [F.], seq 2060359597, ack 2791289878, win 118, options [nop,nop,TS val 33812
34143 ecr 469914146], length 0
11:28:35.745803 IP 192.168.0.166.51242 > 3.216.147.127.443: Flags [.], ack 1, win 501, options [nop,nop,TS val 469914808 ecr 3381234143], leng
th 0
11:28:35.806123 IP 3.219.245.116.443 > 192.168.0.166.36806: Flags [P.], seq 1:95, ack 71, win 186, options [nop,nop,TS val 1250290155 ecr 3174
611898], length 94
11:28:35.806140 IP 192.168.0.166.36806 > 3.219.245.116.443: Flags [.], ack 95, win 501, options [nop,nop,TS val 3174612104 ecr 1250290155], le
ngth 0
^C
11 packets captured
11 packets received by filter
0 packets dropped by kernel
```

Port capture

`tcpdump` allows you to specify network packets that are either using some port **X** as source or destination. For example, to capture DNS traffic, you can use `port 53`. You could prefix the **port** keyword with **src**/**dst** as `src port 53` or `dst port 53` and filter it even further.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i any port 53 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
11:30:12.115807 IP 127.0.0.1.57463 > 127.0.0.53.53: 59669+ [1au] A? securepubads.g.doubleclick.net. (59)
11:30:12.115820 IP 127.0.0.1.57463 > 127.0.0.53.53: 23842+ [1au] AAAA? securepubads.g.doubleclick.net. (59)
11:30:12.115973 IP 127.0.0.53.53 > 127.0.0.1.57463: 59669 1/0/1 A 142.250.70.66 (75)
11:30:12.116045 IP 127.0.0.53.53 > 127.0.0.1.57463: 23842 1/0/1 AAAA 2404:6800:4009:803::2002 (87)
11:30:12.618674 IP 127.0.0.1.58225 > 127.0.0.53.53: 48744+ [1au] A? pagead2.googlesyndication.com. (58)
11:30:12.618909 IP 192.168.0.166.48870 > 192.168.0.1.53: 30256+ A? pagead2.googlesyndication.com. (47)
11:30:12.619055 IP 127.0.0.1.58225 > 127.0.0.53.53: 45435+ [1au] AAAA? pagead2.googlesyndication.com. (58)
11:30:12.619150 IP 192.168.0.166.38578 > 192.168.0.1.53: 6365+ AAAA? pagead2.googlesyndication.com. (47)
11:30:12.621138 IP 192.168.0.1.53 > 192.168.0.166.48870: 30256 1/0/0 A 172.217.174.226 (63)
11:30:12.621299 IP 127.0.0.53.53 > 127.0.0.1.58225: 48744 1/0/1 A 172.217.174.226 (74)
11:30:12.622698 IP 192.168.0.1.53 > 192.168.0.166.38578: 6365 1/0/0 AAAA 2404:6800:4009:832::2002 (75)
11:30:12.622881 IP 127.0.0.53.53 > 127.0.0.1.58225: 45435 1/0/1 AAAA 2404:6800:4009:832::2002 (86)
11:30:12.627669 IP 127.0.0.1.37365 > 127.0.0.53.53: 357+ [1au] A? pagead2.googlesyndication.com. (58)
11:30:12.627883 IP 127.0.0.53.53 > 127.0.0.1.37365: 357 1/0/1 A 172.217.174.226 (74)
11:30:12.627961 IP 127.0.0.1.37365 > 127.0.0.53.53: 37756+ [1au] AAAA? pagead2.googlesyndication.com. (58)
11:30:12.628073 IP 127.0.0.53.53 > 127.0.0.1.37365: 37756 1/0/1 AAAA 2404:6800:4009:832::2002 (86)
^C
16 packets captured
28 packets received by filter
0 packets dropped by kernel
```

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump  -i enp4s0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:57:56.867156 IP lab1003-HP-280-G4-MT-Business-PC.54088 > ae69789f15ba8a942.awsglobalaccelerator.com.https: Flags [.], ack 946124812, win 50
1, options [nop,nop,TS val 4142813175 ecr 2874162909], length 0
11:57:56.932898 IP ae69789f15ba8a942.awsglobalaccelerator.com.https > lab1003-HP-280-G4-MT-Business-PC.54088: Flags [.], ack 1, win 221, optio
ns [nop,nop,TS val 2874173152 ecr 4142731429], length 0
11:57:57.480373 IP lab1003-HP-280-G4-MT-Business-PC.52368 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [P.], seq 2655984
789:2655984828, ack 1638387016, win 501, options [nop,nop,TS val 2466341831 ecr 1861270164], length 39
11:57:57.482451 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.52368: Flags [P.], seq 1:40, a
ck 39, win 501, options [nop,nop,TS val 1861328972 ecr 2466341831], length 39
11:57:57.482452 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.52368: Flags [.], ack 39, win
501, options [nop,nop,TS val 1861328972 ecr 2466341831], length 0
11:57:57.482459 IP lab1003-HP-280-G4-MT-Business-PC.52368 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [.], ack 40, win
501, options [nop,nop,TS val 2466341833 ecr 1861328972], length 0
11:57:57.482464 IP lab1003-HP-280-G4-MT-Business-PC.52368 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [.], ack 40, win
501, options [nop,nop,TS val 2466341833 ecr 1861328972], length 0
11:57:58.447970 IP lab1003-HP-280-G4-MT-Business-PC.44542 > ec2-54-229-31-114.eu-west-1.compute.amazonaws.com.https: Flags [P.], seq 171452828
8:1714528327, ack 4288129207, win 501, options [nop,nop,TS val 3019107970 ecr 2986624119], length 39
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump tcp  port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:03:01.772495 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.39202: Flags [P.], seq 3778152
860:3778152884, ack 2167482120, win 501, options [nop,nop,TS val 1861633268 ecr 2466642715], length 24
12:03:01.772514 IP lab1003-HP-280-G4-MT-Business-PC.39202 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [.], ack 24, win
501, options [nop,nop,TS val 2466646123 ecr 1861633268], length 0
12:03:01.772613 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.39202: Flags [F.], seq 24, ack
 1, win 501, options [nop,nop,TS val 1861633269 ecr 2466642715], length 0
12:03:01.772617 IP lab1003-HP-280-G4-MT-Business-PC.39202 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [P.], seq 1:40, a
ck 24, win 501, options [nop,nop,TS val 2466646124 ecr 1861633268], length 39
12:03:01.772745 IP lab1003-HP-280-G4-MT-Business-PC.39202 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [P.], seq 40:64,
ack 25, win 501, options [nop,nop,TS val 2466646124 ecr 1861633269], length 24
12:03:01.772751 IP lab1003-HP-280-G4-MT-Business-PC.39202 > a23-193-114-56.deploy.static.akamaitechnologies.com.https: Flags [F.], seq 64, ack
 25, win 501, options [nop,nop,TS val 2466646124 ecr 1861633269], length 0
12:03:01.774835 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.39202: Flags [R], seq 37781528
84, win 0, length 0
12:03:01.774837 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.39202: Flags [R], seq 37781528
85, win 0, length 0
12:03:01.774961 IP a23-193-114-56.deploy.static.akamaitechnologies.com.https > lab1003-HP-280-G4-MT-Business-PC.39202: Flags [R], seq 37781528
85, win 0, length 0
^C
9 packets captured
9 packets received by filter
0 packets dropped by kernel
```

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump  -i  enp4s0 -s 0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:11:13.334853 IP lab1003-HP-280-G4-MT-Business-PC.52892 > ec2-34-237-73-95.compute-1.amazonaws.com.https: Flags [P.], seq 2884701084:2884701
323, ack 3749921077, win 501, options [nop,nop,TS val 159759894 ecr 4207543571], length 239
12:11:13.537499 IP ec2-34-237-73-95.compute-1.amazonaws.com.https > lab1003-HP-280-G4-MT-Business-PC.52892: Flags [P.], seq 1:260, ack 239, wi
n 572, options [nop,nop,TS val 4207559574 ecr 159759894], length 259
12:11:13.537522 IP lab1003-HP-280-G4-MT-Business-PC.52892 > ec2-34-237-73-95.compute-1.amazonaws.com.https: Flags [.], ack 260, win 501, optio
ns [nop,nop,TS val 159760096 ecr 4207559574], length 0
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$
```