NETWORK MONITORING TOOL REPORT

LANGUAGES/TOOLS USED:

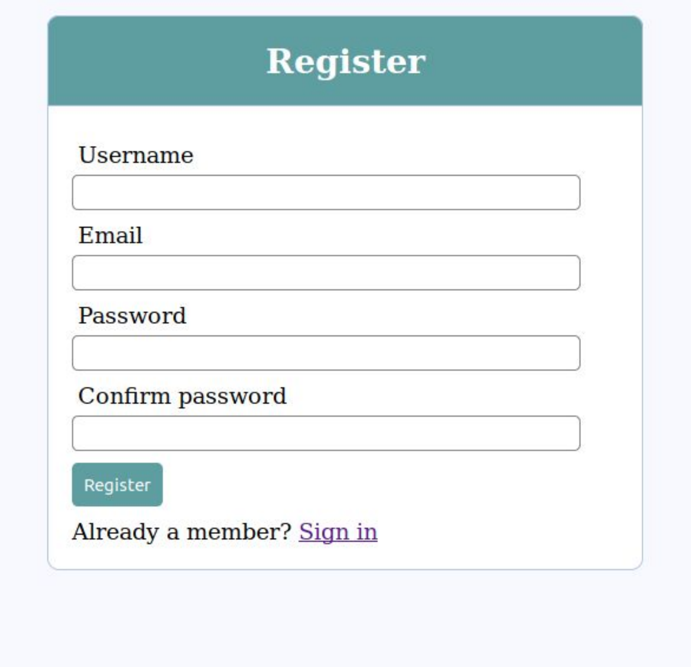
Bash, Sed, Awk, PHP, MYSQL,HTML, CSS

The objective of this project is to capture packets using unix commands in the network and display details of packets on a webpage using PHP and MySQL.The second part of the project includes displaying the details about the machine that is generating most frequent packets in the network.

Features of the project:

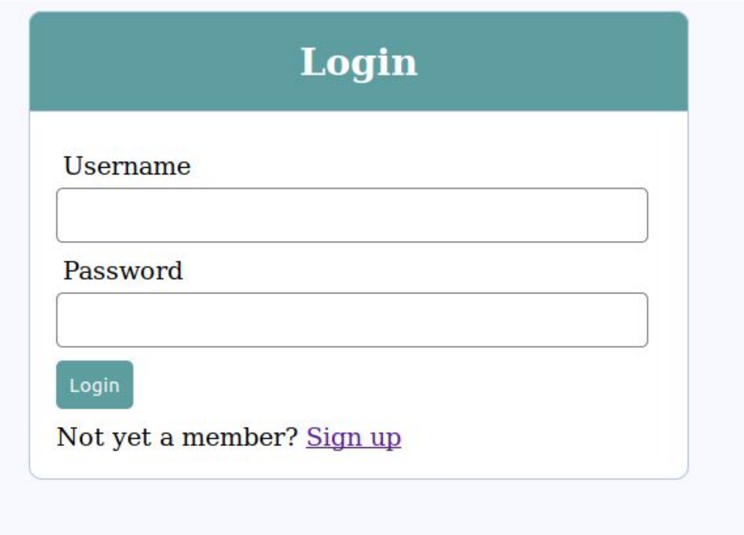
1.Registration
2.Login
3.Packet Details(ARP,UDP,IPV4)
4.Top Users
5.Unix commands running in backend
6.MySQL queries

1.Registration (register.php,functions.php)



A new user can register to view Packet details on this webpage .The queries entered gets stored in MySQL table using PHP after proper validation.If the details are correct then you get redirected to login.html so that you can login according to registered credentials.

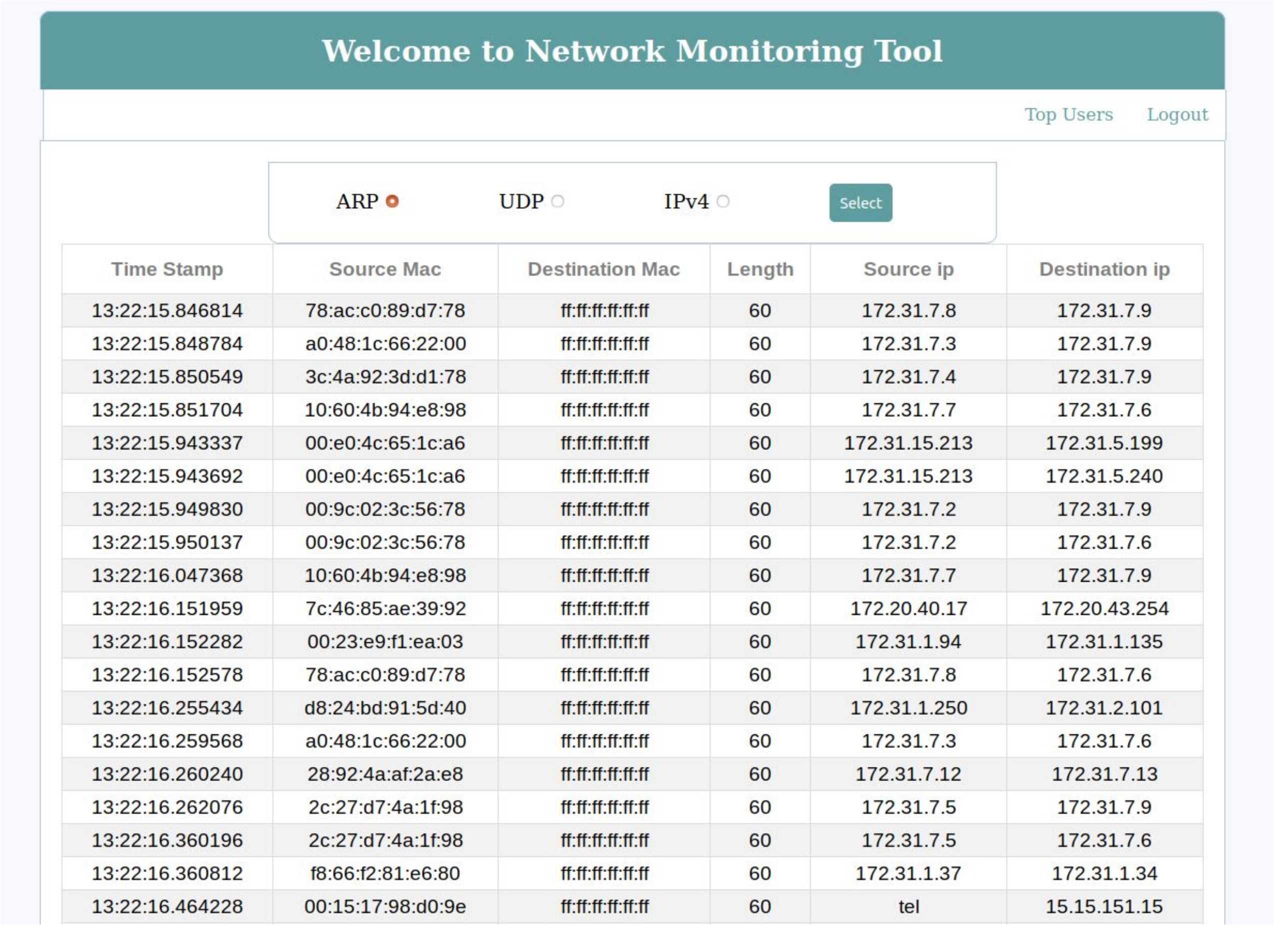
2.Login(login.php,functions.php)



After registration you can login using proper credentials.Necessary from validation takes pace.

3.Packet Details(index.php)

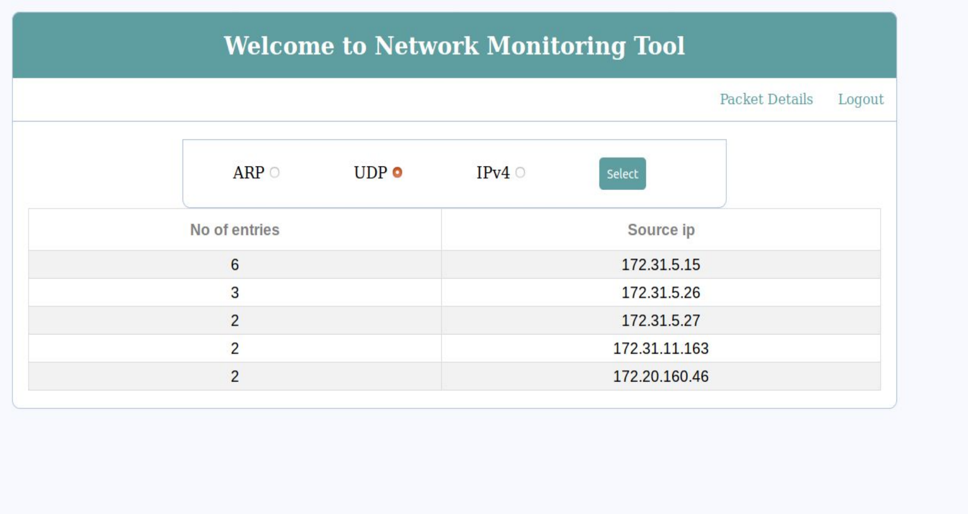
\



Time Stamp	Source Mac	Destination Mac	Length	Source ip	Destination ip
13:22:15.846814	78:ac:c0:89:d7:78	ff:ff:ff:ff:ff:ff	60	172.31.7.8	172.31.7.9
13:22:15.848784	a0:48:1c:66:22:00	ff:ff:ff:ff:ff:ff	60	172.31.7.3	172.31.7.9
13:22:15.850549	3c:4a:92:3d:d1:78	ff:ff:ff:ff:ff:ff	60	172.31.7.4	172.31.7.9
13:22:15.851704	10:60:4b:94:e8:98	ff:ff:ff:ff:ff:ff	60	172.31.7.7	172.31.7.6
13:22:15.943337	00:e0:4c:65:1c:a6	ff:ff:ff:ff:ff:ff	60	172.31.15.213	172.31.5.199
13:22:15.943692	00:e0:4c:65:1c:a6	ff:ff:ff:ff:ff:ff	60	172.31.15.213	172.31.5.240
13:22:15.949830	00:9c:02:3c:56:78	ff:ff:ff:ff:ff:ff	60	172.31.7.2	172.31.7.9
13:22:15.950137	00:9c:02:3c:56:78	ff:ff:ff:ff:ff:ff	60	172.31.7.2	172.31.7.6
13:22:16.047368	10:60:4b:94:e8:98	ff:ff:ff:ff:ff:ff	60	172.31.7.7	172.31.7.9
13:22:16.151959	7c:46:85:ae:39:92	ff:ff:ff:ff:ff:ff	60	172.20.40.17	172.20.43.254
13:22:16.152282	00:23:e9:f1:ea:03	ff:ff:ff:ff:ff:ff	60	172.31.1.94	172.31.1.135
13:22:16.152578	78:ac:c0:89:d7:78	ff:ff:ff:ff:ff:ff	60	172.31.7.8	172.31.7.6
13:22:16.255434	d8:24:bd:91:5d:40	ff:ff:ff:ff:ff:ff	60	172.31.1.250	172.31.2.101
13:22:16.259568	a0:48:1c:66:22:00	ff:ff:ff:ff:ff:ff	60	172.31.7.3	172.31.7.6
13:22:16.260240	28:92:4a:af:2a:e8	ff:ff:ff:ff:ff:ff	60	172.31.7.12	172.31.7.13
13:22:16.262076	2c:27:d7:4a:1f:98	ff:ff:ff:ff:ff:ff	60	172.31.7.5	172.31.7.9
13:22:16.360196	2c:27:d7:4a:1f:98	ff:ff:ff:ff:ff:ff	60	172.31.7.5	172.31.7.6
13:22:16.360812	f8:66:f2:81:e6:80	ff:ff:ff:ff:ff:ff	60	172.31.1.37	172.31.1.34
13:22:16.464228	00:15:17:98:d0:9e	ff:ff:ff:ff:ff:ff	60	tel	15.15.151.15

You can view the packets details of different ARP,UDP,IPV4 packets captured.All the necessary details are displayed in a tabular manner .This has been done by running unix command tcpdump which captures the packet,text processing using sed ,awk and table creation and extraction using MySQL and PHP.

4.Top Users(topusers.php)



ARP ○ UDP ● IPv4 ○

No of entries	Source ip
6	172.31.5.15
3	172.31.5.26
2	172.31.5.27
2	172.31.11.163
2	172.20.160.46

This feature of the project displays the top 5 machines (IP’s) sending most frequent IPv4,ARP,UDP packets.Unix commands like sort ,uniq,head have been useful to encorporate this feature.

5.Unix commands in backend(separate.sh,refresh.sh)

Uniq commands have been a great treat for the completion of this project.The main command to capture the packets is tcpdump.After which text proxessing happens using grep,sed,awk,cut paste.
Then to display top users commands like sort,uniq and head were useful.
Some of the commands that were useful are mentioned below.

```
/usr/sbin/tcpdump -ne -c 100 >file
grep ARP file>arp/ARP
awk '//{print substr($4, 1, length($4)-1)}' arp/request > arp/req/destMAC
cut -d "." -f5 ipv4/temp > ipv4/destport
paste arp/rep/timestamp arp/rep/sourceMAC arp/rep/destMAC arp/rep/length
arp/rep/sourceip >>ARP
awk '//{print $5}' ARP|sort|uniq -c |sort -nr|head -5 >topARP
```

refresh.sh is used to clear out MySQL table so that all registered users can be removed that is to empty the users table.

6.MySQLQueries(functions.php, separate,sh, index.php, top5.php)

There were many mysql queries that were used throughout the project to create the table,from validation,data extraction,data manipulation ,etc.Some of the queries are mentioned below.

```
use packets;

DROP TABLE if exists ipv4;

create table arp(
Time_stamp varchar(20),
Source_mac varchar(20),
Destination_mac varchar(20),
Length varchar(20),
Source_ip varchar(20),
Destination_ip varchar(20));


INSERT INTO user (username, email, password) VALUES('$username', '$email',
'$password')
SELECT * FROM user WHERE username='$username' AND password='$password'
LIMIT 1
SELECT * FROM udp
```

RECOMMENDATIONS:

1.More types of packets can be included to be captured.

2.Better text processing can be done as sometimes due to extra word you can get a particular field of a packet wrong.