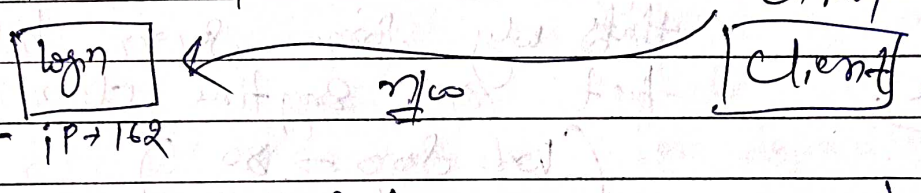
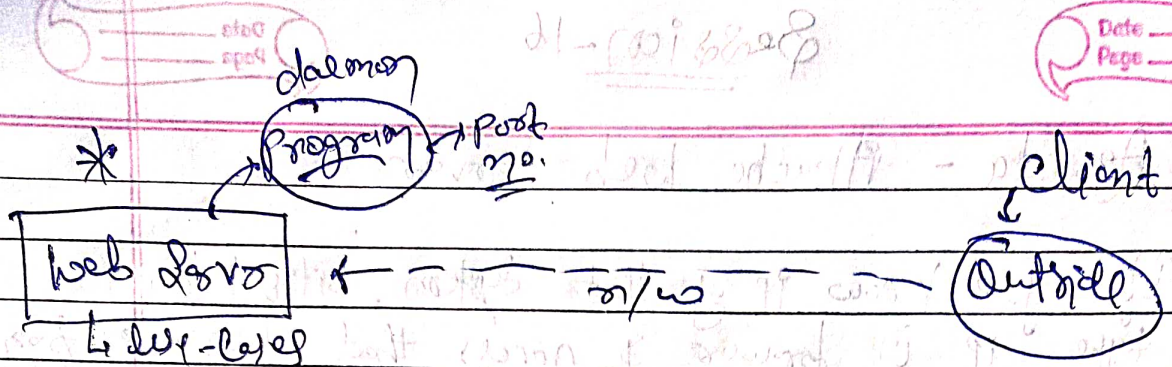
Session-16

* Agenda - Apache web server
* If you know ip of that system, without login type ip in browser & access that programs from that laptop.
* 

* If your system configure as server, you provide services behind the scene scene, that is then you don't have to login to that system.
* This is the main diff b/w firefox / program.
* Server is the kind of program that #date we don't need to login to that system.
* This kind of program / services i.e, daemon.
* program → Login & run the progm
  Server program → without login access the progm, i.e daemon.
* Daemon run in bgnd. if you want to access you don't need to login to that system.
* (Services == daemon)
  ↳ # systemctl status httpd
  # systemctl start httpd.
* Every use case server available →
  ① If your need that any body can use your website or web page if this need use web server.
  ② W.S is a program if you want any body can access / connect to that progm / daemon thy your daemon need one unique no. ↷ Port no.
  ③ Port no. → 2^{16} → 0 to 65536
  (this much range is valid port no.)



* Mainly client should know port no. that's why some servs has std. port no. Eg time clients used.

(web serv → 80
mail → 25)

*(We will change by need)

* Change the port no →

```
#cd /etc/httpd/conf
#ls
#gedit httpd.conf
```

(Change port no.)

Listn 1234 ← 80

* If change it won't update your new program so for this re-start the system.

```
#netstat -tnlp
#Systemctl restart httpd.
```

(failed) → ?

→ Cause also failed at port 80;

* If failed then go to deb dir in see the reason of it →

```
#journalctl -xe
```

(Provide lots of info)

* Due to some kind of security they disable.

(SELinux)

↳ Security Enhanced Linux

(Linux os)

* Source file security.

* Web Server → 80 ✓
→ 81 ✓
(Or)
↳ SELinux
↓
(D.B)

1234 ✗

* If you provide port 80, 81 client → then A/C to S.E Dbase it is ok, but other than that they won't allow.

→ They have set of rules for port no. of wd.
→ SE Linux own internal DB, here defined that.

* for any reason if dev want to allow then at that time dev can use two ways -
(i) SELinux update d.b and allow one to use other port.
(ii) or (ii) Disable SELinux.

* # getenforce (status of SELinux)
# setenforce 0 (disable)
# setenforce 1 (enable)
# getenforce
# systemctl restart httpd.
# netstat -tnlp
(→ now working)

* You can give only those port to the client they have range i.e (0 - 65535).
* OR you can only give those that free in list of.
→ (Same port multiple program → failed)
* If SELinux is enable they only allow those ports that are there in D.B.

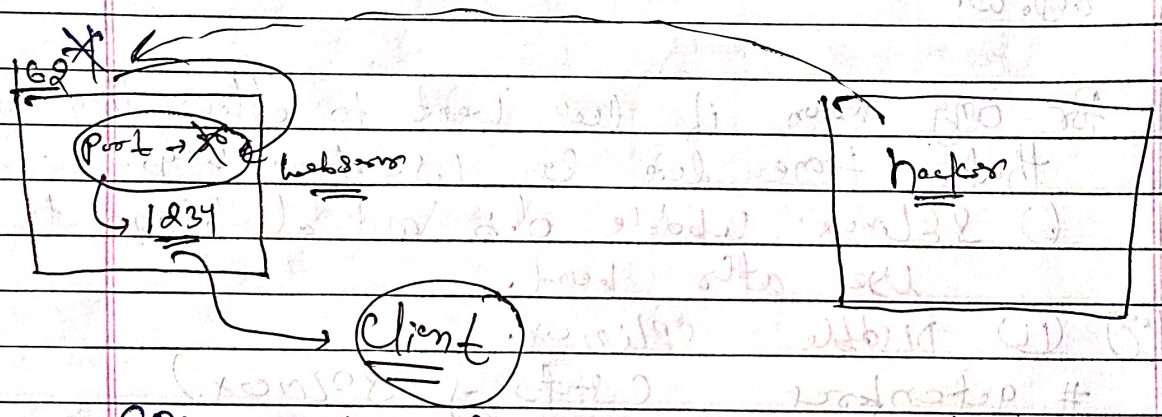
*
1234 → Program/Service
→ P 2
Only one port for any program

Prgm → 80
→ 81
→ 1234
→ have multiple port to one program.

* For all one daemon / source / program have multiple ports.

* Config file → Listen 80
Listen 81
#systemctl restart httpd Listen 123
netstat -tnlp

* Why we want to change the port no. ?
=>



* One of the common reason, hacker guys are scanning the n/w they first get the IP & then for connecting the program they see the port no. If they found the port no then they attack. So, need to change the

Myth

* How hacker come to know about IP?
→ → Scanning IP → Nmap (scanning tool)
yum install nmap
ifconfig enp0s3

System

* now, we do scanning to check IP of 162 & available or not.
[#nmap -sP 192.168.0.2-250]
(list of IP Live right now in this range we have Connectivity)
=
→ same now they show

* Search for IP - 162
* # nmap -sP 192.168.0.162

* from (B) we see A is live.

* See all the service running in IP → 162.

nmap -sT 192.168.0.162
(All Service list)
→
* without going to that system we get it.
* Now, we got port and do any testing like penitest testing.
* If some system change the port then will know.
→ They do default scanning.
nmap -sT -p 1111 192.168.0.162.
(port)
* Get more detailed scanning of that port →
# nmap -sT -p 111 -sV 192.168.0.162
(→ name of service & software name, Version)
↳ All the information.

* If you want to change the port no. & you get security more i.e, myth.
* Change port doesn't impact power.
* Server
↳ tomcat
↳ 8080
↳ Boss
↳ 8080
(multiple server/daemon have same port, then you need to change the port no.)
multiple same program
* have same port no. → Then need to change port no.

* If you want to change something in configuration file don't change directly to that file.
* If something might not work (some spelling mistake done then it will impact your server it might failed crash.

* For this apache has secondary file of configuration file.
* In last line they mention if you create new file inside that repo. with the extension .conf, then it will be treated as configuration file.

cd /etc/httpd/conf.d/
ls
gedit vimal.conf

[Listen 222] (first of your apache log file.)

systemctl restart httpd.

(main file, this will go to vimal.conf get the info & use that.

netstat -tnlp

* change the document root.

gedit vimal.conf
Listen 2222
document root /var/www/vimal

mydir
cd → /var/www/vimal
ls
cat > myindex.html
cat myindex.html

systemctl restart httpd.

* Now our document root is changed.

* Now, we have two config root files
  # ls /etc/httpd/conf/httpd.conf → overriding
  # ls /etc/httpd/conf.d/vimal.conf
  (↳ Secondary / include file)
* Priority give to Secondary file / include file.

* When we run both config. file then they normally connect with secondary one.

* Change the document root of config file →
  # mkdir /web2
  # cd /web2
  # ls
  # vim cat > /w.html
  /w/w vimal
  #pwd
  # cd /etc/httpd/conf.d/
  # ls
  # gedit vimal.conf
  → Listn 222
  → ~~Document root~~ documentroot /web2

* # Systemctl restart httpd.
* We have changed but they doesn't give permission. forbidden.
  → Same case working, some case not working.
* index.html
  ↳ (predefined first home page.) / Default home page index.html.
  ↳ In config. file they have config.