HOW TO INSTALL

Ubuntu And Host a website with the help of MySQL, MariaDB,PhP and Apache2

HOW TO CONFIGURE

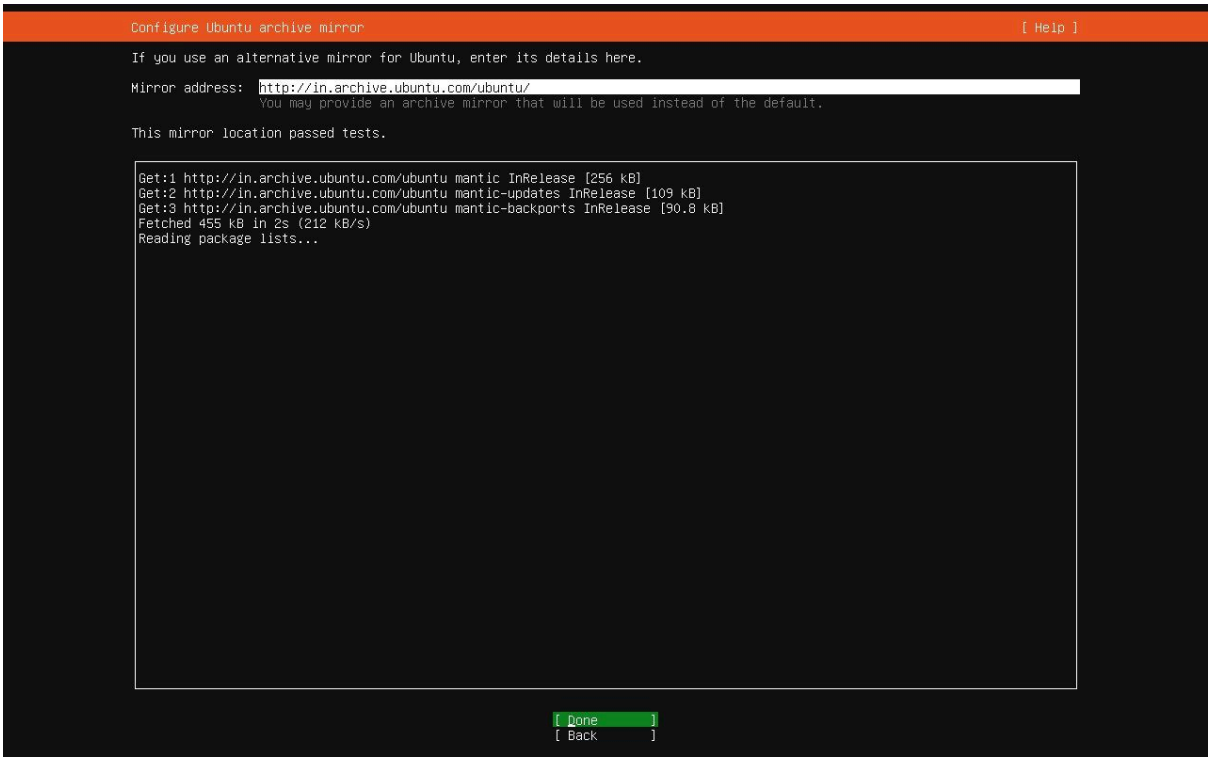
Splunk Universal Forwarder on Ubuntu and Monitor Website Logs

Prepared by,

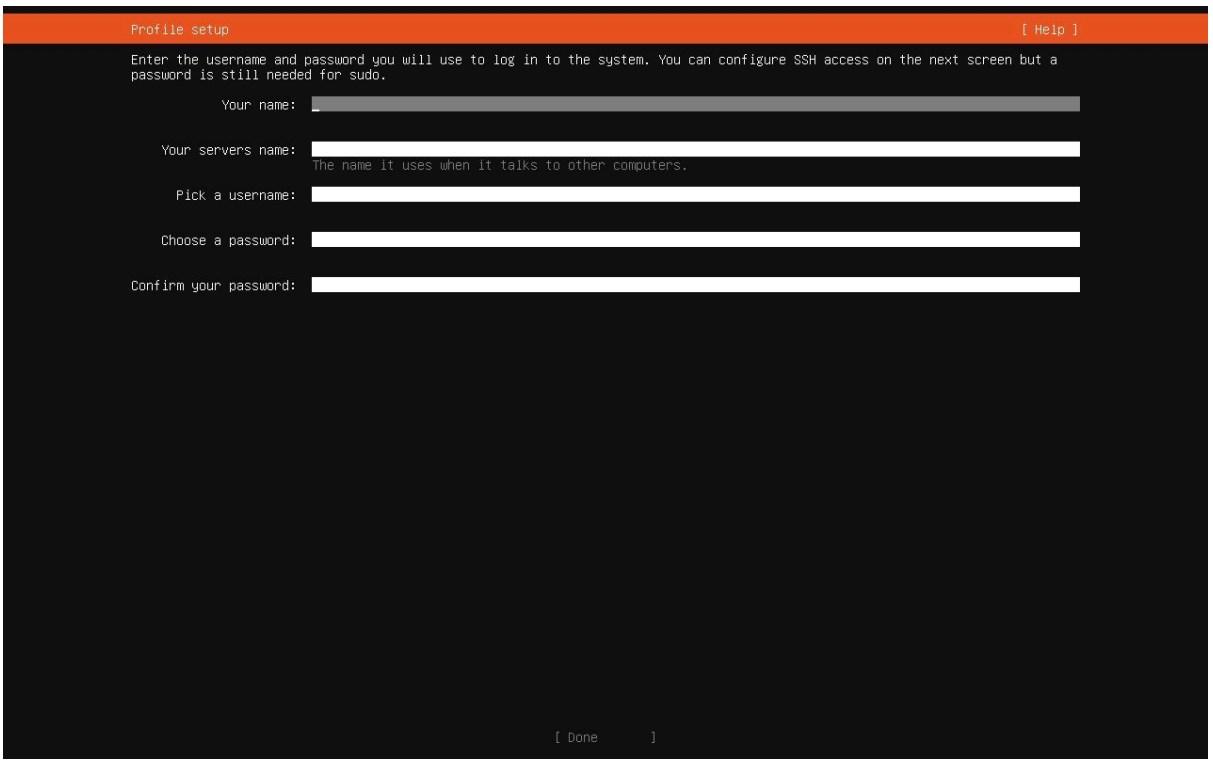
Athira V, Ramki Krishnan M R, Syam Babu

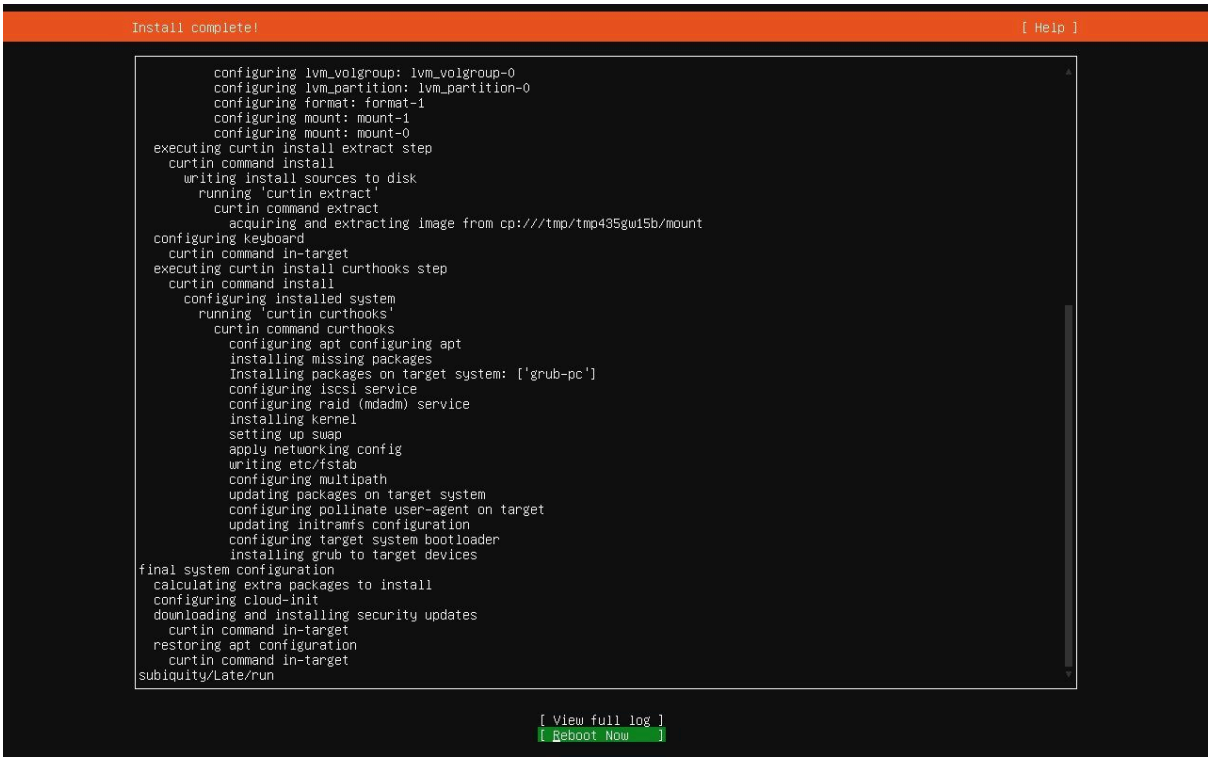
1.Steps to install Ubuntu Server

Download ubuntu server 22.04 . Install and configure a virtual machine in virtual box. Open Ubuntu and lets start it and install now.



Give your name ; server name ; username ; password





Ubuntu Installation is completed. The Ubuntu system terminal page is open and login with our username and password.

```
Ubuntu 23.10 krish tty1

krish login: ramki
Password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Feb  5 03:26:25 PM UTC 2024

  System load:  1.11               Processes:               119
  Usage of /:   18.8% of 11.21GB   Users logged in:         0
  Memory usage: 3%                 IPv4 address for enp0s3: 192.168.18.145
  Swap usage:   0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ramki@krish:~$
```

Step 2: Install Apache

Open the terminal on your Ubuntu system. The terminal is a text interface to your computer, which you will use to run all the commands.

First, update your software package list.

ramki@krish:~$ sudo apt-get update

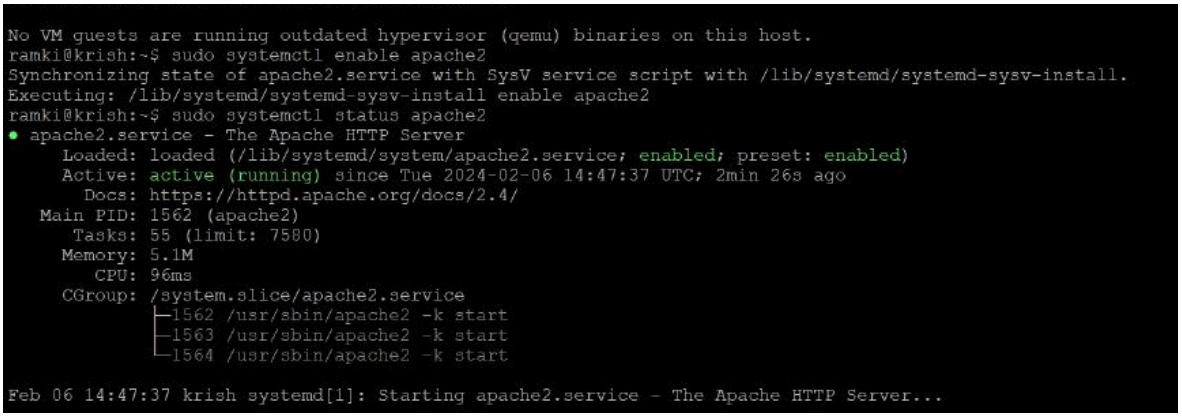
```
ramki@krish:~$ sudo apt-get update
[sudo] password for ramki:
Hit:1 http://in.archive.ubuntu.com/ubuntu mantic InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu mantic-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu mantic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu mantic-security InRelease
Reading package lists... Done
ramki@krish:~$
```

The next step in setting up the LAMP stack will be installing and configuring Apache2, the web server. Run the below command to install Apache 2 on Ubuntu.

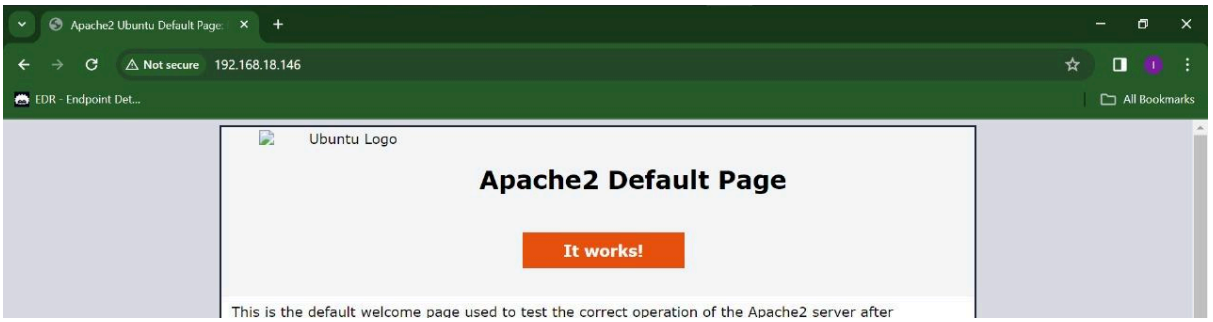
ramki@krish:~$ sudo apt install apache2

```
Last login: Tue Feb  6 14:43:58 2024
ramki@krish:~$ sudo apt install apache2
[sudo] password for ramki:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 41 not upgraded.
Need to get 2,097 kB of archives.
After this operation, 8,130 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

It is necessary to allow Apache2 to start at the system boot time and to start the service to verify its status as well.
ramki@krish:~$ sudo systemctl enable apache2
ramki@krish:~$ sudo systemctl status apache2



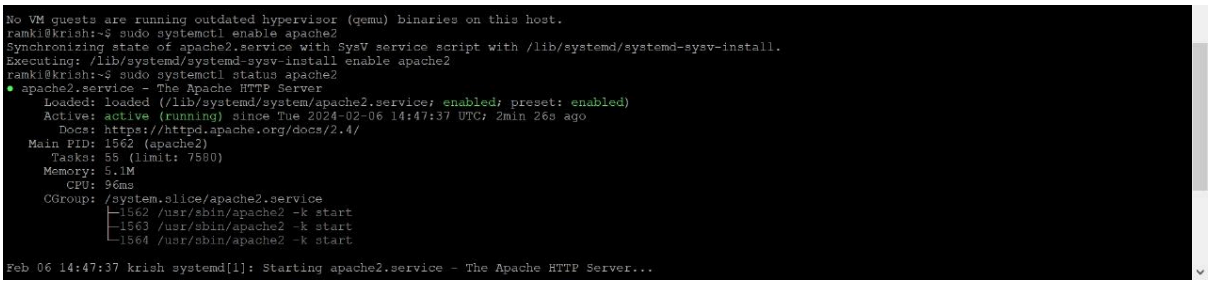
Open your web browser, and type localhost in the address box to verify that the Apache server has been started.If the Apache2 web server is running, it will display the default Apache2 index page



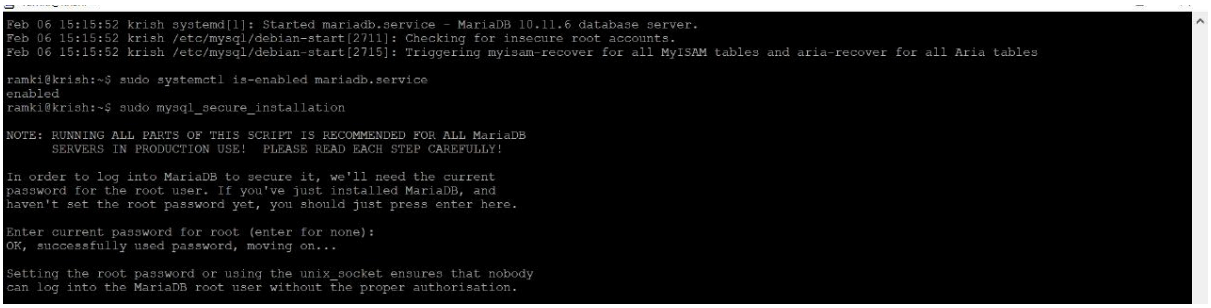
STEP 3: Installing MariaDB

Using the following command

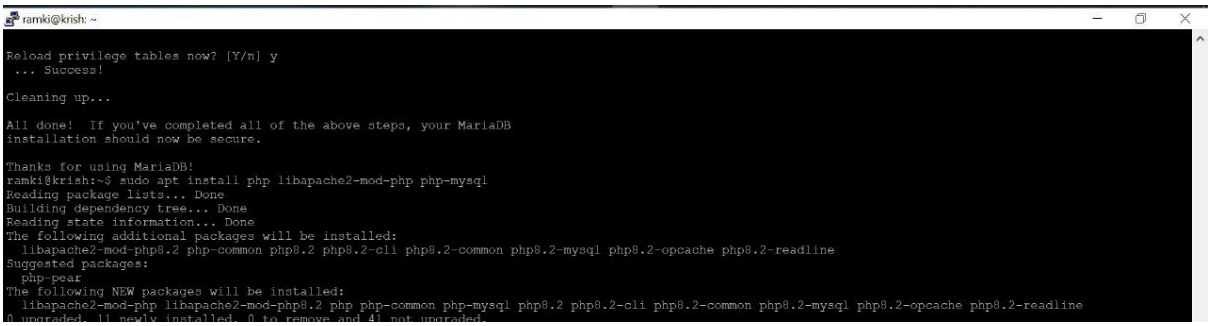
After checking the status of MariaDB services



We enable MariaDB services

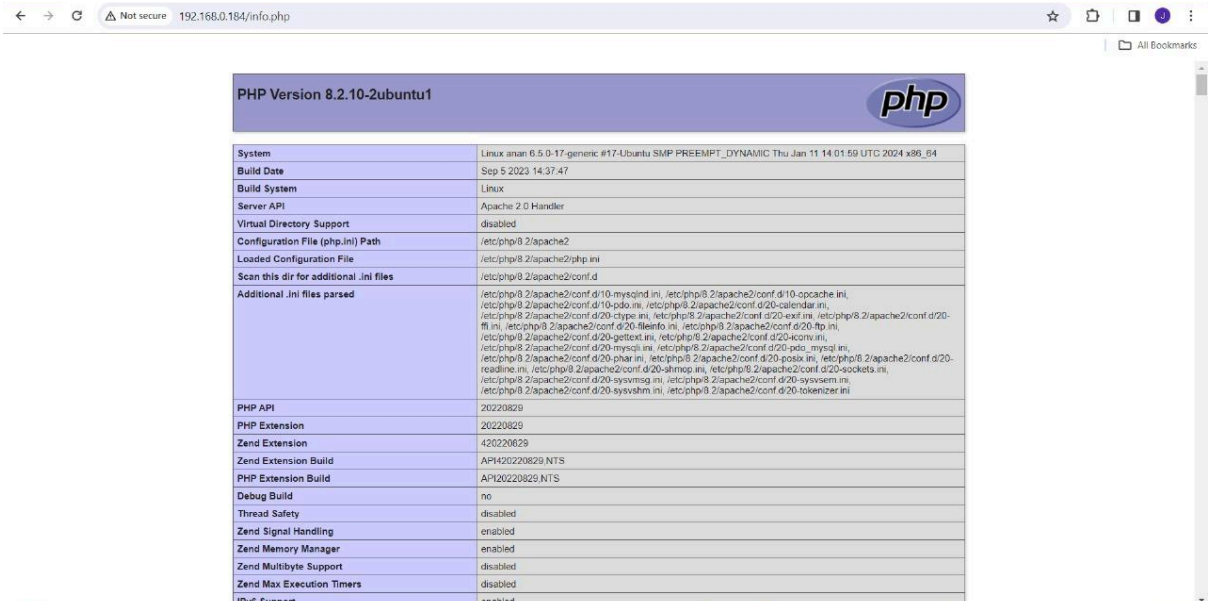


STEP 4: Installing MYSQL, after complete installation we install PHP package. Installing PHP packages.



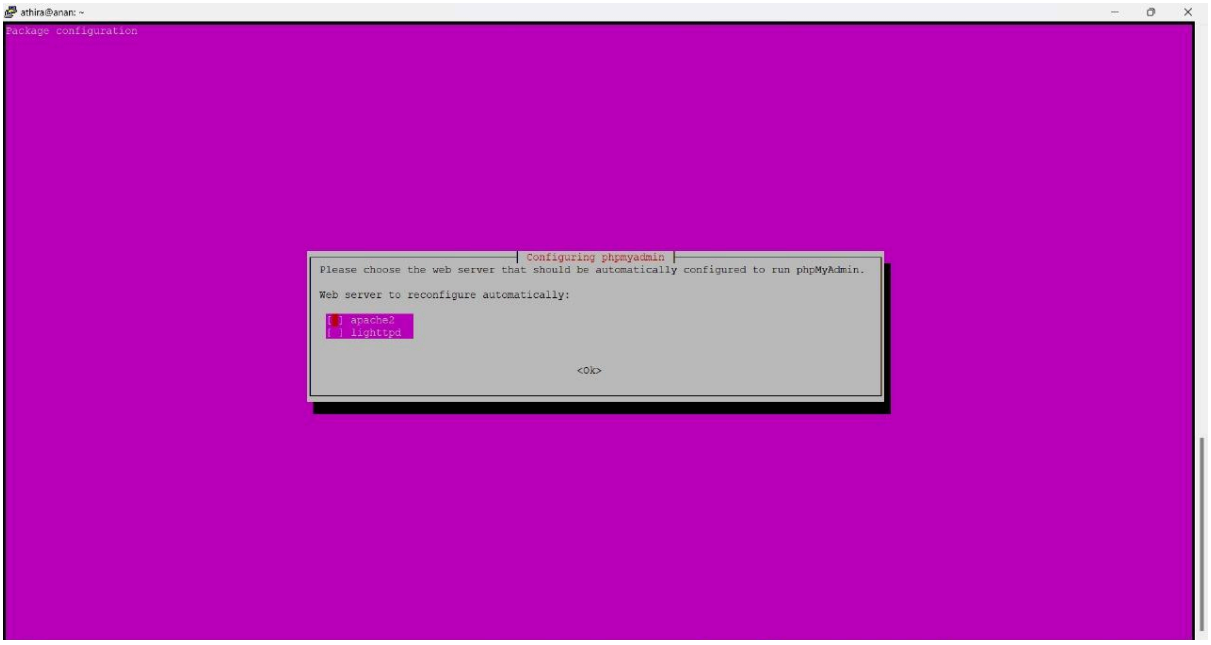
After that we restart Apache2

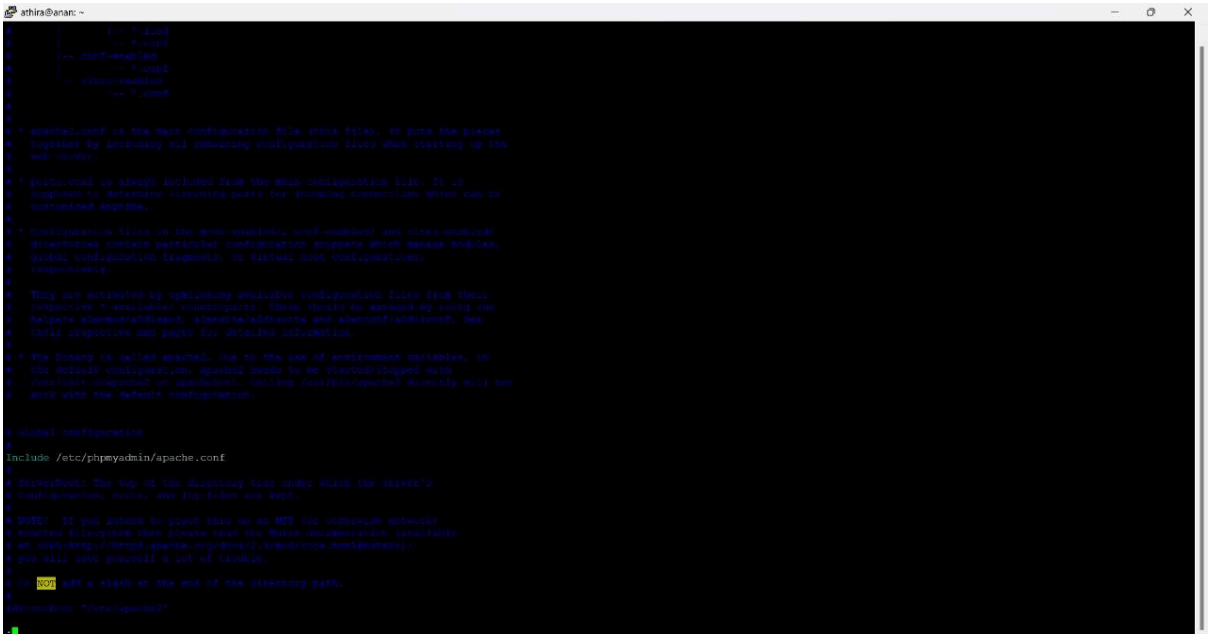
Open your web browser,and type localhost /info.php in the address box to verify that the php has been started.



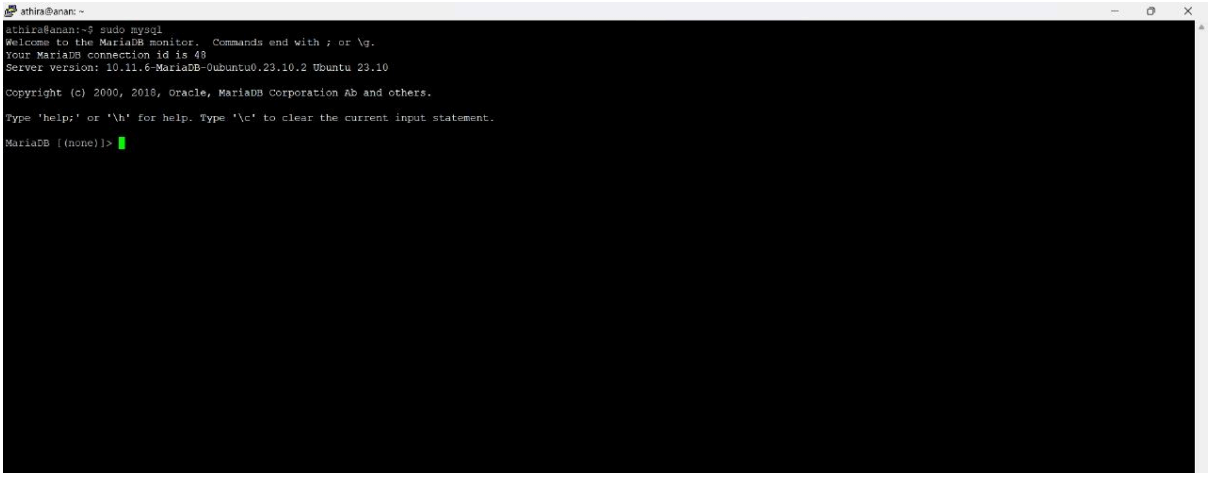
STEP 5: Installing PhP Admin

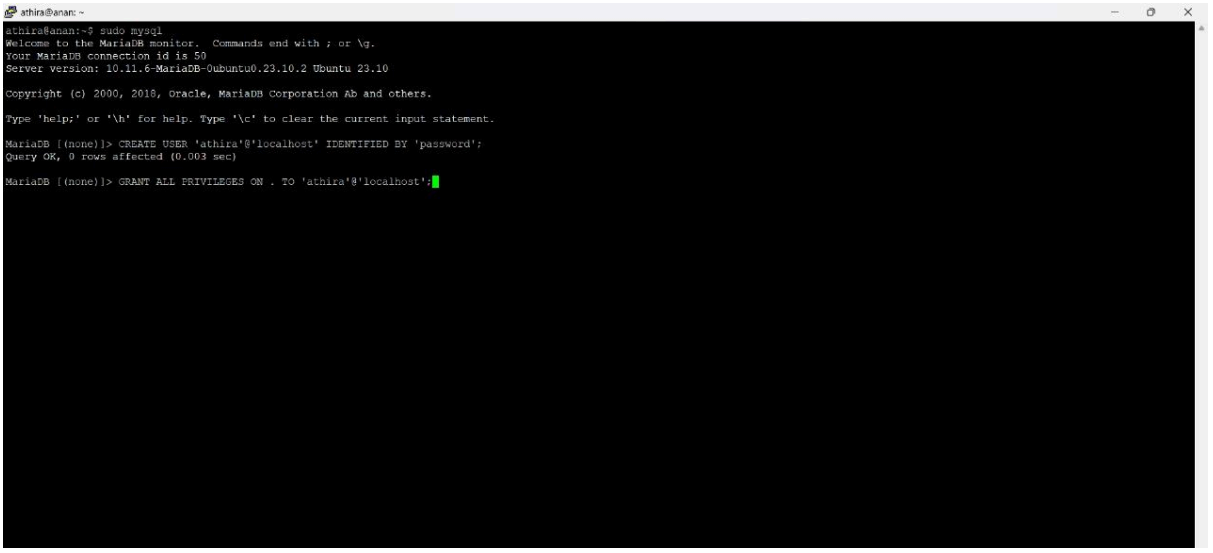
Then we do these configurations as done below in php admin





using admin rights to get sudo mysql





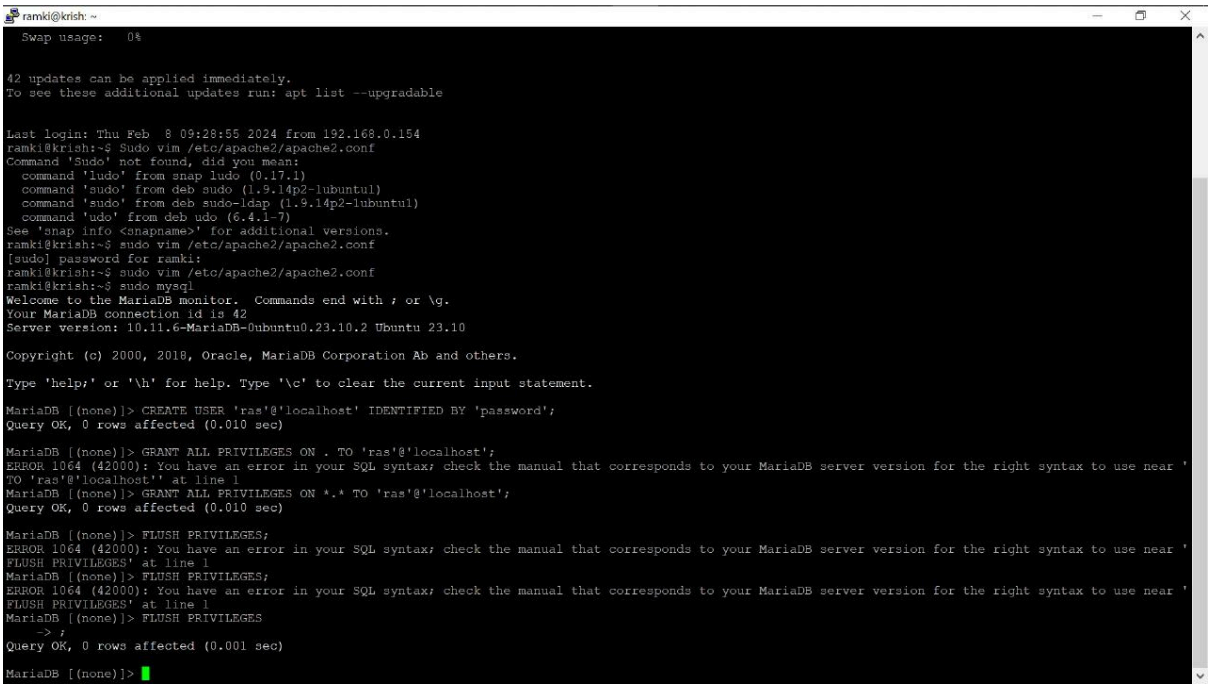
Adding database using my sql,Creating a user local identified by password.

Granting all privileges to the local user.

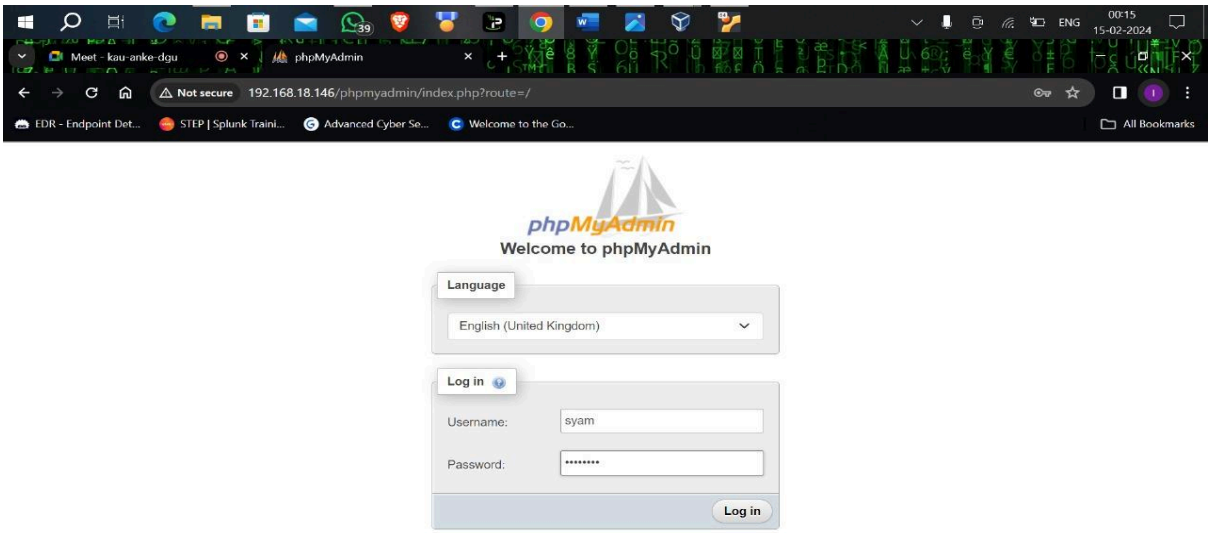
Pushing the privileges in to the db.

Exiting out of the database.

Restarting the Apache again.

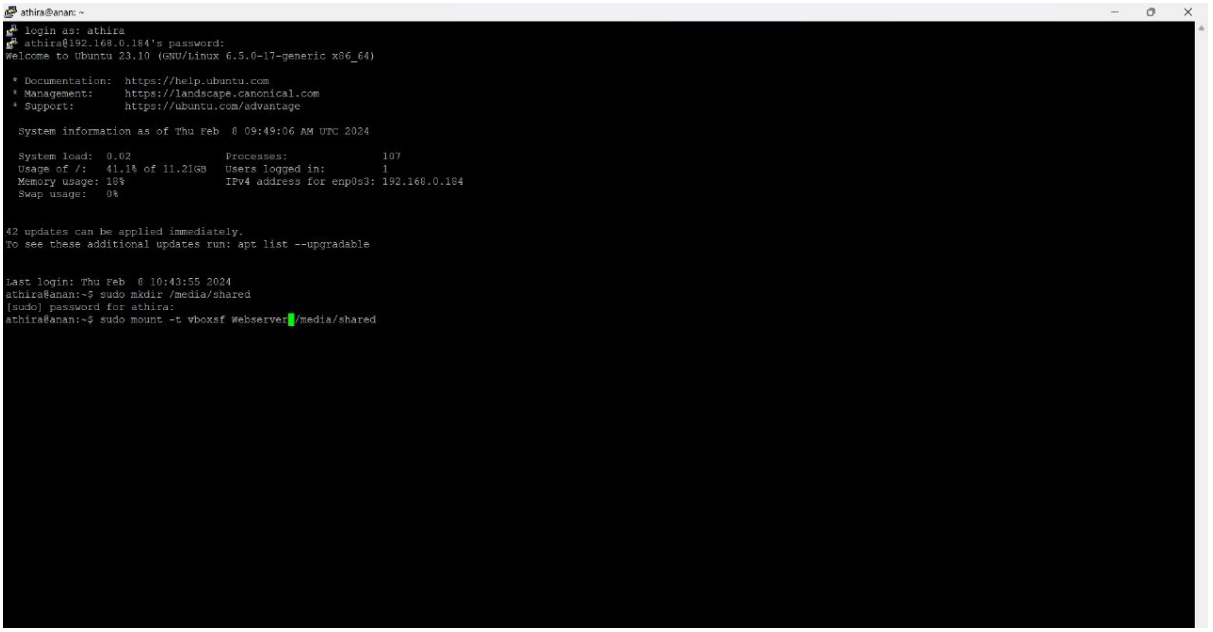


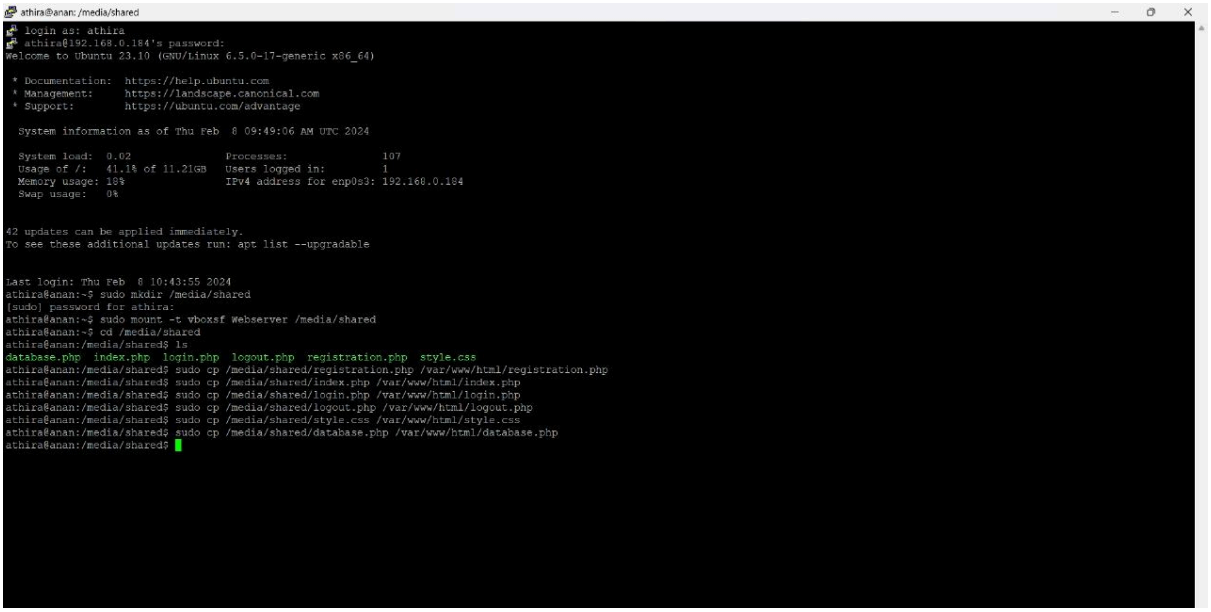
Logging in to the PHP admin.



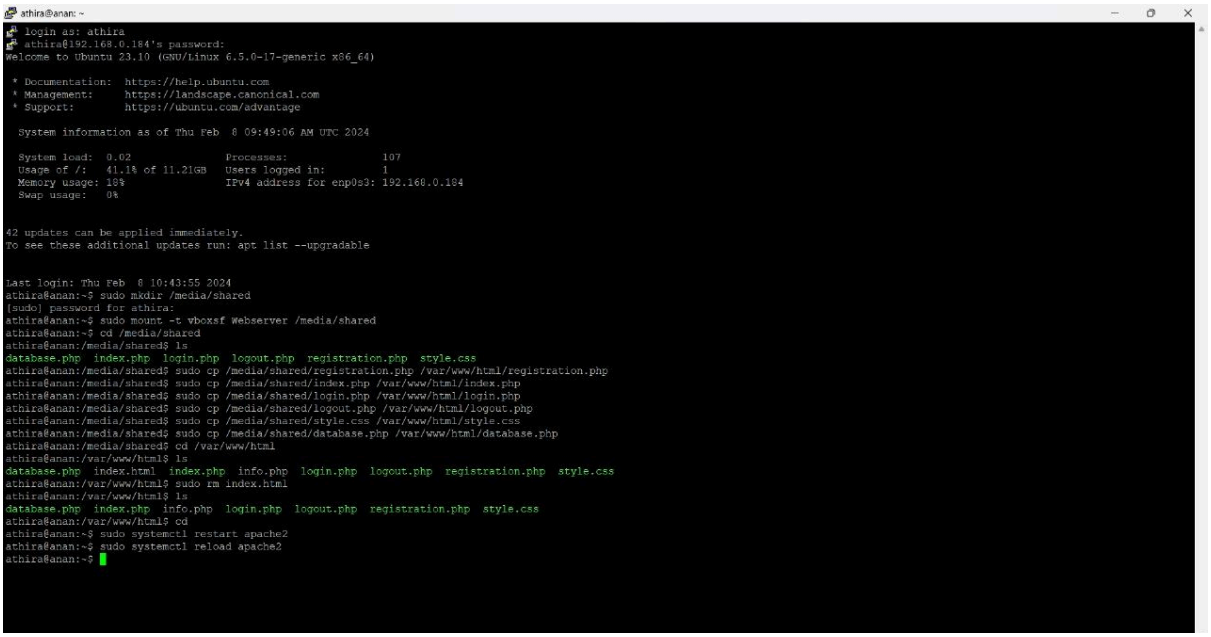
Making a media/shared directory.

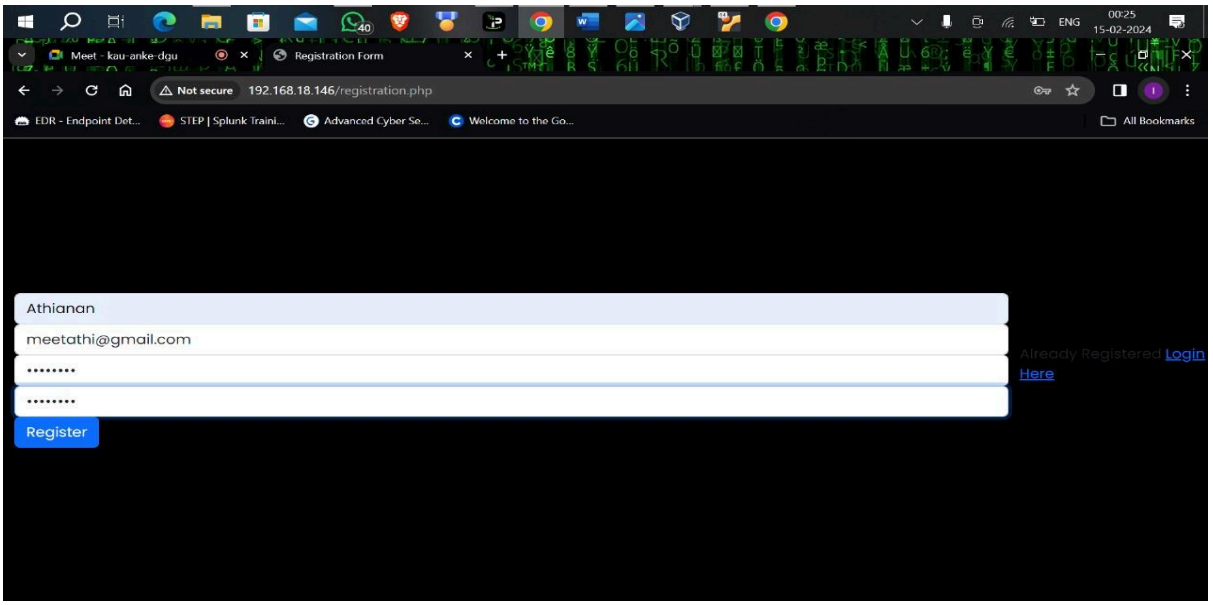
Mounting the media directory.



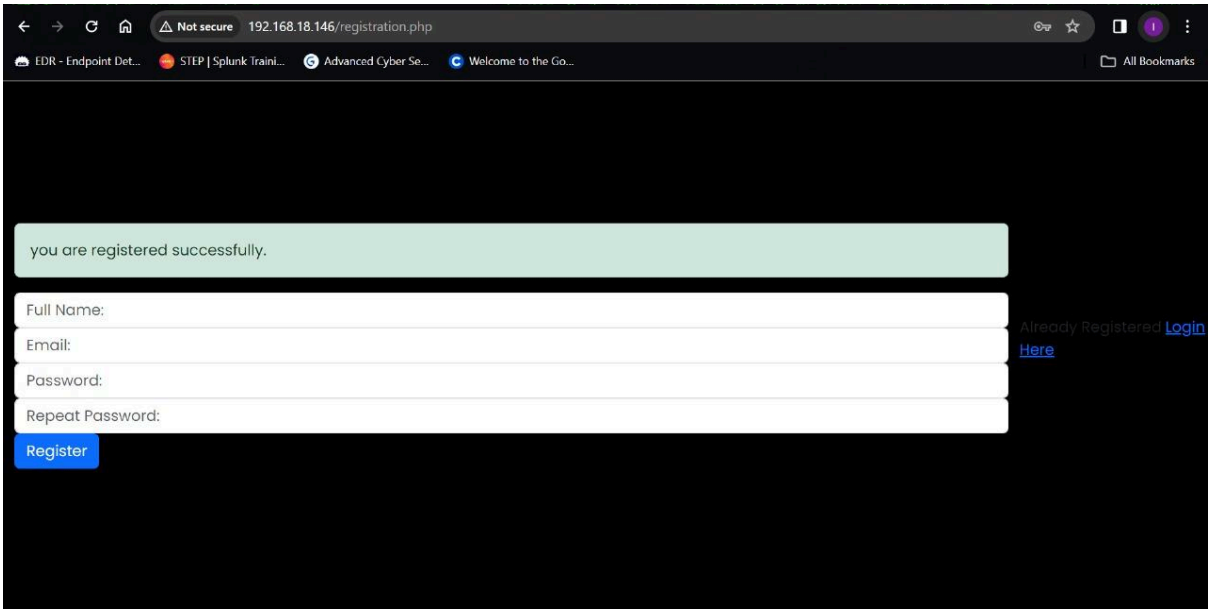


Reload the apache again.

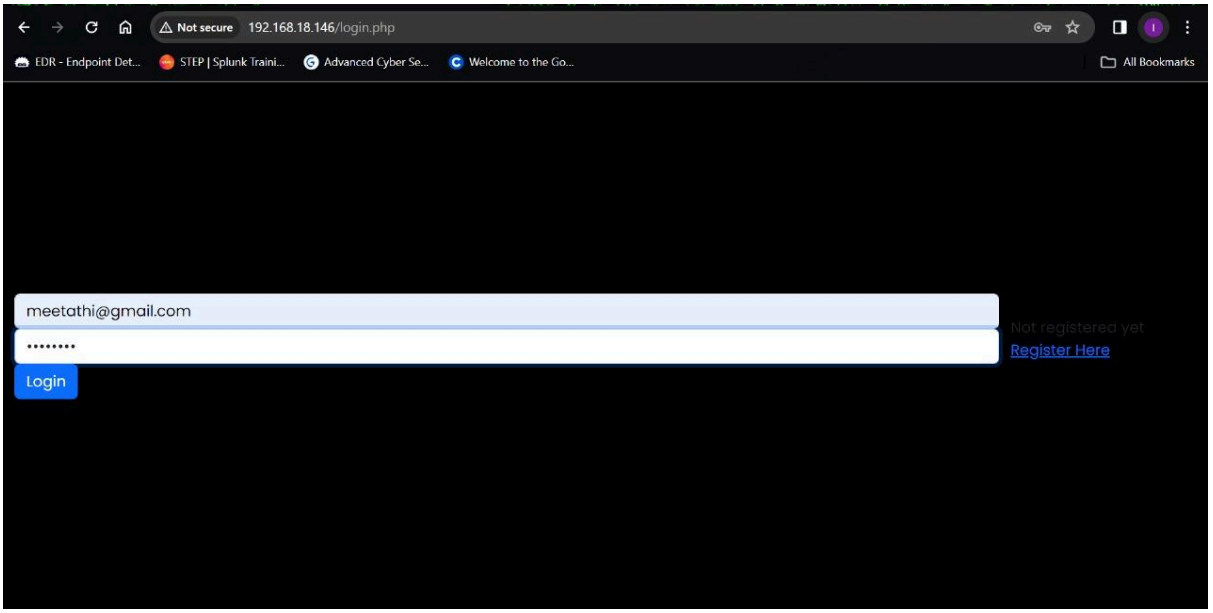


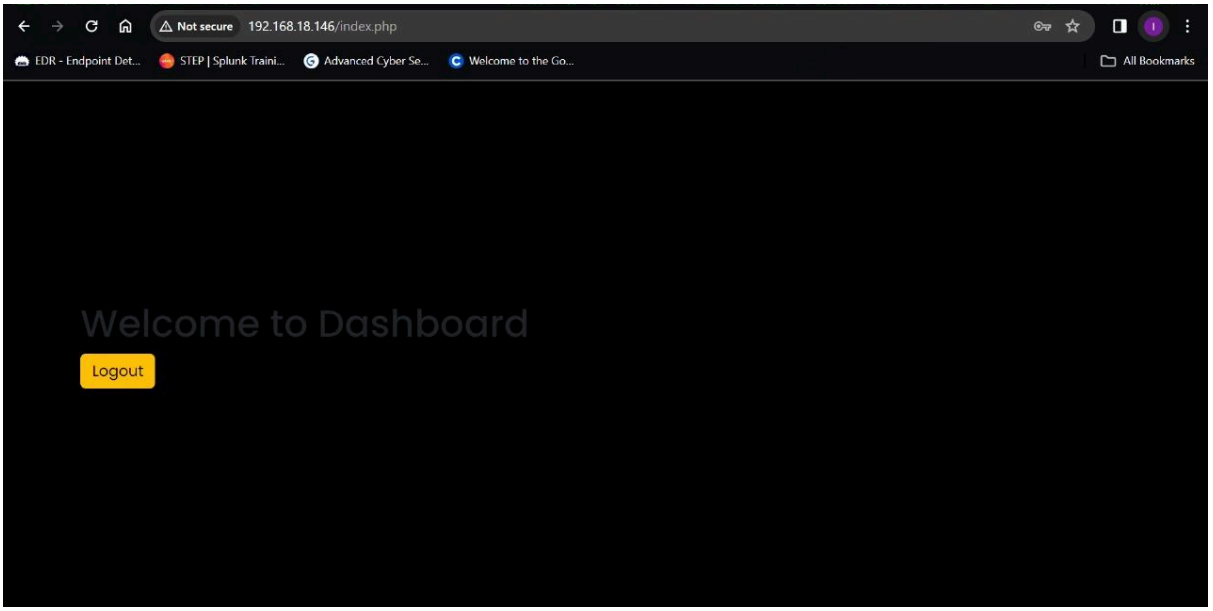


Registering into the PHP server



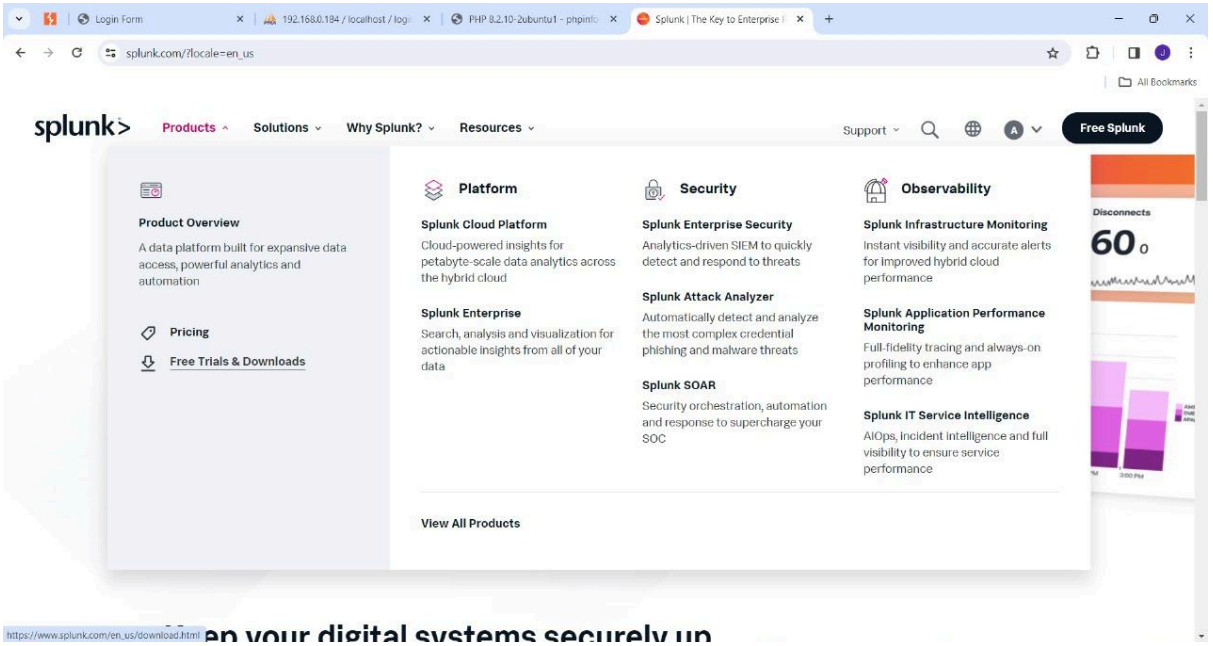
Logging into the server.





STEP 6: Splunk Universal Forwarder Installation

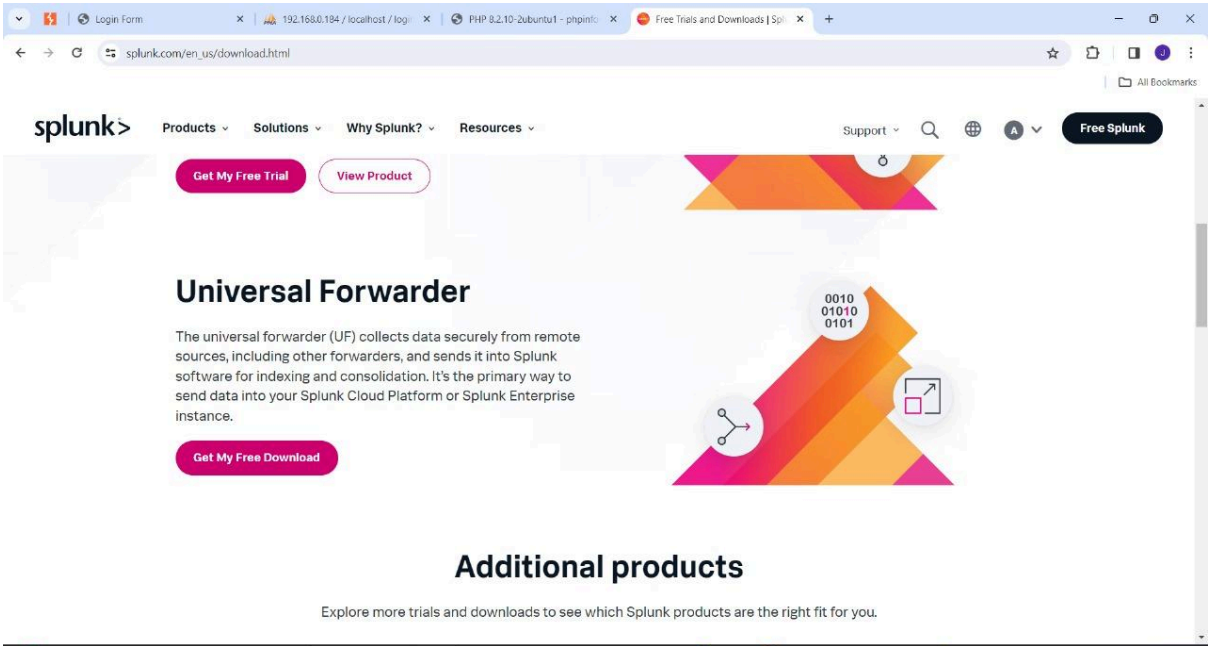
We can begin installing splunk forwarder.First,we will download the splunk forwarder installation file.



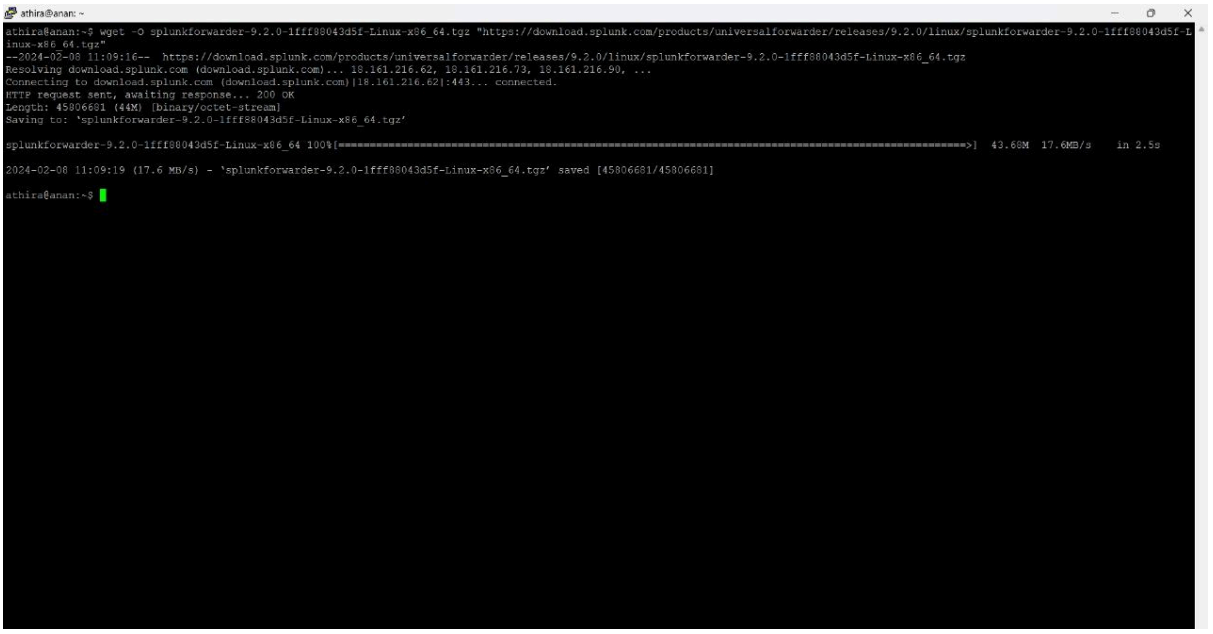
Steps to find universal forwarder Download via command

1. *Free Splunk*
2. *Free trials and downloads*
3. *Universal Forwarder*
4. *Linux*
5. *64-bit.tgz*

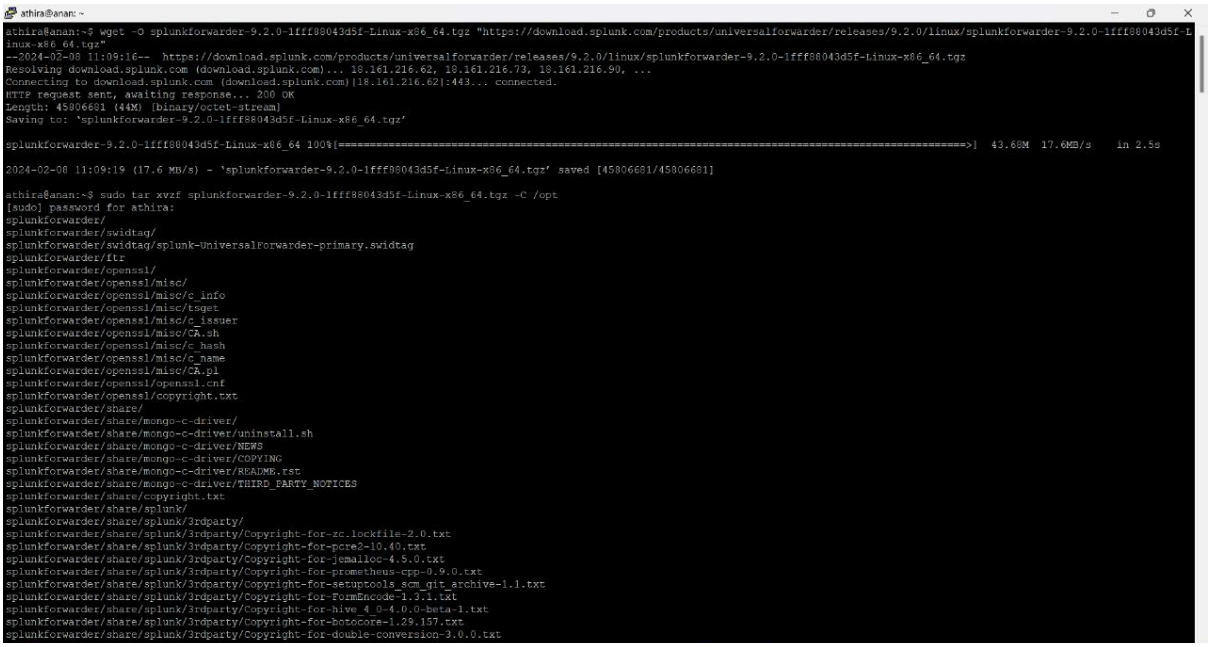
Click the Command Line (wget) and copy it



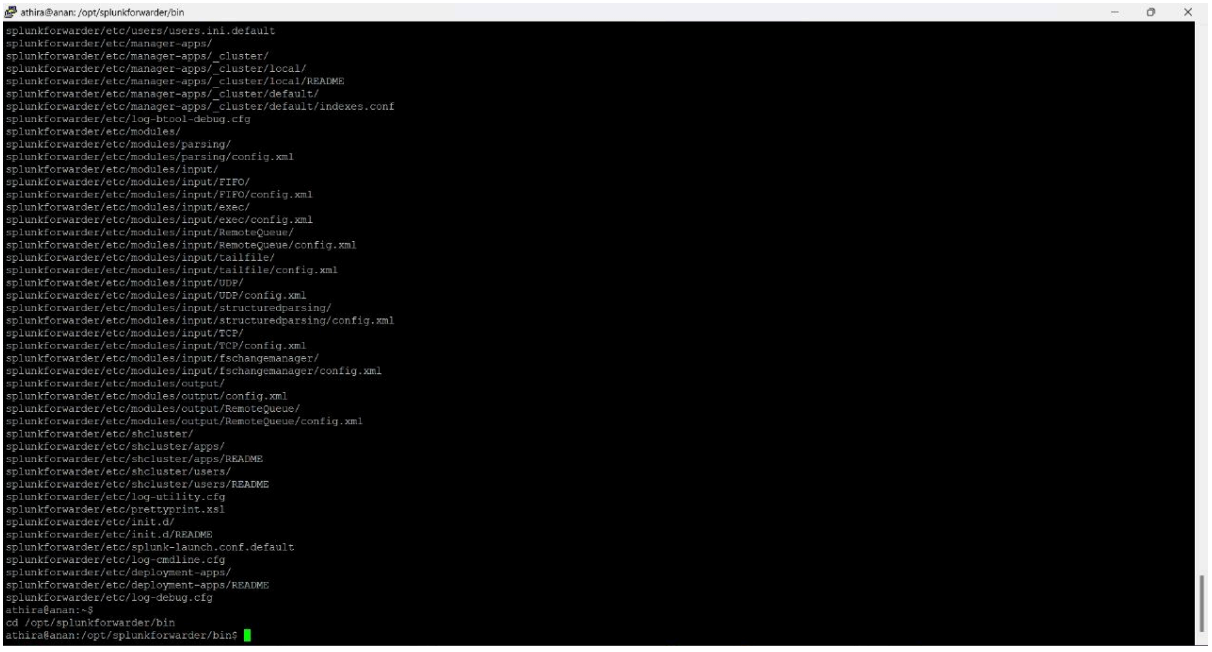
Type wget and the copied link into the terminal.



Extract the splunk forwarder files to opt location

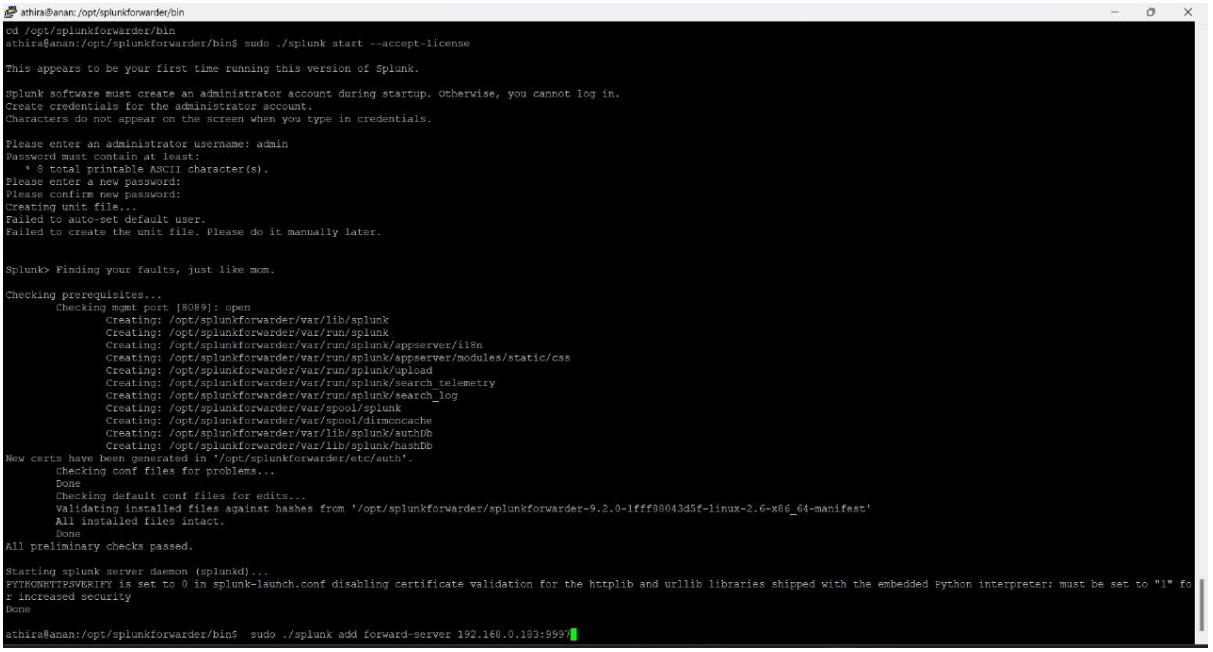


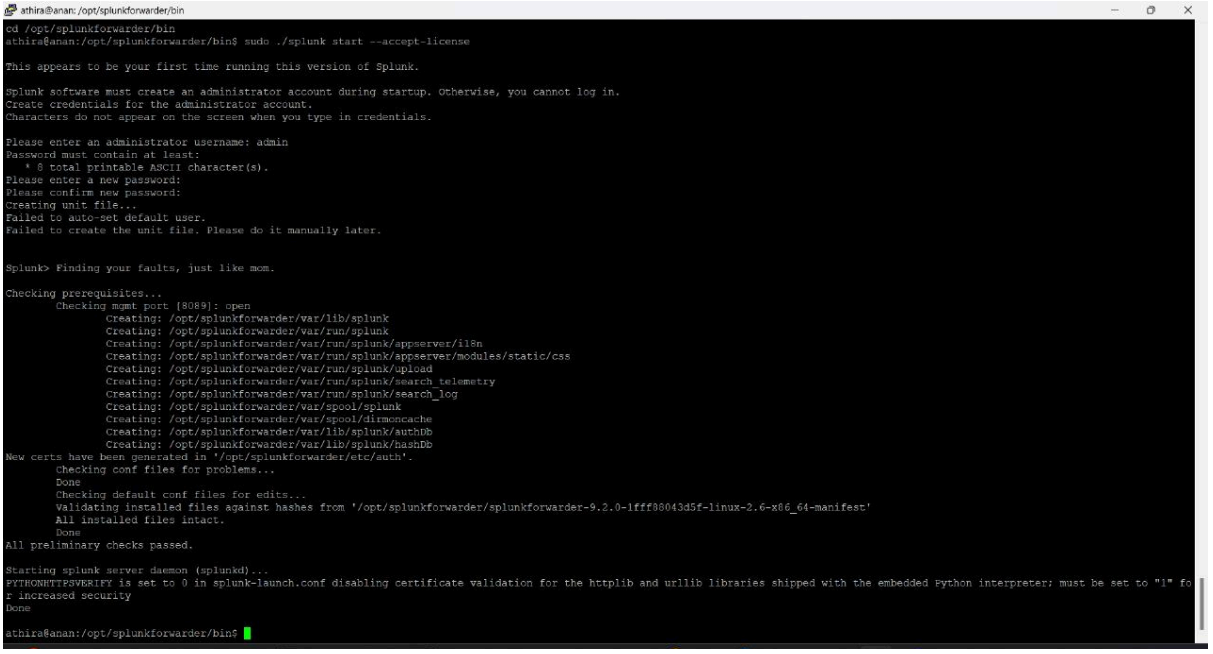
Change to opt directory



ubuntu@ubuntu:/tmp$ cd /opt

ubuntu@ubuntu:/opt$ cd splunkforwarder/bin


athira@anan: /opt/splunkforwarder/bin
cd /opt/splunkforwarder/bin
athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
Please enter an administrator username: admin
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.
Splunk> Finding your faults, just like mom.
Checking prerequisites...
Checking mgmt port [8089]: open
Creating: /opt/splunkforwarder/var/lib/splunk
Creating: /opt/splunkforwarder/var/run/splunk
Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
Creating: /opt/splunkforwarder/var/run/splunk/upload
Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
Creating: /opt/splunkforwarder/var/run/splunk/search_log
Creating: /opt/splunkforwarder/var/spool/splunk
Creating: /opt/splunkforwarder/var/spool/dirmoncache
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.0.183:9997


athira@anan: /opt/splunkforwarder/bin
cd /opt/splunkforwarder/bin
athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
Please enter an administrator username: admin
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.
Splunk> Finding your faults, just like mom.
Checking prerequisites...
Checking mgmt port [8089]: open
Creating: /opt/splunkforwarder/var/lib/splunk
Creating: /opt/splunkforwarder/var/run/splunk
Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
Creating: /opt/splunkforwarder/var/run/splunk/upload
Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
Creating: /opt/splunkforwarder/var/run/splunk/search_log
Creating: /opt/splunkforwarder/var/spool/splunk
Creating: /opt/splunkforwarder/var/spool/dirmoncache
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
athira@anan:/opt/splunkforwarder/bin$

Step 7: Configuring Splunk Server Configuring firewall in windows

When configuring the firewall for a Splunk server on Windows, you need to ensure that the necessary ports are open to allow communication between Splunk components. Splunk uses specific ports for different purposes, and you must adjust your Windows Firewall settings accordingly. Here are the general steps to configure the Windows Firewall for a Splunk server:

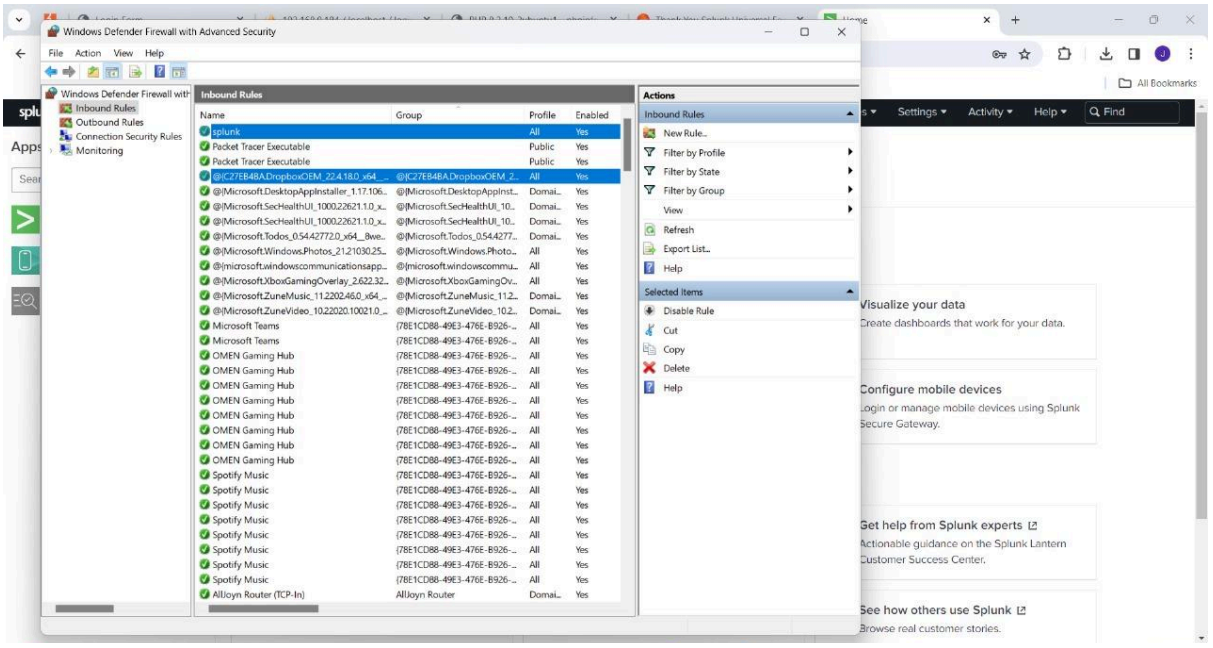
Open Windows Firewall Settings:

Go to the Control Panel on your Windows server.

Click on "System and Security" and then "Windows Defender Firewall."

Create Inbound Rules:

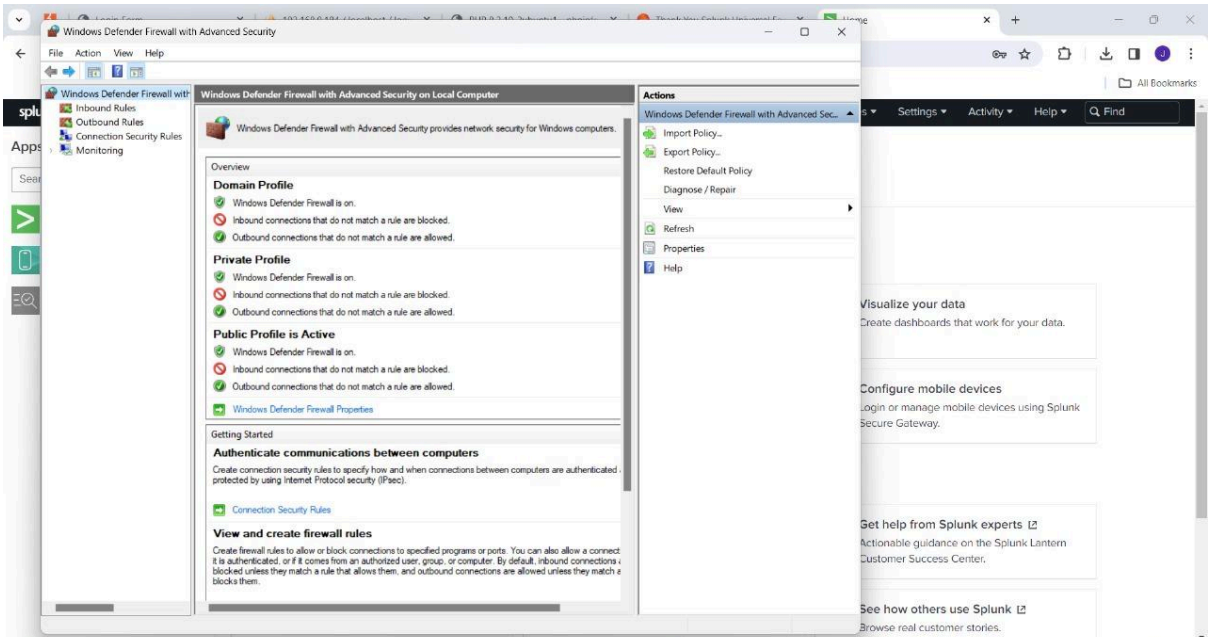
Click on "Advanced settings" on the left side

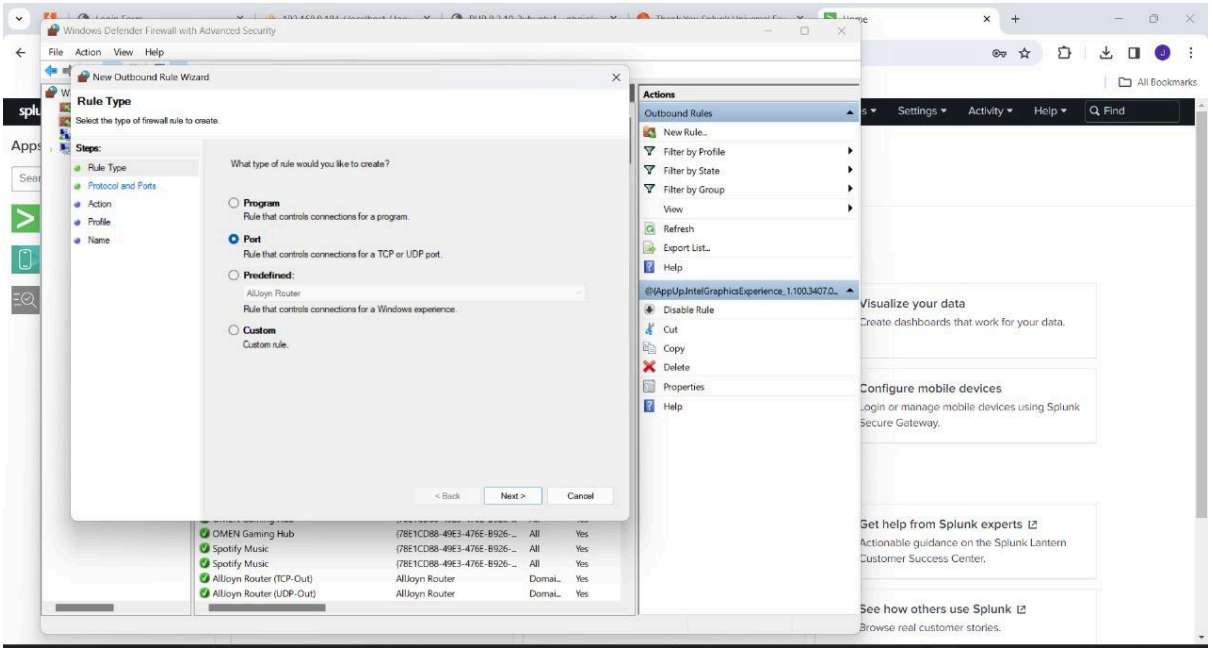


Configure Inbound Rules:

In the “Inbound Rules” section, click on “New Rule….” On the right side.

Select “port” and click “next”

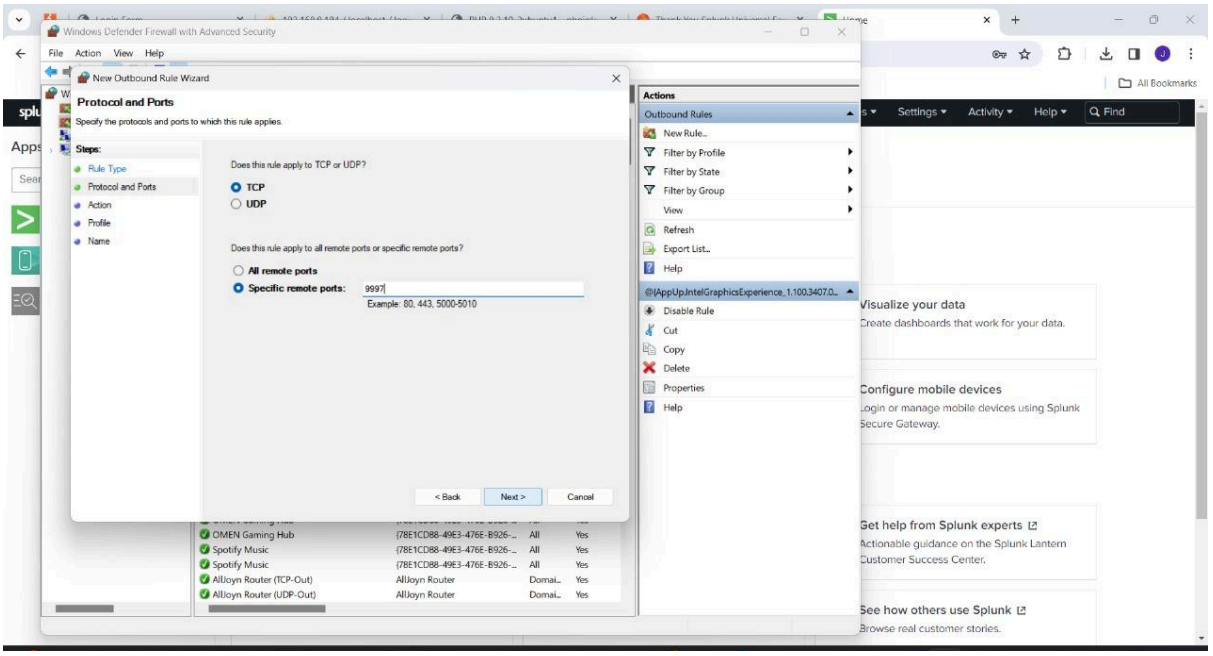




Specify ports:

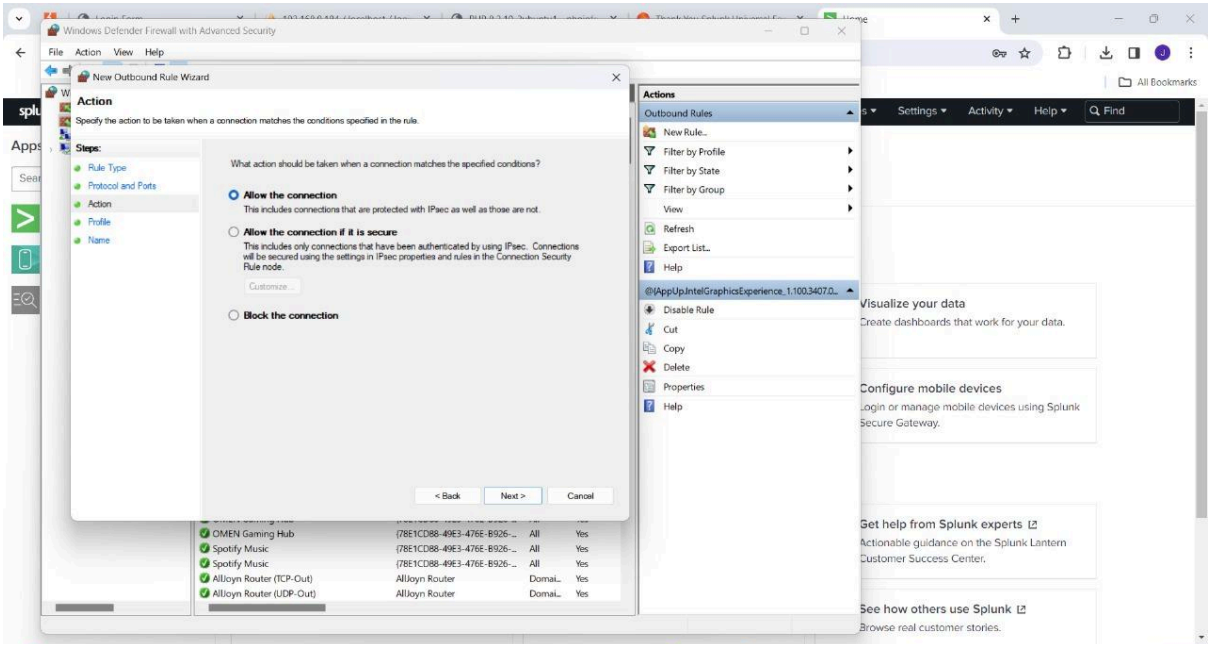
Choose “TCP” and specify the ports relevant to your splunk setup (e.g 9997).

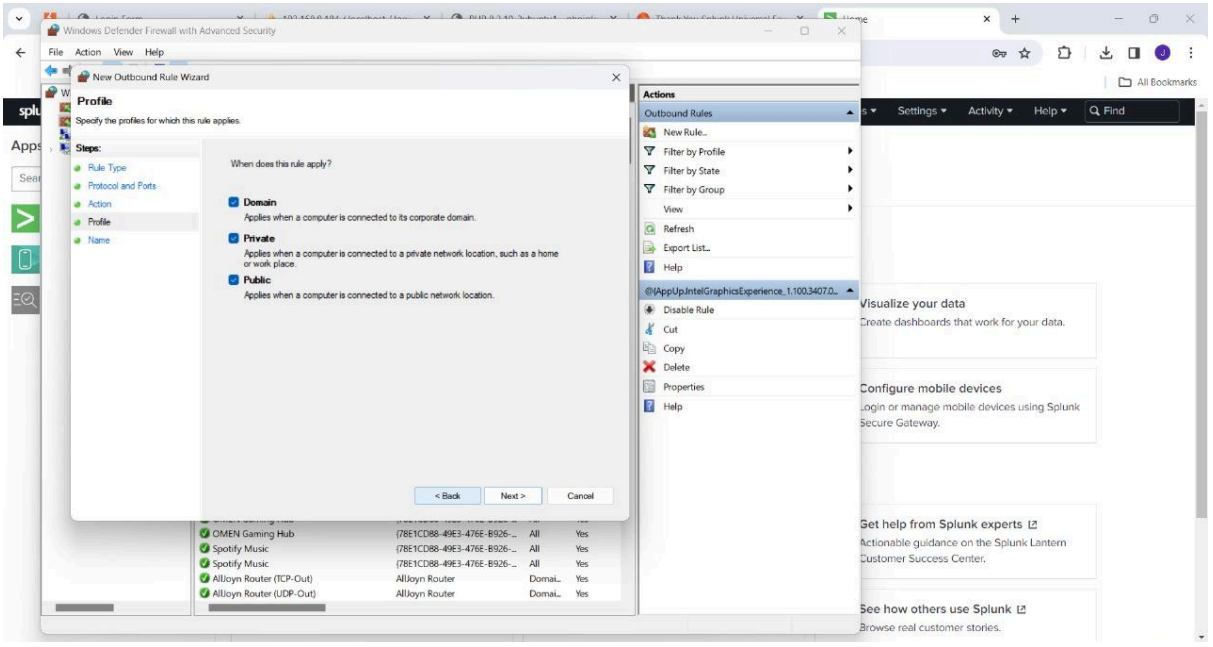
Click “Next.”



Choose Action:

Select “allow the connection” and click “Next.”





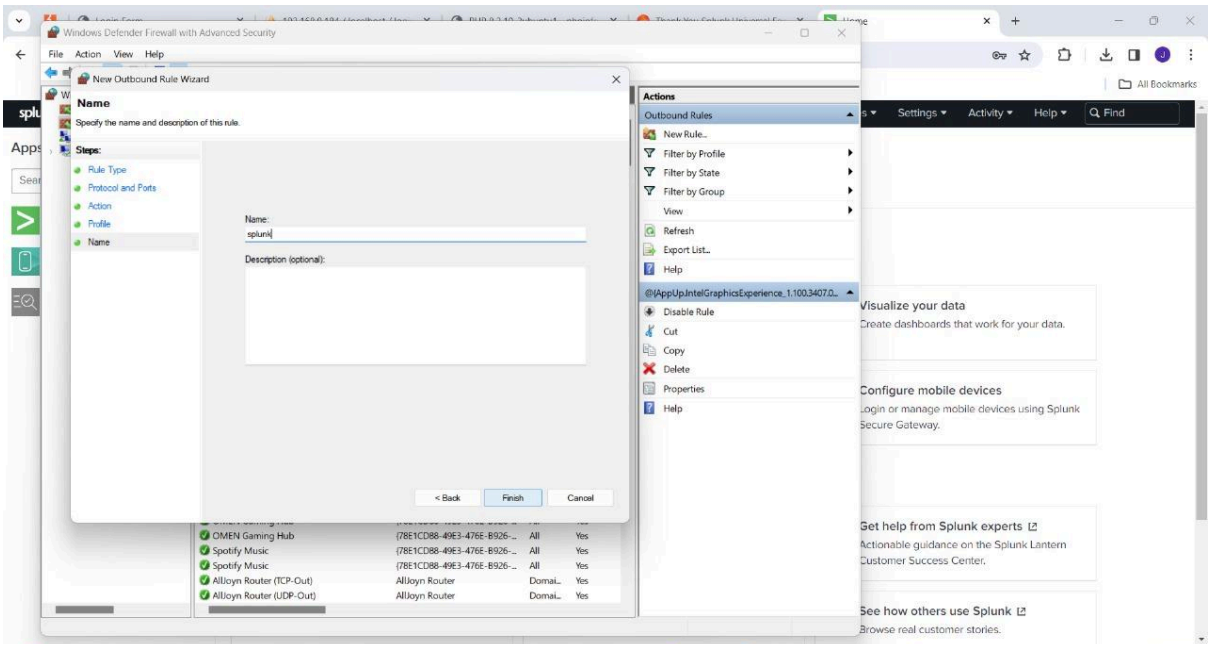
Profile settings:

Choose when to apply the rule based on your network profile settings (Domain,Private,Public).

Click “next.”

Rule name:

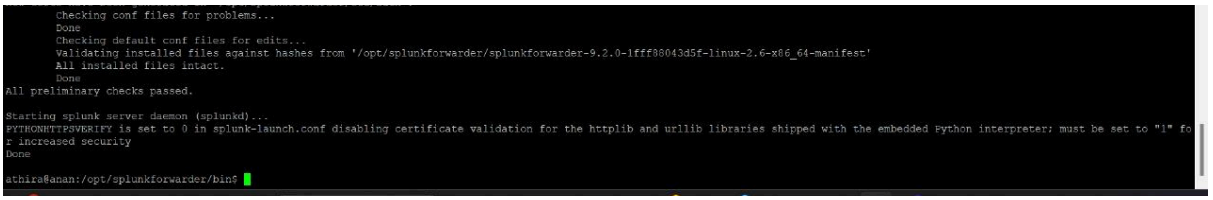
Provide a name for the rule (e.g., splunk web interface)



Click “Finish.”

Step 8 : Configuring Splunk Universal Forwarder

Configuring splunk forwarder on an Ubuntu server to monitor logs from windows machine.



Add this lines ;

[tcpout]

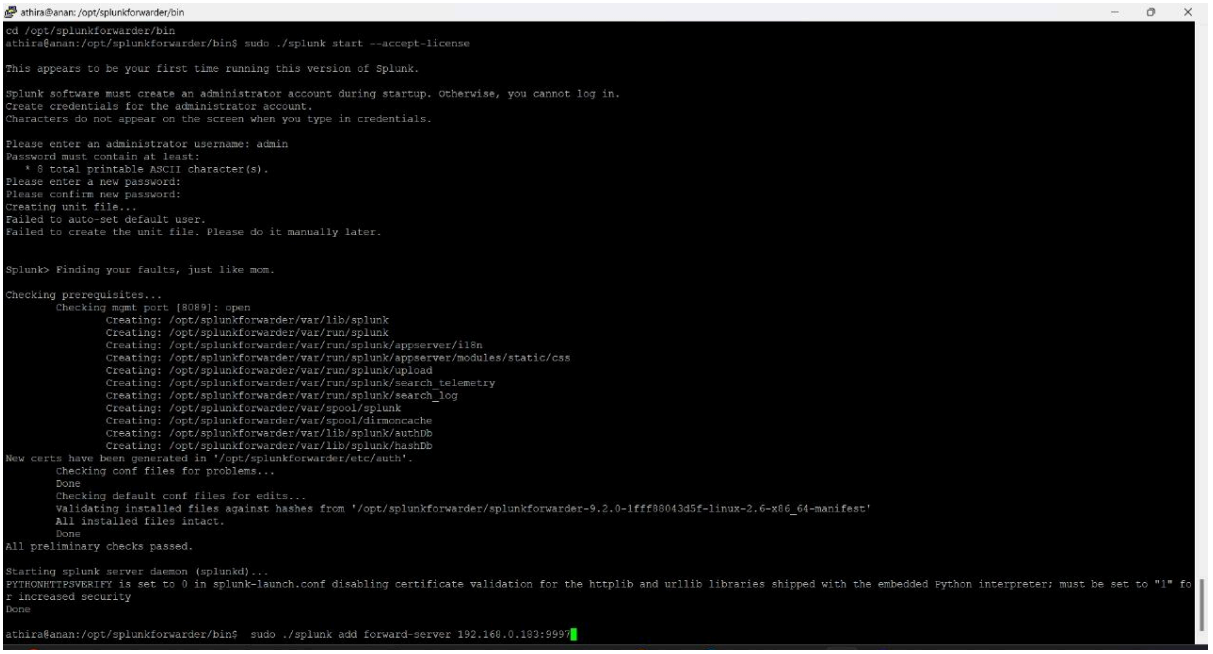
defaultGroup = splunk-group

[tcpout:splunk-group]

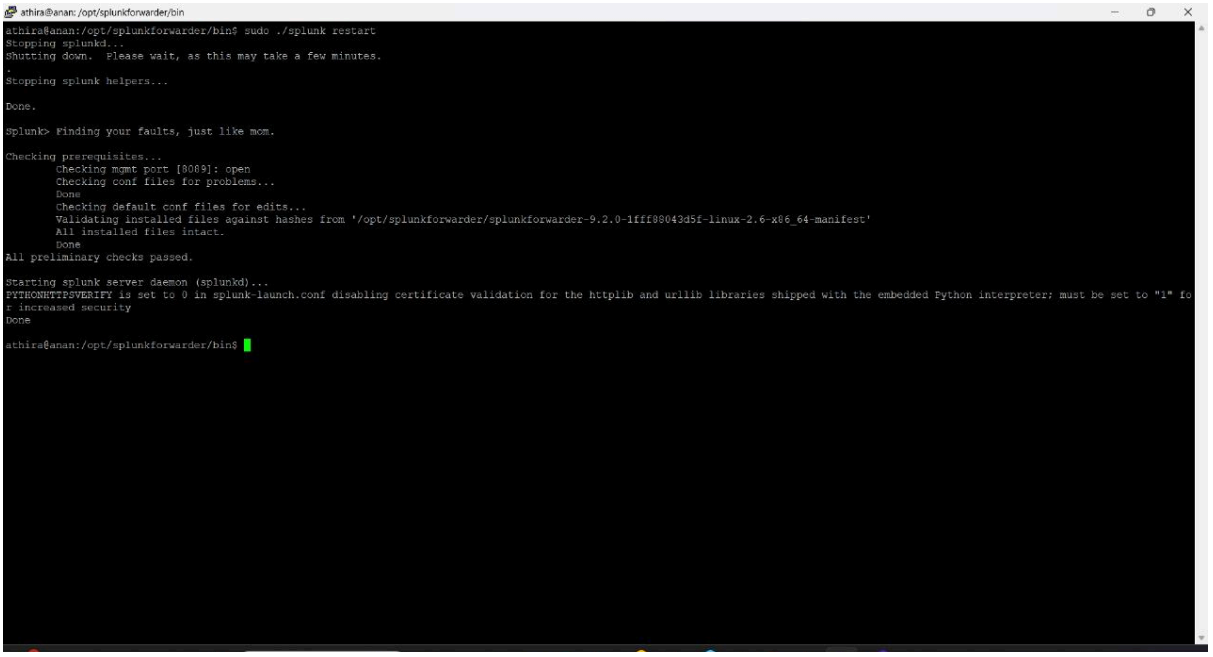
server = <splunk_server_ip>:<splunk_listener_port>

Replace server ip in here (windows machine ip) <splunk_server_ip> and give port

number <splunk_listener_port> (eg; 9997).



Adding forwarding and adding log monitoring and restarting.



Step 9: Splunk enterprise configuration

To set up forwarding and receiving ports in Splunk, you'll typically configure the Universal

Forwarder to send data to the main Splunk Enterprise instance. Below are the general

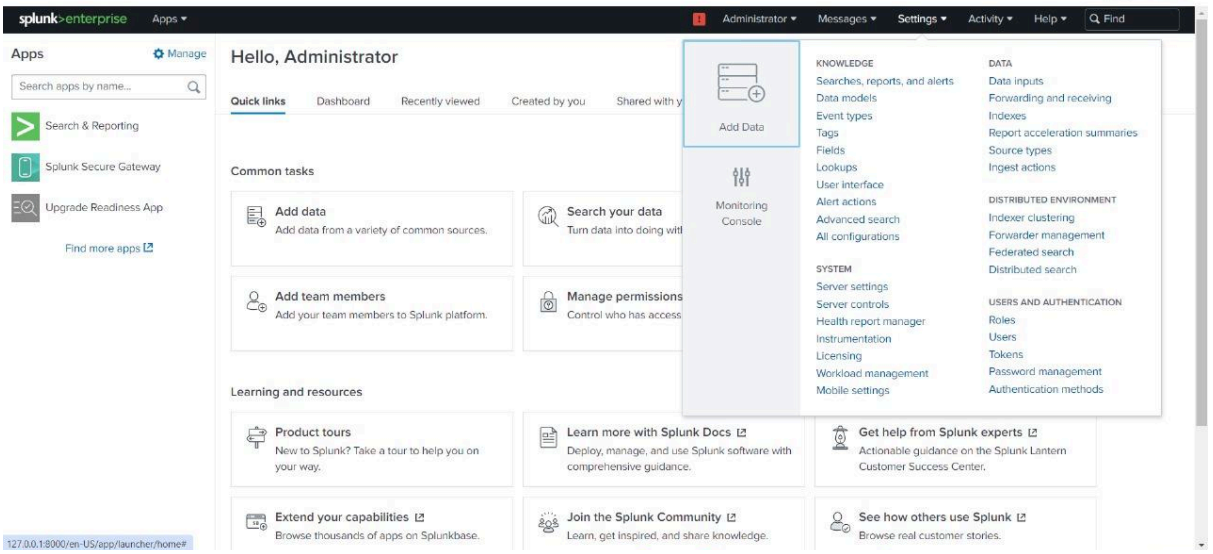
steps to add forwarding and receiving ports in Splunk:

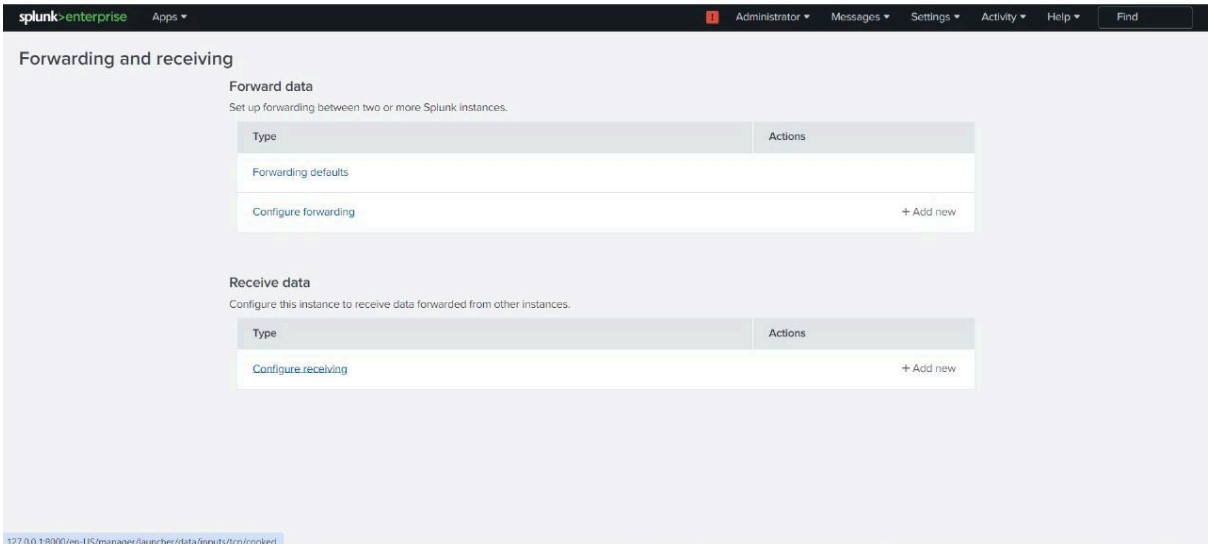
v Receiving Port (Splunk Enterprise): This port is used by Splunk Enterprise to listen for incoming data from Universal Forwarders.

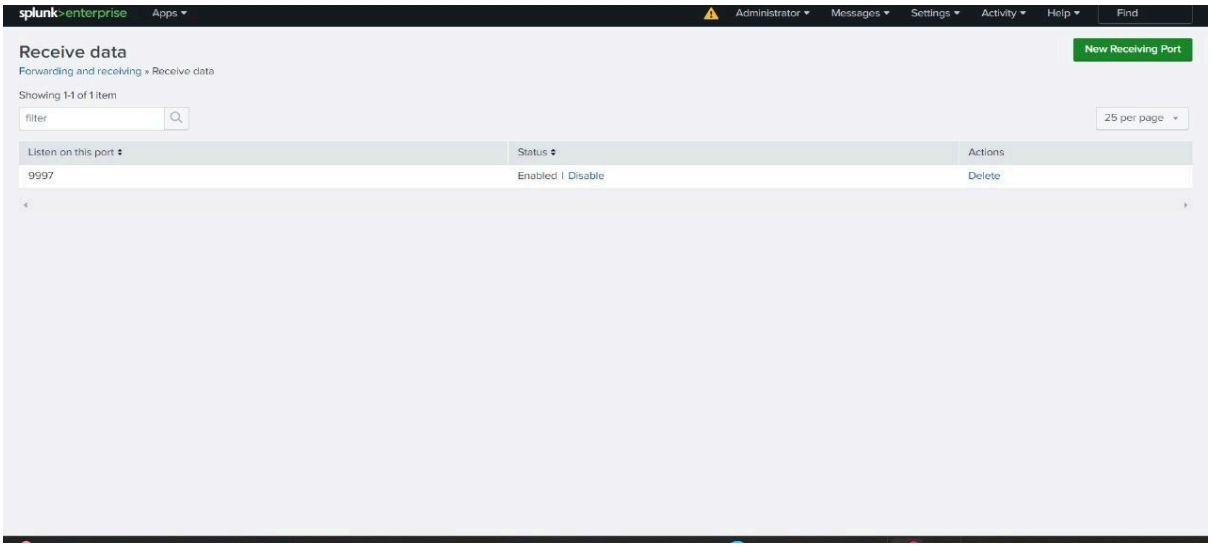
v Access Splunk Web: Open your web browser and navigate to the Splunk Web interface. Log in with appropriate credentials.

v Navigate to Settings: In the Splunk Web interface, go to "Settings" in the top menu.

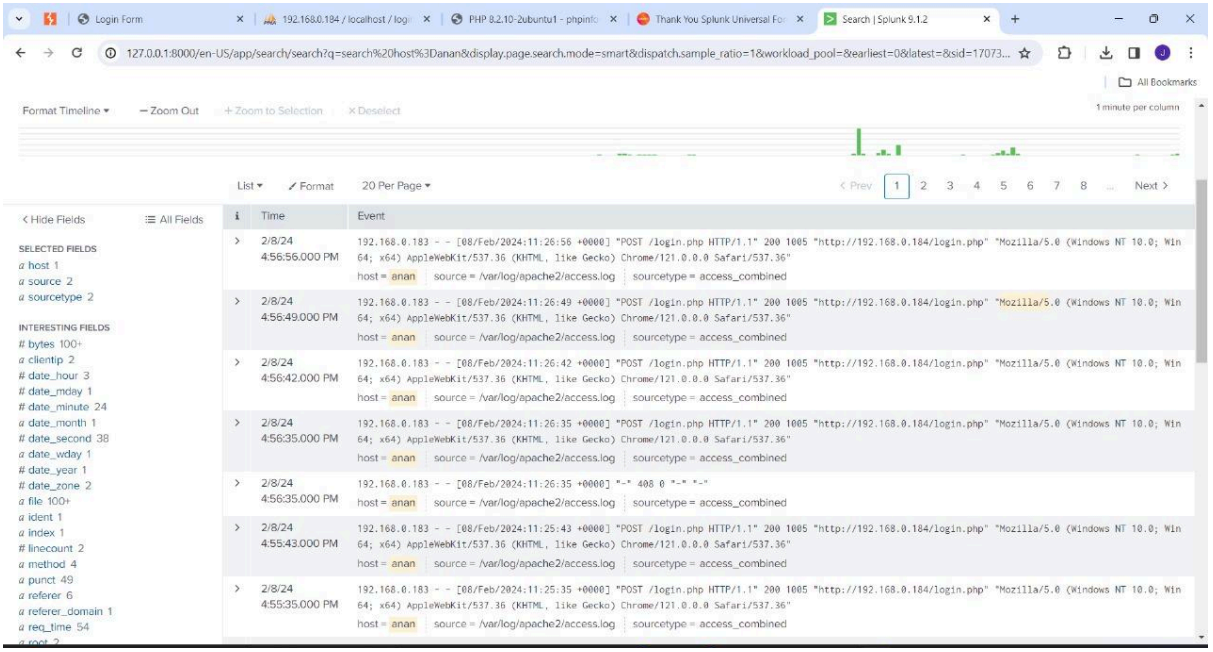
Configure Receiving Port: Under "Settings," click on "Forwarding and Receiving." Click on "Configure receiving" and specify the receiving port (e.g., 9997). Save the configuration







Searching in the splunk



Finally the log of the hosted server is retrieved.

Summary

To host a website on an Ubuntu server and use Splunk to monitor login logs, you'll need to follow a few steps. Here's a general guide:

1. Set up your Ubuntu server: Install a web server like Apache or Nginx, and configure it to serve your website. Ensure that your website's access logs are enabled and accessible.

2. Install and configure Splunk: Install Splunk on your Ubuntu server by following the official installation instructions provided by Splunk. You can download the Splunk package appropriate for your Ubuntu version from the Splunk website.

3. Configure Splunk to monitor logs: Once Splunk is installed, you need to configure it to monitor the log files where login attempts are recorded. This could be the system logs (`/var/log/auth.log` or `/var/log/secure` on Ubuntu), or it could be custom logs generated by your web server.

   - Edit the Splunk inputs configuration file (`inputs.conf`) to specify which log files to monitor. You'll need to define a stanza for each log file you want Splunk to monitor.

   - For example, if you're monitoring Apache access logs, you would add a stanza like this:

   ```

   [monitor:///var/log/apache2/access.log]

   sourcetype = apache_access

   ```

- After making changes to `inputs.conf`, restart Splunk to apply the new configuration.

4. Search and analyse logs in Splunk: Once Splunk is configured to monitor the appropriate log files, you can use the Splunk web interface to search and analyse the logs. You can create custom searches and alerts to monitor for login events or any other specific activity you're interested in.

5. Set up dashboards and alerts: Splunk provides powerful visualisation tools that allow you to create dashboards to monitor and analyse your logs. You can create visualisations of login attempts over time, track failed login attempts, and set up alerts to notify you of suspicious activity.

6. Secure your system and Splunk instance: Make sure your Ubuntu server and Splunk instance are properly secured to prevent unauthorised access to your logs and sensitive data.

By following these steps, you'll be able to host your website on an Ubuntu server and use Splunk to monitor login logs and other activities on your server.