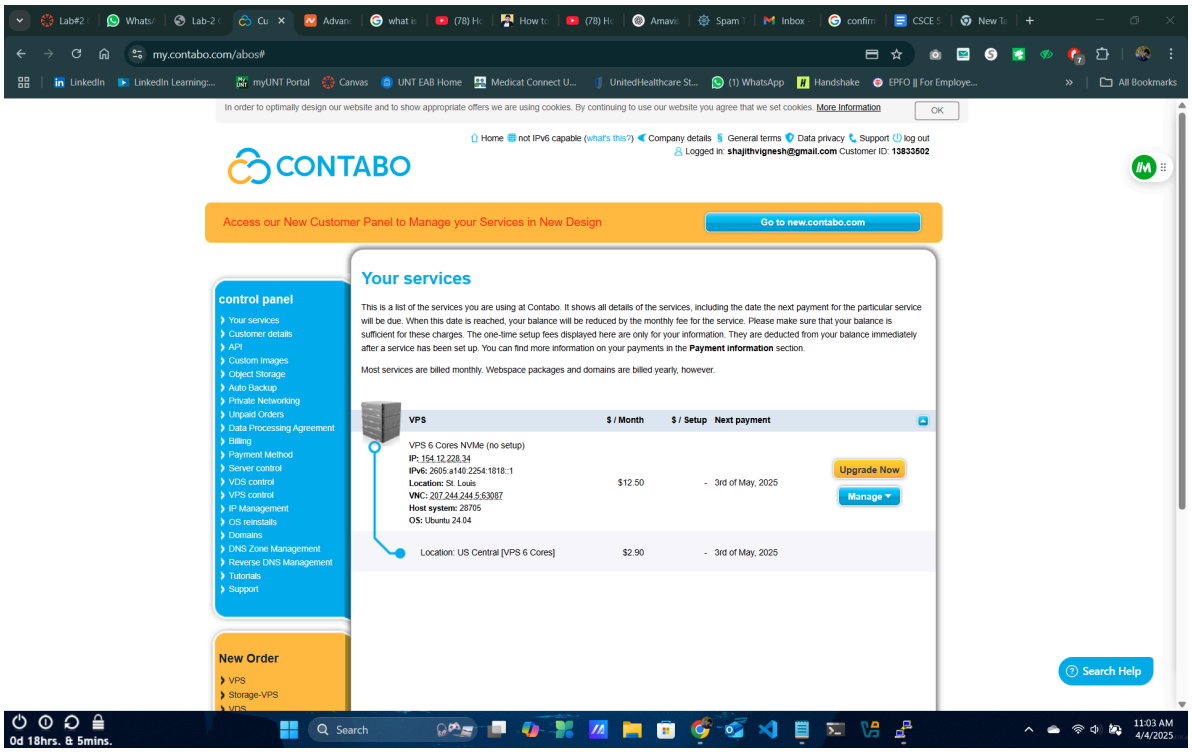
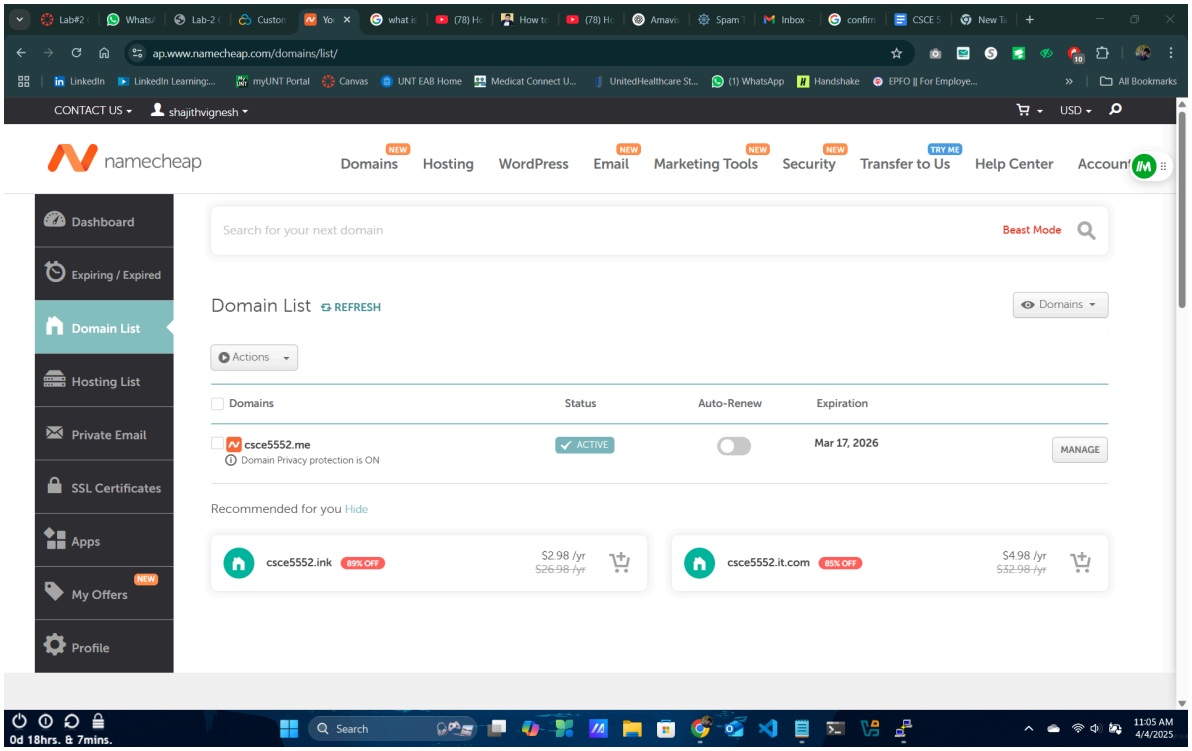
Shajith Vignesh Ananthaneni
11691714

Cybersecurity Lab
Exploring Offensive Security Strategies and Phishing Structures in Mail Servers

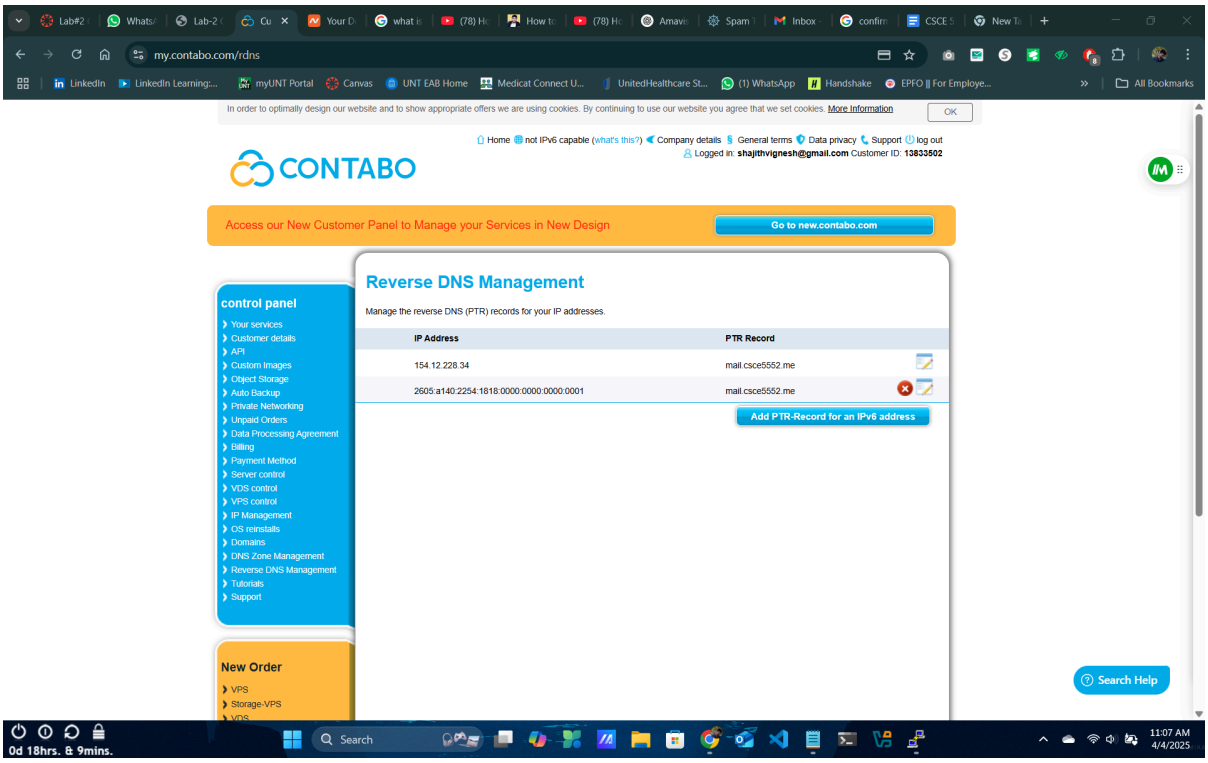
From **Contabo**, I purchased a VPS(**IP: 154.12.228.34**) with the following specifications



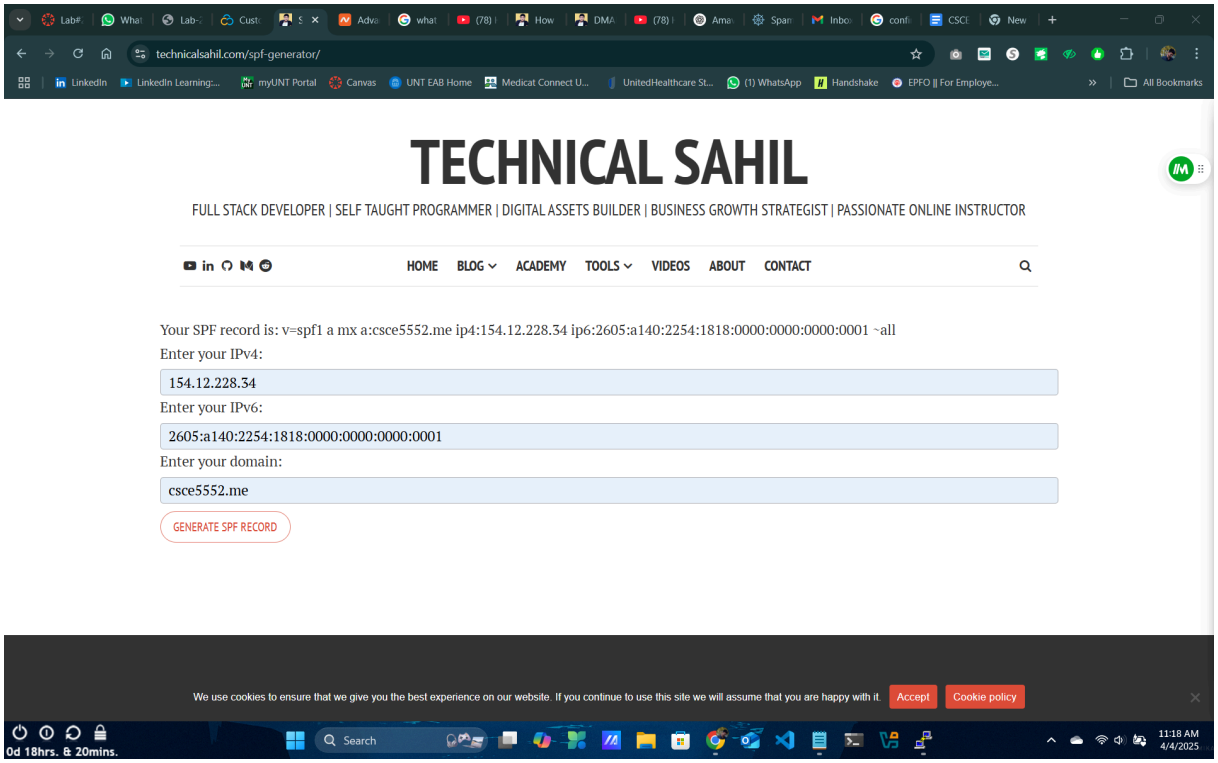
From **Namecheap**, I have purchased the following domain(**csce5552.me**)



Since I'm using this server only for iRedMail, I have updated the **PTR records** with respective hostname.domain.com values as follows under **Reverse DNS Management**



Using the SPF & DMARC generator, I have added the following (**A, TXTs & MX**) records under the **Advanced DNS Section** of my domain



technicalsahil.com/dmarc-generator/

TECHNICAL SAHIL

FULL STACK DEVELOPER | SELF TAUGHT PROGRAMMER | DIGITAL ASSETS BUILDER | BUSINESS GROWTH STRATEGIST | PASSIONATE ONLINE INSTRUCTOR

HOME BLOG ACADEMY TOOLS VIDEOS ABOUT CONTACT

Your DMARC record is: v=DMARC1; p=none; fo=1; rua=mailto:dmarc@csce5552.me; ruf=mailto:dmarc@csce5552.me

Enter your domain:

csce5552.me

GENERATE DMARC RECORD

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it. Accept Cookie policy

0d 18hrs. & 21mins.

11:18 AM 4/4/2025

ap.www.namecheap.com/Domains/DomainControlPanel/csce5552.me/advancedns

namecheap

Domains (NEW) Hosting WordPress Email (NEW) Marketing Tools (NEW) Security (NEW) Transfer to Us (TRY ME) Help Center Account

Dashboard
Expiring / Expired
Domain List
Hosting List
Private Email
SSL Certificates
Apps
My Offers (NEW)
Profile

Domains → Details

csce5552.me

Domain | Products | Sharing & Transfer | Advanced DNS

DNS TEMPLATES — Choose DNS Template

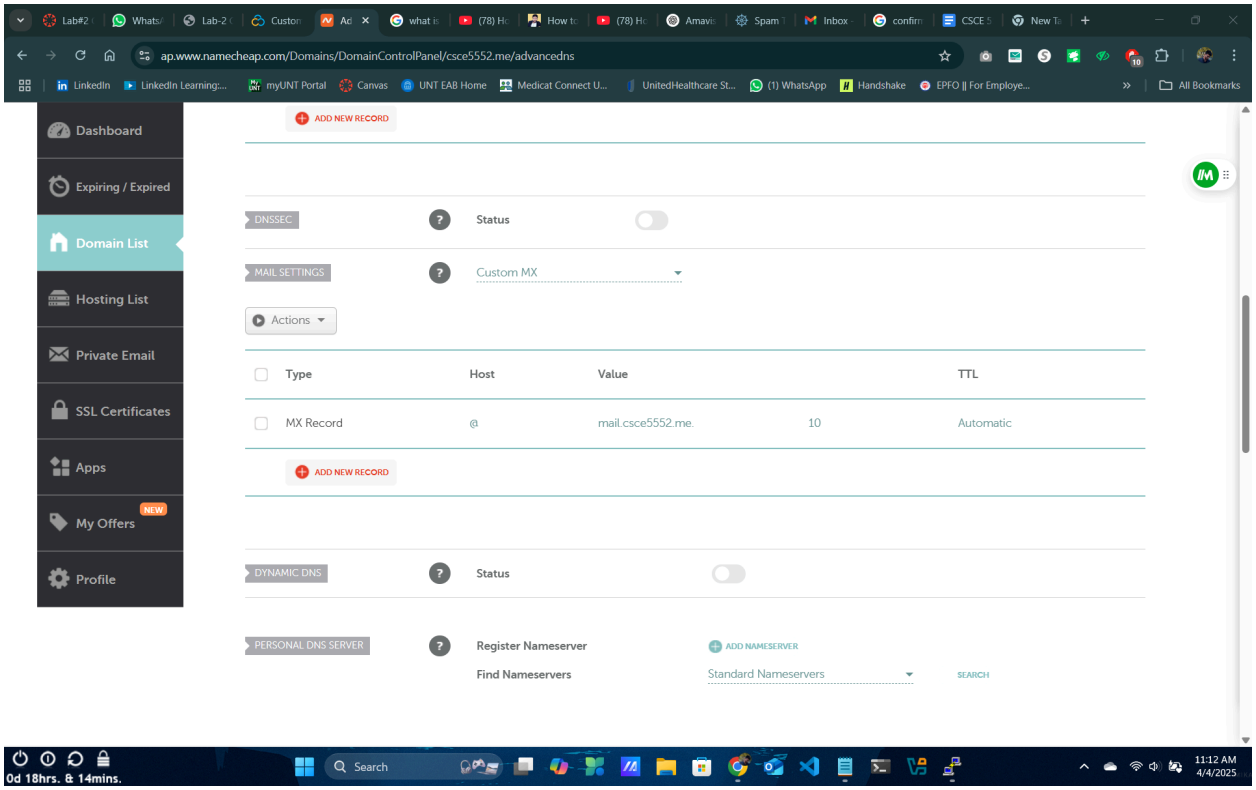
HOST RECORDS

Actions | Filters | Search

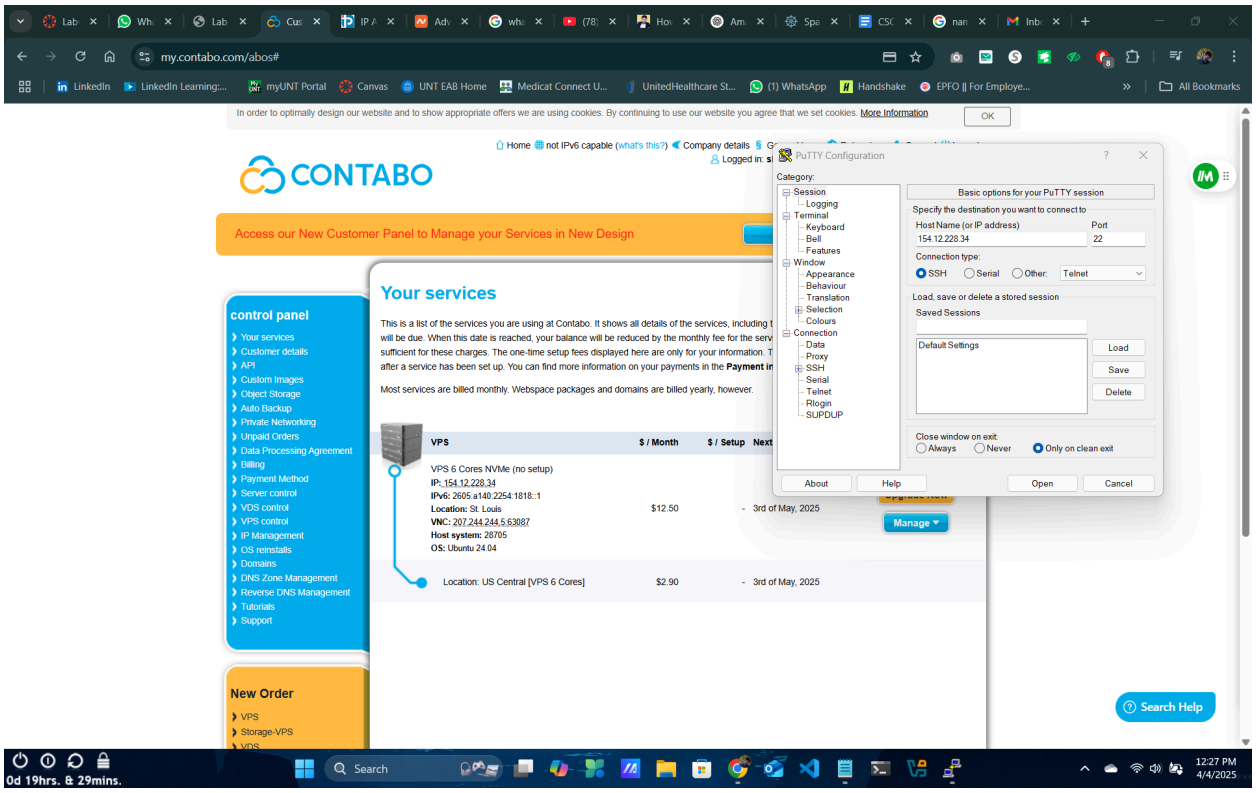
Type	Host	Value	TTL
A Record	mail	154.12.228.34	Automatic
TXT Record	@	v=spf1 a mx a:csce5552.me ip4:154.12.228.34 ip6:2605:a140:22...	Automatic
TXT Record	_dmarc	v=DMARC1; p=none; fo=1; rua=mailto:dmarc@csce5552.me; r...	Automatic

0d 18hrs. & 14mins.

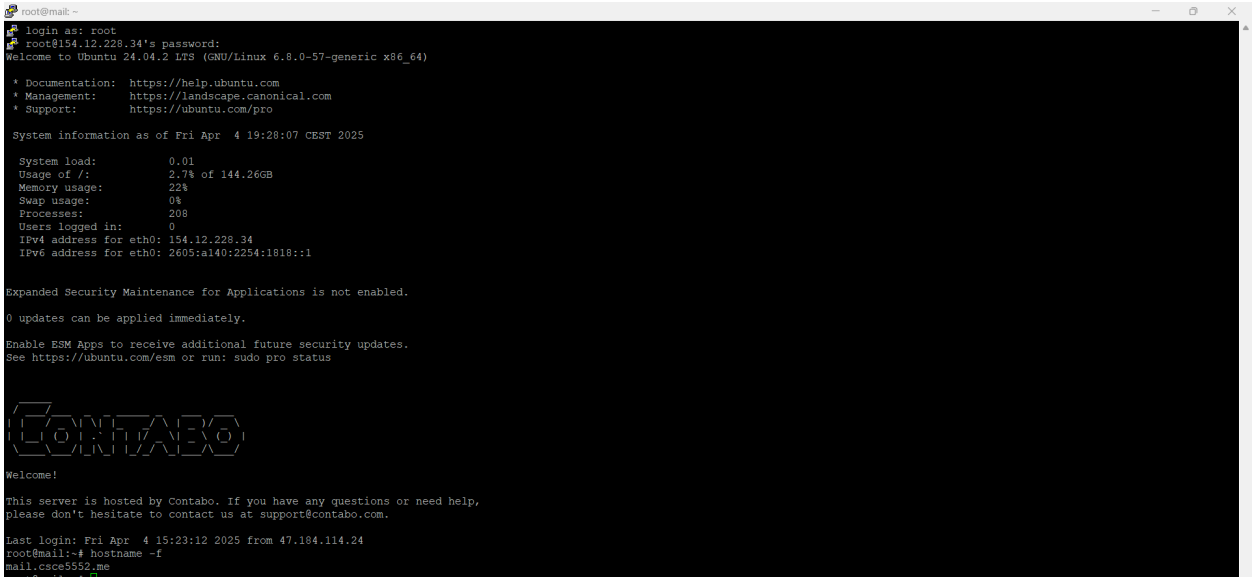
11:11 AM 4/4/2025



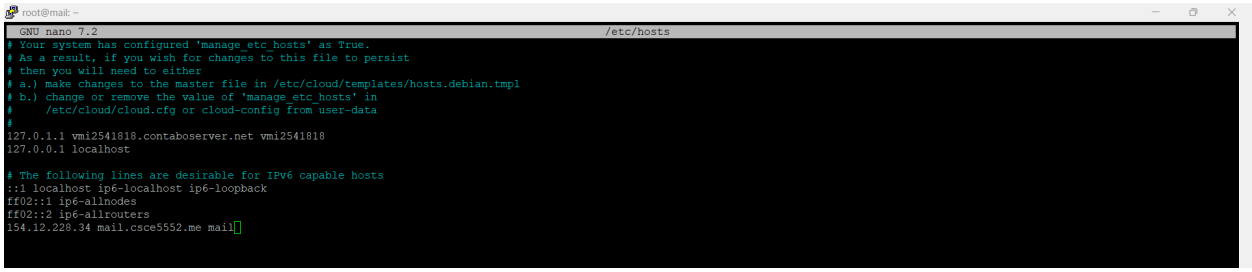
Due to the installation & compatibility issues with Kali & Ubuntu, I have used **PuTTY** to connect with my server directly. **Username** & **Password** are set during Contabo's server setup process



Updated the hostname by using the following commands
i. hostname -f
ii. hostnamectl set-hostname mail.csce552.me



Modified the hosts files by opening it in a text editor (nano /etc/hosts) & by adding my hostname (154.12.228.34 mail.csce5552.me mail)

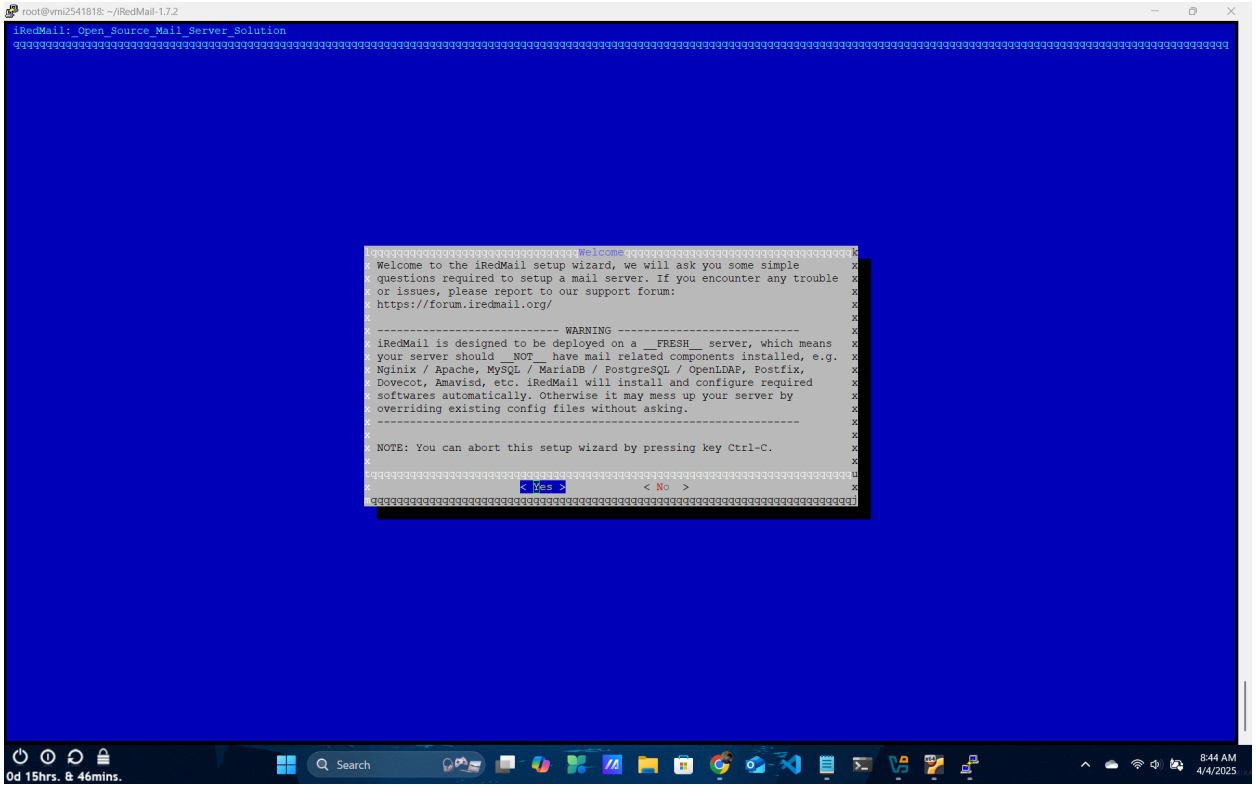


Updated the system packages - apt update && apt upgrade -y

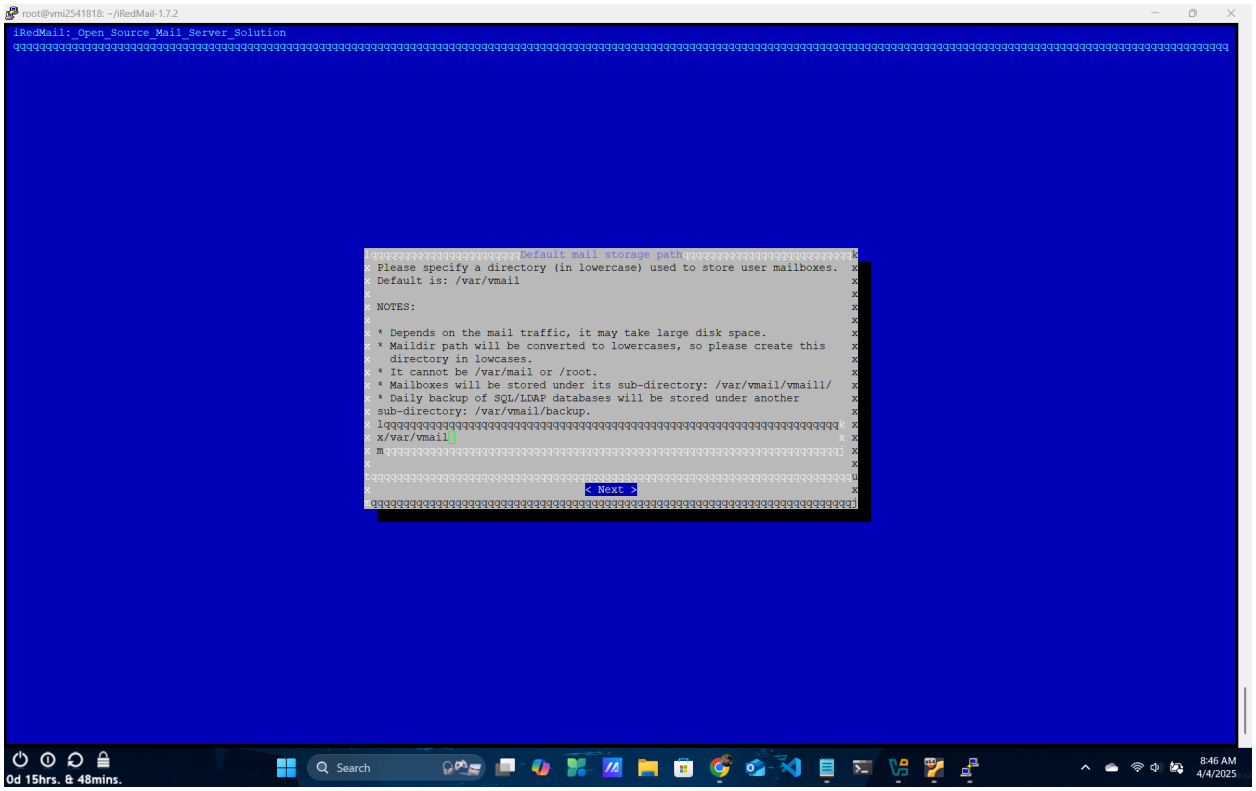
Installed GZIP - apt install gzip

Downloaded iRedMail - wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz

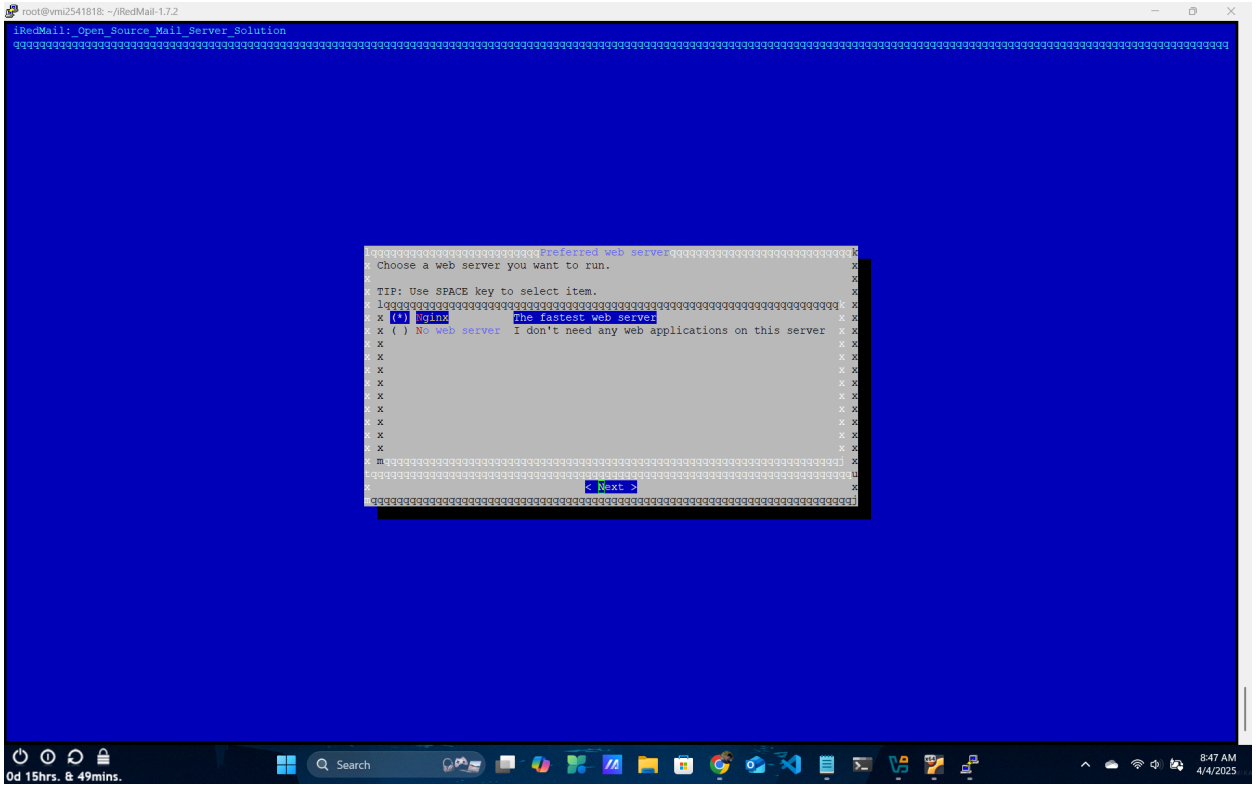
iRedMail Installation -
i. tar zxvf 1.7.2.tar.gz
ii. cd iRedMail-1.7.2
iii. bash iRedMail.sh
Through this, we are directed to the **iRedMail setup wizard**



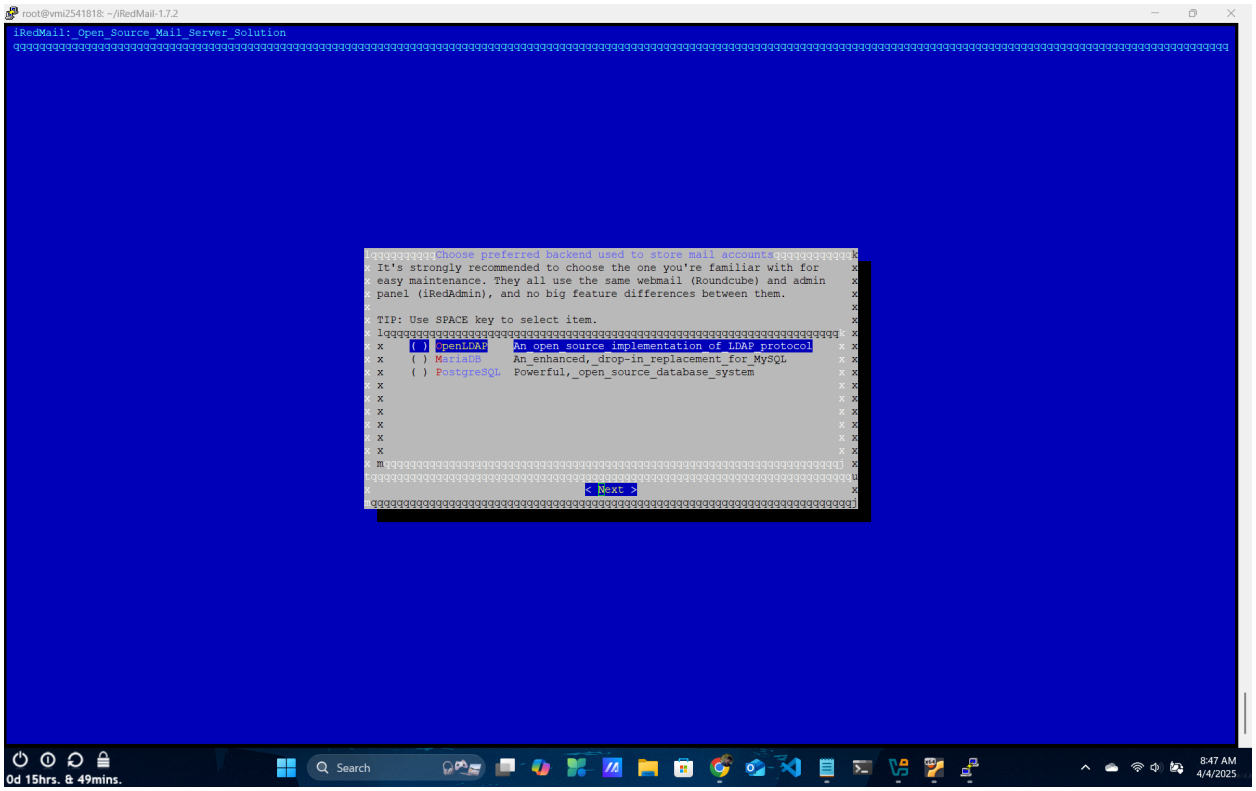
Hit **Yes**



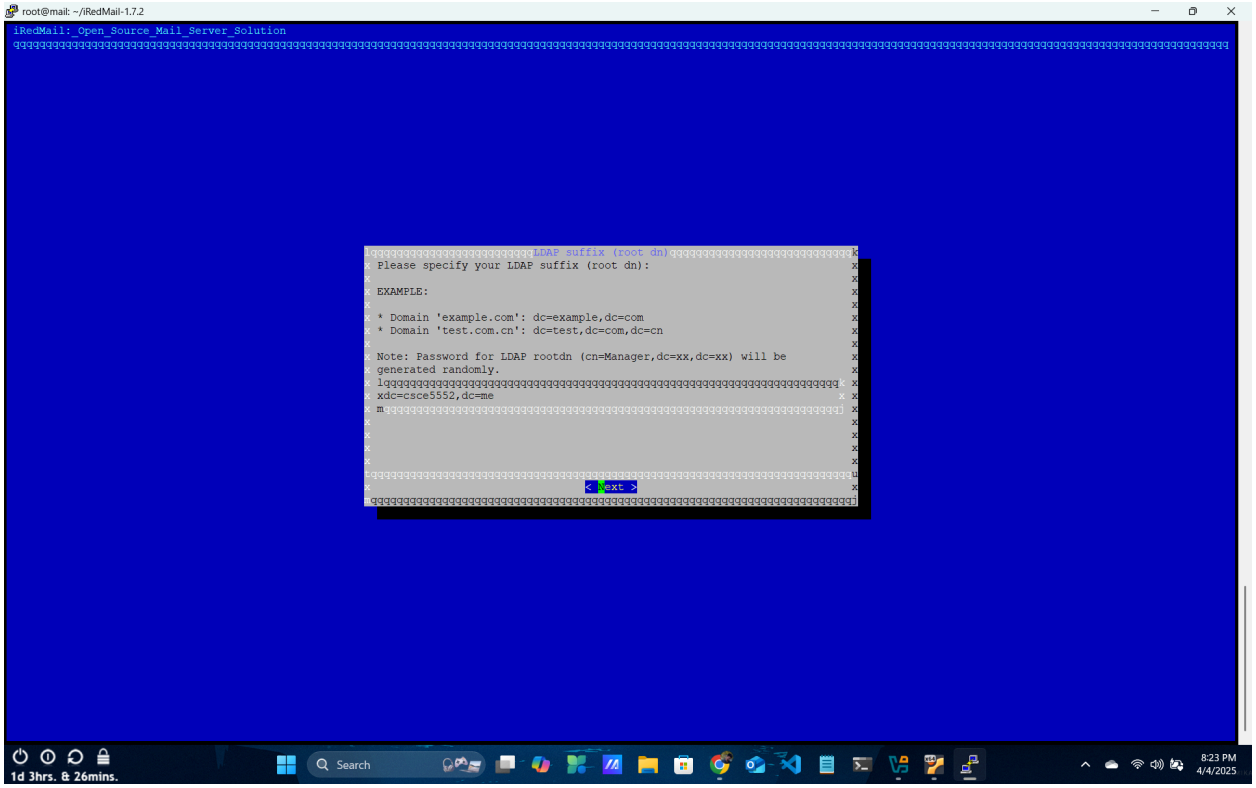
Hit **Next**



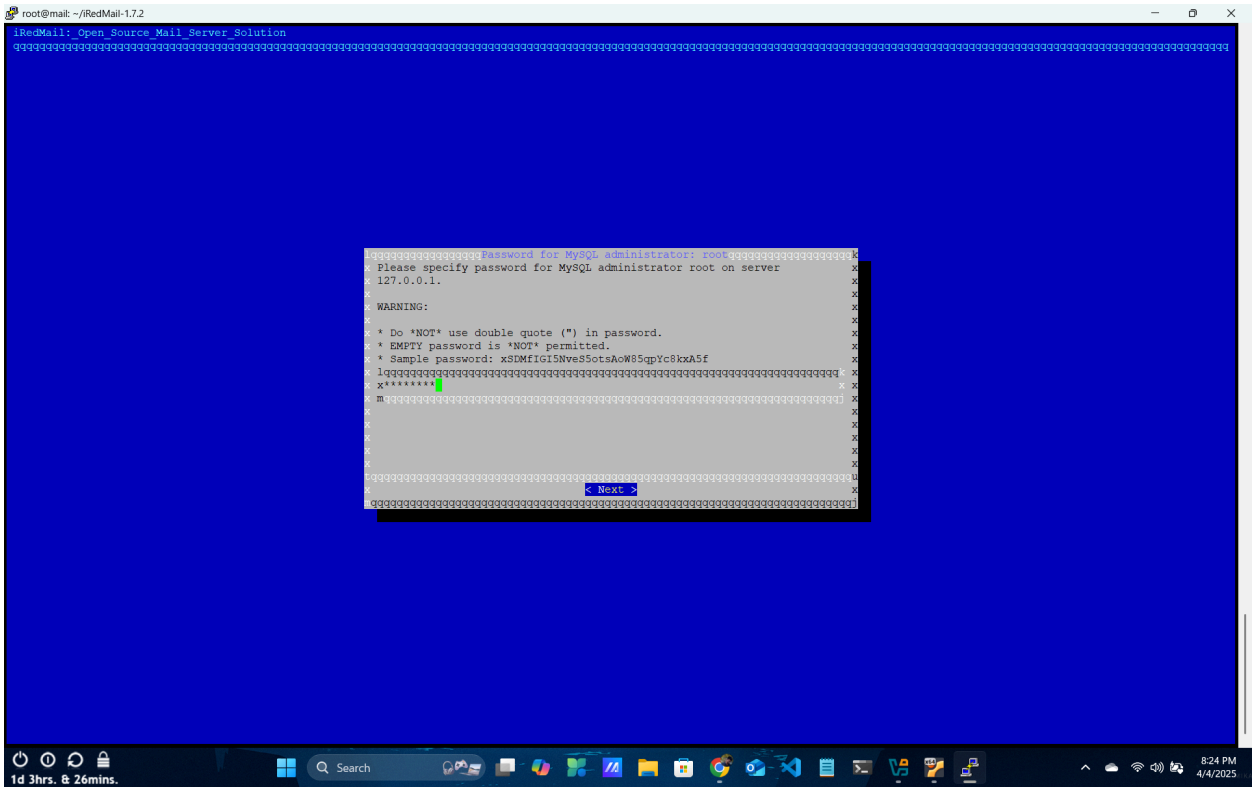
I'm going with iRedMail only server, so **Nginx** should be enough & hit **Next**



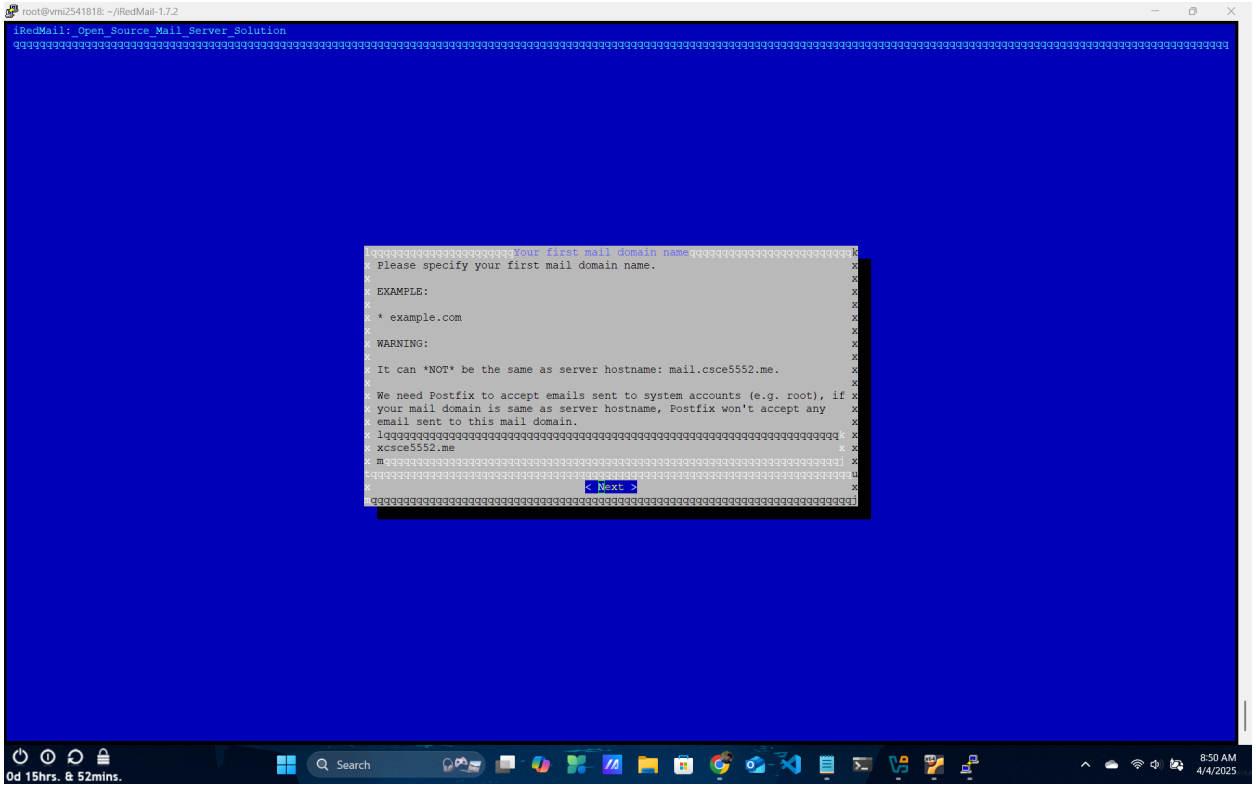
I'm going with iRedMail only server, so **OpenLDAP** should be good & hit **Next**



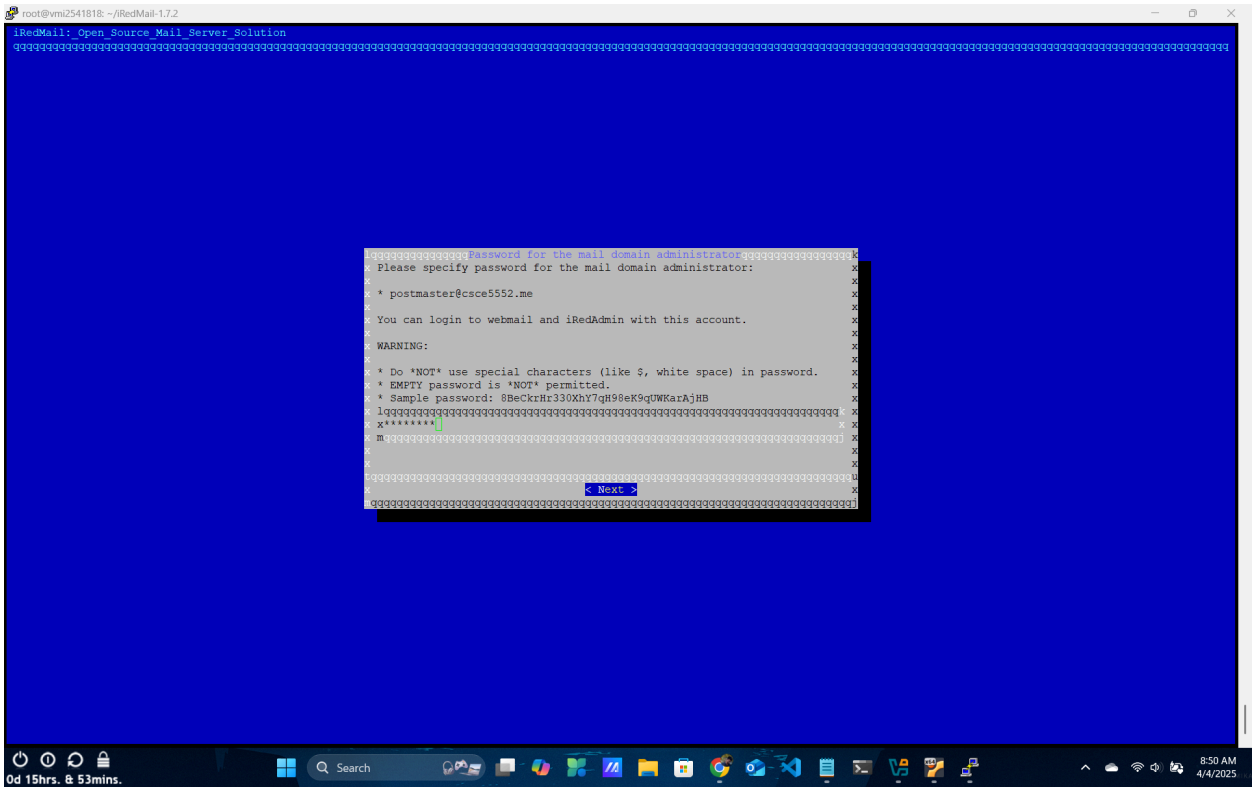
Under **LDAP suffix (root dn)**, I have added **dc=csce5552,dc=me** & hit **Next**



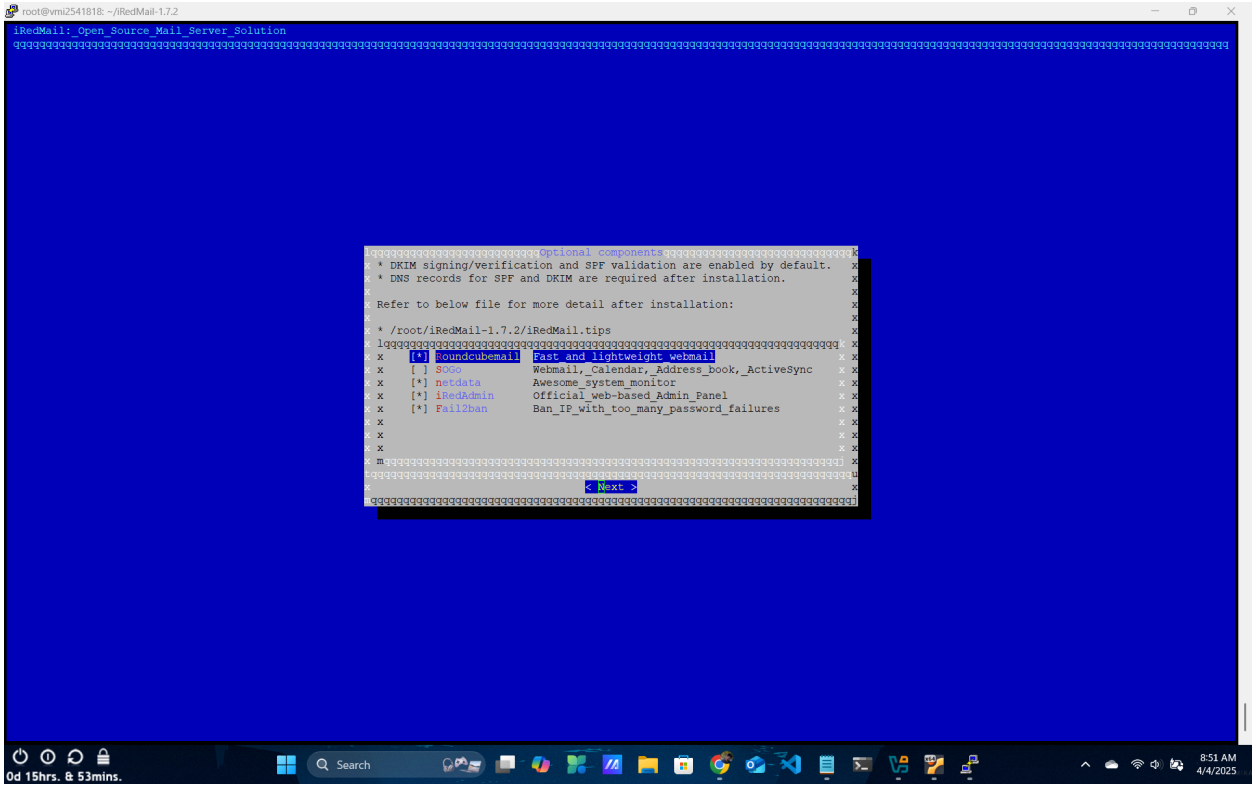
Set the **password for MySQL administrator: root** & hit **Next**



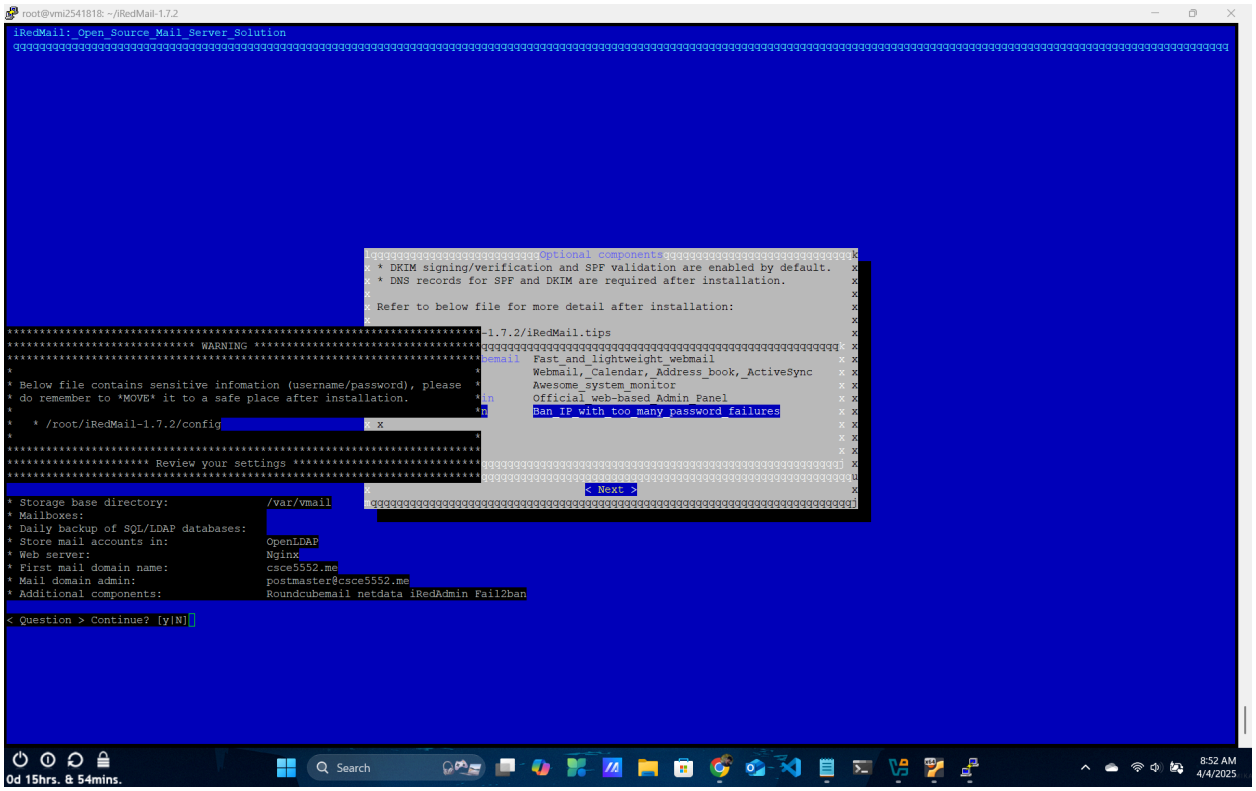
Enter your **domain** here & hit **Next**



Set the **password for Mail Domain Administrator** & hit **Next**



Go with the **default selected options** & hit **Next**



Press **y** & hit **Enter**

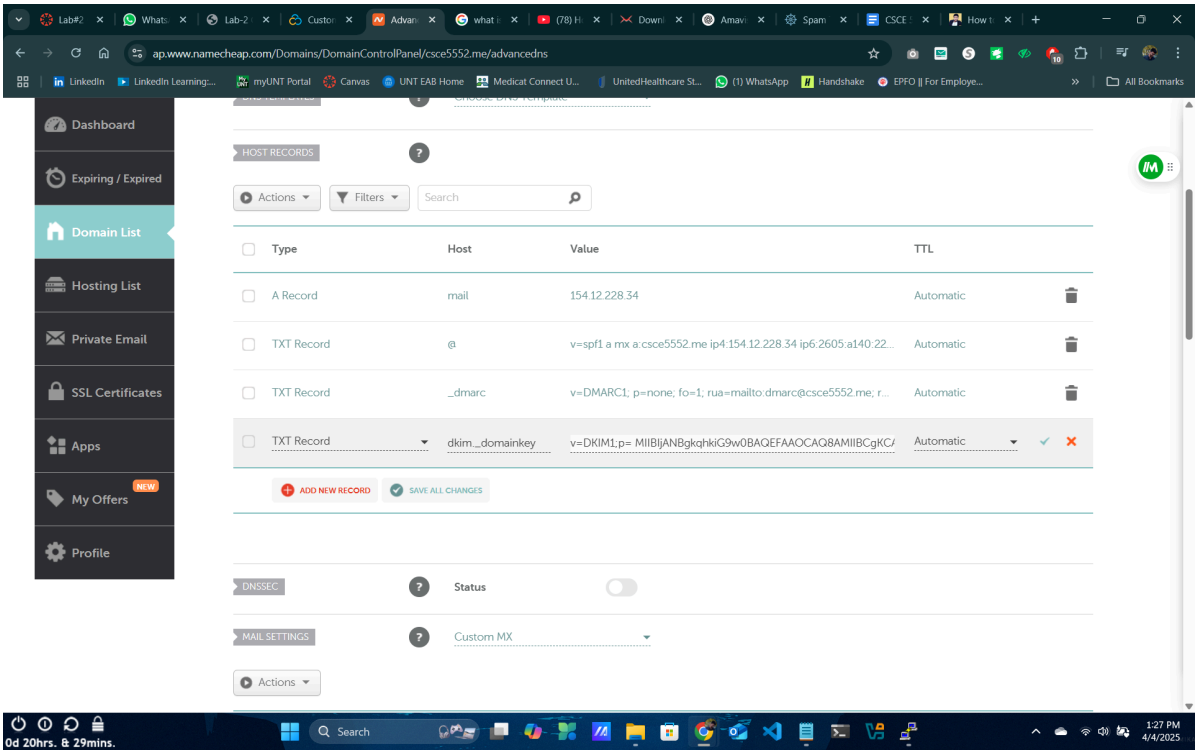
```
root@vmi2541818: ~/iRedMail-1.7.2
[ INFO ] Setup daily cron job to backup LDAP data with /var/vmail/backup/backup_openldap.sh
[ INFO ] Configure MariaDB database server.
[ INFO ] Setup daily cron job to backup SQL databases with /var/vmail/backup/backup_mysql.sh
[ INFO ] Configure Postfix (MTA).
[ INFO ] Configure Dovecot (POP3/IMAP/Managesieve/LMTP/LDA).
[ INFO ] Configure Nginx web server.
[ INFO ] Configure PHP.
[ INFO ] Configure mlmmj (mailing list manager).
[ INFO ] Configure ClamAV (anti-virus toolkit).
[ INFO ] Configure Amavisd-new (interface between MTA and content checkers).
[ INFO ] Configure SpamAssassin (content-based spam filter).
[ INFO ] Configure iRedAPD (postfix policy daemon).
[ INFO ] Configure iRedAdmin (official web-based admin panel).
[ INFO ] Configure Roundcube webmail.
[ INFO ] Configure Fail2ban (authentication failure monitor).
[ INFO ] Configure netdata (system and application monitor).

*************************************************************************
* iRedMail-1.7.2 installation and configuration complete.
*************************************************************************

< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/nftables.conf, with SSHD ports: 22. [Y|n]y
[ INFO ] Copy firewall sample rules.
< Question > Restart firewall now (with ssh ports: 22)? [y|N]y
[ INFO ] Restarting firewall ...
[ INFO ] Updating ClamAV database (freshclam), please wait ...
ERROR: Failed to lock the log file /var/log/clamav/freshclam.log: Resource temporarily unavailable
*******************************************************************
* URLs of installed web applications:
*
* - Roundcube webmail: https://mail.csce5552.me/mail/
* - netdata (monitor): https://mail.csce5552.me/netdata/
*
* - Web admin panel (iRedAdmin): https://mail.csce5552.me/iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@csce5552.me
* - Password: csce5552
*
*******************************************************************
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
*   - /root/iRedMail-1.7.2/iRedMail.tips
*
* And it's sent to your mail account postmaster@csce5552.me.
*
******************** WARNING ****************************************
*
* Please reboot your system to enable all mail services.
*
*******************************************************************
root@vmi2541818:~/iRedMail-1.7.2#
```

My mail server setup is completed successfully

URLs of installed web applications are:
Roundcube webmail: https://mail.csce5552.me/mail/
netdata (monitor): https://mail.csce5552.me/netdata/
Web admin panel (iRedAdmin): https://mail.csce5552.me/iredadmin/

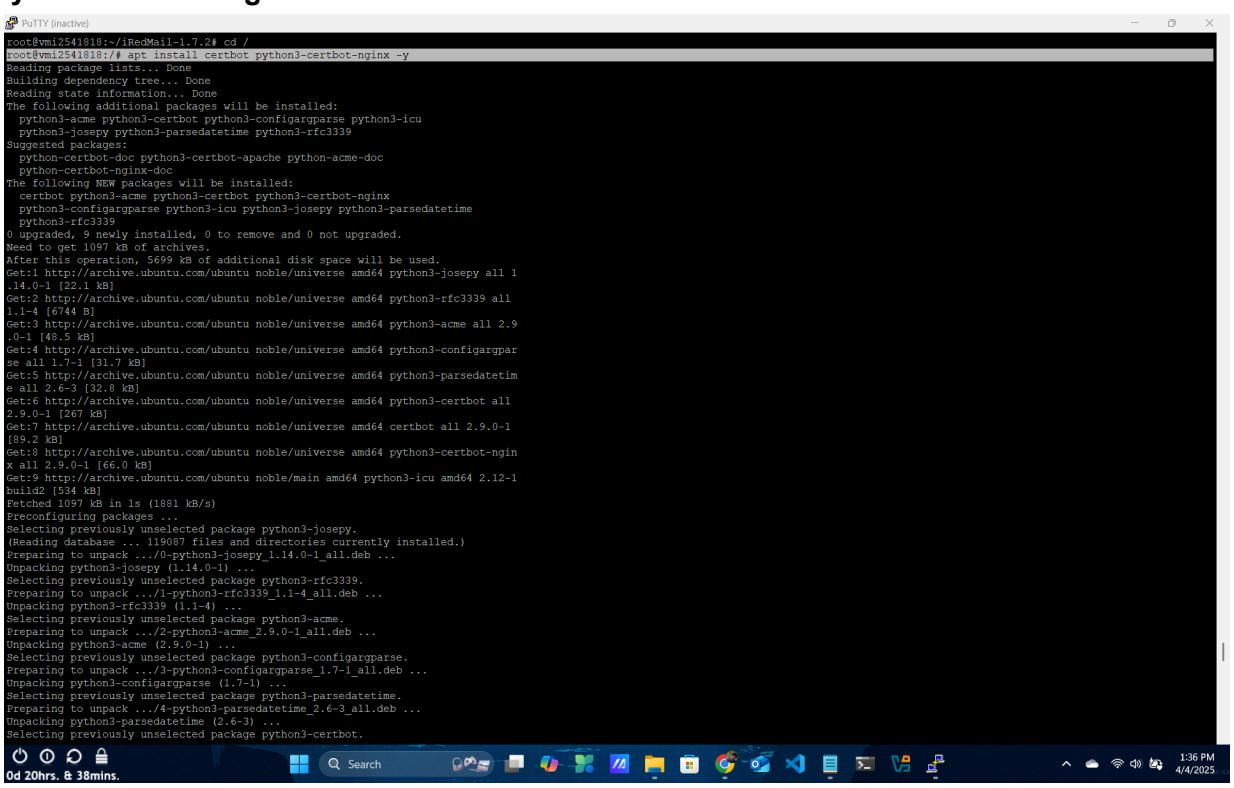
Got the **DKIM record** by running the command (amavisd showkeys) & added it to my **domain records** by removing special characters(‘’)

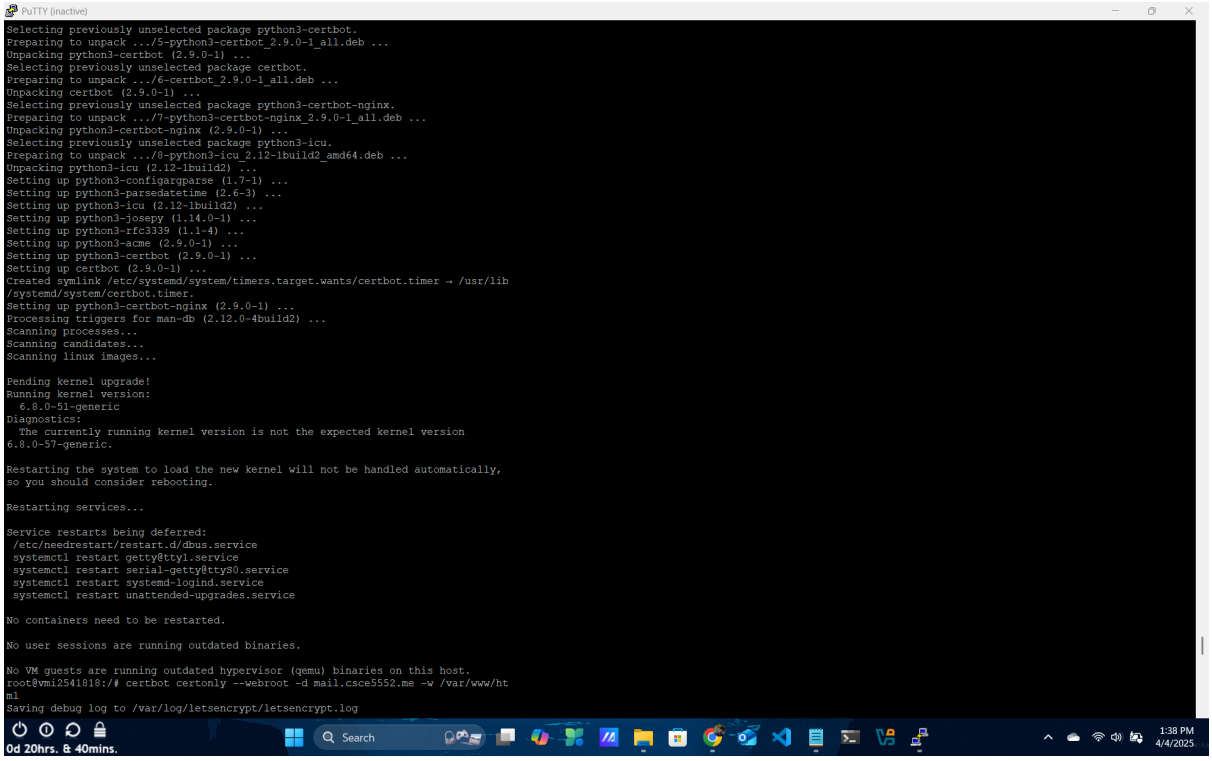
```
root@vmi2541818:~/iRedMail-1.7.2# amavisd showkeys
; key#1 2048 bits, s=dkim, d=csce5552.me, /var/lib/dkim/csce5552.me.pem
dkim._domainkey.csce5552.me.    3600 TXT (
  "v=DKIM1; p="
  "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArVteYNgq1C/3ijw7tT2C"
  "aB9365bIL9RTWrnH8QhTvc0Mh15JzBFu/DUvnE1ye/z2b7FiXWv9PQjZEiVA9AxL"
  "uuzUFMDAbyO+5ErlFPSDNYoS0kMfpwdtA34hU3pOjxB34TJXT3toL5L55wWfrTJe"
  "PiXp7WjeUniOAET7mMfhGQPD6BbiOKyZFtv7iueag3VkLeVTIgQB/bI9qmFqfPuX"
  "9W+NWMmGy861HrfKdDF3Fg/osRqMg21yfvoTwefc/U9QPWr1p6a0bcQ9eKGIWnto"
  "0JRuh7swQ6o5ct/v6rJlIIx4N4BiEGvegOOVCZmh12tWGRIBinZf6kg4ldb/ZZ9Q"
  "IwIDAQAB")
```



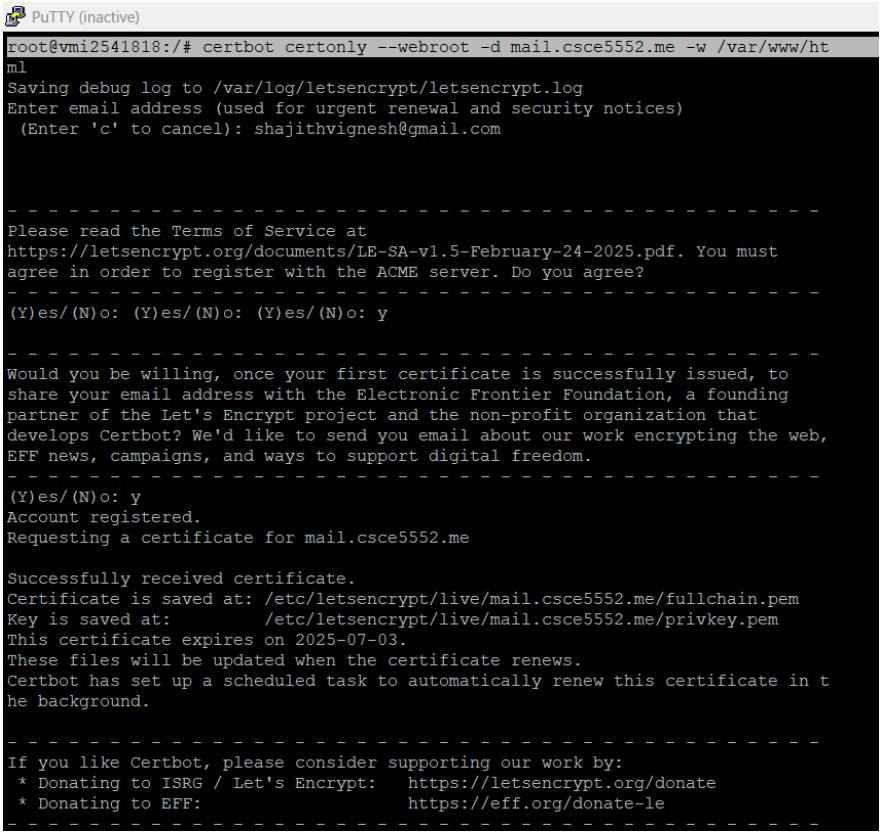
SSL Installation -

Navigated back to the root directory from the iRedMail directory & installed **certbot** and **python3-certbot-nginx**





For generating an **SSL certificate**, I have utilized **Certbot** as this verifies my domain, issues the certificate & stores it on my server, which is ready for manual installation



```
root@vmi2541818:/# ll /etc/letsencrypt/live/mail.csce5552.me
total 12
drwxr-xr-x 2 root root 4096 Apr  4 16:21 ./
drwx------ 3 root root 4096 Apr  4 16:21 ../
-rw-r--r-- 1 root root  692 Apr  4 16:21 README
lrwxrwxrwx 1 root root   40 Apr  4 16:21 cert.pem -> ../../archive/mail.csce5552
.me/cert1.pem
lrwxrwxrwx 1 root root   41 Apr  4 16:21 chain.pem -> ../../archive/mail.csce555
2.me/chain1.pem
lrwxrwxrwx 1 root root   45 Apr  4 16:21 fullchain.pem -> ../../archive/mail.csc
e5552.me/fullchain1.pem
lrwxrwxrwx 1 root root   43 Apr  4 16:21 privkey.pem -> ../../archive/mail.csce5
552.me/privkey1.pem
```

I pointed my applications to these SSL certificate files (fullchain.pem & privkey.pem)

Opened **Nginx SSL template file** by using a text editor (nano /etc/nginx/templates/ssl.tmpl)

i. Commented out the following lines

#ssl_certificate /etc/ssl/certs/iRedMail.crt;

#ssl_certificate_key /etc/ssl/private/iRedMail.key;

ii. Added the following lines & saved

ssl_certificate /etc/letsencrypt/live/mail.csce5552.me/fullchain.pem;

ssl_certificate_key /etc/letsencrypt/live/mail.csce5552.me/privkey.pem;

```
root@mail: /
  GNU nano 7.2                                                    /etc/nginx/templates/ssl.tmpl
ssl_protocols TLSv1.2 TLSv1.3;

# Fix 'The Logjam Attack'.
ssl_ciphers EECDH+CHACHA20:EECDH+AESGCM:EDH+AESGCM:AES256+EECDH;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/ssl/dh2048_param.pem;

# Greatly improve the performance of keep-alive connections over SSL.
# With this enabled, client is not necessary to do a full SSL-handshake for
# every request, thus saving time and cpu-resources.
ssl_session_cache shared:SSL:10m;

# To use your own ssl cert (e.g. "Let's Encrypt"), please create symbol link to
# ssl cert/key used below, so that we can manage this config file with Ansible.
#
# For example:
#
# rm -f /etc/ssl/private/iRedMail.key
# rm -f /etc/ssl/certs/iRedMail.crt
# ln -s /etc/letsencrypt/live/<domain>/privkey.pem /etc/ssl/private/iRedMail.key
# ln -s /etc/letsencrypt/live/<domain>/fullchain.pem /etc/ssl/certs/iRedMail.crt
#
# To request free "Let's Encrypt" cert, please check our tutorial:
# https://docs.iredmail.org/letsencrypt.html
#ssl_certificate /etc/ssl/certs/iRedMail.crt;
#ssl_certificate_key /etc/ssl/private/iRedMail.key;
ssl_certificate /etc/letsencrypt/live/mail.csce5552.me/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/mail.csce5552.me/privkey.pem;
```

Opened **Postfix configuration file** by using a text editor (nano /etc/postfix/main.cf)

i. Commented out the following lines

#smtpd_tls_key_file = /etc/ssl/private/iRedMail.key

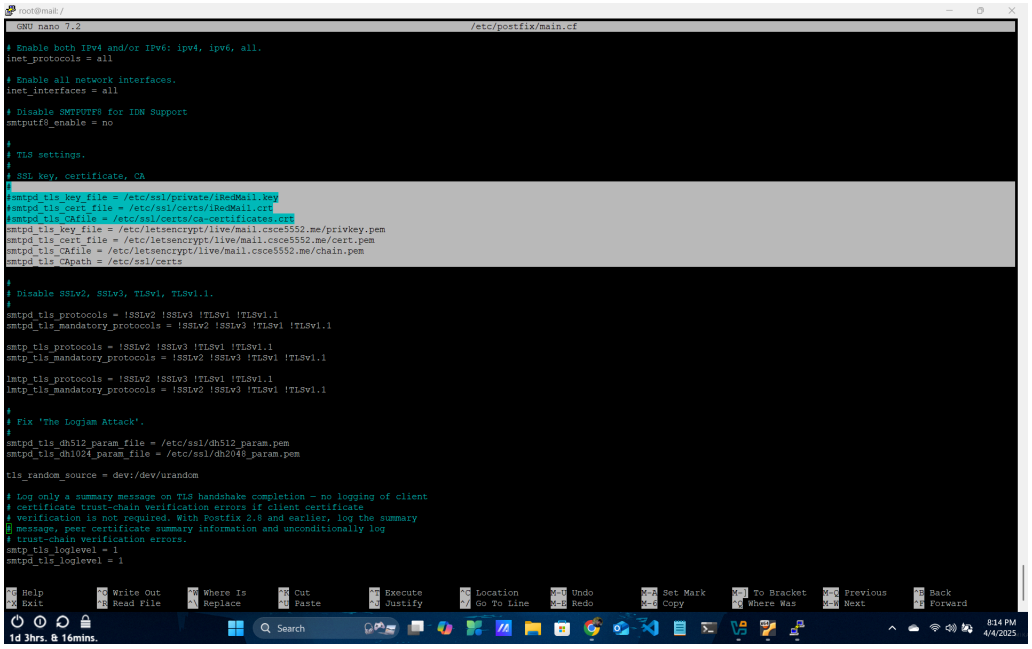
#smtpd_tls_cert_file = /etc/ssl/certs/iRedMail.crt

#smtpd_tls_CAfile = /etc/ssl/certs/iRedMail.crt

ii. Added the following lines & saved

smtpd_tls_key_file = /etc/letsencrypt/live/mail.csce5552.me/privkey.pem

smtpd_tls_cert_file = /etc/letsencrypt/live/mail.csce5552.me/cert.pem
smtpd_tls_CAfile = /etc/letsencrypt/live/mail.csce5552.me/chain.pem



Opened **Dovecot configuration file** by using a text editor (nano /etc/dovecot/dovecot.conf)

i. Commented out the following lines

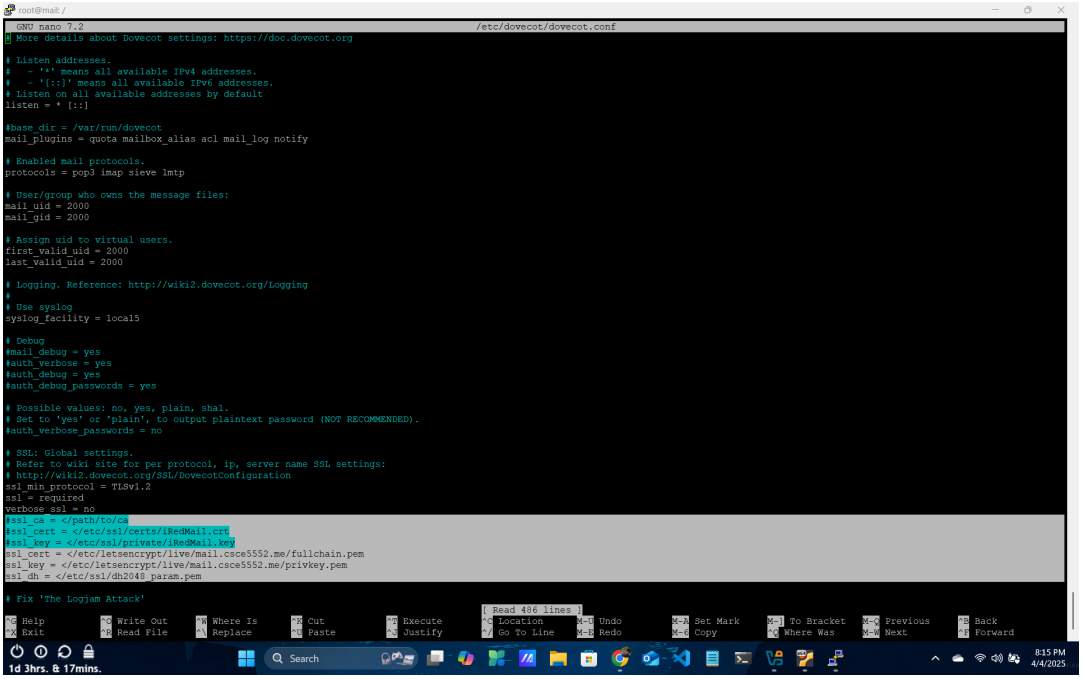
#ssl_cert = </etc/ssl/certs/iRedMail.crt

#ssl_key = </etc/ssl/private/iRedMail.key

ii. Added the following lines & saved

ssl_cert = </etc/letsencrypt/live/mail.csce5552.me/fullchain.pem

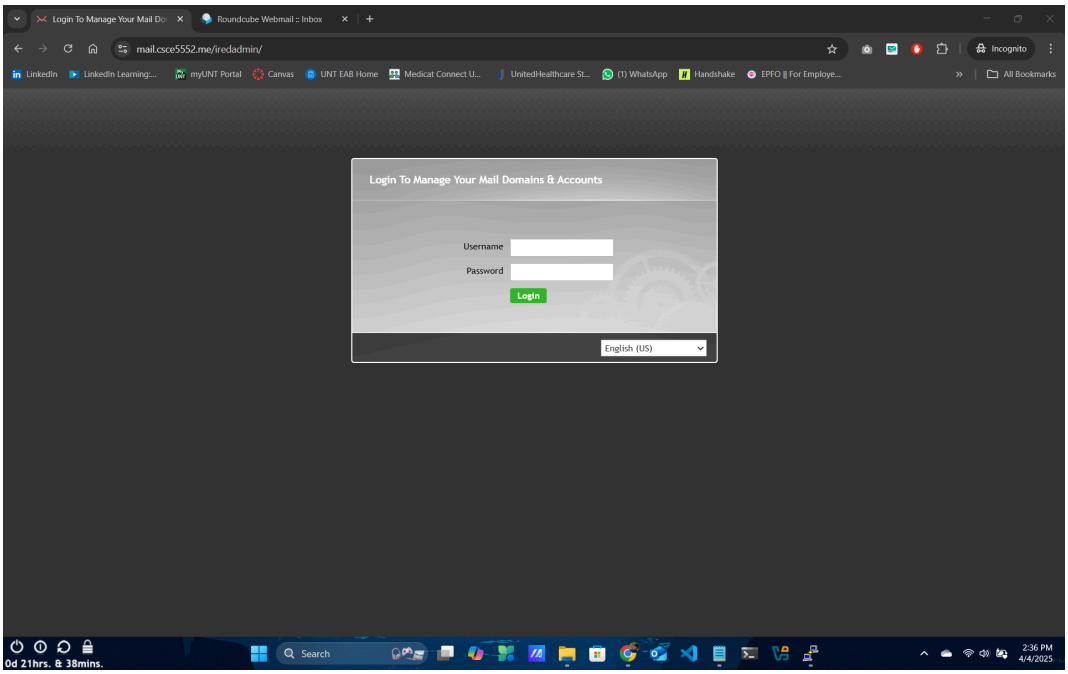
ssl_key = </etc/letsencrypt/live/mail.csce5552.me/privkey.pem

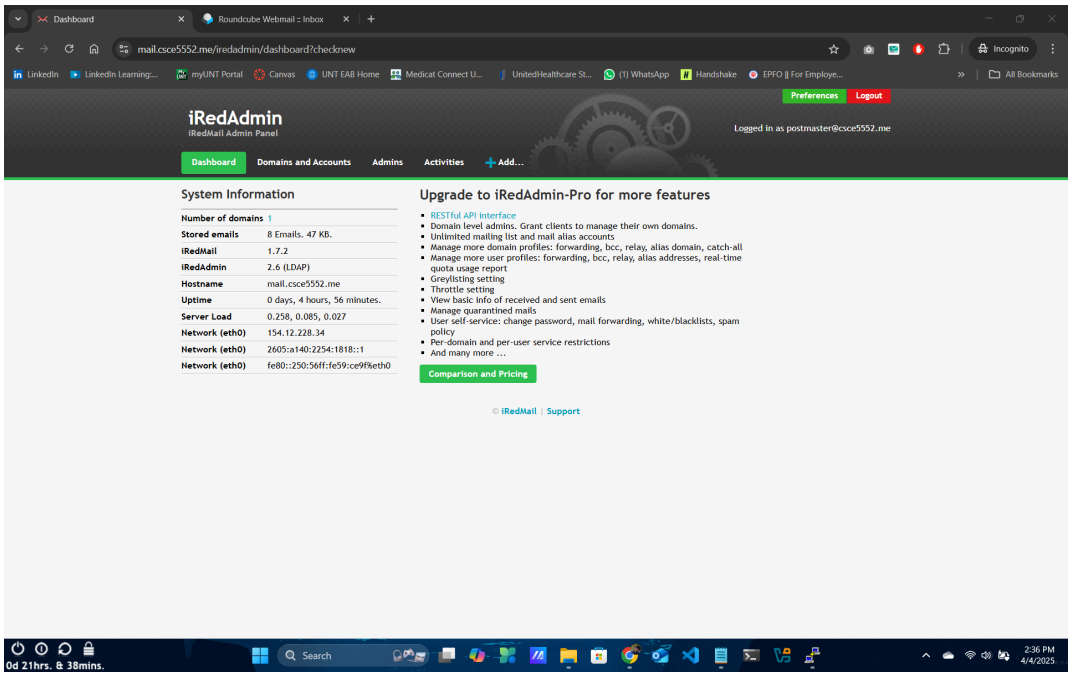


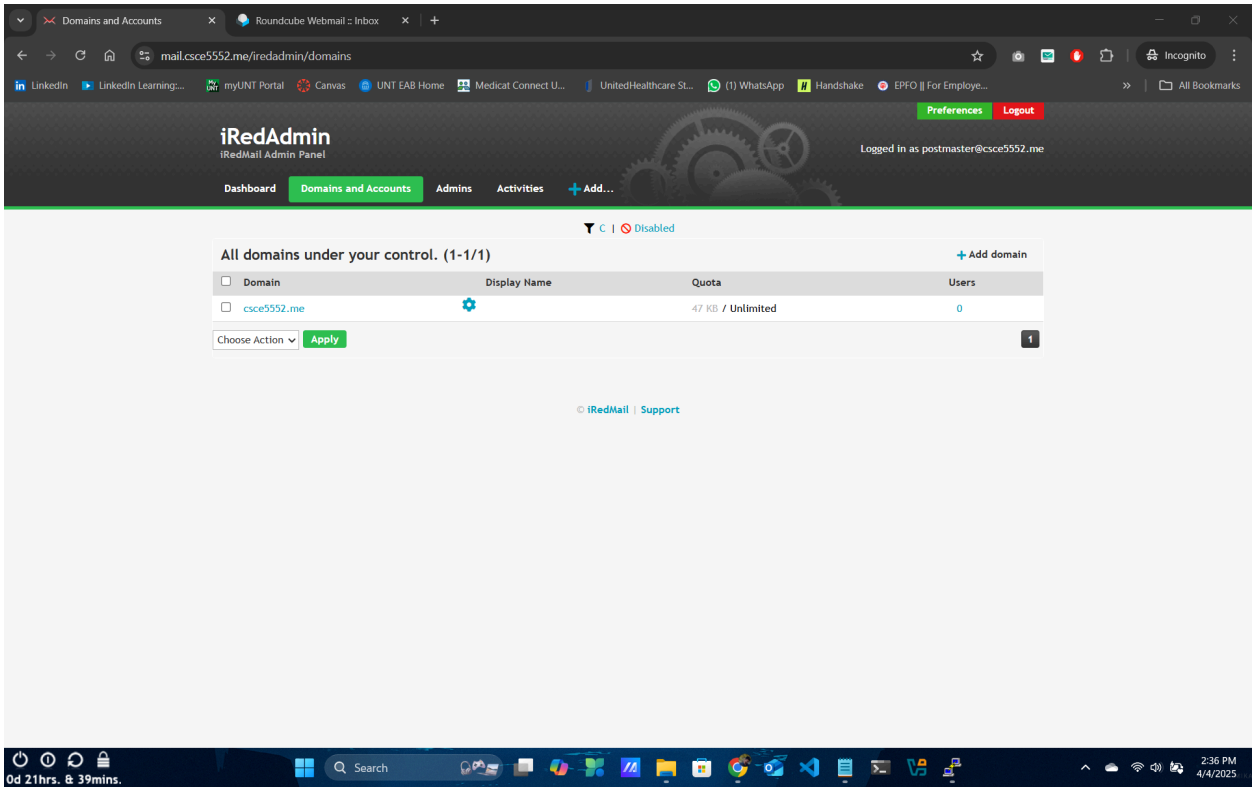
Restarted nginx, postfix, dovecot & rebooted the server

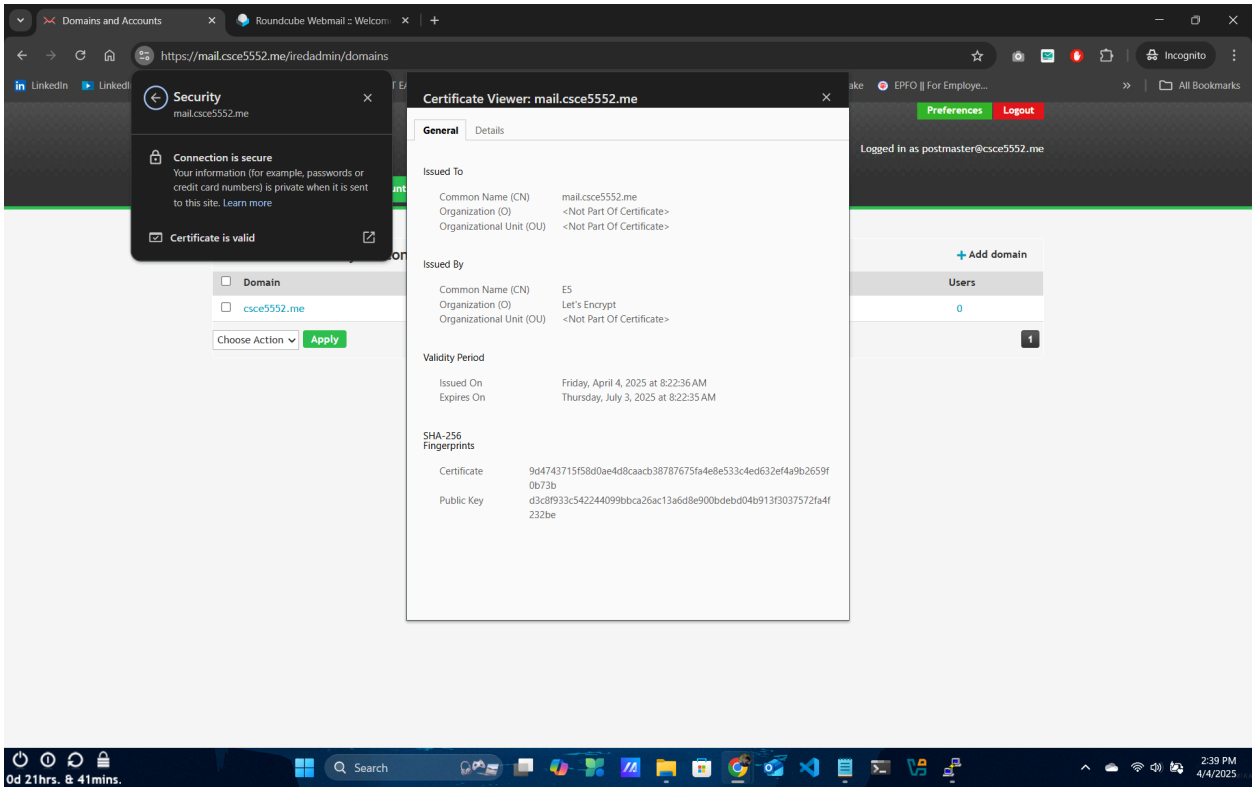
```
root@vmi2541818:/# systemctl restart nginx
root@vmi2541818:/# systemctl restart postfix
root@vmi2541818:/# systemctl restart dovecot
root@vmi2541818:/# reboot
```

Accessing iRedMail -
i. iRedMail Admin Panel:

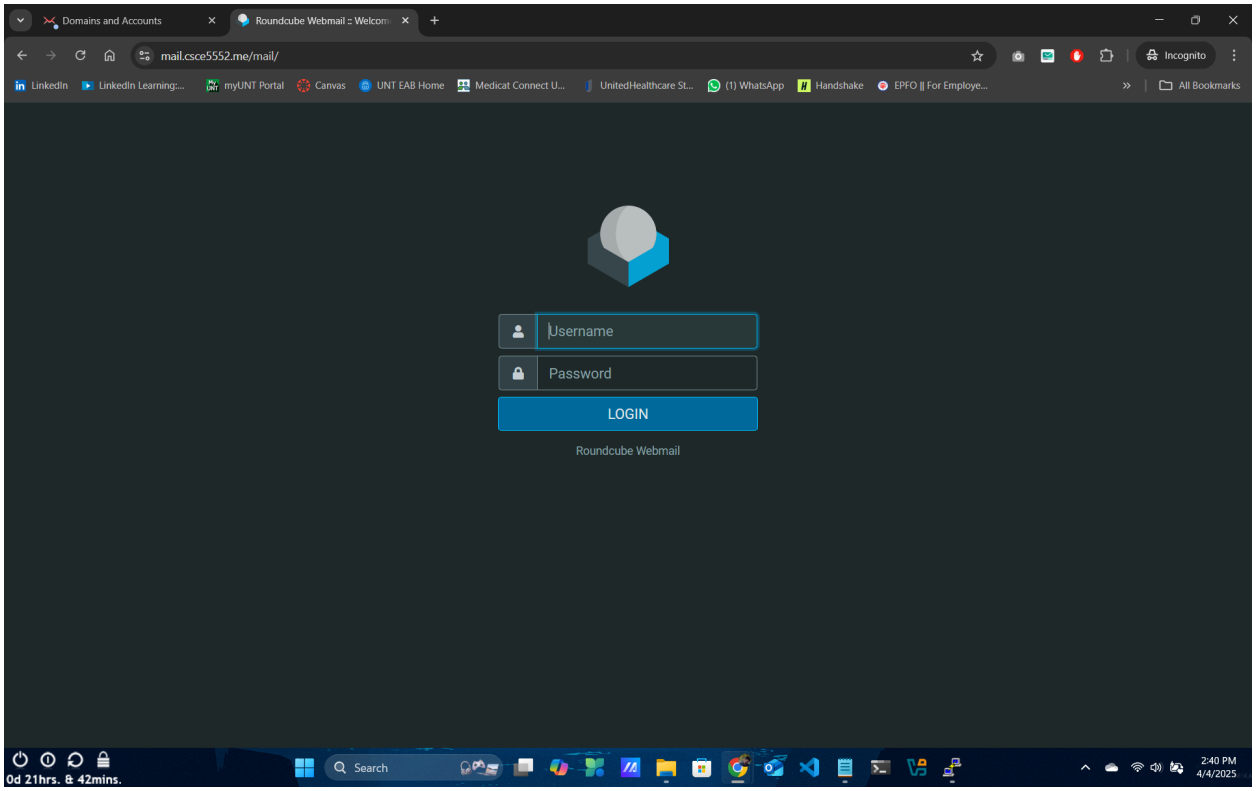


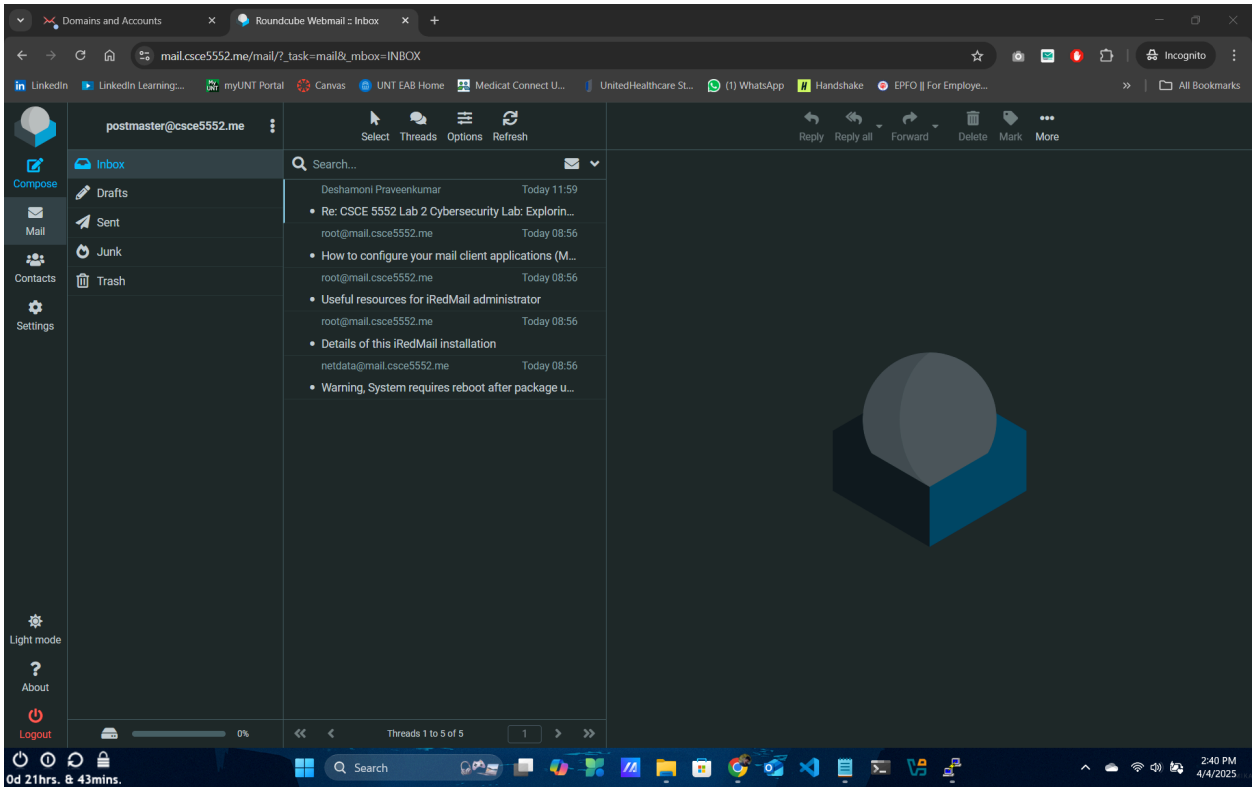



Domains and Accounts
Roundcube Webmail :: Inbox
mail.csce5552.me/iredadmin/domains
Incognito
LinkedIn
LinkedIn Learning:...
myUNT Portal
Canvas
UNT EAB Home
Medicat Connect U...
UnitedHealthcare St...
(1) WhatsApp
Handshake
EPFO || For Employe...
All Bookmarks
Preferences
Logout
iRedAdmin
iRedMail Admin Panel
Logged in as postmaster@csce5552.me
Dashboard
Domains and Accounts
Admins
Activities
Add...
C | Disabled
All domains under your control. (1-1/1)
Add domain
Domain
Display Name
Quota
Users
csce5552.me
47 KB / Unlimited
0
Choose Action
Apply
1
iRedMail | Support
0d 21hrs. & 39mins.
Search
2:36 PM
4/4/2025

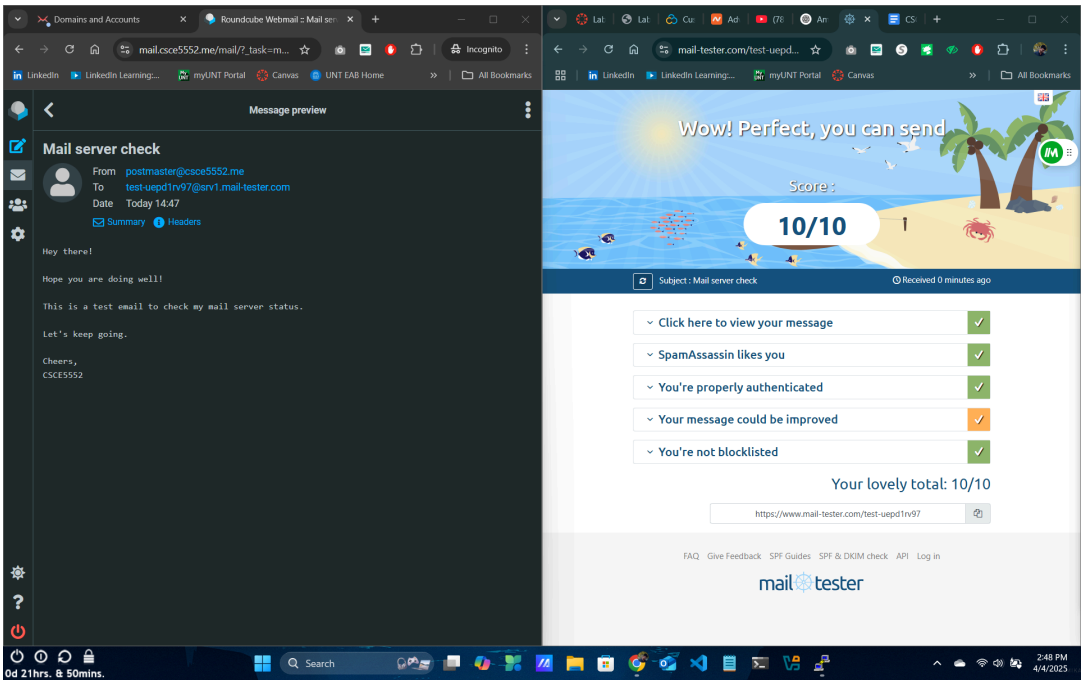

Domains and Accounts
Roundcube Webmail :: Welcom
https://mail.csce5552.me/iredadmin/domains
Incognito
LinkedIn
EPFO || For Employe...
All Bookmarks
Security
mail.csce5552.me
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
Certificate Viewer: mail.csce5552.me
General
Details
Issued To
Common Name (CN) mail.csce5552.me
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) E5
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Friday, April 4, 2025 at 8:22:36 AM
Expires On Thursday, July 3, 2025 at 8:22:35 AM
SHA-256 Fingerprints
Certificate 9d4743715f58d0ae4d8caacb38787675fa4e8e533c4ed632ef4a9b2659f0b73b
Public Key d3c8f933c542244099bbca26ac13a6d8e900bdebd04b913f3037572fa4f232be
Preferences
Logout
Logged in as postmaster@csce5552.me
Add domain
Domain
Users
csce5552.me
0
Choose Action
Apply
1
0d 21hrs. & 41mins.
Search
2:39 PM
4/4/2025

ii. Roundcube Web Mail Interface

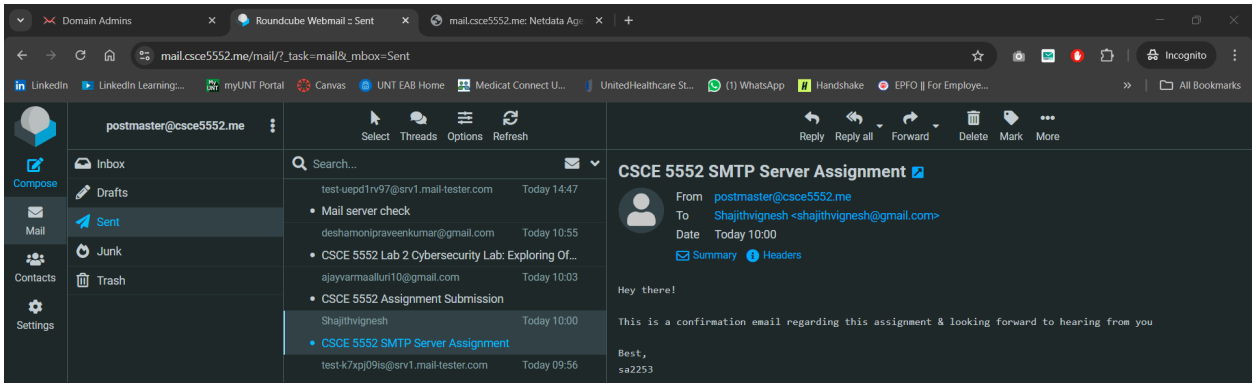


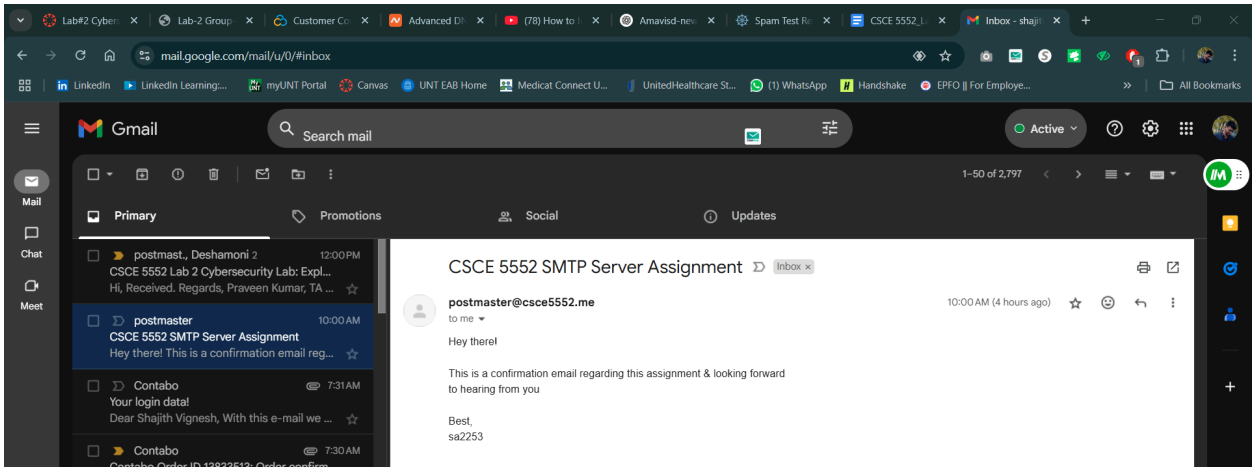


Used **Mail-Tester.com** to check the quality of mail server configuration & everything looks good with my setup

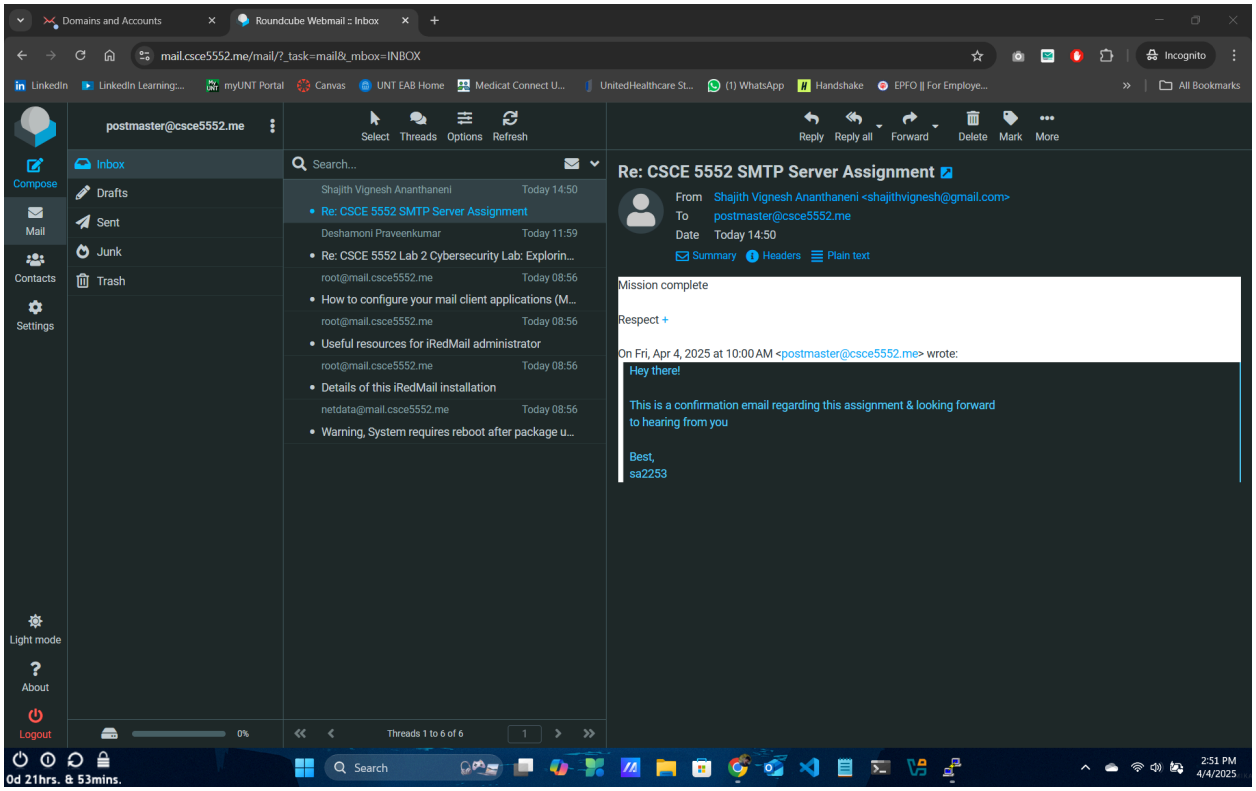


I have sent an email to my personal email address & it was delivered successfully to my **Inbox**

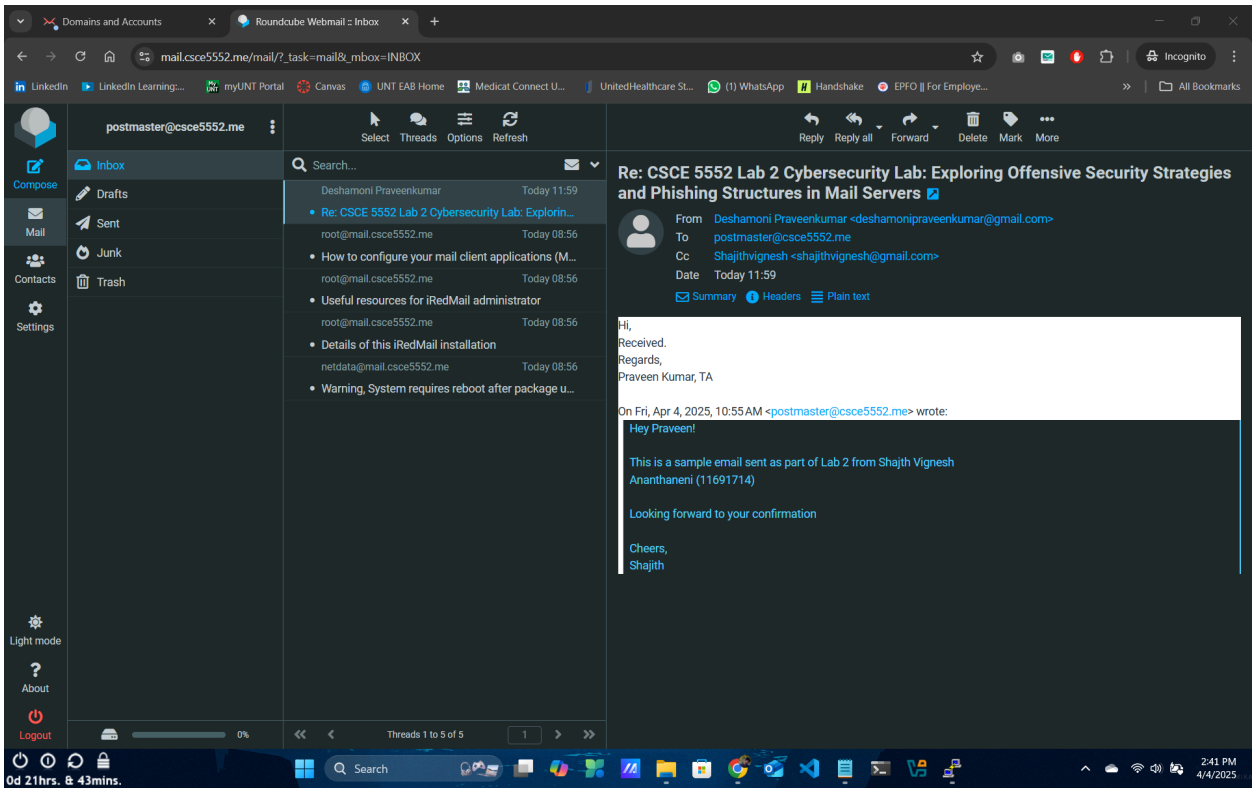




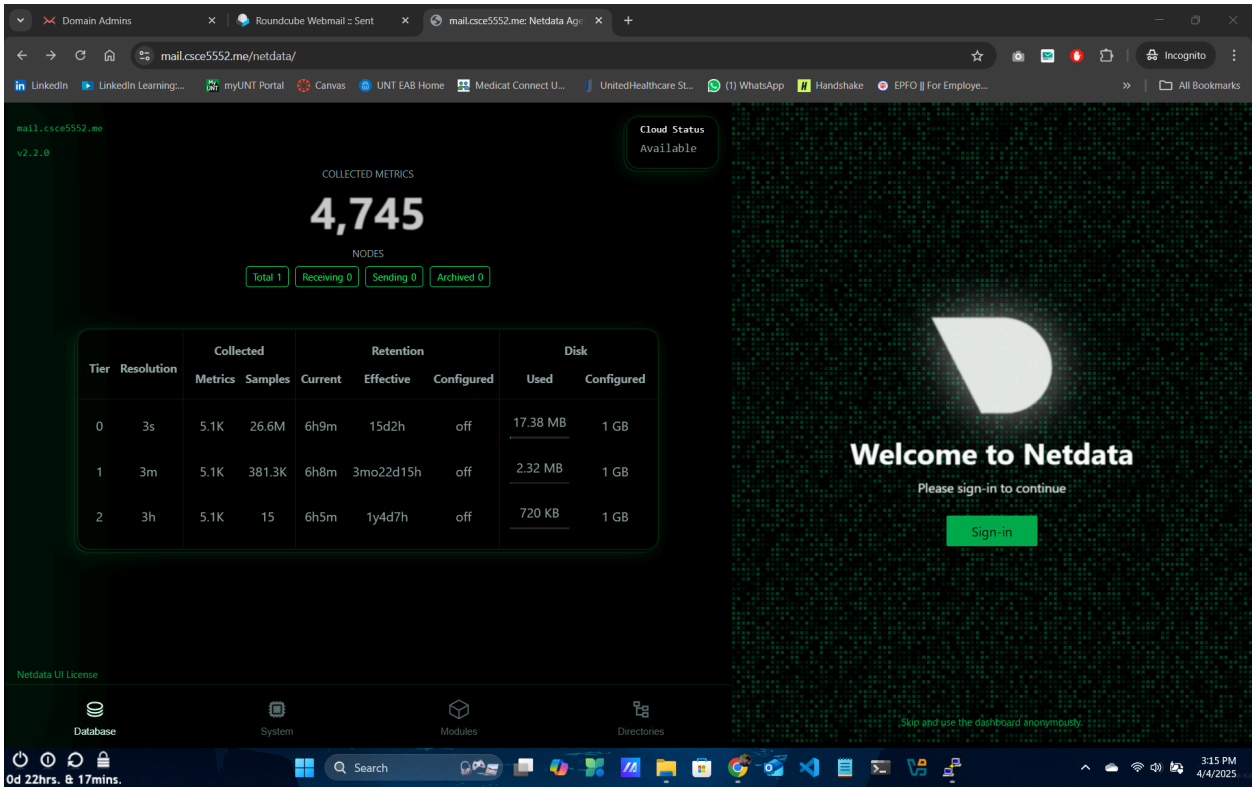
Got the reply back successfully

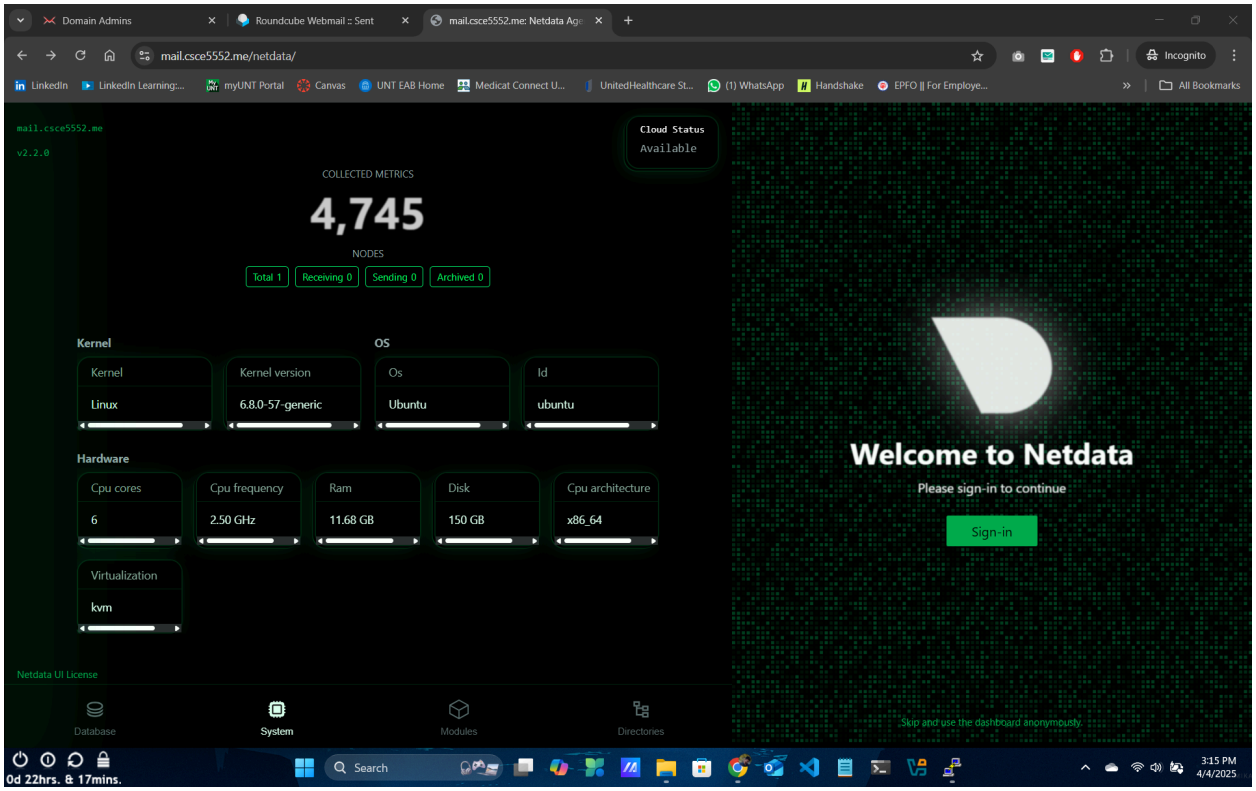


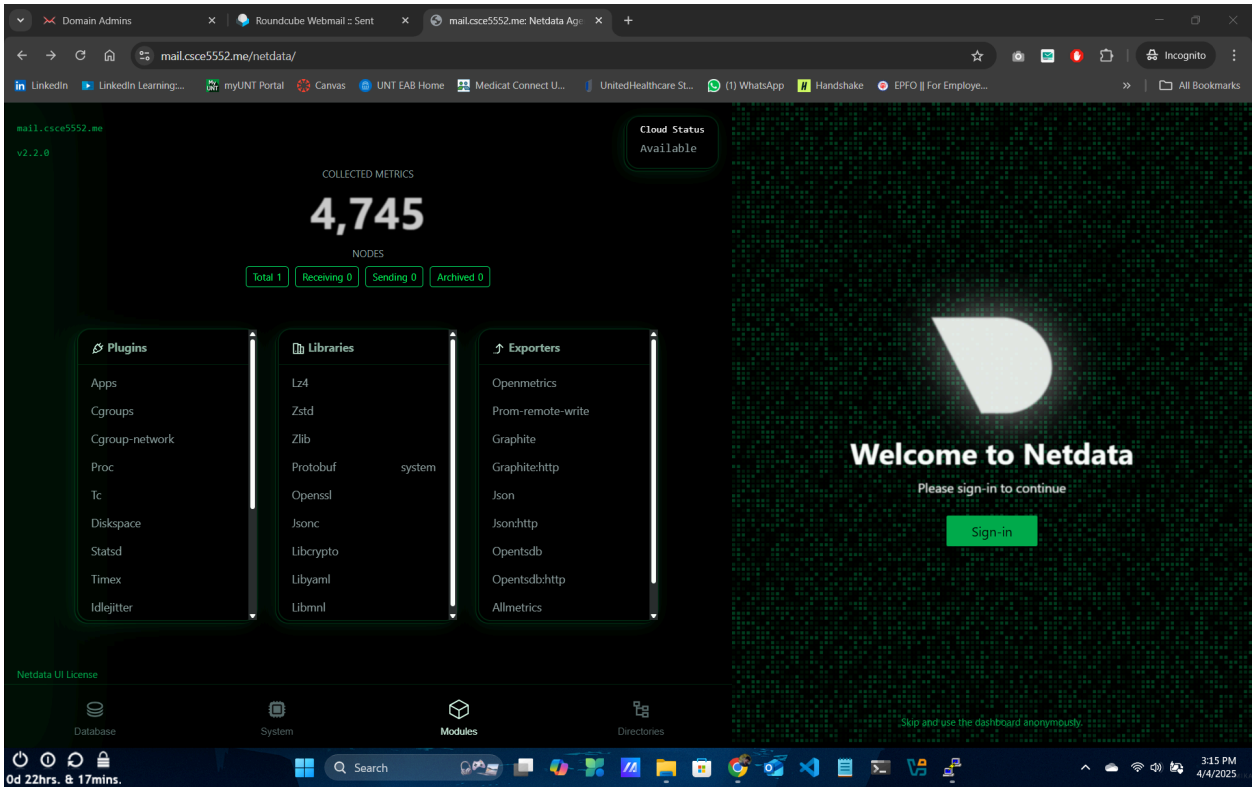
Sent an email to TA & received the confirmation too

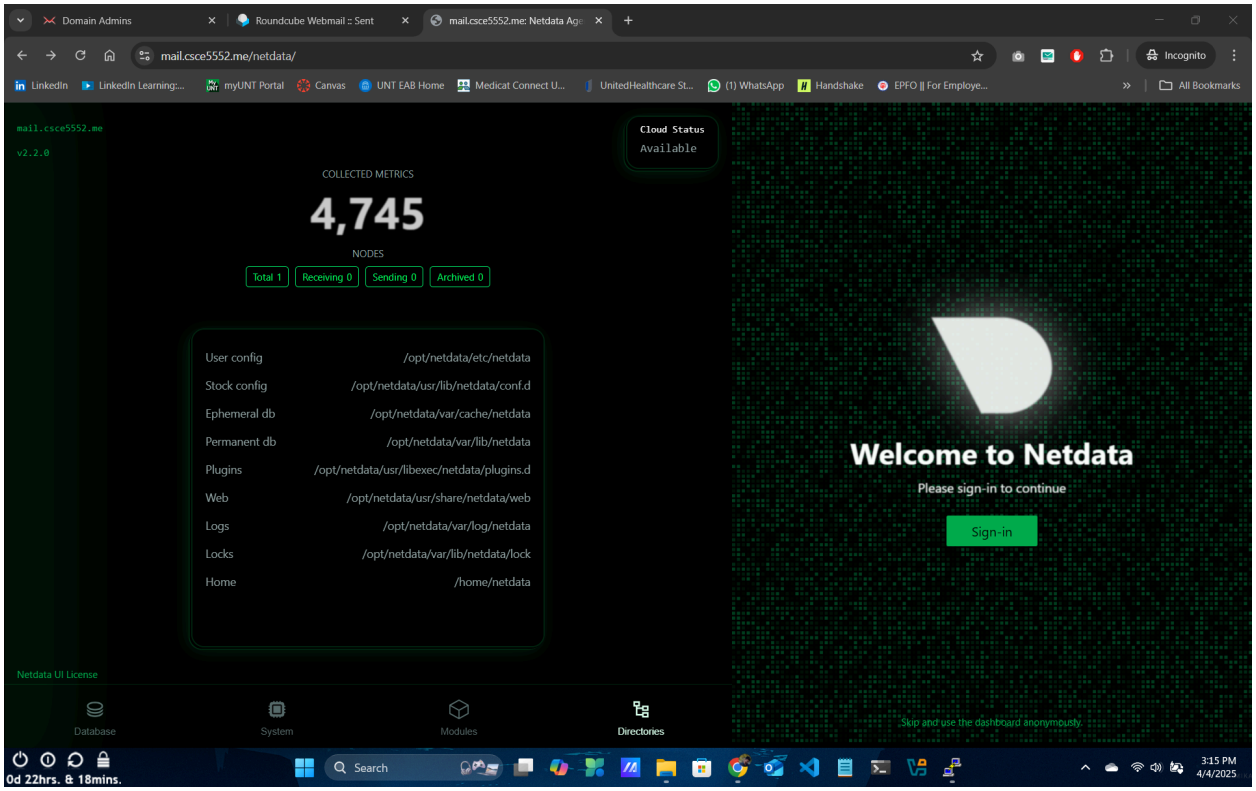


iii. Netdata Monitor:






Domain Admins
Roundcube Webmail :: Sent
mail.csce5552.me: Netdata Age
mail.csce5552.me/netdata/
Incognito
LinkedIn
LinkedIn Learning:...
myUNT Portal
Canvas
UNT EAB Home
Medicat Connect U...
UnitedHealthcare St...
(1) WhatsApp
Handshake
EPFO || For Employe...
All Bookmarks
mail.csce5552.me
v2.2.0
Cloud Status
Available
COLLECTED METRICS
4,745
NODES
Total 1
Receiving 0
Sending 0
Archived 0
Plugins
Apps
Cgroups
Cgroup-network
Proc
Tc
Diskspace
Statsd
Timex
Idlejitter
Libraries
Lz4
Zstd
Zlib
Protobuf
system
Openssl
Jsonc
Libcrypto
Libyaml
Libmnl
Exporters
Openmetrics
Prom-remote-write
Graphite
Graphite:http
Json
Json:http
Opentsdb
Opentsdb:http
Allmetrics
Welcome to Netdata
Please sign-in to continue
Sign-in
Netdata UI License
Database
System
Modules
Directories
Skip and use the dashboard anonymously
0d 22hrs. & 17mins.
Search
3:15 PM
4/4/2025


Domain Admins
Roundcube Webmail :: Sent
mail.csce5552.me: Netdata Age
mail.csce5552.me/netdata/
Incognito
LinkedIn
LinkedIn Learning:...
myUNT Portal
Canvas
UNT EAB Home
Medicat Connect U...
UnitedHealthcare St...
(1) WhatsApp
Handshake
EPFO || For Employe...
All Bookmarks
mail.csce5552.me
v2.2.0
Cloud Status
Available
COLLECTED METRICS
4,745
NODES
Total 1
Receiving 0
Sending 0
Archived 0
User config /opt/netdata/etc/netdata
Stock config /opt/netdata/usr/lib/netdata/conf.d
Ephemeral db /opt/netdata/var/cache/netdata
Permanent db /opt/netdata/var/lib/netdata
Plugins /opt/netdata/usr/libexec/netdata/plugins.d
Web /opt/netdata/usr/share/netdata/web
Logs /opt/netdata/var/log/netdata
Locks /opt/netdata/var/lib/netdata/lock
Home /home/netdata
Welcome to Netdata
Please sign-in to continue
Sign-in
Netdata UI License
Database
System
Modules
Directories
Skip and use the dashboard anonymously
0d 22hrs. & 18mins.
Search
3:15 PM
4/4/2025

1. Set up your domain on Namecheap

a. Why do you need a domain name to create an SMTP mail server?

A domain name is required to create an SMTP mail server because it provides a unique identity for sending and receiving emails

b. Explain the purpose of MX, SPF, and DKIM records in the context of email security.

- Mail Exchange(MX) records specify the mail servers responsible for receiving emails for your domain, without which incoming emails will not be directed to your mail server
- Sender Policy Framework(SPF) records define which mail servers are authorized to send emails on behalf of your domain, thus preventing email spoofing and reducing spam
- DomainKeys Identified Mail(DKIM) records add a digital signature to outgoing emails, allowing recipients to verify that the email was sent by an authorized server and wasn't tampered with during transmission.

c. What is DNS propagation, and why do you need to wait for it after making DNS changes?

DNS propagation is the time taken for DNS changes to be updated across all the DNS servers globally. This process can take anywhere from few minutes to 48 hours and we need to wait for this period because some users may still be directed to the old DNS records causing email delivery failures.

2. Install and configure iRedMail on Kali

a. Why is SSH used to connect to the server for installing iRedMail?

Secure Shell(SSH) is used to connect to the remote Virtual Private Server(VPS) where we install iRedMail. It provides encrypted communication allowing us to execute commands, install software & manage server remotely.

b. What is the significance of choosing "OpenLDAP" as the backend for storing mail accounts?

Lightweight Directory Access Protocol(OpenLDAP) is used as a directory service for managing mail accounts centrally. It provides:

- Scalability for large numbers of users
- Centralized authentication & account management
- Integration with other directory services

c. Compare and contrast Roundcube and SOGo as webmail options. When would you choose one over the other?

Feature	**Roundcube**	**SOGo**
Interface	Simple, Lightweight	Modern, Feature-rich
Calender & Contacts	Limited	Full groupware support (calender, contacts, tasks)

Protocols	IMAP-based webmail	Supports ActiveSync & CalDAV
Customization	Basic plugins	Advanced customization
Best Use Case	Simple email usage	Business environments needing full collaboration feacture
When to Choose?	When we need a lightweight, user-friendly email client for personal ot basic email usage	When we need advanced collaboration tools like shared calendars, contacts, & mobile sync

d. What is the importance of reviewing and confirming the installation choices before proceeding?

Reviewing installation choices is crucial because:

- It prevents misconfiguration that leads to email delivery failure
- Changing settings after installation is complex
- Incorrect selections like wrong database backend may required reinstallation

3. Configure your mail client

a. Why is it necessary to configure your mail client after setting up the SMTP mail server?

Configuring the mail client configuration firstly ensures us(users) to send and receive emails using the new SMTP server without which email clients will not be able to authenticate & communicate with the server

b. What specific information or settings would you need to configure your mail client to work with the iRedMail server?

For configuring the mail client to work with the server, we need to know the authentication details(email address & password), server's IP address, choosing right database for mail accounts storage, required components configurations & so on.