PART TWO PROJECT

11/22/2024

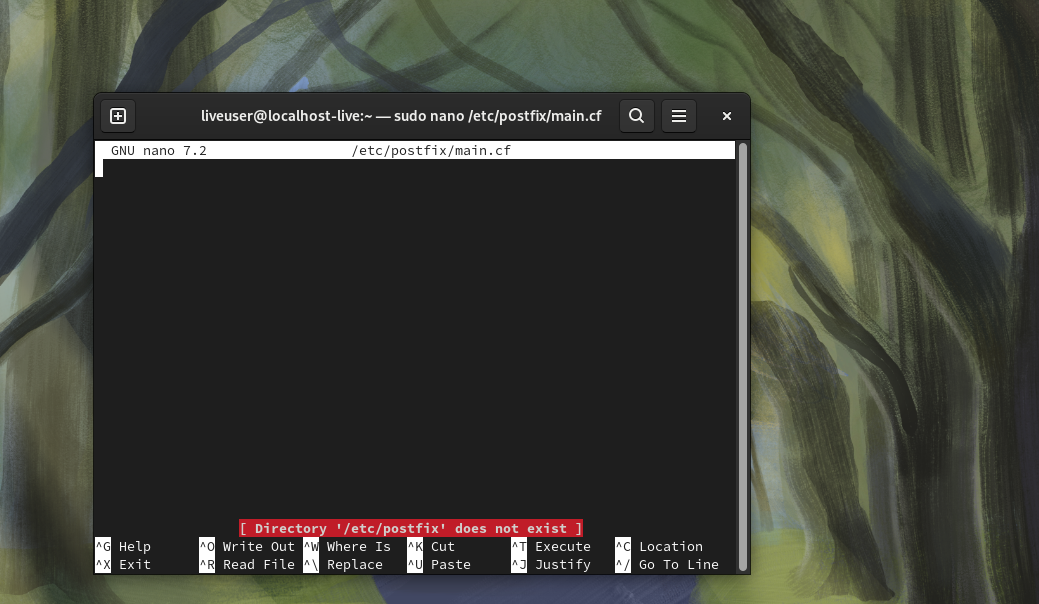
Part 4: Configuring Postfix Using Postconf Command

Task: Configure Postfix to handle virtual domains and users using the `postconf` command.

1. Set Postfix to use MySQL for virtual domains and users:

```bash

sudo postconf -e 'virtual\_mailbox\_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf'



Task: Enable SMTP authentication to secure the email submissions.

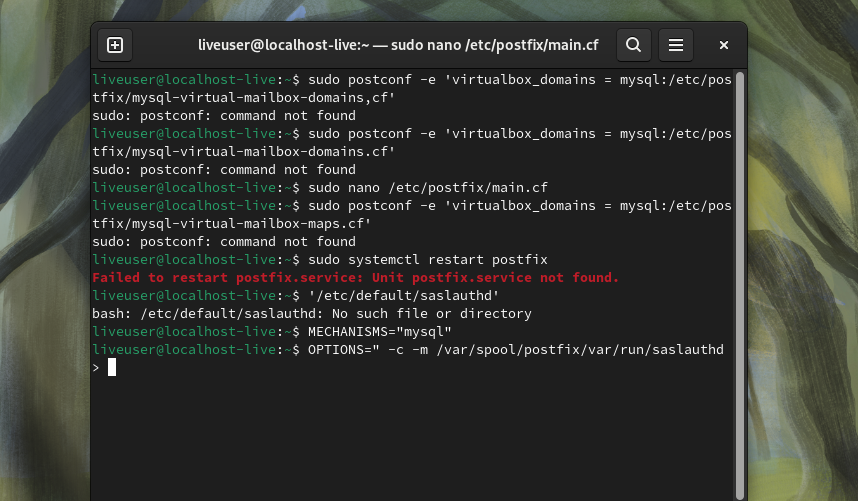
1. Configure SASL authentication by editing `/etc/default/saslauthd`:

```bash

MECHANISMS="mysql"

OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"

```



2. Create MySQL lookup for SASLAUTHD to authenticate users against the MySQL database.

3. Restart SASLAUTHD and Postfix:

```bash

sudo systemctl restart saslauthd postfix

```

Deliverables:

- SASLAUTHD configuration files and command output showing the service is running.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 6: Configuring Dovecot (POP3/IMAP)

Task: Set up Dovecot to handle email retrieval via POP3 and IMAP.

1. Configure Dovecot by editing `/etc/dovecot/dovecot.conf` and related files to:

- Use MySQL for user authentication.

- Enable both POP3 and IMAP services.

2. Configure the Dovecot MySQL connection in `/etc/dovecot/dovecot-sql.conf.ext`.

3. Restart Dovecot:

```bash

sudo systemctl restart dovecot

```

Deliverables:

- Dovecot configuration files showing POP3/IMAP setup.

- Screenshot or command output confirming Dovecot is running.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 7: Adding Domains and Virtual Users

Task: Add virtual domains and users to the MySQL database.

1. Insert domains into the MySQL table:

```sql

INSERT INTO `virtual\_domains` (name) VALUES ('example.com');

```

2. Add virtual users:

```sql

INSERT INTO `virtual\_users` (domain\_id, email, password) VALUES (1, 'user@example.com', ENCRYPT('secure\_password'));

```

Deliverables:

- SQL queries used to add virtual domains and users.

- Command output showing that the users were successfully added.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 8: Enabling SMTPS (Port 465) in Postfix for Email Submissions

Task: Enable Postfix to listen on port 465 for secure email submissions.

1. Edit the Postfix master configuration to enable SMTPS:

- Add the following to `/etc/postfix/master.cf`:

```

smtps inet n - n - - smtpd

-o syslog\_name=postfix/smtps

-o smtpd\_tls\_wrappermode=yes

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_relay\_restrictions=permit\_sasl\_authenticated,reject

```

2. Restart Postfix to apply the changes:

```bash

sudo systemctl restart postfix

```

Deliverables:

- Postfix master configuration file showing SMTPS enabled on port 465.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 9: Configuring Virus Scanning with Amavis and ClamAV

Task: Set up Amavis and ClamAV for virus scanning.

1. Edit the Amavis configuration to integrate with Postfix by modifying `/etc/amavis/conf.d/50-user`.

- Ensure that Amavis is configured to use ClamAV as the virus scanner.

2. Restart Amavis and ClamAV services:

```bash

sudo systemctl restart amavis clamav-daemon

```

3. Configure Postfix to route emails through Amavis for scanning.

Deliverables:

- Amavis configuration file showing integration with ClamAV.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 10: Testing Amavis and ClamAV

Task: Test the virus-scanning functionality of Amavis and ClamAV.

1. Send a test email with the EICAR virus test file to ensure that Amavis and ClamAV catch and quarantine it.

2. Check the logs to confirm the virus was detected and processed by Amavis and ClamAV.

Deliverables:

- Log entries showing successful virus detection and quarantine.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 11: Fighting Spam

Using Postfix Access Restrictions

Task: Implement spam control using Postfix access restrictions.

1. Configure Postfix HELO restrictions:

```bash

smtpd\_helo\_restrictions = reject\_invalid\_helo\_hostname, permit

```

2. Configure recipient restrictions:

```bash

smtpd\_recipient\_restrictions = permit\_mynetworks, reject\_unauth\_destination

```

3. Configure sender restrictions:

```bash

smtpd\_sender\_restrictions = reject\_unknown\_sender\_domain

```

4. Restart Postfix to apply the changes:

```bash

sudo systemctl restart postfix

```

Deliverables:

- Postfix configuration files showing HELO, recipient, and sender restrictions.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 12: Installing and Configuring Rspamd for Spam Protection

Task: Install and configure Rspamd to enhance spam filtering.

1. Install Rspamd:

- Ubuntu/Mint:

```bash

sudo apt install rspamd

```

- CentOS:

```bash

sudo yum install rspamd

```

2. Integrate Rspamd with Postfix by editing the `/etc/postfix/main.cf` and adding Rspamd as a milter.

3. Restart Postfix and Rspamd:

```bash

sudo systemctl restart postfix rspamd

```

Deliverables:

- Rspamd configuration and Postfix integration settings.

----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Part 13: Monitoring Postfix Logs Using Pflogsumm

Task: Use Pflogsumm to generate detailed reports from the Postfix logs.

1. Install Pflogsumm (it may already be installed with Postfix).

2. Generate a Postfix report:

```bash

sudo pflogsumm /var/log/mail.log

```

3. Review the report for any suspicious activity or mail delivery issues.

Deliverables:

- Pflogsumm report showing email statistics and issues.

