**Lab Exercise 15- Configuring SSL Encryption in PostgreSQL**

**Objective**

* Enable SSL connections to PostgreSQL
* Generate self-signed certificates
* Configure PostgreSQL to use SSL
* Test SSL-enabled connections

**Prerequisites**

* PostgreSQL installed on Windows
* OpenSSL installed and accessible from Command Prompt
* Administrator access to modify PostgreSQL configuration files

**Step 1: Generate SSL Certificates Using OpenSSL**

1. Open **Command Prompt** and run the following commands to generate server keys and certificates

openssl genrsa -out server.key 2048

openssl req -new -key server.key -out server.csr

openssl x509 -req -in server.csr -signkey server.key -out server.crt -days 365

* When prompted, enter dummy certificate information (name, org, etc.)
* This creates three files: server.key, server.csr, and server.crt

1. Move server.key and server.crt to the PostgreSQL data directory, typically at:

C:\Program Files\PostgreSQL\17\data

1. Set appropriate file permissions:
   * On Windows, ensure only the PostgreSQL service account (usually postgres) has access to server.key.

**Step 2: Modify postgresql.conf**

1. Open postgresql.conf in a text editor. It is usually located in the data directory.
2. Set or update the following parameters:

ssl = on

ssl\_cert\_file = 'server.crt'

ssl\_key\_file = 'server.key'

Save the file after editing.

**Step 3: Modify pg\_hba.conf**

1. Open pg\_hba.conf in the same directory.
2. Add or modify a line to enforce SSL for local or remote connections. Example for local user:

hostssl all all 127.0.0.1 255.255.255.255 md5

Explanation:

* hostssl enforces SSL
* all all allows all users and databases
* 127.0.0.1 restricts to local access
* md5 requires password authentication

Save and close the file.

**Step 4: Restart PostgreSQL Service**

To apply changes:

1. Open **Services** panel on Windows
2. Locate **PostgreSQL** service
3. Right-click and choose **Restart**

**Step 5: Test SSL Connection**

1. Use **psql** or a GUI client like pgAdmin.
2. To check SSL usage in psql:

SELECT ssl\_is\_used();

Expected output: true

You can also check session encryption info with:

SELECT \* FROM pg\_stat\_ssl;

**Step 6: (Optional) Force SSL for All Users**

In pg\_hba.conf, make sure all host lines are replaced with hostssl.

This ensures all remote connections must use SSL.

**Summary**

| **Task** | **Command or File** |
| --- | --- |
| Generate key and cert | openssl genrsa and openssl x509 |
| Enable SSL in config | ssl = on in postgresql.conf |
| Configure access | pg\_hba.conf with hostssl |
| Restart PostgreSQL | Windows Services or net stop and net start |
| Check SSL status | SELECT ssl\_is\_used(); |