**Lab Exercise 6- Configuring pg\_hba.conf in PostgreSQL on Windows**

**Objective**

Learn how to locate, edit, and apply access control rules in the pg\_hba.conf file to control how users connect to PostgreSQL.

**Step 1. Locate the pg\_hba.conf File**

1. Open the SQL Shell (psql).
2. Connect to your PostgreSQL instance.
3. Run this command to get the file path

SHOW hba\_file;

1. Note the file path displayed. It will look like this:

C:\Program Files\PostgreSQL\15\data\pg\_hba.conf

**Step 2. Open the File in a Text Editor**

1. Go to the path from step 1 using File Explorer.
2. Right-click on pg\_hba.conf and choose Open with, then select Notepad.

**Step 3. Understand the File Format**

Each line defines an access rule. The structure is

* Connection type
* Database name
* User name
* Address (if host)
* Authentication method

**Step 4. Add Example Access Rules**

Scroll to the bottom of the file and add these lines for practice:

1. Allow local users to connect without a password

local all all trust

1. Allow password-based connections from localhost using MD5

host all all 127.0.0.1 255.255.255.255 md5

1. Allow a specific user from a specific IP using SCRAM

host mydatabase myuser 192.168.1.100 255.255.255.255 scram-sha-256

Replace mydatabase and myuser with your actual database and user names.

**Step 5. Save and Restart PostgreSQL**

1. Save the file and close Notepad.
2. Press the Windows key and search for Services.
3. Open the Services app.
4. Find the service called something like postgresql-x64-15.
5. Right-click it and choose Restart.

**Step 6. Test the Connection**

Open SQL Shell (psql) and try connecting as a user. You should be prompted based on the rules you configured.

**Step 7. Revert Changes if Needed**

If PostgreSQL does not start after editing pg\_hba.conf, open the backup or remove problematic lines and restart the service again.

**Notes**

* Always restart the PostgreSQL service after changing pg\_hba.conf.
* Be careful with the trust method; it allows anyone to connect without a password.
* Use scram-sha-256 or md5 for secure password-based connections.