DATABASE SECURITY

What is security?

Database security is the set of strategies and practices required to protect database management systems from unauthorized access and malicious cyberattacks.

Authentication:

It is a process in DBMS of verifying the identity of the user to prevent unauthorized access to any database.

- Validating the credentials
- pg_hba.conf : has the authentication details
- trust : anybody can access
- md5 : password based authentication (hash)
- scram-sha-256 : advanced hashing
- peer : applicable for only linux systems

Encryption:

Data Encryption is a security technique that translates data into code (or ciphertext) that can be read only by people with access to a password or secret key.

- pgcrypto extension
- pgp_sym_encrypt(‘data_to_be_encrypted', 'encryption_key')
- pgp_sym_decrypt(‘data_to_be_decrypted', 'encryption_key')

Access Control:

Access control in DBMS is a critical security measure that ensures only authorized users can access or manipulate data.

Auditing:

Database auditing involves monitoring activities within a database to maintain data integrity, protect against data breaches, and comply with regulations. Auditing aims to record events for accountability, identifying errors or fraud, and troubleshooting.