EXPT-7 using kali linux

Objective:

Audit database passwords to detect weak or default passwords for MySQL/PostgreSQL.

Step 1: Set Up the Lab Environment

1. **Install MySQL (if not already installed)**:

```
sudo apt update
sudo apt install mysql-server
sudo systemctl start mysql
sudo mysql_secure_installation
```

2. **Create test database and user**:

```
mysql -u root -p
CREATE DATABASE testdb;
CREATE USER 'testuser'@'localhost' IDENTIFIED BY 'password123';
GRANT ALL PRIVILEGES ON testdb.* TO 'testuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Make sure you have a **known weak password** like password123 for demonstration.

Step 2: Identify Database Users

- **MySQL:**

```
SELECT User, Host, authentication_string FROM mysql.user;
```

- **PostgreSQL:**

```
sudo -u postgres psql
\du
```

Step 3: Database Password Auditing Using Tools

3a. Using Hydra (Brute-force MySQL Login)

1. **Check if Hydra is installed** (Kali comes with it):

```
hydra -h
```

2. **Create username and password lists**:

   users.txt

```
root
testuser
admin
```

3. **pass.txt**

```
123456
password
password123
admin
```

4. **Run Hydra on MySQL**:

```
hydra -L users.txt -P pass.txt 127.0.0.1 mysql
```

5. **Interpret Results**:
   Hydra will show accounts with weak passwords.

3b. Using Metasploit

1. **Launch Metasploit**:

```
msfconsole
```

2. **Select MySQL login scanner module**:

```
use auxiliary/scanner/mysql/mysql_login
set RHOSTS 127.0.0.1
set USERNAME testuser
set PASSWORD password123
run
```

3. **Check output**:
    - Successful login = weak password.

3c. Using Ncrack (Optional)

- Ncrack is another brute-force tool:

```
ncrack -p 3306 --user testuser --pass pass.txt 127.0.0.1
```

Step 4: Analyze Password Policy

- **MySQL password policy**:

```
SHOW VARIABLES LIKE 'validate_password%';
```

- Ensure policies:
    - Minimum length ≥ 8

- Complexity (uppercase, lowercase, digits, symbols)
- Password expiration

Step 5: Document Weak Passwords

Username	Weak Password Found	Recommendation
testuser	password123	Change immediately
root	123456	Enforce password complexity

Step 6: Remediation

- **Change weak passwords**:

```
ALTER USER 'testuser'@'localhost' IDENTIFIED BY 'NewStrong@123';
```

- **Enable password expiration**:

```
ALTER USER 'testuser'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;
```