НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Комп’ютерний практикум № 6
з дисципліни
“Основи захисту інформації”
Варіант 11

Виконав студент групи ІС-72
Кривохижа Р.А

Перевірив викладач
Ільїн К.І.

Київ-2020

Тема: механізми безпеки даних.

Мета: Набуття навичок налаштування системи безпеки MS SQL Server

Результат виконання:

1. Напишіть команди Transact SQL для наступних дій:
   1.1. Створити новий обліковий запис
   ```
   CREATE LOGIN Kryvokhyzha WITH PASSWORD='Rk1234567890'
   ```

   1.2. Назначити користувачу роль БД:
   ```
   EXECUTE sp_addsrvrolemember 'Kryvokhyzha', 'sysadmin'
   ```

   1.3. Надати користувачу Bill повноваження на доступ к збереженої процедури:
   ```
   GRANT EXECUTE ON dbo.my_procedure TO Bill
   ```

   1.4. Відкликати всі надані користувачу John привілегії:
   ```
   REVOKE ALL PRIVILEGES TO John
   ```
2. Поясніть призначення наступних команд Transact SQL:
   2.1.
   ```
   GRANT SELECT, INSERT
   ON SUPPLIES
   TO J_Smith
   WITH GRANT OPTION AS Economists
   ```

   надання користувачу J_Smith дозволів на виконання команд SELECT, INSERT до таблиці SUPPLIES зі здатністю передавати іншим користувачам будь-які привілеї, котрі даний користувач в рівні доступу Economists.

   2.2.
   ```
   EXEC[UTE] sp_addlogin ‘king_of_the_db',
   ‘a2h7d0f7dg84mdf94',
   ‘PROJECTS',
   ‘Ukrainian',
   ‘master',
   ‘NULL'
   ```

   Створює новий логін king_of_the_db, що дозволяє користувачу під'єднуватись до SQL Server, використовуючи SQL Server Authentication. Для нього визначено пароль імені входу - a2h7d0f7dg84mdf94, база даних, що використовується за замовчуванням іменем входу (база, до якої підключається користувач після фходу з цим іменем) - PROJECTS, мова за замовчуванням - українська (Ukrainian), ідентифікатор безпеки SID = master, а також останній аргумент визначає, що пароль передається як відкритий текст.

   2.3.
   ```
   REVOKE ALL TO ‘M_Ivanenko'
   CASCADE
   ```

   Видаляє дозволи, видані чи заборонені раніше.

ALL

Цей параметр не відміняє всі можливі дозволи. Вказування ALL аргументу при відклику відміняє наступні дозволи.

Якщо об'єктом, що захищається, є база даних, аргумент ALL відноситься до дозволів BACKUP DATABASE, BACKUP LOG, CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATE RULE, CREATE TABLE і CREATE VIEW.

Якщо об'єктом, що захищається, є скалярна функція, аргумент ALL відноситься до дозволів EXECUTE і REFERENCES.

Якщо об'єктом, що захищається, є функція з табличним значенням, аргумент ALL відноситься до дозволів DELETE, INSERT, REFERENCES, SELECT і UPDATE.

Якщо об'єктом, що захищається, є процедура, що зберігається, аргумент ALL має на увазі дозвіл EXECUTE.

Якщо об'єктом, що захищається, є таблиця, аргумент ALL відноситься до дозволів DELETE, INSERT, REFERENCES, SELECT і UPDATE.

Якщо об'єктом, що захищається, є представлення, аргумент ALL відноситься до дозволів DELETE, INSERT, REFERENCES, SELECT і UPDATE.

Синтаксис REVOKE ALL є застарілим. в майбутній версії Microsoft SQL Server цей компонент буде видалено, тому слід уникати його використання в нових розробках, а також запланувати зміну додатків, що вже існують, в яких він застосовується. Замість цього слід відміняти конкретні дозволи.

3. Напишіть послідовність команд, яка шифрує вміст однієї з колонок таблиці в створеній БД:
   3.1. Впевнитися, що для екземпляра SQL Server створено мастер-ключ. Мастер-ключ є вершиною ієрархії методів криптографічного захисту. Він створюється при інсталяції екземпляра сервера

```
USE master;
GO
SELECT *
FROM sys.symmetric_keys
WHERE name ='##MS_ServiceMasterKey##';
GO
```

3.2. Створити мастер-ключ бази даних my_db

```
USE some_db;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Rk0123456789';
GO
```

3.3. Створити сертифікат. Сертифікат підписується SQL Server

```
USE some_db;
GO

CREATE CERTIFICATE MyCertificate
WITH SUBJECT = 'Protect Data';
GO
```

3.4. Створення симетричного ключа

```
USE some_db;
GO
CREATE SYMMETRIC KEY SymmetricKey1
WITH ALGORITHM = AES_128
ENCRYPTION BY CERTIFICATE MyCertificate;
GO
```

3.5. Зміна схеми даних. Для зберігання зашифрованої інформації даних тип колонки має бути varbinary, тому в таблицю додається колонка такого типу з іменем Valuable_Info_Column

```
USE some_db;
GO
ALTER TABLE some_table
ADD Valuable_Info_Column varbinary(MAX) NULL
GO
```

3.6. Шифрування колонки таблиці. Для шифрування використовується команда EncryptByKey. Перед шифруванням необхідно відкрити симетричный ключ, а по закінченню закрити

```
USE some_db;
GO
OPEN SYMMETRIC KEY SymmetricKey1
```

```
DECRYPTION BY CERTIFICATE MyCertificate;
GO
UPDATE some_table
SET Valuable_Info_Column = EncryptByKey
(Key_GUID('SymmetricKey1'), Valuable_Info)
FROM dbo.some_table;
GO
CLOSE SYMMETRIC KEY SymmetricKey1;
GO
```

Відповіді на питання:

1. ***Які етапи автентифікації проходять користувачі для роботи з MS SQL Server?***

   Спочатку перевіряється, чи співставлене дане ім'я користувацькому запису, яка має дозвіл на підключення до екземпляра SQL Server. Далі ядро бази перевіряє, чи має даний обліковий запис дозвіл на доступ до тієї бази, до якої намагається він підключитися.

2. ***Як можна встановити довірче з'єднання?***

   При підключення до SQL Server необхідно використати ім'я входу Windows.

3. ***Коли варто використовувати змішаний режим аутентифікації?***

   Деякі сторонні програми підтримують лише змішану автентифікацію, а деякі мови програмування, такі як Java, не підтримують автентифікацію Windows для з'єднань SQL Server. В інших випадках архітектори програм можуть визначити, що змішана автентифікація забезпечує найшвидший і найпростіший шлях для розробки, або вам може знадобитися працювати з існуючими програмами, які використовують змішану автентифікацію, поки у вас не буде часу або персоналу переписати їх для використання автентифікації Windows.

4. ***Який термін використовується фактично при доступі об'єкта до БД? (login чи user)***

   user

5. ***Яке призначення ролі сервера і ролі БД?***

   SQL Server надає ролі на рівні сервера, щоб допомогти вам керувати дозволами на сервері. Ці ролі є основами безпеки, які групують інших принципи безпеки. Ролі сервера є загальносерверними за обсягом дозволів.

Ролі бази даних можна використовувати для призначення дозволів бази даних в групі користувачів.

6. ***Що значить параметр CASCADE?***

   Виконання зазначеної операції або запиту відносно записів або об’єктів, що пов’язані з тим, над яким виконується операція або запит.

7. ***Коли виникає конфлікт доступу?***

   Два користувачі зчитують одні й ті самі дані. Користувач 1 оновлює дані та записує ці зміни назад у базу даних, перш ніж користувач 2 зробить те саме. Тепер у вас виник конфлікт, оскільки користувач 1 прочитав дані, перш ніж користувач 2 записав їх назад до бази даних.

8. ***Яким є призначення сертифікату в системі криптографічного захисту MS SQL Server?***

   Сертифікат забезпечує безпеку шифрування та доступу до зашифрованих даних. Користувач, який намагається отримати доступ до зашифрованих даних має вказати сертифікат, який був використаний при їх шифруванні.

Висновок: під час виконанн даної лабораторної роботи я набув базові навички налаштування системи безпеки MS SQL Server, а саме: як вибирати режим автентифікації, як надавати доступ користувачам і групам Windows та іменам входу SQL Server. Також дізнався, які є права доступу до екземпляра SQL Server, як вони реалізовані та як ними керувати. І на зварешення я ознайомився із криптографічним захистом в БД. Результати виконання завдань приведені у вигляді лістингів запитів, які реалізують поставлені завдання