Национальный исследовательский ядерный университет «МИФИ» (Московский Инженерно–Физический Институт)
Кафедра №42 «Криптология и кибербезопасность»

Лабораторная работа №2-4: «Аутентификация и базовый контроль доступа»

Рекомендуемая дата защиты: 02.12.2021
Предельная дата защиты: 21.12.2021

Цель работы

Рассмотреть различные подходы к аутентификации пользователей. Рассмотреть примитивные механизмы разграничения доступа к столбцам и записям базы данных.

Теоретическая подготовка

Существует 4 различных типа аутентификации пользователей в СУБД.

1. Schema-only accounts. При создании таких пользователей используются ключевые слова NO AUTHENTICATION. Эти пользователи не могут пройти аутентификацию и, соответственно, подключиться к СУБД. Их назначение: «обладать» объектами базы данных.

2. Пользователи, идентифицируемые по разделяемому секрету. В ходе аутентификации, при помощи отображения PBKDF2 из пароля пользователя формируется разделяемый секрет, который служит для взаимной аутентификации сервера и клиента и, при необходимости, для шифрования данных. Создаются с ключевыми словами IDENTIFIED BY.

3. Пользователи, идентифицируемые внешними по отношению к СУБД службами: операционной системой, SSL, Kerberos, RADIUS. Для корректной работы требуется дополнительная настройка сервера СУБД и, в ряде случаев, клиента. Создаются с ключевыми словами IDENTIFIED EXTERNALLY.

4. Пользователи, управляемые службой каталогов (например, Microsoft Active Directory или Oracle Internet Directory). В этом случае внешняя служба отвечает не только за аутентификацию, но также за авторизацию пользователей. Требуют дополнительной настройки сервера СУБД и клиента. Создаются с ключевыми словами IDENTIFIED GLOBALLY.

Несложные задачи разграничения доступа можно решать при помощи представлений (VIEW). Представление — это сохранённый в СУБД SQL-запрос. Можно создать представления, содержащие не все столбцы и строки таблиц и предоставить пользователям привилегию SELECT ON на них, а не на саму таблицу. Таким образом, можно ограничить доступ пользователей к данным. Представление «работает» с привилегиями создавшего его пользователя, но при его реализации можно использовать переменную USER, которая разрешается в имя исполняющего запрос пользователя.

Ход работы

1. Создать schema-only пользователя, добавить один или несколько объектов в его схему данных, убедиться в их успешном создании и работоспособности. Обосновать, почему (не) планируется использовать пользователя такого типа для хранения объектов базы данных в разрабатываемой схеме;

2. Создать пользователя, проходящего аутентификацию средствами операционной системы. Важно: имя пользователя должно начинаться с OS_AUTHENT_PREFIX (по умолчанию ‘OPS$’). Если работа выполняется с учётной записи администратора, необходимо создать ещё одну учётную запись в операционной системе, так как административная учётная запись уже связана с SYSDBA;

3. (дополнительное кармическое задание) Развернуть RADIUS-сервер. Создать пользователя, который проходит аутентификацию посредством RADIUS-сервера. Важно: настройки сервера СУБД для работы с RADIUS-сервером могут конфликтовать с настройками для аутентификации средствами операционной системы. Необходимо убедиться, что возможно войти в учётную запись администратора без использования этого механизма;

4. Ограничить доступ пользователей/ролей к особо важным данным за счёт использования представлений. Убедиться в работоспособности решения;

5. Оформить отчёт.

Оформление отчёта

1. Титульный лист: название института, название лабораторной работы, имя, фамилия, номер группы, год,…
2. Лист с диаграммой отношения сущностей (полная страница);
3. Описание хода работы: процесса создания и тестирования пользователей;
4. Описание разработанных представлений, результаты тестирования их работоспособности;
5. Приложение: использованные в работе SQL-инструкции.