# Дисциплина «Защита информации»

# Лабораторная работа № 1

**Восстановление паролей в Windows XP**

# Теоретическое введение

Cистема защиты в СУБД Oracle 11g.

В системе защиты СУБД Oracle 11g реализованы практически все широко используемые элементы защиты БД:

-аутентификация пользователя, причем не только через парольную защиту, но и при необходимости через биометрию;

-несколько моделей защиты (смотри ниже);

-шифрование данных в том числе прозрачное .

- есть хранимые процедуры и триггеры;

- реализован аудит данных;

- реализация политики безопасности в Oracle может опираться на представления.

Представление – это динамически поддерживаемая сервером выборка из одной или нескольких таблиц.

С точки зрения политики безопасности система защиты СУБД Oracle является разноплановой (эклетичной), так как в ней нет четко выделенной одной политики безопасности. При этом данная система защиты может рассматриваться как сочетание двух разных политик: дискреционной и мандатной, но можно пользоваться и какой-нибудь одной из них.

При этом основной (базовой) системой защиты является дискреционная, а мандатная модель реализуется на ее основе. Кроме этого могут использоваться парольная защита, шифрование и проверка целостности.

Реализация системы защиты в СУБД MS SQL 2008 .

Система безопасности SQL Server 2008 включает в себя:

- внешняя и внутренняя аутентификация. Внешняя аутентификация рекомендуется, когда система работает с ОС UNIX/Linux, Solaris.

- дискреционная модель реализована. Есть встроенные роли. Мандатную модель можно реализовать.

- прозрачное шифрование данных позволяет шифровать информацию без внесения изменений в приложения. Содержит встроенные средства шифрования, цифровой подписи и верификации данных с помощью симметричных ключей (алгоритмы шифрования RC4, RC2, DES, AES) и асимметричных ключей (алгоритм RSA). Весь трафик между клиентом и сервером по умолчанию шифруется с применением протоколов IP Security (IP SEC) и Secure Sockets Layer (SSL), причем подобная функциональность доступна во всех редакциях продукта. Шифрование на уровне колонок, кода хранимых процедур и данных в службах отчетов;

- есть хранимые процедуры и триггеры;

- SQL Server 2008 поддерживает несколько способов поддержки аудита. Он может использовать Windows Security EventLog (механизм отслеживания обращений к объектам, использования прав, попыток аутентификации), SQL Profiler (средство осуществления детального аудита попыток доступа к объектам БД), триггеры, связанные с изменением метаданных. Создание подобных триггеров может позволить как отслеживать попытки изменения метаданных пользователями, так и полностью их запретить.

- управление на основе политик позволяет обеспечить выполнение политик безопасности для служб данных по всему предприятию.

**Система защиты DB2.**

Система безопасности DB2 включает в себя:

- Аутентификация и авторизация - DB2 использует внешний метод - аутентификацию внешними средствами, (операционной системой). В связи с этим, пользователь не является объектом базы данных, в базе данных сохраняется информация не о пользователе, а только о данных ему грантах - разрешениях использования привилегий. Поэтому в DB2 возможна даже такая "странная" ситуация: пользователь создан в базе данных и ему назначены некоторые привилегии, но работать с базой данных он не может, так как, не будучи зарегистрирован в системе, не может пройти аутентификацию.

- в DB2 применяются группы пользователей для ролевой модели безопасности. В DB2 разрешения пользователю выполнять те или иные действия делятся на полномочия и привилегии. Полномочие является методом группирования привилегий и возможности управлять менеджером базы данных и системными утилитами.

- можно реализовать дискреционную модель безопасности.

**-** шифрование в DB2 доступно только для резервных копий данных

**-** Есть хранимые процедуры и триггеры;

- реализован аудит данных.

- реализация политики безопасности в DB2 может опираться на представления.

## Сравнительный анализ систем защиты СУБД Oracle 11g, MS SQL Server 2008, DB2

|  |  |  |  |
| --- | --- | --- | --- |
| * Механизмы безопасности | * SQL Server 2008 | * Oracle 11g | * DB2 |
| * Внешняя аутентификация (с помощью Windows) | * + | * + | * + |
| * Внутренняя аутентификация | * + | * + | * - |
| * Прозрачное шифрование данных | * + | * + | * - |
| * Шифрование колонок | * + | * + | * - |
| * Механизмы безопасности | * SQL Server 2008 | * Oracle 11g | * DB2 |
| * Наличие хранимых процедур | * + | * + | * + |
| * Наличие триггеров | * + | * + | * + |
| * Наличие аудита | * + | * + | * + |
| * Наличие политика безопасности | * + | * + | * + |
| * Дескрипционная модель безопасности | * + | * + | * + |
| * Мандатная модель безопасности | * Может быть реализована | * + | * Может быть реализована |
| * Ролевая модель безопасности (встроенные роли) | * + | * + | * + |
| * Наличие бесплатных версий | * + | * - | * + |

Перечисленные механизмы безопасности и удобные средства их администрирования доступны во всех редакциях SQL Server 2008, включая бесплатную редакцию Express Edition и относительно недорогие версии Workgroup Edition и Standard Edition, вполне доступные небольшим предприятиям. В то же время аналогичные механизмы и утилиты Oracle 11g присутствуют только в наиболее дорогостоящей редакции этой СУБД или в виде дополнительных платных модулей.

SQL Server является лидером в безопасности платформ данных и более безопасен, чем DB2. С 2004 года в SQL Server 2008 была найдена только одна уязвимость, в то время как в DB2 — 61, а в Oracle - 250.  Будучи только что установленным, SQL Server 2008 более надежно защищен, чем IBM DB2. Без дополнительных затрат он обеспечивает защитную функциональность, которая в DB2 и Oracle либо недоступна, либо продается за отдельную немалую плату.

# Практические задания

1. Запустить MySQL ( см. практику по курсу СУБД). - можно в консоли, можно в графич. оболочке.

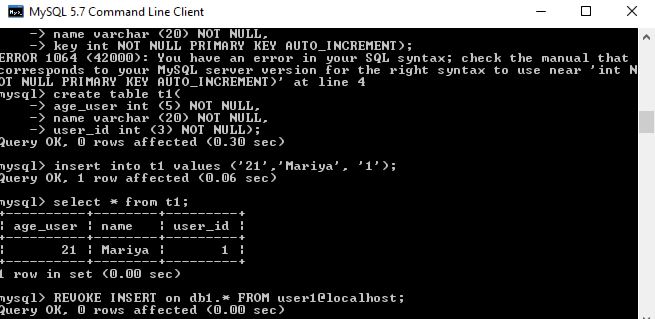
2. Создать трех пользователей., каждому пользователю приписать ( создать по 1 БД/таблице),

которая (БД) - непустая (как минимум одна запись )

3. Каждый пользователь имеет доступ к СВОЕЙ БД, и НЕ ИМЕЕТ к чужой БД.

4. Продемонстрировать знание GRANT, REVOKE. Вспомнить SELECT, SHOW DATABASES , USER и т.п.

### Пример выполнения практической части



Пример использования команды Revoke

# Контрольные вопросы

1. Какие алгоритмы шифрования используются в MySQL?

2. Прокомментировать таблицу сравнительных мер защиты в основных коммерческих

СУБД ( Oracle, MS SQL , DB2). Какие СУБД являются сейчас актуальными?

3. СУБД Oracle по Грушо и ее меры защиты и найденные уязвимости.

**Литература.**

1. Скляров. Хакерские фишки.

2. Xaker.ru

3. Алферов, Зубов, Кузьмин, Черемушкин. Основы криптографии.2-е изд.М.Гелиос.2002 г.

4. Википедия.

5. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации