**Рекомендации по повышению уровня безопасности базы данных MySQL**

В современном информационном обществе объемы персональных данных, хранящихся в электронном виде на многочисленных устройствах и в базах данных, достигли колоссальных масштабов. Проблема утечки этой конфиденциальной информации стала одной из основных в сфере информационной безопасности. Часто мы не осознаем риска того, что злоумышленники могут успешно добыть доступ к нашим личным данным. Мы можем даже не подозревать, что наша личная информация подверглась утечке.

В связи с этим я хочу представить вам метод защиты от несанкционированного доступа к вашей базе данных. В данном материале вы узнаете, как злоумышленники могут получить доступ к вашим данным и какие шаги можно предпринять для предотвращения утечки информации, включая своевременное обновление версии MySQL.

Для более комфортного восприятия информации предлагается прочитать словарь терминов.

Брутфорс — это метод взлома, при котором хакер или тестировщик подбирают данные для входа в систему.

Уязвимость - Ослабленное место в системе, которое может быть использовано злоумышленниками для атак или несанкционированного доступа.

Кибербезопасность - Область защиты компьютерных систем, сетей и данных от киберугроз, включая несанкционированный доступ, утечку данных и атаки вредоносного программного обеспечения.

Угрозы - Потенциальные опасности для информационной безопасности, такие как вирусы, хакерские атаки и фишинг.

Версионность - Управление версиями программного обеспечения или компонентов для

Аутентификация - Процесс проверки личности или подлинности пользователя, обычно с помощью пароля, биометрических данных или других методов.

Целостность данных - Гарантирование, что данные остаются нетронутыми и неизменными в процессе их передачи или хранения.

Конфиденциальность данных - Защита данных от несанкционированного доступа или разглашения.

Злоумышленники - Лица, действующие противозаконно или вредоносно, в том числе в области компьютерной безопасности.

Несанкционированный доступ - Получение доступа к данным или системам без соответствующих разрешений или авторизации.

Информационная безопасность - Защита информации от угроз, обеспечение конфиденциальности, целостности и доступности данных.

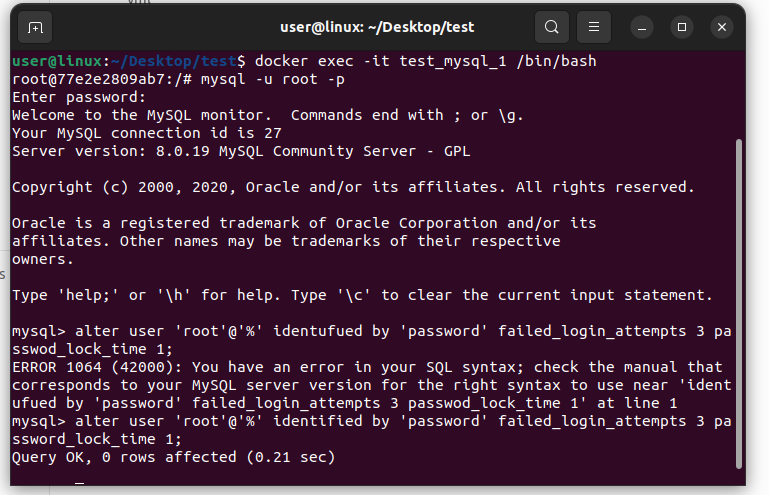
На практике уязвимости базы данных часто используются злоумышленниками для несанкционированного доступа, изменения или удаления данных. Поэтому осознание и активное устранение уязвимостей в базе данных MySQL является критически важным аспектом общей стратегии информационной безопасности.

Разработчики активно работают над обнаружением и устранением уязвимостей в новых версиях, что позволяет повысить общий уровень безопасности базы данных. Это означает, что многие известные уязвимости и уязвимые места, обнаруженные в предыдущих версиях, могут быть исправлены в более новых выпусках.

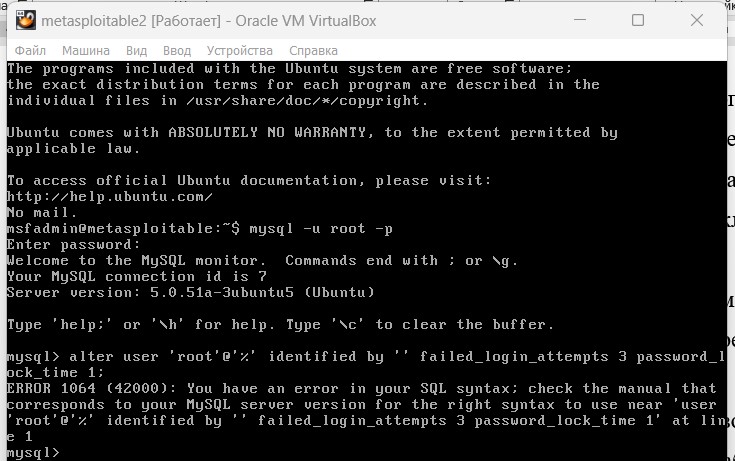
Давайте более подробно разберем классический пример атаки на базу данных. Брутфорс — попытка угадать или подобрать пароль. Во время атаки человек или программа за короткое время вводят в систему множество комбинаций паролей на случай, если одна из них окажется верной. Атака может быть инициирована удалённо. Это делает систему уязвимой перед возможными атаками. Она обладает высокой степенью опасности, так как позволяет злоумышленникам легко проникнуть в систему.

В специальной программе была произведена атака брутфорс на версии MySQL 8.0.19 и 5.0.51а. В результате перебора в обоих версиях стал известен пароль пользователя, а значит злоумышленник получил возможность подключиться к базе данных, что могло привести к утечке конфиденциальных данных, нарушению целостности информации, а также к отказу в обслуживании.

Для предотвращения данного сценария мы можем войти в базу данных от имени пользователя и установить ограничения на количество попыток ввода пароля. После определенного количества неудачных попыток входа пользовательская учетная запись будет временно заблокирована на указанный пользователем период.



*Рисунок 1 – Настройка ограничений попыток ввода пароля на версии 8.0.19*



*Рисунок 2 - Настройка ограничений попыток ввода пароля на версии 5.0.51а*

Как мы видим, данная функция поддерживается на более новой версии MySQL, но не поддерживается на версии 5.0.51а.

После проведения атаки с новыми настройками злоумышленнику не удается получить пароль от нашей базы данных версии 8.0.19. Ведь начиная с этой версии администраторы могут настраивать учетные записи пользователей таким образом, чтобы некорректные попытки входа в систему приводили к временной блокировке учетной записи. В данном контексте "некорректная попытка входа" означает, что клиент не смог предоставить правильный пароль при попытке подключения.

Для того, чтобы правильно провести настройку ограничения попыток ввода пароля необходимо войти в базу данных от имени пользователя, для которого мы хотим применить настройку. Необходимые ограничения мы будем настраивать с помощью опций FAILED\_LOGIN\_ATTEMPTS и PASSWORD\_LOCK\_TIME.

FAILED\_LOGIN\_ATTEMPTS определяет количество ошибочных попыток входа, после которых учетная запись будет заблокирована, а PASSWORD\_LOCK\_TIME указывает продолжительность блокировки учетной записи в случае превышения числа неудачных попыток входа.

Предоставленная команда ALTER USER используется для изменения параметров учетной записи пользователя в MySQL.

'root'@'%' - указывает на имя пользователя и хост, для которых требуется изменить параметры. Здесь 'root' обозначает имя пользователя, а '%' указывает, что это применимо ко всем удаленным хостам.

identified by 'password' - этот параметр задает новый пароль для пользователя 'root'@'%'. В данном случае 'password' должно быть заменено на фактический пароль, который вы хотели бы использовать для этой учетной записи.

failed\_login\_attempts - параметр , который определяет количество попыток неудачного входа пользователя, прежде чем его учетная запись будет блокирована.

password\_lock\_time - указывает на какое время будет заблокирована учетная запись пользователя после достижения предельного количества неудачных попыток входа, в данном случае 1 день.

Таким образом, эта команда позволяет изменить пароль для пользователя и также настроить параметры блокировки учетной записи после определенного числа неудачных попыток входа.

Разработанные рекомендации представляют собой эффективную меру по повышению безопасности информационной системы. Анализ показывает, что установка ограничения на количество неудачных попыток ввода пароля помогает предотвратить брутфорс-атаки и другие формы злоупотребления, направленные на получение несанкционированного доступа к базе данных.

Данные рекомендации, направленные на повышение уровня защиты базы данных от несанкционированного доступа являются актуальными и целесообразными в контексте обеспечения информационной безопасности. Внедрение данной меры позволяет замедлить или полностью заблокировать попытки несанкционированного доступа, обеспечивая дополнительный уровень защиты.