АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ СУБД ORACLE

Клепцов М.Я.[1], Любимова Л.В.[2], Миронов М.М.[3]

В статье рассмотрены основные виды внешних и внутренних атак на систему управления базами данных (далее – СУБД) Oracle. Проанализированы возможные последствия данных атак, и проведена оценка подверженности СУБД Oracle различным уязвимостям и угрозам. Среди внешних атак выделены атаки на лисенер, атаки через приложения и подключение к СУБД напрямую. Среди внешних атак рассмотрены PL/SQL–инъекции, SQL–инъекции, обход защиты процедуры DBMS_ASSERT, переполнение буфе, а также некорректная работа объединений и представлений. В статье описаны основные требования по информационной безопасности СУБД и основные задачи администратора. На основе проведенного анализа сделан вывод о необходимости использования дополнительных мер обеспечения безопасности. Авторы рекомендуют использовать технологию проведения оперативного аудита, которая является небольшим вспомогательным ключом для получения данных о текущем состоянии системы. Эта технология дает возможность защитить базу данных от несанкционированных действий, отследить определенные действия, проанализировать доступ к данным В статье рассмотрены преимущества и недостатки использования технологии аудита. Данная технология является важной частью комплексного подхода к организации системы защиты информации на предприятии.

***Ключевые слова**: БД, внешние атаки, внутренние атаки, системный идентификатор, аутентификация, лисенер, PL/SQL–инъекции, SQL–инъекции, аудит.*

DOI: 10.21681/2311-3456-2018-2-16-23

Введение. Для того чтобы управлять большим количеством данных, любая современная организация всегда имеет в арсенале своей компьютерной системы сервер с системой управления базами данных. К настоящему времени на рынке существует множество различных СУБД, каждая из которых имеет свои плюсы и минусы, поэтому, когда компания сталкивается с выбором той или иной системы, необходимо понимать весь ее функционал, а также угрозы и уязвимости, которые могут навредить правильной работе [1]. Для того чтобы СУБД была наиболее защищенной и обеспечивала гарантию того, что конфиденциальная информация не может быть получена третьей стороной, необходимо понимать ее уязвимости и постараться минимизировать или ликвидировать их.

Попытки проникновения в СУБД Oracle могут быть внешними и внутренними [2]. Всё зависит от степени осведомленности злоумышленника. Если у злоумышленника нет никаких данных о СУБД, то ему будет необходимо прибегнуть к внешним атакам, а именно к атакам, позволяющим получить необходимые параметры (IP-адрес, порт службы Oracle Net Listener, системный идентификатор (SID) или имя сервиса, имя пользователя, пароль) для подключения к СУБД. Помимо этого, заинтересованная в получении конфиденциальной информации сторона, уже может иметь доступ к системе и запрашивать необходимые сведения (например, сотрудник часто запрашивает данные о состоянии счетов клиентов). В связи с этим, администраторы и разработчики баз данных (далее – БД) должны предусмотреть все возможные меры, которые оперативно помогут вычислить попытки компрометации информации изнутри, то есть уметь быстро выявлять внутренние атаки на СУБД.

I Внешние атаки на СУБД. Начнем рассмотрение защищенности СУБД Oracle снаружи. На рисунке 1 изображены основные виды возможных внешних атак.

Если у злоумышленника полностью отсутствует информация о системе, то первое на что он обратит внимание – открытые порты сервера, на котором функционирует СУБД. Подключение к СУБД Oracle происходит от удаленного пользователя по сетевой инфраструктуре через Oracle Net Listener (далее лисенер). Со стороны клиента, находится файл, в котором задается путь к расположению базы данных (хост и протокол). Пользователь должен прописать путь к базе данных (далее – БД). Когда пользователь пытается подключиться к БД, то, прежде всего, запрос отправляется в сетевую

1 Клепцов Михаил Яковлевич, доктор технических наук, профессор, профессор Российского университета транспорта (МИИТ), г. Москва, Россия. E-mail: mkleptsov@mail.ru

2 Любимова Лариса Владимировна, ведущий инженер Акционерного общества «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС») г. Москва, Россия. E-mail: lv.lyubimova@gmail.com

3 Миронов Михаил Михайлович, студент Российского университета транспорта (МИИТ), г. Москва, Россия. E-mail: mikhailmironoff@yandex.ru

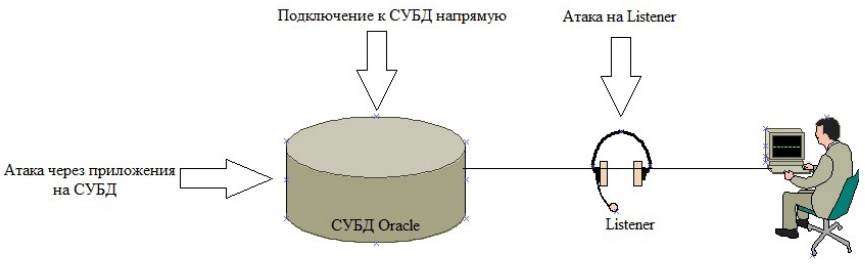

***Рис.1**. Основные виды внешних атак*

систему Oracle Net Listener. По умолчанию порт подключений к лисенеру – 1521. Лисенер – самостоятельное программное обеспечение Oracle на сервере БД, он принимает входящие запросы на определенный порт. Когда запрос получен, лисенер узнает какой экземпляр БД выбран в качестве цели и устанавливает соединение.

Также необходимо отметить файл, который является добавочным конфигурационным файлом. В него добавляются дополнительные параметры для Oracle Net. На сервере данный файл существует для воздействия на процесс работы лисенера, а на клиентской стороне – для влияния на настройки лисенера.

Для администрирования лисенером используется консольная утилита (lsnrctl). Управление может происходить локально или удаленно

Когда подключение установлено и создана сессия, лисенер разрешает соединение между БД и клиентом (рис.2). Каждая сессия клиента имеет собственный серверный процесс на стороне сервера.

После проверки пакетов на подключение к СУБД, лисенер создает новый процесс, который будет взаимодействовать с подключением. Данный процесс называется серверным процессом. Лисенер подключается к процессу и передает сведения, включающие адрес пользователя. Далее функции лисенера завершаются, и вся основная работа передается непосредственно серверному процессу (рис.3). Серверный процесс проверяет пользовательские полномочия через аутентификацию [3]. В случае прохождения проверки, создается сессия пользователя. Затем серверный процесс начинает вести себя как агент пользователя на сервере. Он нужен для:

- разбора и выполнения SQL запросов;
- проверки буферного кэша на требуемые в запросе данные;
- чтения и переноса необходимых блоков данных из файлов диска в буферный кэш, если они еще не находятся в системной глобальной памяти (SGA);
- управления сортировкой. Область сортировки – это место памяти, которое используется для работы с сортировкой. Она содержится в части памяти, связанной с программной глобальной областью (PGA).

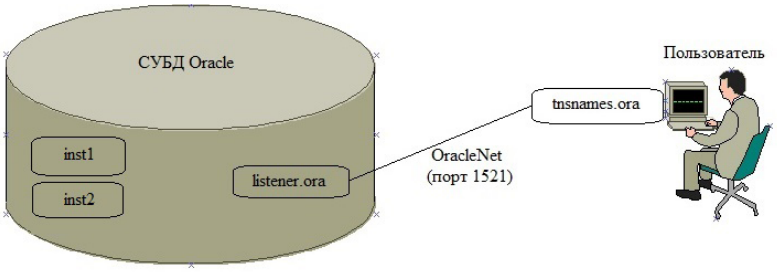

***Рис.2.** Соединение между БД и клиентом*

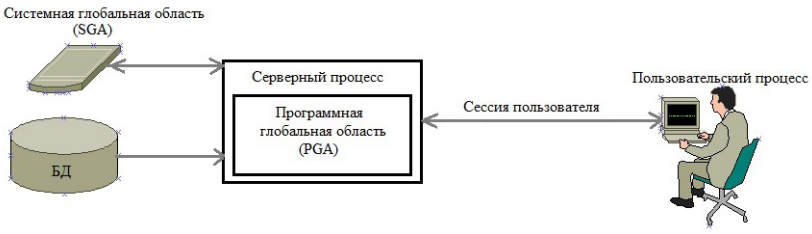

***Рис.3**. Порождение серверного процесса*

Выделяют два вида атак на лисенер:

- атаки на незащищенную службу лисенера;
- атаки на защищенную службу лисенера [4].

Для первого вида атак на лисенер возможно наступление следующих опасных событий:

- получение подробных сведений о системе;
- отказ в обслуживании (DoS, DDoS-атаки);
- выполнение запросов;
- удаленное управление.

Рассмотрим основные опасные команды, использующиеся в консольной утилите администрирования (lsnrctl) и способствующие вышеуказанным возможностям злоумышленника при атаках на незащищенный лисенер.

Чтобы получить подробные сведения о системе, необходимо использовать команду «status». Благодаря этому, злоумышленник будет обладать необходимыми сведениями о версии СУБД, системном идентификаторе БД (SID), пути к log-файлу, операционной системе (далее ОС), на которой установлена СУБД, переменной окружения ORACLE_HOME, приложениях, установленных на сервере.

Другая опасная атака на незащищенную службу лисенера – отказ в обслуживании. Она может быть осуществлена при применении различных команд. Злоумышленник сможет остановить лисенер, тем самым повлияв на работу приложений СУБД. Это можно выполнить командой «stop». А после этого установить пароль на доступ к лисенеру. Таким образом, когда администратор заметит, что лисенер остановился, то у него не получится включить его удаленно, так как потребуется изменять конфигурационный файл на сервере. DDoS-атаки также могут быть проведены через команду «set trc_level», означающую настройку уровня трассировки. В случае установки максимального значения этого уровня, в то время как у сервера слабый процессор, или же на нем происходит большое количество обработки запросов, сервер будет сильно перегружен.

Команда «set log_file» позволяет произвести смену директории и названия файлов, в которых содержатся логи лисенера. Благодаря данной команде возможно создать нового пользователя. Каждый раз при запуске на сервере утилиты sqlplus, которая применяется для подключения к локальной или удаленной СУБД, автоматически происходит чтение файла glogin.sql. Алгоритм по добавлению нового пользователя, с помощью команды «set log_file»:

-указание нового значения переменной, ссылающейся на файл журнала регистрации событий [5];

-запись определенных команд в glogin.sql, которые будут ошибочными для выполнения и зафиксируются в лог файле, но одновременно будет состоять из команд, которые нам необходимы.

Перейдем к рассмотрению второго типа атак на лисенер: атаки на защищенную службу лисенера. При этих атаках возможно:

- перехватить пароль;
- аутентифицироваться с помощью хэша;
- расшифровать пароль, установленный на лисенер [6];
- перебрать пароли.

Что касается перехвата пароля, то он подразумевает уязвимость передающегося в открытом виде пароля, с помощью использующейся команды «set password». В данном случае, у всех пользователей, располагающихся в этой же подсети с сервером СУБД и прослушивающих сетевой трафик, появляется возможность заполучить пароль к лисенеру.

Для того чтобы установить пароль, утилита lsnrctl предлагает два способа: первый заключается во вводе одной командной строки, а второй способ подразумевает использование команды «set password», не используя аргументы, при этом пароль запрашивается в интерактивном режиме.

Таким образом, lsnrctl создает хэш пароля, и в дальнейшем отправляет новый хэш по сети. У способа с вводом командной строки, есть возможность получения пароля в открытом виде. У второго – нет.

Когда злоумышленник заполучил хэш пароля, то он будет пытаться аутентифицироваться с помощью особенностей протокола. Необходимо будет воспользоваться первым способом перехвата пароля, а именно вводом командной строки, но при условии замены пароля на хэш.

Если же возможности аутентификации при помощи хэша – нет, то придется надеяться, что для лисенера установлен слабый пароль. При поиске пароля можно задействовать различные существующие программы по перебору паролей СУБД Oracle. Отличием при расшифровке является тот факт, что используется не имя пользователя, а перманентное значение «arbitrary». Создадим пароль и увидим новый хэш. В завершении, будет добавлен хэш на новый пароль в файл listener.ora. Для расшифровки пароля используется утилита Cain&Arbel.

Для осуществления перебора паролей, необходимо посмотреть стандарты на пароли лисенера, располагающиеся в примере файле listener.ora. Довольно часто, администраторы БД создают пароли на основе стандартов.

Продолжим рассматривать внешние атаки на СУБД Oracle и перейдем к случаям, когда злоумышленник не обнаружил уязвимости лисенера. Тогда вторым этапом будет непосредственное подключение к СУБД напрямую. Для этого необходимо обладать информацией о следующих параметрах:

- IP-адрес сервера;
- порт лисенера;
- системный идентификатор (SID) или имя сервиса;
- имя пользователя;
- пароль.

Два первых параметра получить достаточно просто. Заострим внимание на системном идентификаторе и имени сервиса. Существует три подхода к получению злоумышленником системного идентификатора:

- проверка стандартного значения системного идентификатора;
- перебор системного идентификатора по словарю;
-метод полного перебора (Brute force).

Довольно часто системный идентификатор не подвергается изменениям со стороны администратора БД, то есть при установке СУБД по умолчанию предложено значение, которое и применяется. Это и будет являться методом проверки стандартного значение SID.

Помимо этого, можно прибегнуть к перебору системного идентификатора по словарю с помощью различных утилит (sidguess, oscanner, ora-getsid, ora-brutsid, sidguesser и другие).

Если предыдущие методы не дали нужного результата (получения SID), то на помощь приходит третий метод – метод полного перебора (Brute force). К основным минусам данного подхода можно, во-первых, отнести время, которое будет потрачено, во-вторых, системы обнаружения могут запросто его обнаружить. Когда системный идентификатор состоит не более чем из 5 символов, перебор займет примерно 3 суток.

Чаще всего СУБД Oracle работает вместе с дополнительными продуктами данной компании или же сторонних производителей. Иногда данное взаимодействие позволяет получить системный идентификатор или имя сервиса БД. Рассмотрим один из таких способов получения SID. При установке СУБД автоматически устанавливается приложение Oracle Enterprise Manager, позволяющее производить управление и необходимую конфигурацию. При подключении к нему можно увидеть имя сервиса БД вместе с окном, запрашивающим логин и пароль. Стоит отметить, что работать с данным приложением можно и удаленно.

После получения системного идентификатора следующим шагом злоумышленника является преодоление парольной защиты. Способы получения пароля делятся на три основные вида:

- присутствие в СУБД учетных записей, созданных производителем;
- подбор пароля;
- вычисление пароля из файлов, сетевого трафика и приложений.

Одна из самых распространённых уязвимостей СУБД, как и иных приложений – существование учетных записей, созданных производителем. Поэтому, естественно, первым путем злоумышленника будет перебор стандартных логинов и паролей. В интернете можно найти сведения о подобных учетных записях. При установке СУБД существуют учетные записи, на которые изначально устанавливаются стандартные пароли, которые позже могут быть изменены администратором (например, SYS и SYSTEM). С помощью утилиты oscanner можно проверить, есть ли в текущей СУБД стандартные учетные записи.

Следующим шагом после отрицательного действия по поиску стандартных учетных записей является подбор аутентификационных данных. Относительно часто данный способ оказывается успешным по следующим причинам:

- стандартные логины известны, следовательно, остается только подобрать пароль к ним;
- сложность и длина пароля не ограничиваются;
- перебор паролей не приводит к блокировке.

Третий способ получения пароля подойдет при условии, что злоумышленник обладает некоторыми сведениями или правами в ИС. Зачастую в ИС компания имеет не одну СУБД, а несколько различных. Если злоумышленнику удалось получить доступ к одной СУБД, то у него увеличиваются возможности по получению доступа к другим. Для этого ему потребуется использовать программу Oscanner. Допустим, злоумышленник получил доступ к одному серверу Oracle. Тогда, просканировав известный сервер программой Oscanner, в выходных данных будет получена информация о ссылках на БД, где будет указан системный идентификатор, пользователь и, иногда, аутентификационные данные.

Третий вид внешних атак на СУБД Oracle – атаки через приложения, находящиеся на сервере вместе с СУБД. Нередко, даже если СУБД защищена на должном уровне, обнаруживаются уязвимости со стороны самих приложений, интегрированных с СУБД. Рассмотрим одно из основных приложений,

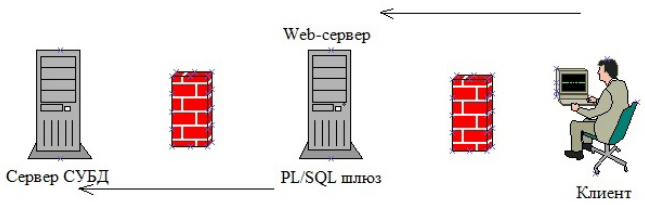

***Рис.4**. Взаимодействие клиента с БД через PL/SQL шлюз сервера приложений*

которое занимает вторую ступень после СУБД по количеству уязвимостей, которые могут помочь злоумышленнику.

Сервер приложений (Oracle Application Server) связывает непосредственно БД и Web-приложения. В нем задействованы различные технологии, помогающие реализовывать взаимодействие БД и клиента. Относительно подключения к СУБД, прежде всего, нам интересен язык PL/SQL (процедурное расширение языка SQL, позволяет отправлять блок операторов в БД, что существенно уменьшает трафик между приложениями и БД). Реализация PL/SQL-процедур осуществляется благодаря PL/SQL-шлюзу: клиент выполняет подключение к web-приложению, совершает определенные действия, которые приводят к выполнению запроса к БД, затем запрос отправляется на PL/SQL-шлюз, а в конце данный шлюз передает запрос в СУБД (рис.4) [4]. Назад к пользователю, результат направляется по той же схеме.

Атаки через приложения на СУБД могут приводить к управлению системой без наличия пароля администратора.

II Внутренние атаки на СУБД. Рассмотрим и проследим влияние уязвимых мест СУБД Oracle, учитывая тот факт, что злоумышленник уже получил непосредственный доступ к СУБД, независимо от его привилегий. Рассматриваемые уязвимости, в основном, применяются локально, поэтому администраторы и разработчики довольно часто не уделяют им должного внимания. К основным видам внутренних атак, прежде всего, относятся (рис.5):

- PL/SQL-инъекции;
- SQL-инъекции [7];
- обход защиты процедуры DBMS_ASSERT;
- переполнение буфера;
- некорректная работа объединений и представлений.

Под PL/SQL инъекциями понимается изменение алгоритма работы PL/SQL-процедуры, благодаря прописыванию различных команд во входные параметры. Инъекция данного типа будет реализована только в том случае, если перед внедрением отсутствует проверка входных параметров. Обычно, в СУБД Oracle присутствует большое количество пакетов и процедур, следовательно, существует большой риск, при котором злоумышленник найдет уязвимую процедуру.

Следующая внутренняя атака - SQL-инъекция. Она применяется против приложений, которые формируют SQL-запросы, на основе вводимых пользователем данных. При данном типе атаки цель злоумышленника заключается в реализации непредусмотренного логикой приложения запроса. SQL-инъекции делятся на два вида:

- атаки первого рода;
- атаки второго рода [8,9].

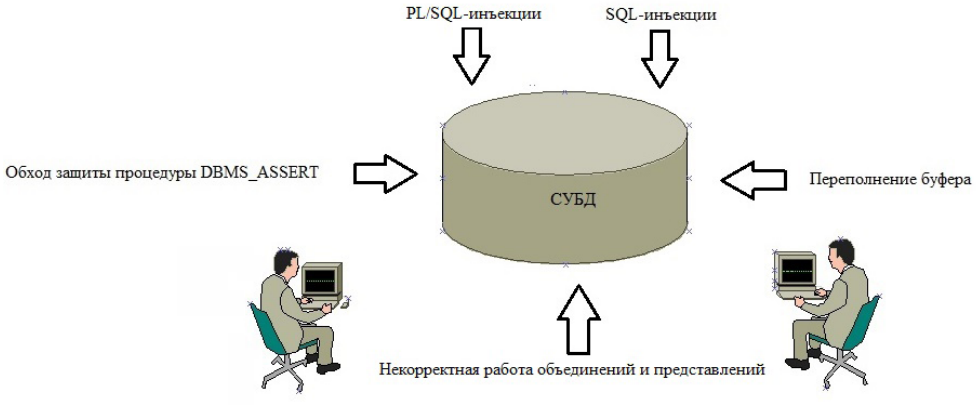

***Рис.5**. Основные виды внутренних атак*

Атаки первого рода подразумевают, что злоумышленник вводит некорректное значение одного из параметров, тем самым изменяет структуру предполагаемого SQL-запроса, который немедленно выполняется.

Атаки второго рода заключается в том, что злоумышленник изменяет данные на устройстве хранения (например, строку таблицы), а сама атака выполняется уже другим процессом.

Процедура DBMS_ASSERT проверяет входные параметры. Сама по себе, процедура является отличным помощником, но у нее тоже есть уязвимости, используя которые злоумышленник получит доступ к таблицам, хранящимся в схеме SCOTT.

Следующая опасная уязвимость – переполнение буфера. Основной риск при этой атаке заключается в том, что при переполнении буфера злоумышленник может получить права администратора, но не просто СУБД, а целого сервера.

К следующей атаке относится некорректная работа объединений и представлений [10]. Объединение (join) помогает объединить столбцы разных таблиц. Существует три типа:

- внутреннее объединение (inner join): получение записей, в которых есть соответствие первой и второй таблиц;

-внешнее объединение (outer join), состоящее из левого (выборка всех записей из первой таблицы и сопоставления со второй), правого (выборка всех записей из второй таблицы и сопоставления с первой) и внутреннего (выборка всех записей из двух таблиц) внешних объединений;

- декартово произведение (cross join).

Некорректная работа объединений заключается в том, что пользователь, обладающий минимальными правами, может получить хэши паролей других пользователей СУБД. Благодаря данному соединению даже из схемы простого пользователя мы увидим сведения о хэшах паролей.

Еще к одному известному типу такой атаки относится некорректная работа представления. Представление (view) – определенный запрос к БД, отражающий текущие данные из таблицы. Иногда называется виртуальной таблицей. С помощью данной атаки можно изменить пароль любой схеме.

Рассмотрев основные виды внешних и внутренних атак на СУБД Oracle, а также проанализировав возможные последствия этих атак, можно сделать вывод, что СУБД Oracle, как и другие СУБД, подвержена различным уязвимостям и угрозам. Конечно, корпорация Oracle регулярно запускает обновления, которые ликвидирует множество атак, они становятся неактуальными и уже не предоставляют той опасности, которую создавали раньше. Однако наиболее известной из перечисленных атак, по-прежнему, остается SQL-инъекция.

III Технология аудита в СУБД. Для того чтобы сократить количество атак при построении защищенной системы, следует применять комплексный подход, а для этого необходимо четко понимать архитектуру СУБД, знать весь ее встроенный функционал и не пренебрегать аудитом [11]. Одной из основных задач администратора БД Oracle является обеспечение безопасности системы, потому что конфиденциальные данные не должны быть изменены, повреждены или получены третьей стороной [12,13].

Ограничение прав и контроль действий пользователей в СУБД считаются первым шагом по обеспечению безопасной. После установки СУБД необходимо разграничить доступ к данным. У разных пользователей свои задачи, а, следовательно, каждому необходимы различные сведения из БД. Имя пользователя (имя схемы) помогает проверить ресурс (пользователя, программу, другой компьютер), пытающийся подключиться к БД [14].

Парольная защита – следующий шаг, позволяющий защитить данные в системе. Аутентификация пользователей позволяет идентифицировать их. Необходимо не забывать об основных правилах при создании (изменении) пароля:

- не задавать идентичный имени пользователя пароль;

- использовать в пароле различные символы;

- в течение определенного компанией периода менять пароль;

- не создавать новый пароль идентичный старому.

После того, как пользователь создан, следует определить, какие действия и с какими объектами БД ему будут позволены, то есть предоставить привилегии (раздать гранты) [15]. Администратор определяет, что пользователь может делать с помощью привилегий. СУБД Oracle имеет два типа привилегий:

- системные;

- объектные.

Системные привилегии – первые привилегии, которые понадобятся пользователю. Перед тем как пользователь попробует что-нибудь сделать с БД, ему понадобится подключиться к БД. Привилегия CREATE SESSION дает пользователю право на подключение к БД. Без этой привилегии – остальные не имеют значения. К системным привилегиям также относятся: CREATE TABLE; CREATE VIEW; CREATE SEQUENCE; CREATE PROCEDURE; ALTER TABLE; GRANT ANY OBJECT; и другие.

Объектные привилегии контролируют доступ к данным и их изменения. У администратора есть возможность предоставить 8 объектных привилегий: SELECT; INSERT; UPDATE; DELETE; REFERENCES; INDEX; ALTER; EXECUTE.

После предоставления определенные привилегии возможно сгруппировать с помощью создания ролей, а после этого прикрепить нужных пользователей к определенным ролям.

Когда пользователь получает доступ к БД, он может посчитать, что теперь ему разрешены любые действия. Благодаря использованию технологии аудита (AUDIT) в СУБД Oracle действия пользователя начинают фиксироваться. Данная технология может:

- защитить БД от несанкционированных действий пользователей или злоумышленника;

- помочь отследить, кто отвечает за определенные действия в БД;

- помочь проанализировать доступ к данным [14].

Преимуществом данной технологии является возможность выбора различных опций:

- аудит может быть включен для отслеживания всех действий конкретных пользователей: от входа в систему до того, какие SQL-запросы они выполняют;

- аудит каждого действия по отношению к объектам может быть проверен;

-аудит отслеживает конкретные SQL-запросов (ALTER, DROP, CONNECT и другие);

- аудит различных комбинаций опций.

Стоит отметить, что подсистема аудита не может проверять все в БД по следующим причинам:

- операции аудита выполняются внутри БД с каждым оператором SQL или подключением. Чем больше проверяется, тем больше работы в фоновом режиме;

- технология аудита генерирует записи в журнале, а, значит, чем больше проверяемых данных, тем больше записей создается в журнале;

- просмотр и анализ записей журнала аудита является отдельной работой, если имеется большая БД с большим количеством пользователей.

Заключение. Рассмотрев основные виды внешних и внутренних атак на СУБД Oracle можно сделать следующие выводы:

1. СУБД Oracle подвержена различным уязвимостям и угрозам, а именно:

- злоумышленник может вычислить системный идентификатор БД, имя сервиса, логины (имена пользователей), аутентификационные данные и сведения о СУБД из интегрирующих с ней приложений;

- злоумышленник может получить абсолютный контроль над СУБД, зная некоторые уязвимости.

2. Для выполнения основных требований информационной безопасности СУБД Oracle, которых необходимо придерживаться для наилучшего обеспечения защиты системы, следует применять технологию аудита, которая поможет выявить атаку, тем самым увеличив возможности администратора базы данных по быстрому противодействию ей.

3. Несмотря на недостатки, использование технологии аудита является важной частью комплексного подхода к организации системы защиты информации на предприятии.

***Рецензент**: Безродный Борис Федорович, доктор технических наук, профессор заместитель руководителя Центра кибербезопасности АО «НИИАС», г.Москва, Россия E-mail: boris-bezrodny@yandex.ru*

Литература

1. Смирнов С.Н.. Безопасность систем баз данных . – М .: Гелиос АРВ , 2007. – 352 с.
2. Хуторов В.С., Беленькая М.Н. Основные проблемы и цели мониторинга базы данных средствами СУБД Oracle // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 7. С. 133-134/
3. Клементьева С.С., Мошкович С.М., Синицин Н.А. Аутентификация, основанная на знании на примере СУБД // В сборнике: Студенческая наука: современные реалии Сборник материалов Международной студенческой научно-практической конференции. Редколлегия: О.Н. Широков [и др.]. 2017. С. 88-90.
4. Поляков А. М. Безопасность Oracle глазами аудитора: нападение и защита // Под редакцией И. Медведовского, 2010, издательство «ДМК Пресс».
5. Кривонос, Н. Журналирование изменений структуры БД и данных. – URL: http://www.compdoc.ru/bd/sql/log_change_of_structure_bd
6. Пудовченко Ю.Е. О шифровании паролей в СУБД Oracle // Защита информации. Инсайд. 2006. №6(12). С. 43-47
7. Егоров М. Выявление и эксплуатация SQL инъекций в приложениях // Защита информации. Инсайд. 2011. № 2 (38). С. 76-82.
8. Фейерштейн С., Прибыл Б. Oracle PL/SQL для профессионалов, 6-е издание // Перевел с английского Е. Матвеев, 2014, ООО «Питер Пресс».
9. Урман, С. Oracle8: Программирование на языке PL/SQL. – М.: Изд-во Лори, 1999. – 607 с.
10. Мишра С., Бьюли А. Секреты Oracle SQL // 2006, издательство «Символ-Плюс».
11. Смирнов С.Н., Киреев С.А. Анализ средств аудита информационной безопасности в СУБД Oracle // Информационное противодействие угрозам терроризма. 2013. №20. С. 112-116.
12. Горбачевская Е.Н., Катьянов А.Ю., Краснов С.С. Информационная безопасность средствами СУБД Oracle // Вестник Волжского университета имени В.Н. Татищева. 2015. №2(24). С. 72-85.

13. Бондаренко Е.С. Обеспечение информационной безопасности СУБД инфраструктуры в промышленных автоматизированных системах на примере СУБД Oracle // Аллея науки. 2017. № 5. С. 493-496.
14. Официальная документация Oracle: https://docs.oracle.com/en/database/
15. Завгородний С.Д., Швейкин В.В. Управление привилегиями на основе ролевой модели доступа в СУБД Oracle // В сборнике: Научные исследования и разработки студентов Сборник материалов IV Международной студенческой научно-практической конференции. Редколлегия: О.Н. Широков [и др.]. 2017. С. 162-164.

ANALYSIS OF THREATS AND VULNERABILITIES OF DBMS ORACLE

Mironov, M.M.[4], Kleptsov M.Y.[5], Lyubimova L.V.[6]

Abstract. *The article describes the main types of external and internal attacks on the database management system (DBMS) Oracle. Analysis of possible consequences of these attacks, and the vulnerability assessment of Oracle database various security vulnerabilities and threats. Among the external attacks are attacks on lisener, attacks through applications and connect to the DBMS directly. Among external attacks are considered PL/SQL injection, SQL injection, bypass the security procedures DBMS_ASSERT, the overflow buffet, as well as incorrect operation of associations and perceptions. The article describes the basic requirements for information security database and the main tasks of the administrator. Based on the analysis, it is concluded that the use of additional security measures is necessary. The authors recommend using the technology of operational audit, which is a small auxiliary key to obtain data on the current state of the system. This technology makes it possible to protect the database from unauthorized actions, to track certain actions, to analyze data access the article discusses the advantages and disadvantages of using audit technology. This technology is an important part of an integrated approach to the organization of the information security system in the enterprise.*

Keywords. *DBMS, DB, external attacks, internal attacks, SID, authentication, listener, PL / SQL injection, SQL injection, audit.*

References

1. Smirnov S.N.. Bezopasnost' sistem baz dannyh . – M .: Gelios ARV , 2007. – 352 s.
2. Hutorov V.S., Belen'kaya M.N. Osnovnye problemy i celi monitoringa bazy dannyh sredstvami SUBD Oracle // T-Comm: Telekommunikacii i transport. 2013. T. 7. № 7. S. 133-134/
3. Klement'eva S.S., Moshkovich S.M., Sinicin N.A. Autentifikaciya, osnovannaya na znanii na primere SUBD // V sbornike: Studencheskaya nauka: sovremennye realii Sbornik materialov Mezhdunarodnoj studencheskoj nauchno-prakticheskoj konferencii. Redkollegiya: O.N. SHirokov [i dr.]. 2017. S. 88-90.
4. Polyakov A. M. Bezopasnost' Oracle glazami auditora: napadenie i zashchita // Pod redakciej I. Medvedovskogo, 2010, izdatel'stvo «DMK Press».
5. Krivonos, N. ZHurnalirovanie izmenenij struktury BD i dannyh. – URL: http://www.compdoc.ru/bd/sql/log_change_of_structure_bd
6. Pudovchenko YU.E. O shifrovanii parolej v SUBD Oracle // Zashchita informacii. Insajd. 2006. №6(12). S. 43-47
7. Egorov M. Vyyavlenie i ehkspluataciya SQL in»ekcij v prilozheniyah // Zashchita informacii. Insajd. 2011. № 2 (38). S. 76-82.
8. Fejershtejn S., Pribyl B. Oracle PL/SQL dlya professionalov, 6-e izdanie // Perevel s anglijskogo E. Matveev, 2014, OOO «Piter Press».
9. Urman, S. Oracle8: Programmirovanie na yazyke PL/SQL. – M.: Izd-vo Lori, 1999. – 607 s.
10. Mishra S., B'yuli A. Sekrety Oracle SQL // 2006, izdatel'stvo «Simvol-Plyus».
11. Smirnov S.N., Kireev S.A. Analiz sredstv audita informacionnoj bezopasnosti v SUBD Oracle // Informacionnoe protivodejstvie ugrozam terrorizma. 2013. №20. S. 112-116.
12. Gorbachevskaya E.N., Kat'yanov A.YU., Krasnov S.S. Informacionnaya bezopasnost' sredstvami SUBD Oracle // Vestnik Volzhskogo universiteta imeni V.N. Tatishcheva. 2015. №2(24). S. 72-85.
13. Bondarenko E.S. Obespechenie informacionnoj bezopasnosti SUBD infrastruktury v promyshlennyh avtomatizirovannyh sistemah na primere SUBD Oracle // Alleya nauki. 2017. № 5. S. 493-496.
14. Oficial'naya dokumentaciya Oracle: https://docs.oracle.com/en/database/
15. Zavgorodnij S.D., SHvejkin V.V. Upravlenie privilegiyami na osnove rolevoj modeli dostupa v SUBD Oracle // V sbornike: Nauchnye issledovaniya i razrabotki studentov Sbornik materialov IV Mezhdunarodnoj studencheskoj nauchno-prakticheskoj konferencii. Redkollegiya: O.N. SHirokov [i dr.]. 2017. S. 162-164.

4 Mikhail Mironov, Russian University of transport (MIIT), Moscow, Russia. E-mail: mikhailmironoff@yandex.ru

5 Mikhail Kleptsov, Doctor of technical Sciences, Professor, Russian University of transport (MIIT), Moscow, Russia. E-mail: mkleptsov@mail.ru

6 Larisa Lyubimova, joint stock company «Research and design Institute of Informatization, automation and communication in railway transport» (JSC» NIIAS») Moscow, Russia. E-mail: lv.lyubimova@gmail.com