Авторы:

Клементьева Светлана Сергеевна

студентка

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

Мошкович Софья Михайловна

студентка

ФГАОУ ВО «Самарский государственный

аэрокосмический университет

им. академика С.П. Королёва (НИУ)»

г. Самара, Самарская область

Синицин Никита Александрович

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

АУТЕНТИФИКАЦИЯ, ОСНОВАННАЯ НА ЗНАНИИ НА ПРИМЕРЕ СУБД «ORACLE»

Аннотация: *в данной статье рассмотрены основные способы аутентификации, в частности, способ, основанный на знании пароля. Описаны некоторые способы преодоления парольной защиты, а также приведены рекомендации по защите от компрометации.*

Ключевые слова*: аутентификация, пароль, компрометация, СУБД, защита.*

Любая информационная система, содержащая в себе личные данные пользователей либо иные секретные данные, нуждается в организованном разделе-

нии доступа к ее ресурсам. Обычно получение доступа к ресурсам системы предусматривает выполнение трех этапов: идентификации, аутентификации и авторизации. Сущность центральной процедуры состоит в подтверждении подлинности пользователя, объекта или процесса, представившего идентификатор [1]

В общем случае можно выделить три вида аутентификации: основанный на знании, основанный на наличии и основанный на проверке характеристик.

Первый вид проверки соответствует знанию пользователем некоторой информации, которая однозначно его идентифицирует, например, индивидуального пароля. Второй вид подразумевает наличие у пользователя определенного предмета, такого как USB-ключ или смарт-карта. Последний же вид аутентификации сканирует личные характеристики человека – отпечаток пальца, сетчатку глаза, спектр голоса и т. д.

Если рассматривать системы баз данных, самым простым и удобным способом аутентификации является вход в систему с помощью логина и пароля, то есть основанный на знании. В СУБД «ORACLE» процесс проверки осуществляется так: субъект вводит свои личные данные – логин и пароль, затем данные шифруются и отправляются на сервер, где сравниваются с эталонными значениями, при совпадении данных аутентификация признается успешной, а иначе – субъекту отказывают в доступе.

Рассмотрим несколько причин, по которым такую защиту можно обойти и попасть в систему, не зная идентификационных данных.

Использование стандартных учетных записей и настроек в конфигурации по умолчанию можно считать самой распространенной уязвимостью. В СУБД «ORACLE» изначально создается множество учетных записей со стандартными паролями, в результате чего СУБД может быть скомпрометирована любым желающим, способным найти в Интернете список стандартных логинов и паролей. Для защиты от такого банального проникновения в систему следует после установки СУБД проверять список пользователей и, при необходимости, менять стандартные пароли.

Если в СУБД не обнаружено стандартных учетных записей, то злоумышленник может воспользоваться более грубым способом – удаленным перебором паролей. Так как у «ORACLE» по умолчанию не установлено ограничение на сложность, длину и количество вводов пароля, а имена стандартных учетных записей часто известны, то банальный перебор имеет большие шансы на успех. Чтобы уменьшить вероятность подбора пароля в «ORACLE» предусмотрены методы ограничения пароля, которые можно включить, посредством создания профиля с конкретными ограничениями и последующим назначением этого профиля пользователям. Обычно требуется, чтобы каждый пароль состоял не менее чем из четырех символов, не совпадал с идентификатором пользователя, включал хотя бы один символ, одну цифру и один знак пунктуации, не совпадал ни с одним из слов внутреннего списка простых слов, таких как «welcome», «account», «database», user и т. д. и отличался от предыдущего пароля хотя бы тремя символами.

Еще одна атака – это перехват трафика. То есть при вводе пароля злоумышленник может перехватить его на этапе передачи значения на сервер. В СУБД «ORACLE» на этот случай предусматривается шифрование пароля, которое осуществляется на стороне клиента. Используемый способ можно охарактеризовать как двойное шифрование алгоритмом DES с промежуточным ключом, который получается на первом этапе шифрования нигде не хранится. При отсутствии специализированного ПО или аппаратных средств, осуществить подбор ключа к перехваченному в канале связи сообщению за разумное время невозможно, что делает вероятность успеха атаки в СУБД ничтожно малой [2]

Последний метод получения пароля, который стоит упомянуть, – это «подсматривание» его в файлах системы. Можно найти пароли в открытом виде в таких местах как: файлы истории командной оболочки (такие, как bash_history), командные скрипты (к примеру, скрипты автозапуска), файлы журналов (DBCreation.log), конфигурационные файлы (emoms.properties), трассировочные файлы, файлы дампов; в зашифрованном виде пароли всегда можно обнару-

жить в файле системной базы [3] Но способом предотвращения такого вторжения является лишь защита файловой системы сервера.

Какой бы защищённой не была система, парольной аутентификации, она не является предельно надежной, но при использовании СУБД этот способ является самым приемлемым из-за его простоты, удобства и вполне достаточного уровня надежности.

Список литературы

1. Додонов М.В. Методические указания к лабораторной работе. Аутентификация и управление пользователями в СУБД Oracle. – Самара, 2010. – 11 с.

2. Поляков А.М. Безопасность Oracle глазами аудитора: нападение и защита. – М.: ДМК Пресс, 2010. – 336 с.

3. Пудовченко Ю.Е. Шифрование паролей в СУБД Oracle // Форум о СУБД Oracle, базы данных, запросы SQL [Электронный ресурс]. – Режим доступа: http://www.oracloid.ru/index.php?t=265