

УДК 004.4  
ББК 32.973.26-018.2  
П49

П49 Поляков А. М.

Безопасность Oracle глазами аудитора: нападение и защита. – М.: ДМК Пресс, 2017. – 336 с.: ил.

ISBN 978-5-97060-469-4

Эта книга является первым исследованием, написанным отечественным автором, которое посвящено проблеме безопасности СУБД Oracle. Материал книги основан на практическом опыте автора, полученном им в результате проведения тестов на проникновение и обширной исследовательской деятельности в области безопасности СУБД.

Книга построена таким образом, что вначале читатель ставится на место потенциального злоумышленника и изучает все возможные способы получения доступа к базе данных, вплоть до поиска новых уязвимостей и написания эксплоитов. Получив достаточно знаний об основных уязвимостях СУБД и о способах проникновения, читатель переходит ко второй части книги, в которой подробно описаны методы защиты СУБД Oracle как с помощью безопасной конфигурации и следования стандартам (в частности, PCI DSS), так и при помощи дополнительных средств обеспечения ИБ.

Книга предназначена как специалистам по безопасности, так и сетевым администраторам, разработчикам и администраторам баз данных, а также всем тем, кто интересуется вопросами информационной безопасности.

УДК 004.4  
ББК 32.973.26-018.2

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-97060-469-4

© Поляков А. М.  
© Оформление, издание, ДМК Пресс



# Содержание

|  |    |
|--|----|
| <b>Благодарности</b> .....   | 10 |
| <b>Предисловие от редактора</b> .....  | 11 |
| <b>Введение</b> .....  | 13 |
| <b>Часть I. Анализ защищенности СУБД Oracle снаружи</b> .....                | 18 |
| <b>Глава 1. Архитектура СУБД</b> .....                                       | 18 |
| 1.1. База данных .....   | 18 |
| 1.1.1. Физический уровень .....  | 18 |
| 1.1.2. Логический уровень .....  | 20 |
| 1.2. Структуры памяти .....  | 20 |
| 1.3. Процессы .....  | 21 |
| 1.4. Прочие компоненты СУБД .....  | 22 |
| 1.5. Заключение .....  | 22 |
| 1.6. Полезные ссылки .....   | 22 |
| <b>Глава 2. Анализ защищенности службы TNS Listener</b> .....                | 23 |
| 2.1. Описание службы Листенера .....   | 23 |
| 2.1.1. Режимы работы Листенера .....   | 25 |
| 2.2. Атаки на незащищенную службу Листенера .....                            | 26 |
| 2.2.1. Получение детальной информации о системе через службу Листенера ..... | 27 |
| 2.2.2. Атака на отказ в обслуживании через службу Листенера .....            | 28 |
| 2.2.3. Отказ в обслуживании через set trc_level .....                        | 30 |
| 2.2.4. Отказ в обслуживании через set log_file .....                         | 30 |
| 2.2.5. Добавление пользователя с правами DBA через set log_file .....        | 31 |
| 2.2.6. Получение административных прав на сервере через set log_file ....    | 33 |
| 2.2.7. Прочие атаки .....  | 35 |
| 2.3. Атаки на защищенную службу Листенера .....                              | 38 |
| 2.3.1. Перехват пароля .....   | 39 |
| 2.3.2. Аутентификация при помощи хэша .....                                  | 40 |
| 2.3.3. Расшифровка пароля на доступ к службе Листенера .....                 | 41 |
| 2.3.4. Удаленный перебор пароля на доступ к службе Листенера .....           | 43 |
| 2.4. Атаки на Листенер, защищенный дополнительными опциями .....             | 44 |
| 2.4.1. Опция безопасности ADMIN_RESTRICTIONS .....                           | 44 |

|   |    |
|---|----|
| 2.4.2. Опция безопасности LOCAL_OS_AUTHENTICATION ..... | 45 |
| 2.5. Заключение .....                                   | 46 |
| Сводная таблица .....                                   | 47 |
| 2.6. Полезные ссылки .....                              | 49 |

## Глава 3. Подключение к СУБД. Получение SID базы данных

|  |    |
|--|----|
| 3.1. Подбор SID .....  | 50 |
| 3.1.1. Проверка на стандартные значения SID .....                              | 53 |
| 3.1.2. Перебор SID по словарю .....  | 55 |
| 3.1.3. Подбор SID методом полного перебора (Brute force) .....                 | 55 |
| 3.2. Поиск информации о SID и SERVICE_NAME в сторонних приложениях ....        | 56 |
| 3.2.1. Получение SERVICE_NAME через Enterprise Manager Control .....           | 57 |
| 3.2.2. Получение SERVICE_NAME через Oracle Application Server .....            | 59 |
| 3.2.3. Получение SID через систему SAP R/3 и SAP Web Application Server .....  | 60 |
| 3.2.4. Получение SERVICE_NAME через Oracle XDB .....                           | 63 |
| 3.2.5. Получение SID через доступ к СУБД MsSQL .....                           | 63 |
| 3.2.6. Получение SID или SERVICE_NAME через уязвимое веб-приложение .....      | 67 |
| 3.3. Получение SID с помощью дополнительных знаний или прав в сети ....        | 67 |
| 3.3.1. Получение SID с помощью общедоступных данных о корпоративной сети ..... | 68 |
| 3.3.2. Получение SID из соседних СУБД в корпоративной сети .....               | 68 |
| 3.3.3. Получение SID из соседних серверов корпоративной сети .....             | 69 |
| 3.3.4. Получение SID или SERVICE_NAME прослушиванием сетевого трафика .....    | 70 |
| 3.4. Заключение .....  | 71 |
| 3.5. Полезные ссылки .....   | 72 |

## Глава 4. Преодоление парольной защиты

|   |    |
|---|----|
| 4.1. Настройка «по умолчанию» .....   | 73 |
| 4.1.1. Установка СУБД .....   | 74 |
| 4.1.2. Стандартные учетные записи .....                                       | 74 |
| 4.1.3. Проверка на наличие стандартных паролей .....                          | 78 |
| 4.2. Подбор аутентификационных данных .....                                   | 80 |
| 4.2.1. Подбор имен пользователей .....  | 80 |
| 4.2.2. Подбор паролей .....   | 82 |
| 4.2.3. Подбор паролей AS SYSDBA .....   | 83 |
| 4.3. Альтернативные способы получения паролей .....                           | 85 |
| 4.3.1. Получение паролей с помощью общедоступных данных об ИС ....            | 85 |
| 4.3.2. Получение паролей из соседних СУБД .....                               | 86 |
| 4.3.3. Подключение к СУБД с использованием локального доступа к серверу ..... | 86 |
| 4.3.4. Получение паролей через доступ к файловой системе сервера ..           | 87 |
| 4.4. Перехват аутентификационных данных .....                                 | 95 |

## Содержание



|  |    |
|--|----|
| 4.4.1. Процесс аутентификации пользователей .....                | 95 |
| 4.4.2. Перехват процесса аутентификации и расшифровка хэша ..... | 96 |
| 4.5. Заключение .....  | 97 |
| 4.6. Полезные ссылки .....                                       | 98 |

## Глава 5. Безопасность сервера приложений

|   |           |
|---|-----------|
| <b>и сторонних компонентов .....</b>                        | <b>99</b> |
| 5.1. Низко висящие фрукты (Oracle XDB) .....                | 100       |
| 5.2. Oracle Application Server .....                        | 102       |
| 5.2.1. Архитектура Oracle Application Server .....          | 102       |
| 5.2.2. Обнаружение Oracle Application Server .....          | 105       |
| 5.2.3. Атаки на Oracle Application Server .....             | 106       |
| 5.2.4. Современные атаки на Oracle Application Server ..... | 109       |
| 5.3. Автоматическая проверка .....                          | 112       |
| 5.4. Заключение .....                                       | 115       |
| 5.5. Полезные ссылки .....                                  | 116       |

|                                   |            |
|-----------------------------------|------------|
| <b>Заключение к части I .....</b> | <b>117</b> |
|-----------------------------------|------------|

|  |            |
|--|------------|
| <b>Часть II. Анализ защищенности СУБД Oracle изнутри .....</b> | <b>118</b> |
|--|------------|

## Глава 6. Повышение привилегий.

|  |            |
|--|------------|
| <b>Локальные уязвимости СУБД .....</b>                             | <b>119</b> |
| 6.1. PL/SQL-инъекции .....   | 120        |
| 6.1.1. Введение в PL/SQL .....                                     | 120        |
| 6.1.2. PL/SQL-инъекции .....                                       | 121        |
| 6.1.3. Blind SQL Injection .....                                   | 123        |
| 6.1.4. Внедрение PL/SQL-процедур .....                             | 126        |
| 6.1.5. Анонимный PL/SQL-блок .....                                 | 128        |
| 6.1.6. Выполнение PL/SQL-команд напрямую .....                     | 132        |
| 6.1.7. Cursor Injection .....                                      | 136        |
| 6.1.8. Защита с помощью DBMS_ASSERT и ее обход .....               | 138        |
| 6.1.9. История продолжается. Lateral SQL Injection .....           | 141        |
| 6.1.10. Заключение .....   | 147        |
| 6.2. Атаки на переполнение буфера .....                            | 148        |
| 6.2.1. Анализ одной уязвимости .....                               | 149        |
| 6.2.2. Написание POC-эксплоита к новой уязвимости .....            | 152        |
| 6.2.3. Выполнение произвольного кода на сервере .....              | 154        |
| 6.3. Фокусы с представлениями .....                                | 155        |
| 6.3.1. Представления .....   | 155        |
| 6.3.2. Объединения .....   | 156        |
| 6.3.3. Первая уязвимость, связанная с обработкой объединений ..... | 158        |
| 6.3.4. Объединения + представления .....                           | 159        |
| 6.3.5. История продолжается .....                                  | 161        |
| 6.4. Cursor snarfing .....   | 163        |

|  |     |
|--|-----|
| 6.4.1. Стандартная атака .....                                     | 163 |
| 6.4.2. Продвинутая атака .....                                     | 164 |
| 6.5. DLL Patching .....  | 168 |
| 6.5.1. Модификация библиотеки .....                                | 168 |
| 6.5.2. Посылка команд по сети .....                                | 169 |
| 6.6. Прочие уязвимости .....                                       | 171 |
| 6.6.1. Примеры нестандартных уязвимостей из CPU July 2008 .....    | 172 |
| 6.6.2. Примеры нестандартных уязвимостей из CPU April 2008 .....   | 172 |
| 6.6.3. Примеры нестандартных уязвимостей из более ранних CPU ..... | 173 |
| 6.7. Поиск и эксплуатация уязвимостей .....                        | 174 |
| 6.7.1. Поиск уязвимостей .....                                     | 175 |
| 6.7.2. Написание эксплоита .....                                   | 180 |
| 6.7.3. Системы обнаружения вторжений и методы их обхода .....      | 182 |
| 6.8. Заключение .....  | 184 |
| 6.9. Полезные ссылки .....   | 185 |

## Глава 7. Вскрытие паролей ..... 187

|  |     |
|--|-----|
| 7.1. Хранение паролей .....                                      | 188 |
| 7.2. Алгоритм шифрования паролей .....                           | 189 |
| 7.3. Подбор паролей .....  | 192 |
| 7.3.1. Подбор паролей по словарю .....                           | 192 |
| 7.3.2. Подбор пароля методом грубого перебора (bruteforce) ..... | 194 |
| 7.3.3. Перебор с использованием Rainbow Tables .....             | 195 |
| 7.4. Oracle 11g и нововведения .....                             | 200 |
| 7.4.1. Хранение паролей .....                                    | 200 |
| 7.4.2. Алгоритм шифрования паролей .....                         | 201 |
| 7.5. Заключение .....  | 204 |
| 7.6. Полезные ссылки .....                                       | 205 |

## Глава 8. Получение доступа к операционной системе .... 206

|   |     |
|---|-----|
| 8.1. Выполнение команд ОС через СУБД .....                                      | 206 |
| 8.1.1. Выполнение команд ОС, используя внешние библиотеки .....                 | 207 |
| 8.1.2. Выполнение команд ОС, используя JAVA-процедуры .....                     | 212 |
| 8.1.3. Выполнение команд ОС, используя пакет DBMS_SCHEDULER ..                  | 217 |
| 8.1.4. Выполнение команд ОС с помощью пакета Job Scheduler .....                | 222 |
| 8.1.5. Выполнение команд ОС путем модификации системных переменных Oracle ..... | 224 |
| 8.2. Доступ к файловой системе ОС через СУБД .....                              | 225 |
| 8.2.1. Доступ к файловой системе через UTL_FILE-процедуры .....                 | 225 |
| 8.2.2. Доступ к файловой системе через DBMS_LOB-процедуры .....                 | 229 |
| 8.2.3. Доступ к файловой системе через JAVA-процедуры .....                     | 231 |
| 8.2.4. Доступ к файловой системе через DBMS_ADVISOR-процедуры ..                | 235 |
| 8.3. Заключение .....   | 236 |
| 8.4. Полезные ссылки .....  | 236 |

|   |     |
|---|-----|
| <b>Глава 9. Поэтапные способы повышения привилегий и другие атаки</b> | 239 |
| 9.1. Поэтапные способы повышения привилегий                           | 240 |
| 9.1.1. Привилегия GRANT ANY [OBJECT] PRIVILEGE/ROLE                   | 241 |
| 9.1.2. Привилегия SELECT ANY DICTIONARY                               | 242 |
| 9.1.3. Привилегия SELECT ANY TABLE                                    | 243 |
| 9.1.4. Привилегия INSERT/UPDATE/DELETE ANY TABLE                      | 245 |
| 9.1.5. Привилегия EXECUTE ANY PROCEDURE                               | 245 |
| 9.1.6. Привилегия CREATE/ALTER ANY PROCEDURE                          | 246 |
| 9.1.7. Привилегия ALTER SYSTEM  | 247 |
| 9.1.8. Привилегия ALTER USER  | 247 |
| 9.1.9. Привилегия ALTER SESSION                                       | 248 |
| 9.1.10. Привилегия ALTER PROFILE                                      | 249 |
| 9.1.11. Привилегия CREATE LIBRARY                                     | 249 |
| 9.1.12. Привилегия CREATE ANY DIRECTORY                               | 250 |
| 9.1.13. Привилегия CREATE/ALTER ANY VIEW                              | 250 |
| 9.1.14. Привилегия CREATE ANY TRIGGER                                 | 251 |
| 9.1.15. Привилегия CREATE ANY/EXTERNAL JOB                            | 252 |
| 9.1.16. Роль JAVASYSPRIV  | 253 |
| 9.1.17. Роль SELECT_CATALOG_ROLE                                      | 253 |
| 9.2. Нестандартные способы повышения привилегий                       | 255 |
| 9.2.1. Атака на Листенер при помощи пакета UTL_TCP                    | 255 |
| 9.2.2. Поиск паролей и конфиденциальной информации                    | 256 |
| 9.3. Заключение   | 260 |
| 9.4. Полезные ссылки  | 261 |
| <b>Глава 10. Закрепление прав в системе, руткиты для Oracle</b>       | 262 |
| 10.1. СУБД и ОС   | 262 |
| 10.2. Руткиты первого поколения                                       | 263 |
| 10.2.1. Скрытие посторонних пользователей                             | 263 |
| 10.2.2. Скрытие посторонних заданий (Jobs)                            | 264 |
| 10.3. Руткиты второго поколения                                       | 267 |
| 10.3.1. Модификация исполняемых файлов                                | 268 |
| 10.4. Заключение  | 269 |
| 10.5. Полезные ссылки   | 269 |
| <b>ЧАСТЬ III. Защита СУБД Oracle</b>                                  | 270 |
| <b>Глава 11. Безопасная настройка СУБД Oracle</b>                     | 271 |
| 11.1. Методы защиты СУБД Oracle от атак на Листенер                   | 271 |
| 11.1.1. Защита Листенера от сканирования                              | 271 |
| 11.1.2. Ограничение доступа к службе Листенера                        | 273 |

|  |     |
|--|-----|
| 11.1.3. Защита от неавторизированных подключений к Листенеру .....       | 273 |
| 11.1.4. Установка патчей и удаление лишних компонентов .....             | 274 |
| 11.1.5. Защита от атак, направленных на перехват пароля .....            | 275 |
| 11.1.6. Защита от неправомерного доступа к конфигурационным файлам ..... | 275 |
| 11.1.7. Мониторинг обращений к Листенеру и защита от перебора ....       | 276 |
| 11.1.8. Защита от получения злоумышленником SID .....                    | 278 |
| 11.1.9. Последние штрихи .....   | 280 |
| 11.2. Настройка парольной защиты .....                                   | 280 |
| 11.2.1. Стандартные учетные записи и пароли .....                        | 280 |
| 11.2.2. Установка паролей и конфигурирование парольной политики ..       | 282 |
| 11.2.3. Настройка OS Authentication и Remote OS Authentication .....     | 285 |
| 11.2.4. Защита от неправомерного доступа к хэшам паролей .....           | 286 |
| 11.3. Механизмы внутренней защиты .....                                  | 286 |
| 11.3.1. Первичная настройка и установка критических обновлений ....      | 287 |
| 11.3.2. Безопасное назначение привилегий .....                           | 288 |
| 11.3.3. Ограничение доступа к ОС .....                                   | 291 |
| 11.3.4. Защита от руткитов .....   | 293 |
| 11.4. Заключение .....   | 293 |
| 11.5. Полезные ссылки .....  | 294 |

## **Глава 12. Аудит и расследование инцидентов .....**

|   |     |
|---|-----|
| 12.1. Введение в подсистему аудита СУБД Oracle .....                    | 295 |
| 12.1.1. Уровни подсистемы аудита .....                                  | 296 |
| 12.1.2. Включение ведения журнала аудита .....                          | 300 |
| 12.1.3. Защита журналов аудита .....                                    | 302 |
| 12.2. Настройка аудита событий для обнаружения злоумышленника .....     | 303 |
| 12.2.1. Отслеживание атак на Листенер и подбора SID .....               | 303 |
| 12.2.2. Отслеживание попыток подбора имен пользователей и паролей ..... | 303 |
| 12.2.3. Отслеживание попыток повышения привилегий .....                 | 306 |
| 12.2.4. Отслеживание доступа к таблицам с паролями .....                | 308 |
| 12.2.5. Отслеживание доступа к ОС .....                                 | 309 |
| 12.2.6. Отслеживание попыток скрытия следов пребывания .....            | 310 |
| 12.3. Заключение .....  | 311 |
| 12.4. Полезные ссылки .....   | 311 |

## **Глава 13. Соответствие стандартам безопасности .....**

|   |     |
|---|-----|
| 13.1. Законы и стандарты в сфере ИБ .....                                 | 312 |
| 13.2. Стандарт PCI DSS .....  | 314 |
| 13.2.1. Начальные сведения о PCI DSS .....                                | 315 |
| 13.2.2. СУБД Oracle и PCI DSS .....                                       | 315 |
| 13.3. Решения Oracle для соответствия СУБД требованиям безопасности ..... | 316 |
| 13.3.1. Oracle Advanced Security .....                                    | 316 |
| 13.3.2. Oracle Secure Backup .....  | 316 |

## Содержание



|   |            |
|---|------------|
| 13.3.3. Oracle Enterprise Manager Configuration .....                 | 317        |
| 13.3.4. Oracle Database Vault .....                                   | 317        |
| 13.3.5. Oracle Identity Management .....                              | 317        |
| 13.3.6. Oracle Audit Vault .....                                      | 317        |
| 13.4. Заключение .....  | 318        |
| 13.5. Полезные ссылки .....   | 318        |
| <b>Заключение .....</b>   | <b>319</b> |
| <b>Соответствие СУБД Oracle требованиям PCI DSS .....</b>             | <b>320</b> |
| <b>Приложение А. Применимость PCI DSS к хостинг-провайдерам .....</b> | <b>331</b> |
| <b>Приложение В. Компенсирующие меры .....</b>                        | <b>333</b> |