Digital Security

Проблемы безопасности СУБД Oracle. Последние тенденции

Необходимость глубоко эшелонированной защиты

Александр Поляков,
аналитик по информационной безопасности Digital Security,
руководитель исследовательского центра DSecRG

Oracle: проблемы безопасности

Digital Security

Разработка СУИБ

Аудит безопасности

Тесты на проникновение

Аудит на соответствие PCI DSS

Исследовательская лаборатория DSecRG

и многое другое

Почему Oracle?

1. Oracle присутствует практически в каждой крупной компании

2. Oracle защищена слабее, чем та же Windows

3. Oracle — сложная система. (Работает — НЕ ТРОГАЙ!)

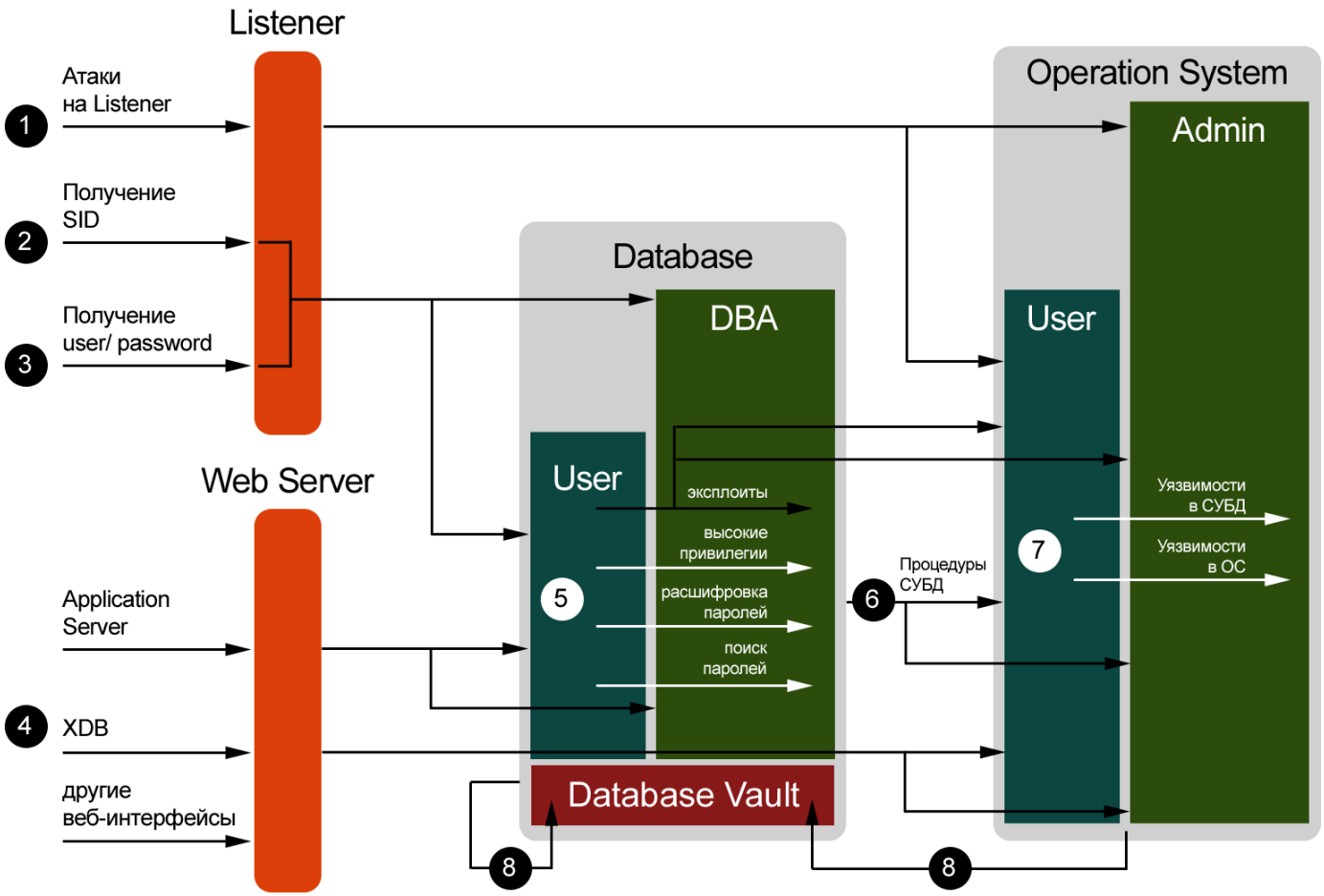
4. В Oracle существует огромное количество различных проблем в безопасности

- — Архитектурные
- — Программные
- — Администрирование

5. Отсутствие квалифицированных специалистов

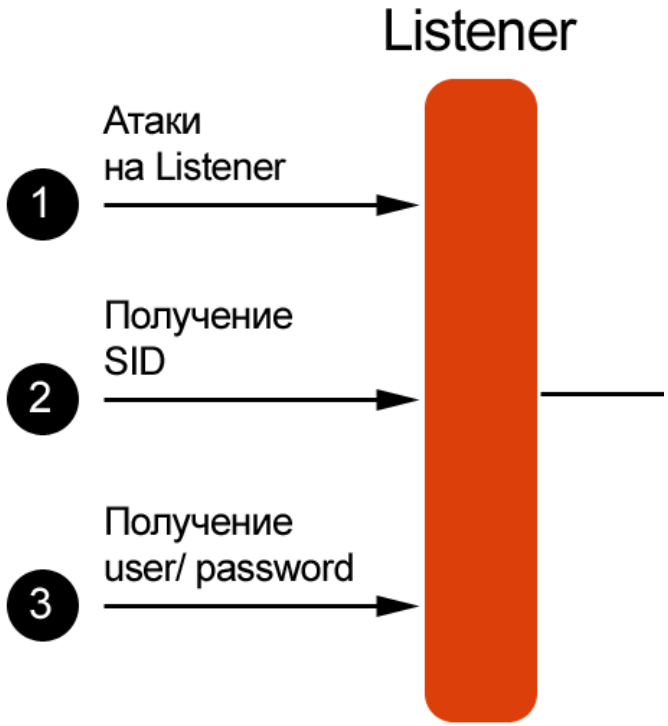
6. Сложность учета всех нюансов особенно в случае интеграции с другими системами

Этапы проникновения злоумышленника



1. Атаки на службу Listener

1. Получение информации
   - — SERVICE_NAME и SID
   - — Версия СУБД
   - — Пути к журналам регистрации событий
   - — Версия ОС
   - — Переменные окружения (ORACLE_HOME и т.п.)
2. Различные атаки на отказ в обслуживании
3. Выполнение SQL-команды от имени DBA
4. Получение удаленного доступа к ОС
5. Подбор паролей к Listener
6. Перехват паролей и хэшей
7. Аутентификация хэшем



2. Атаки направленные на получение SID

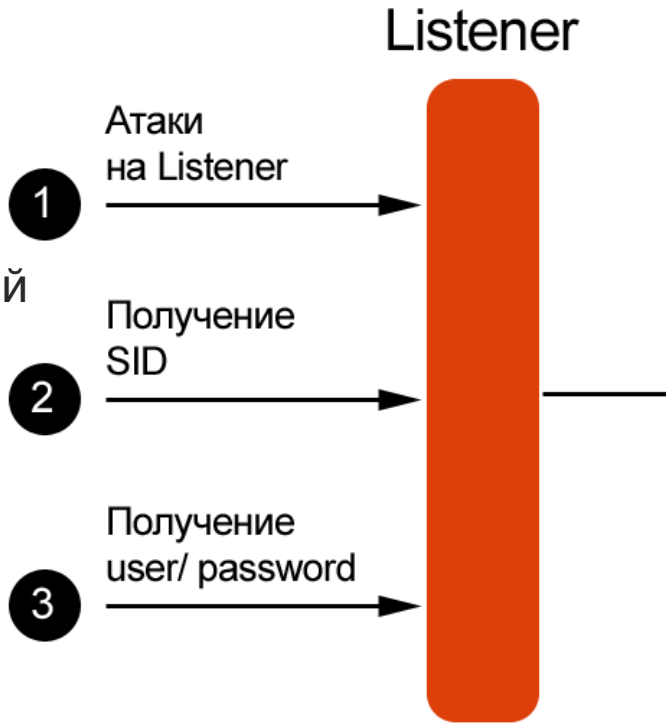
1. Подбор SID
- — Стандартные SID
- — Подбор по словарю
- — Bruteforce

2. Получение информации из сторонних приложений
- — Oracle Enterprise Manager Control
- — Oracle Application Server
- — Oracle XDB NEW
- — SAP Web Application Server NEW
- — MsSQL NEW

3. Сторонние сервера (Listener.ora)

4. Сторонние СУБД (Links)

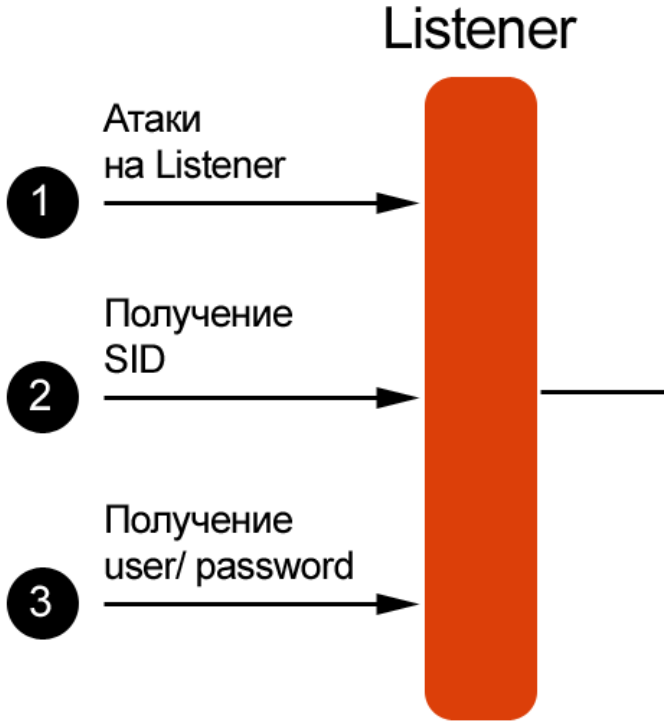
5. Перехват сетевого трафика



http://dsecrg.ru/files/pub/pdf/Different_ways_to_guess_Oracle_database_SID.pdf

3. Атаки, направленные на получение аутентификационных данных

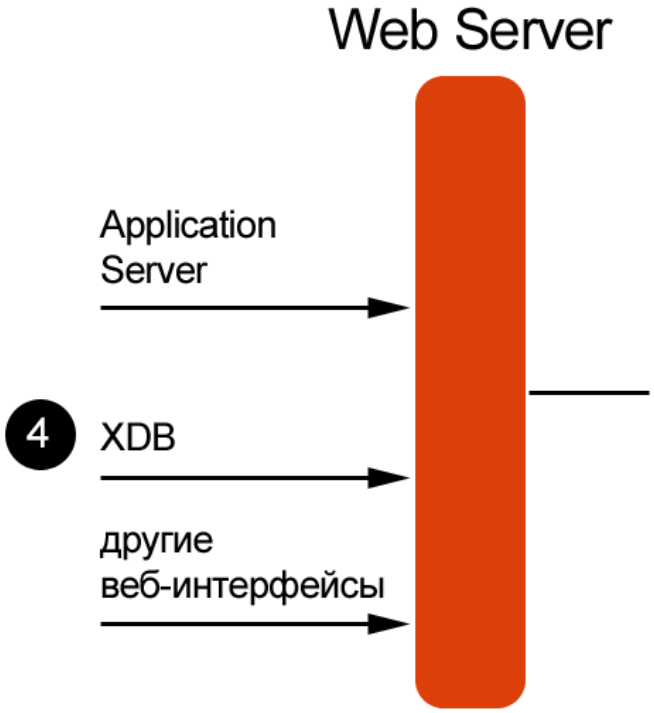
1. Стандартные учетные записи (95% СУБД)
   — DBSNMP — до сих пор работает!
2. Подбор аутентификационных данных
   — Подбор имен пользователей
   — Подбор паролей
   — Подбор паролей “AS sysdba”
3. Альтернативные способы получения паролей
   — Из соседних СУБД
   — Local OS Authentication
   — Поиск паролей в файлах (командных скриптах,файлах истории, конфигурационных файлах,файлах трассировки и т.п.)
4. Хэши паролей в файле системной базы
5. Перехват и расшифровка хэшей



4. Атаки на веб-интерфейсы доступа к СУБД

Компоненты:
Oracle Application Server
Oracle XDB
…

Уязвимости:
Buffer overflow
SQL Injection
XSS
Response Splitting
Information disclosure
…

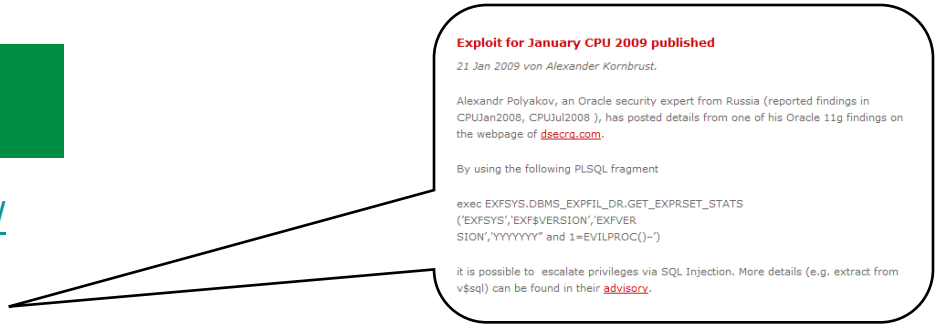


Обнаружены в рамках исследований DSecRG:

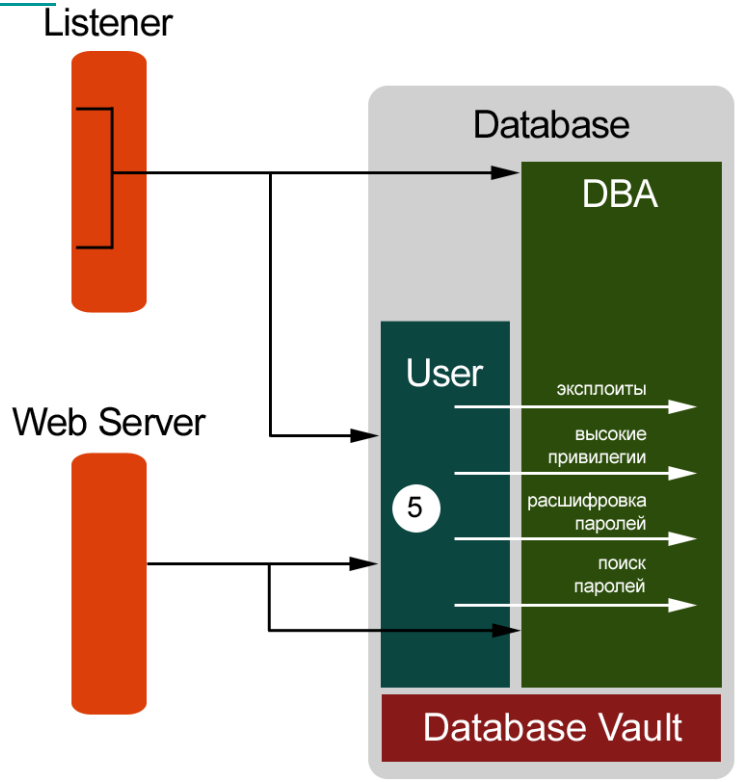
[DSECRG-09-001]	Oracle Application Server	(Published)
[DSECRG-063]	(21.01.2009)	(in work)
[DSECRG-074]	(21.01.2009)	(in work)
[DSECRG-080]	(03.03.2009)	(in work)

http://dsecrg.ru/pages/vul/

5. Повышение привилегий в СУБД



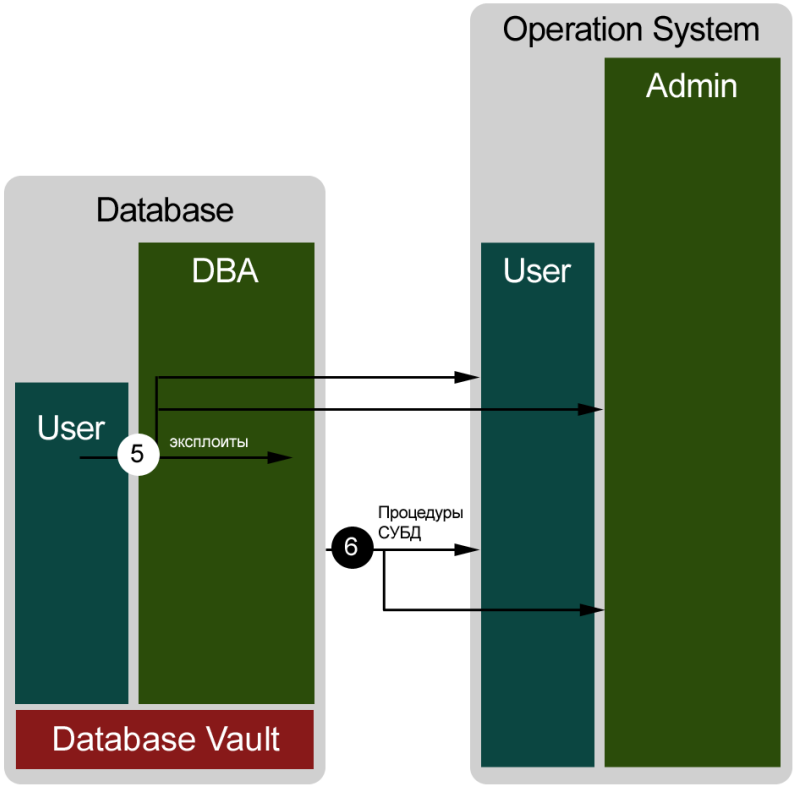
1. **Уязвимости СУБД** http://dsecrg.ru/pages/expl/
   - Buffer overflow http://dsecrg.ru/pages/vul/
   - PL/SQL Injection http://milw0rm.com
   - Cursor Snarfing http://trac.metasploit.com/changeset/6234
   - Views …
2. **“Опасные” привилегии**
   - SELECT ANY DICTIONARY
   - CREATE DIRECTORY..
3. **Расшифровка паролей**
   - Перебор — 8 символов порядка 8 суток
   - Rainbow таблицы — 8 символов менее 1часа!
   - Словарные Rainbow таблицы
   - Взлом паролей используя графические процессоры (CUDA, CTM)
   - Взлом паролей Oracle 11g (Gsauditor) NEW
   - http://www.evilfingers.com/tools/GSAuditor.php
4. **Поиск паролей в таблицах**
   - В открытом виде (sysman.MGMT_CREDENTIALS2)
   - В зашифрованном виде ~100 таблиц!



6. Получение доступа к ОС через процедуры СУБД

1. Выполнение команд ОС через СУБД
- — Exploits
- — ExtProc
  http://dsecrg.ru/pages/expl/show.php?id=22
- — JAVA
  http://dsecrg.ru/pages/expl/show.php?id=23
- — DBMS_SCHEDULER
  http://dsecrg.ru/pages/expl/show.php?id=24
- — Job Scheduler
- — Alter SYSTEM
- **— CtxApp + SMBRELAY** NEW
  http://dsecrg.ru/pages/pub/show.php?id=20

2. Доступ к ФС ОС через СУБД
- Exploits
- JAVA
- UTL_FILE
- DBMS_LOB
- DBMS_ADVISOR
- CtxApp



7. Повышение привилегий в ОС

1. При помощи уязвимостей в СУБД

— SUID файлы

— библиотеки

2. При помощи уязвимостей ОС

— огромное множество локальных уязвимостей в различных ОС и прикладных приложениях

8. Обход средств защиты

1. Выполнение команд в обход журналов

— Выполнение процедур через dbms_ijob не логируется

Автор - Volker Solinus (CVE-2008-5437)

http://blog.red-database-security.com/2009/01/16/proof-of-concept-how-to-bypass-oracle-auditing-using-dbms_ijob/

— Доступ к SYS.USER$ не логируется

— Особенность СУБД

2. Обход Database Vault

— На уровне ОС

Автор - Jakub Wartak (21 ноября 2008)

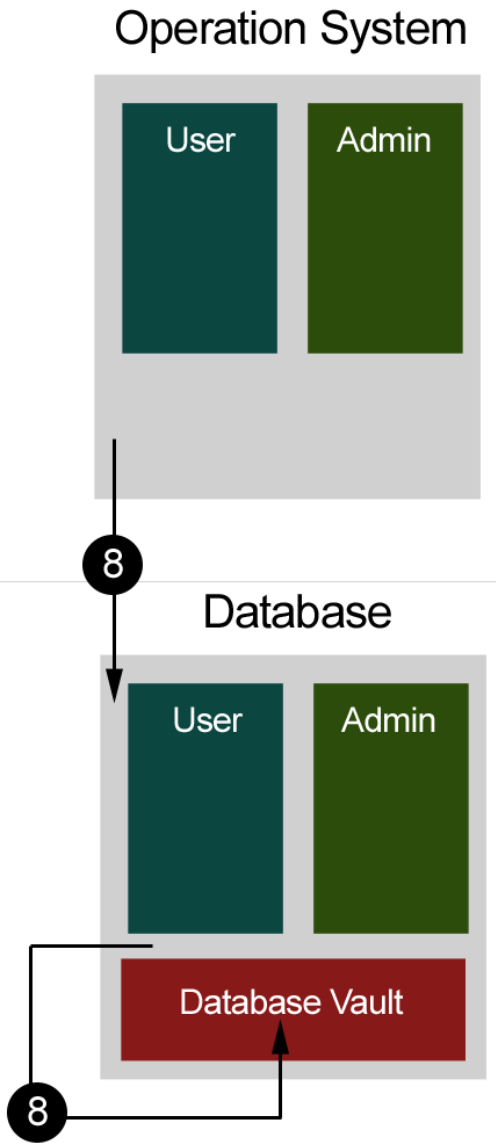
http://vnull.pcnet.com.pl/codez/ora_dv_mem_off.c

— На уровне СУБД

Автор - Alexander Kornbrust (ноябрь 2008)

http://blog.red-database-security.com/2008/11/21/oracle-database-vault-privilege-escalation-exploit-published/

```
SQL>exec sys.kupp$proc.change_user('DVA');
```



Автоматизация процесса проникновения в СУБД

1. Oraspoit

Год: 2007

Сайт: http://oraspoit.com/

Автор: Red-Database-Security

2. Inguma

Год: 2007

Сайт: http://inguma.sourceforge.net/

Автор: Joxean Koret

3. Oracle Mixin for Metasploit

Oracle с 2008

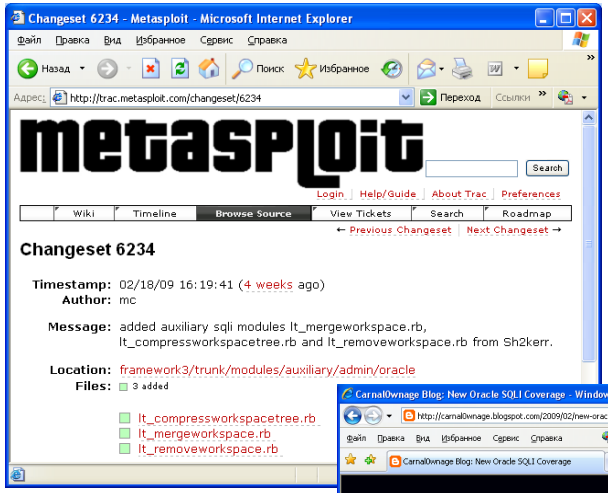
Сайт: http://metasploit.com/

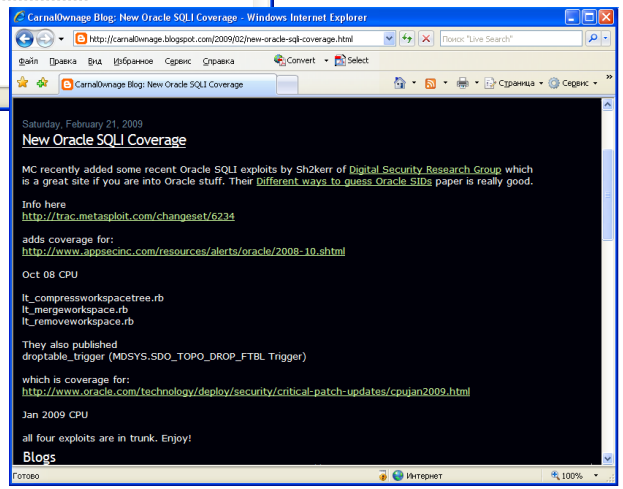
Авторы: CG, MC, DSecRG

Автоматизированная эксплуатация (Metasploit)

Модули для:

- Подключения
- Обнаружения SID
- Повышения привилегий
  - lt_compressworkspacetree.rb
  - lt_mergeworkspace.rb
  - lt_removeworkspace.rb
  - Droptable_trigger.rb
- Получение доступа к ОС
  - ora_ntlm_stealer.rb **NEW**





Пример

Пример

CPU July 2008

Уязвимость существует из-за недостаточной проверки входных данных в процедуре «SHOW» в пакете «WWV_RENDER_REPORT». Удаленный пользователь может внедрить и выполнить произвольный PL/SQL код и получить полный контроль над Oracle Database.

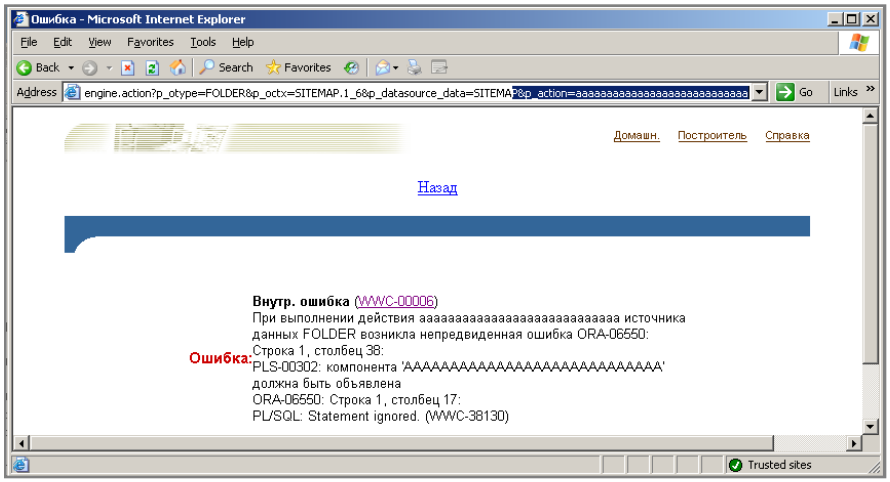
— Выполняется от имени пользователя PORTAL

— Пользователь PORTAL по умолчанию DBA

— В случае успеха можем выполнять любые команды вплоть до создания нового пользователя

До сих пор есть уязвимые порталы крупных финансовых компаний !!!

Пример




```
SQL> select sql_text from v$sql where sql_text like '%aaaaaaaaaaaaaa%';

begin htp.init;
wwexp_explore_FOLDER.aaaaaaaaaaaaaaaaaa(wwexp_datatype.g_exp_param);end;
```

http://server/pls/portal/PORTAL.wwexp_api_engine.action?p_otype=FOLDER&p_octx=SITEMAP.1_6&p_datasource_data=SITEMAP&p_action=**show(wwexp_datatype.g_exp_param);[evil_payload_code]**

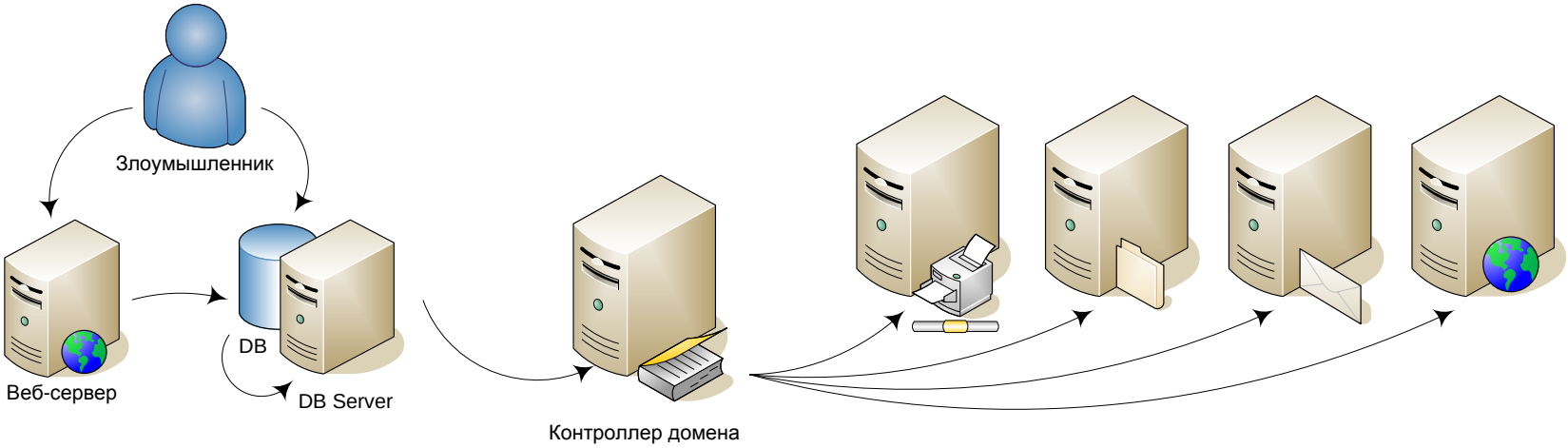
Итоги

СУБД один из наиболее важных компонентов инфраструктуры, присутствующий в каждой крупной компании

Зачастую доступ возможен через уязвимости в WEB-приложениях (порталах)

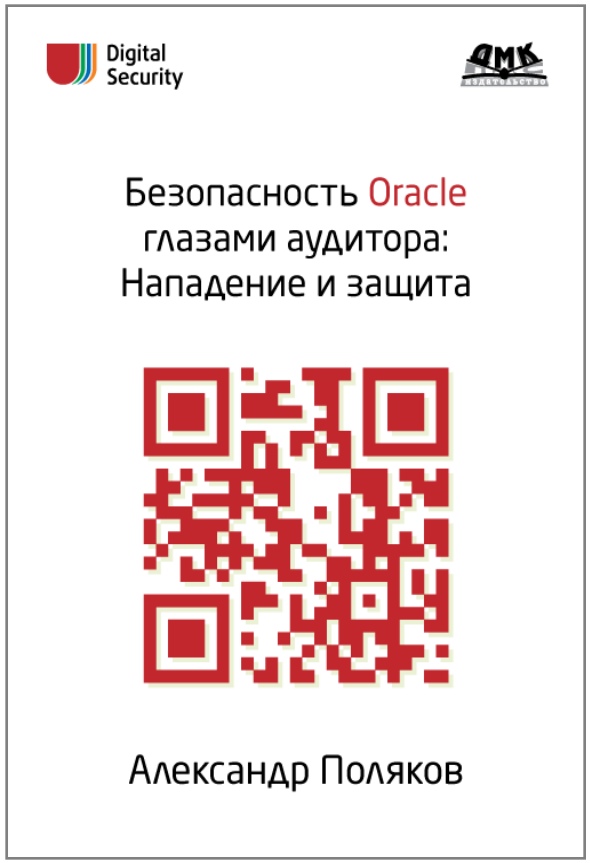
Небезопасная настройка СУБД может привести к получению административного доступа к серверу

Получение доступа к серверу может привести к компрометации всей системы



Полезные источники

1. Блог Пита Финнигана
   http://petefinnigan.com
2. Блог компании Red-Database-Security
   http://blog.red-database-security.com
3. Блог Пола Врайта
   http://oracleforensics.com
4. Сайт исследовательского центра Digital Security Research Group
   http://dsecrg.ru
5. Первая книга по безопасности Oracle, написанная отечественным автором:



«Безопасность Oracle глазами аудитора: Нападение и защита»

(Александр Поляков)