

30 октября 2008

# Различные способы получения SID базы данных в СУБД Oracle

Digital Security Research Group (DSecRG)

Александр Поляков

[a.polyakov@dsec.ru](mailto:a.polyakov@dsec.ru)

<http://dsecrg.ru>

## Содержание

---

Введение.....	3
Коротко о SID и SERVICE_NAME .....	4
Получение SID и SERVICE_NAME .....	4
Подключение к СУБД при известном SERVICE_NAME .....	5
Подключение к СУБД при известном SID .....	5
Проблемы получения SID и SERVICE_NAME в новых версиях СУБД.....	6
Подбор SID.....	7
Проверка на значения SID по умолчанию .....	7
Проверка на типовые значения SID .....	8
Подбор SID по словарю .....	9
Подбор SID методом полного перебора (Brute force).....	10
Поиск информации о SID и SERVICE_NAME в сторонних приложениях.....	12
Oracle Enterprise Manager Control .....	13
Oracle Application Server .....	14
Oracle XDB.....	16
SAP.....	16
Стандартная страница администрирования SAP Web Application Server.....	16
Запрос несуществующей страницы SAP Web Application Server .....	18
SAP RFC.....	18
SAP SID Bruteforcing.....	19
Уязвимое веб-приложение .....	20
Получение SID при использовании дополнительных прав на атакуемом сервере и в сети	21
Получение SID при использовании дополнительных прав на атакуемом сервере .....	21
Получение SID при наличии учетной записи в ОС, на которой установлена СУБД .....	21
Получение SID при наличии учетной записи на ftp-сервере .....	21
Получение SID при наличии учетной записи в СУБД MsSQL.....	23
Получение SID через список сервисов в ОС .....	24
Получение SID из ключа реестра HKLM\SOFTWARE\ORACLE .....	25
Получение SID через список директорий .....	25
Получение SID при использовании дополнительных прав в сети .....	26
Получение SID при наличии доступа к “соседним” СУБД в сети.....	27
Получение SID при наличии доступа к “соседним” серверам в сети .....	28
Получение SID или SERVICE_NAME прослушиванием сетевого трафика .....	29
Заключение .....	30
Дополнительные материалы.....	31

## Введение

---

В публичных источниках довольно много рассказано о проблемах безопасности СУБД Oracle и о способах проникновения в вышеупомянутую СУБД. Стандартный сценарий атаки на СУБД Oracle включает в себя следующую последовательность шагов:

- Атаки на Листенер (переполнение буфера, подмена лог-файла);
- Подбор имен пользователей и паролей;
- Получение *SID*;
- Повышение привилегий в СУБД (SQL-инъекции, атаки на представления, подбор паролей);
- Получение доступа к ОС (*Extproc*, *Java*, *UTL\_FILE*, *DBMS\_LOB*);
- Закрепление прав (руткит, бэкдор);
- Удаление следов пребывания (*SYS.AUD\$*).

Большинство из этих шагов достаточно хорошо освещено в Сети и не вызывает затруднений. Учетные записи по умолчанию и простые пароли – это проблема, которая регулярно имеет место, человеческий фактор неизбежен. Обновления, судя по последним исследованиям компании Sentrigo, устанавливает только треть администраторов и то не регулярно. Доступ к ОС возможен множеством различных способов, начиная подключением внешних библиотек и заканчивая чтением файлов при помощи *DBMS\_LOB*, *DBMS\_ADVISOR*, и прочими. Руткиты обнаруживает лишь малая часть администраторов, также как и модификацию таблиц аудита, тем более, что аудит, как таковой, встречается довольно редко.

Среди такого обилия информации по проникновению в СУБД существует одна тема, которая до сих пор недостаточно освещена и может сделать невозможным проникновение в СУБД, даже если все перечисленные выше уязвимости присутствуют и администратор не следит за системой. Это третий пункт из приведенного выше списка – получение *SID* базы данных. Без знания *SID* злоумышленник не сможет подключиться к СУБД, даже если ему известны аутентификационные данные. С выходом версии СУБД Oracle 10g получение *SID* не является такой тривиальной задачей, что подвигло автора на исследование этого вопроса, результатом которого стал настоящий документ.

В этом документе будут собраны воедино все существующие на данный момент способы получения *SID*, которые были обнаружены в Интернете и дополнены несколькими альтернативными вариантами, найденными автором.

## Коротко о SID и SERVICE NAME

---

Каждый экземпляр базы данных идентифицируется с помощью *SID* (*System Identifier – системный идентификатор*). *SID* состоит из алфавитно-цифровых символов, хранится в переменной среды *ORACLE\_SID* и используется утилитами и сетевыми компонентами для доступа к базе данных. Кроме понятия *SID* существует также и понятие *SERVICE NAME*, которые зачастую не различают.

Имя сервиса (*SERVICE\_NAME*) – это сравнительно новое понятие, введенное начиная с СУБД Oracle 8i. *SERVICE\_NAME* определяет одно или ряд имен для подключения к одному экземпляру базы данных. То есть можно указать несколько имен сервиса, ссылающихся на один экземпляр, с различными настройками.

Если нам удастся узнать *SID* или *SERVICE\_NAME*, используемый в СУБД, то это значительно упростит дальнейшее проникновение в СУБД.

## Получение SID и SERVICE\_NAME

---

Стандартный способ получения *SID*, который работал до десятой версии СУБД Oracle – это использование утилиты *lsnrctl*. Для этого достаточно воспользоваться командой *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...
Service "orcl" has 1 instance(s).
  Instance "orcl", status READY, has 1 handler(s) for this service...
The command completed successfully
LSNRCTL>
```

В выводе команды мы можем видеть системный идентификатор, он же – *SID* (Instance), и имя сервиса – *SERVICE\_NAME* (Service). В нашем случае они совпадают, но это бывает не всегда.

## Подключение к СУБД при известном SERVICE\_NAME

---

Для того чтобы подключиться к СУБД, зная *SERVICE\_NAME*, можно воспользоваться утилитой *sqlplus*:

```
C:\ >sqlplus system/manager@192.168.40.33/orcl
SQL*Plus: Release 10.1.0.5.0 - Production on Tue Aug 26 17:18:23 2008

Copyright (c) 1982, 2005, 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>
```

## Подключение к СУБД при известном SID

---

В случае если *SID* и *SERVICE\_NAME* не совпадают, и мы знаем только *SID*, то для того, чтобы подключиться к СУБД, следует в первую очередь прописать данные, необходимые для подключения (*connection descriptor*), в конфигурационном файле *tnsnames.ora*.

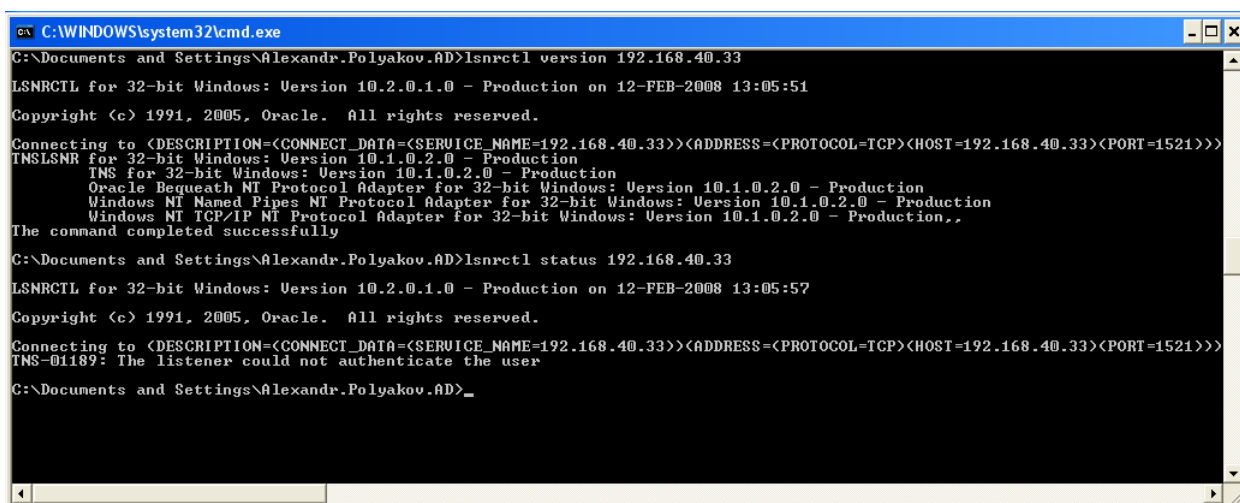
```
ORCL_192.168.40.33 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = 192.168.40.33) (PORT = 1521)))
    (CONNECT_DATA =
      (SID = ORCL)
      (SERVER = DEDICATED))
  )
```

В результате этого у нас будет создана строка подключения – *orcl\_192.168.40.33*, которую можно использовать в утилите *sqlplus*:

```
C:\ >sqlplus system/manager@orcl_192.168.40.33
SQL*Plus: Release 10.1.0.5.0 - Production on Tue Aug 26 17:18:23 2008
Copyright (c) 1982, 2005, 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>
```

## Проблемы получения *SID* и *SERVICE\_NAME* в новых версиях СУБД

В новых версиях СУБД Oracle, начиная с 10g R1 и выше, включена по умолчанию опция *LOCAL\_OS\_AUTHENTICATION*, запрещающая удаленное выполнение команд *services* или *status*, которые используются для получения *SID* и *SERVICE\_NAME*.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Alexandr.Polyakov.AD>lsnrctl version 192.168.40.33
LSNRCTL for 32-bit Windows: Version 10.2.0.1.0 - Production on 12-FEB-2008 13:05:51
Copyright (c) 1991, 2005, Oracle. All rights reserved.
Connecting to (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.40.33))<ADDRESS=(PROTOCOL=TCP)<HOST=192.168.40.33)<PORT=1521)>>
TNSLSNR for 32-bit Windows: Version 10.1.0.2.0 - Production
TNS for 32-bit Windows: Version 10.1.0.2.0 - Production
Oracle Bequeath NT Protocol Adapter for 32-bit Windows: Version 10.1.0.2.0 - Production
Windows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 10.1.0.2.0 - Production
Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.1.0.2.0 - Production,,
The command completed successfully
C:\Documents and Settings\Alexandr.Polyakov.AD>lsnrctl status 192.168.40.33
LSNRCTL for 32-bit Windows: Version 10.2.0.1.0 - Production on 12-FEB-2008 13:05:57
Copyright (c) 1991, 2005, Oracle. All rights reserved.
Connecting to (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.40.33))<ADDRESS=(PROTOCOL=TCP)<HOST=192.168.40.33)<PORT=1521)>>
TNS-01189: The listener could not authenticate the user
C:\Documents and Settings\Alexandr.Polyakov.AD>_
```

Попытка выполнить команду *status* в версии Oracle 10g

Аналогичная ситуация наблюдается в случае установки пароля на Листенер версии 9.2.0.6 и выше. В этом случае команды *services* и *status* запрещены на выполнение без знания пароля. Таким образом, в новых версиях СУБД Oracle вопрос альтернативных подходов к определению *SID* базы данных является весьма актуальным и может стать первым шагом на пути к получению административного доступа ко всей СУБД.

Все существующие способы получения *SID* можно разбить на три группы:

- Подбор *SID*;
- Поиск *SID* в сторонних приложениях;
- Получение *SID* имея дополнительные права.

## Подбор SID

Подбор *SID* – первое, что обычно предпринимают в случае, если стандартным способом получить *SID* не удалось. Подбор *SID* можно разбить на 4 подкласса:

- Проверка на значение *SID* по умолчанию;
- Проверка на типовые значения *SID*;
- Перебор *SID* по словарю;
- Подбор *SID* методом полного перебора (*Brute force*).

### Проверка на значения *SID* по умолчанию

Известен тот факт, что зачастую администраторы оставляют *SID*, предлагаемый по умолчанию в процессе установки самой СУБД или сторонних приложений, таких как *SAP*. Например, стандартным *SID* при установке версии Oracle 10G является “*ORCL*”, а стандартное значение *SID* при установке Oracle 10G Express edition – “*XE*”.

Oracle Database 10g Installation - Installation Method

### Select Installation Method

**Basic Installation**  
Perform full Oracle Database 10g installation with standard configuration options requiring minimal input. This option uses file system for storage, and a single password for all database accounts.

Oracle Home Location: C:\oracle\product10.2.0\db\_1

Installation Type: Enterprise Edition (1.3GB)

Create Starter Database (additional 720MB)

Global Database Name: orcl

Database Password:  Confirm Password:

This password is used for the SYS, SYSTEM, SYSMAN, and DBSNMP accounts.

**Advanced Installation**  
Allows advanced selections such as different passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP accounts, database character set, product languages, automated backups, custom installation, and alternative storage options such as Automatic Storage Management.

ORACLE

Процессе установки СУБД со стандартным *SID*

Полный список стандартных *SID* можно найти по адресу <http://www.red-database-security.com/scripts/sid.txt>. Для того чтобы проверить все *SID*, перечисленные в этом списке, можно воспользоваться утилитами, реализующими атаку перебора *SID* по заданному списку.

### **Проверка на типовые значения *SID***

---

Следующим шагом является проверка использования в качестве *SID* различных общедоступных данных о компании, к примеру, название компании, отдела, проекта, их те или иные сокращения и аббревиатуры. Довольно часто *SID* состоит из названия или аббревиатуры и символов “*DB*”, дописанных справа. Например, *SID* СУБД в компании “*Super Big Company*” может быть *SBC* или *SBCDB*.

По статистике, примерно в 10 процентах случаев *SID* попадает под указанные критерии

Еще один распространенный вариант – использование в качестве *SID* базы данных *DNS/NETBIOS-имени* хоста, на котором установлена СУБД, возможно, с некоторыми модификациями.

По статистике, в 5 процентах случаев *SID* совпадает в *DNS/NETBIOS-именем* хоста и в 8 процентах случаев совпадает с ним частично

## Подбор SID по словарю

В случае если SID не является одним из стандартных, то следующим этапом будет проверка того, является ли SID словарным. На практике данная проверка осуществляется специализированными утилитами. Самые известные утилиты, реализующие атаку подбора SID, приведены в таблице «Утилиты для подбора SID».

Таблица «Утилиты для подбора SID»

Утилита	Автор	Ссылка
sidguess	Red database Security	<a href="http://www.red-database-security.com/software/sidguess.zip">http://www.red-database-security.com/software/sidguess.zip</a>
oscanner	Patrik Karlsson	<a href="http://www.cgure.net/tools/oscanner_bin_1_0_6.zip">http://www.cgure.net/tools/oscanner_bin_1_0_6.zip</a>
ora-getsid, ora-brutesid from OAK	David Litchfield	<a href="http://www.vulnerabilityassessment.co.uk/oak.htm">http://www.vulnerabilityassessment.co.uk/oak.htm</a>
sidguesser	Patrik Karlsson	<a href="http://inguma.sourceforge.net/index.php">http://inguma.sourceforge.net/index.php</a>
CsidGuess.py from Inguma	Joxean Koret	<a href="http://sourceforge.net/projects/inguma">http://sourceforge.net/projects/inguma</a>

При подборе SID по словарю решающее значение имеет скорость. С этой целью было проведено два теста по измерению скорости работы приведенных выше утилит (Таблица «Результаты сравнения скоростей работы утилит по перебору SID»):

- Первый тест – замер времени перебора списка стандартных SID (~600 слов);
- Второй тест – замер времени подбора известного SID “ORCL” методом полного перебора.

Таблица «Результаты сравнения скоростей работы утилит по перебору SID»

Утилита	Скорость перебора	Время проверки по списку стандартных SID	Время перебора SID “ORCL”
Ora-brutesid	90 SID/сек	Опция не реализована	114 минут
Ora-getsid	88 SID/сек	7 сек.	Опция не реализована
Oscanner	80 SID/сек	8 сек.	Опция не реализована
Sidguesser	71 SID/сек	10 сек	Опция не реализована
Sidguess	11 SID/сек	58 сек.	Программа не смогла завершить работу

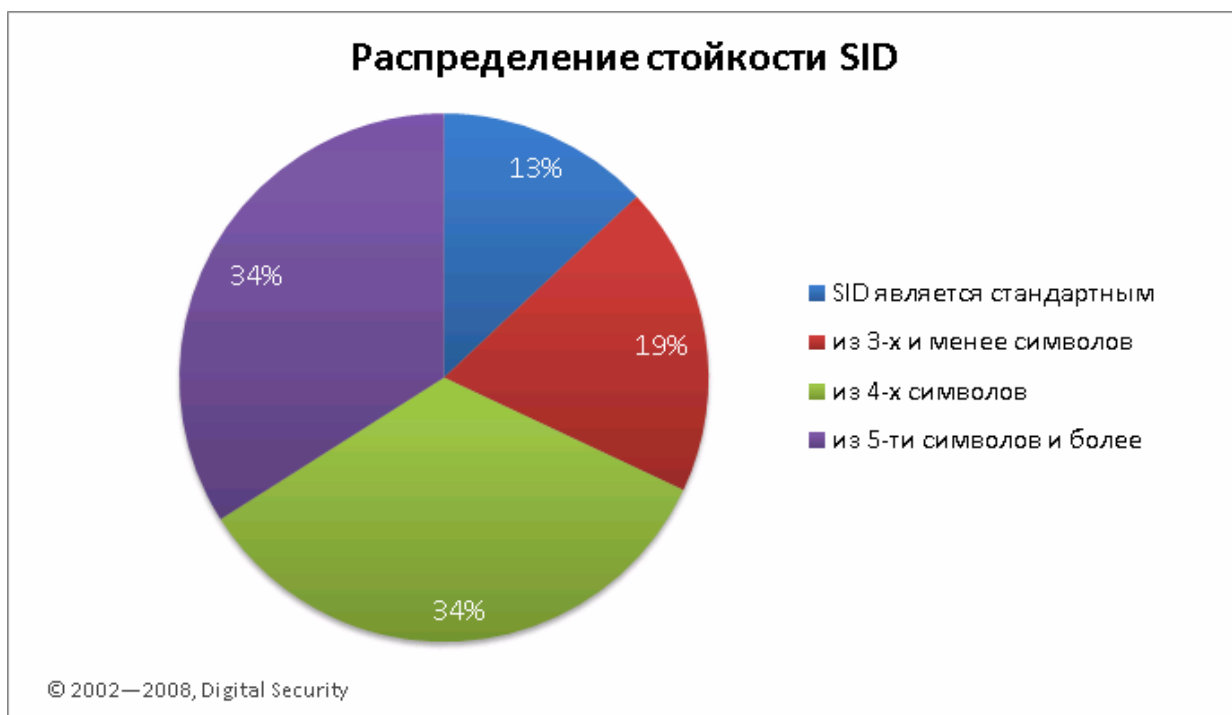
Исходя из результатов полученных тестов, наилучшие результаты по подбору по словарю показала утилита *Ora-getsid*, а наихудшие результаты по перебору по словарю показала утилита *sidguess*.

### **Подбор SID методом полного перебора (Brute force)**

В случае если подбор по словарю не дает желаемого результата, логично перейти к подбору *SID* методом полного перебора. Что касается скорости подбора методом полного перебора, то наилучшие результаты показала утилита *ora-brutesid* (Таблица «Результаты сравнения скоростей работы утилит по перебору *SID*»). С помощью нее все 4-символьные *SID* можно перебрать примерно за 3 часа; в случае если *SID* содержит 5 символов, то его придется перебирать порядка 3-х суток, что вполне осуществимо.

По проведенным тестовым запускам утилиты ширина пропускного канала незначительно влияет на скорость перебора, так как основное время занимает инициализация соединения. Учитывая эти особенности, можно запустить параллельно несколько экземпляров утилиты на разные СУБД.

Статистика проведения тестов на проникновение в крупных компаниях показывает: в 13% случаев *SID* является стандартным, в 19% – состоит из 3-х и менее символов и в 34% случаев – из 4-х символов.



Таким образом, в среднем в 2-х случаях из трех (66%) возможно получение *SID* базы данных, для чего потребуется не более 3-х часов (время перебора всех 4-х символьных значений). Если учитывать возможность перебора *SID* по словарю, то вероятность увеличивается

## Поиск информации о SID и SERVICE\_NAME в сторонних приложениях

---

Перебор – это, конечно, удобный способ, но он не всегда заканчивается успехом, а также создает много постороннего трафика и записей в журналах подключений, что способствует обнаружению. Таким образом, перед тем, как запускать перебор *SID*, рекомендуется сначала воспользоваться более незаметными способами, речь о которых пойдет в этом разделе.

В крупных в компаниях СУБД Oracle зачастую используется в связке с серверами приложений, такими как, например, *Oracle Application Server* и *Oracle SOA Suite*, а также со сторонними продуктами, к примеру, такими, как *SAP R/3*.

Наличие того или иного доступа к интерфейсу систем, интегрируемых с СУБД Oracle, позволяет в некоторых случаях узнать *SID* или *SERVICE\_NAME* базы данных даже при условии, что доступ к службе Листенера закрыт, а перебор не дал ожидаемых результатов. Ниже приведены основные приложения, через которые можно получить *SID* базы данных, не обладая дополнительными правами:

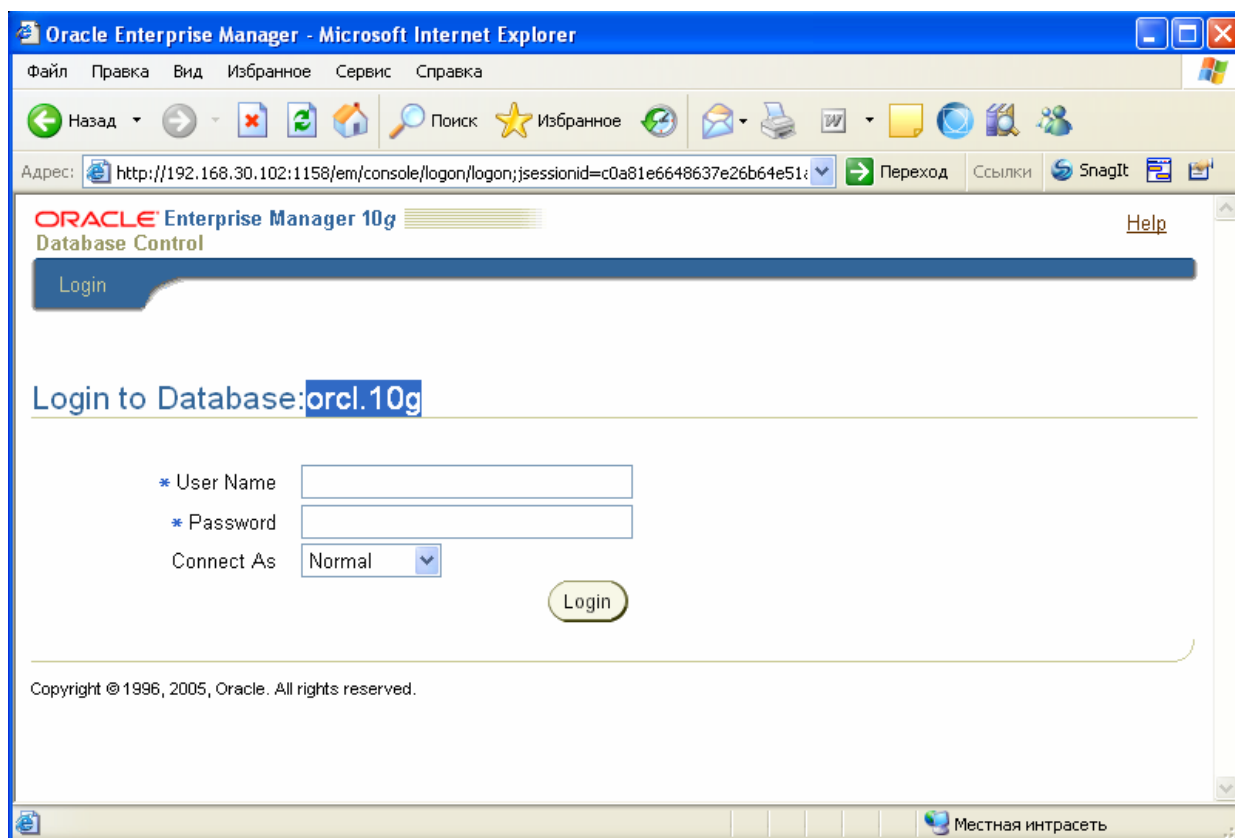
- Oracle Enterprise Manager Control;
- Oracle Application Server;
- Oracle XDB;
- SAP Web Application Server;
- Уязвимые веб-приложения.

Рассмотрим более подробно существующие методы.

## Oracle Enterprise Manager Control

Одним из самых простых и распространенных способов является получение *SERVICE\_NAME* через веб-интерфейс компонента *Enterprise Manager Control*. При установке СУБД Oracle 10g R2 по умолчанию устанавливается приложение *Enterprise Manager Control*, которое прослушивает порт *1158/tcp* и позволяет удаленно управлять настройками СУБД.

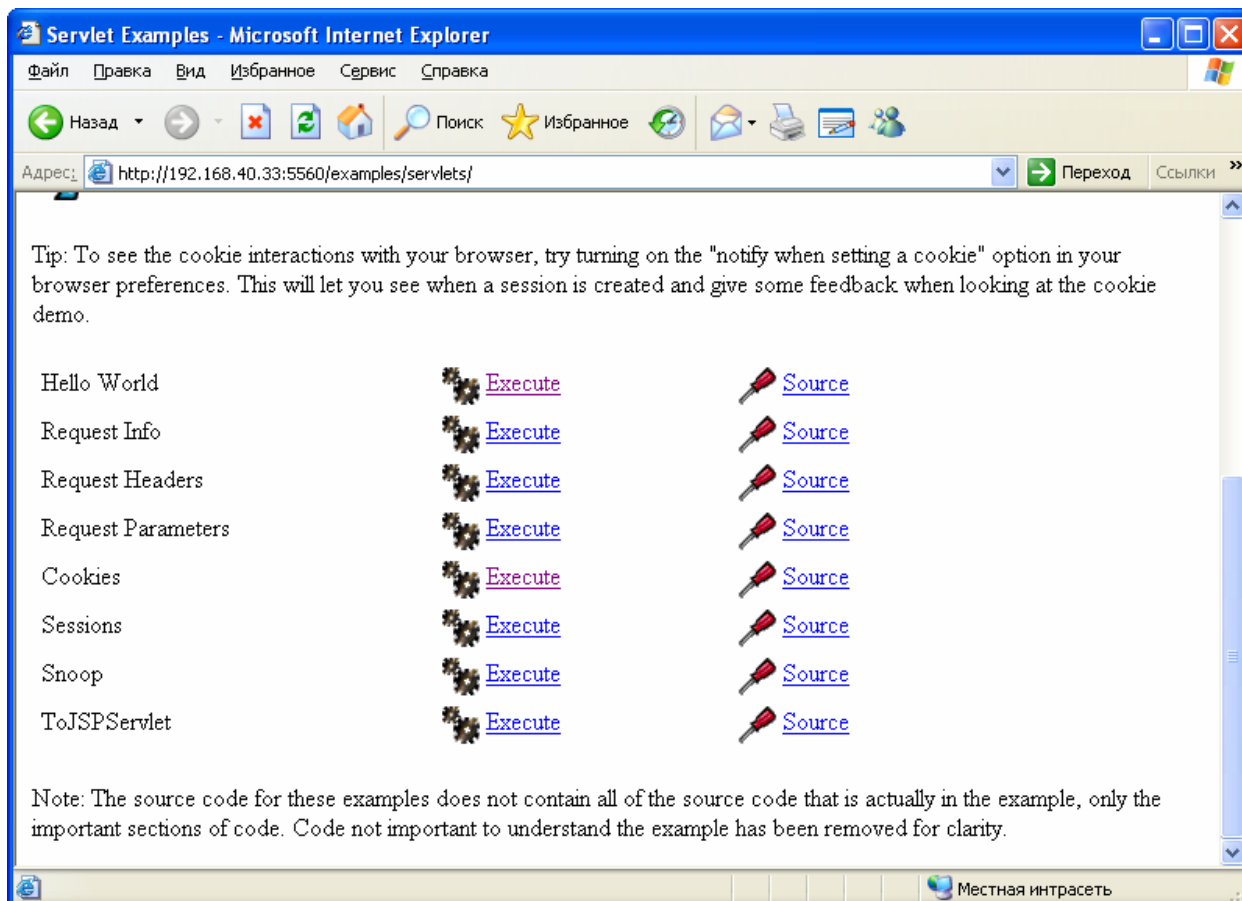
При обращении с помощью браузера к странице *http://hostname:1158/em/console* мы получаем страницу с окном ввода логина и пароля, на которой, кроме того, присутствует значение *SERVICE\_NAME* базы данных. В некоторых источниках пишут, что на странице мы получаем *SID*; это не верно, на самом деле мы получаем *SERVICE\_NAME*, но так как они зачастую совпадают, то обычно этому не придают значения.



*Получение SERVICE\_NAME через Enterprise Manager Database Control*

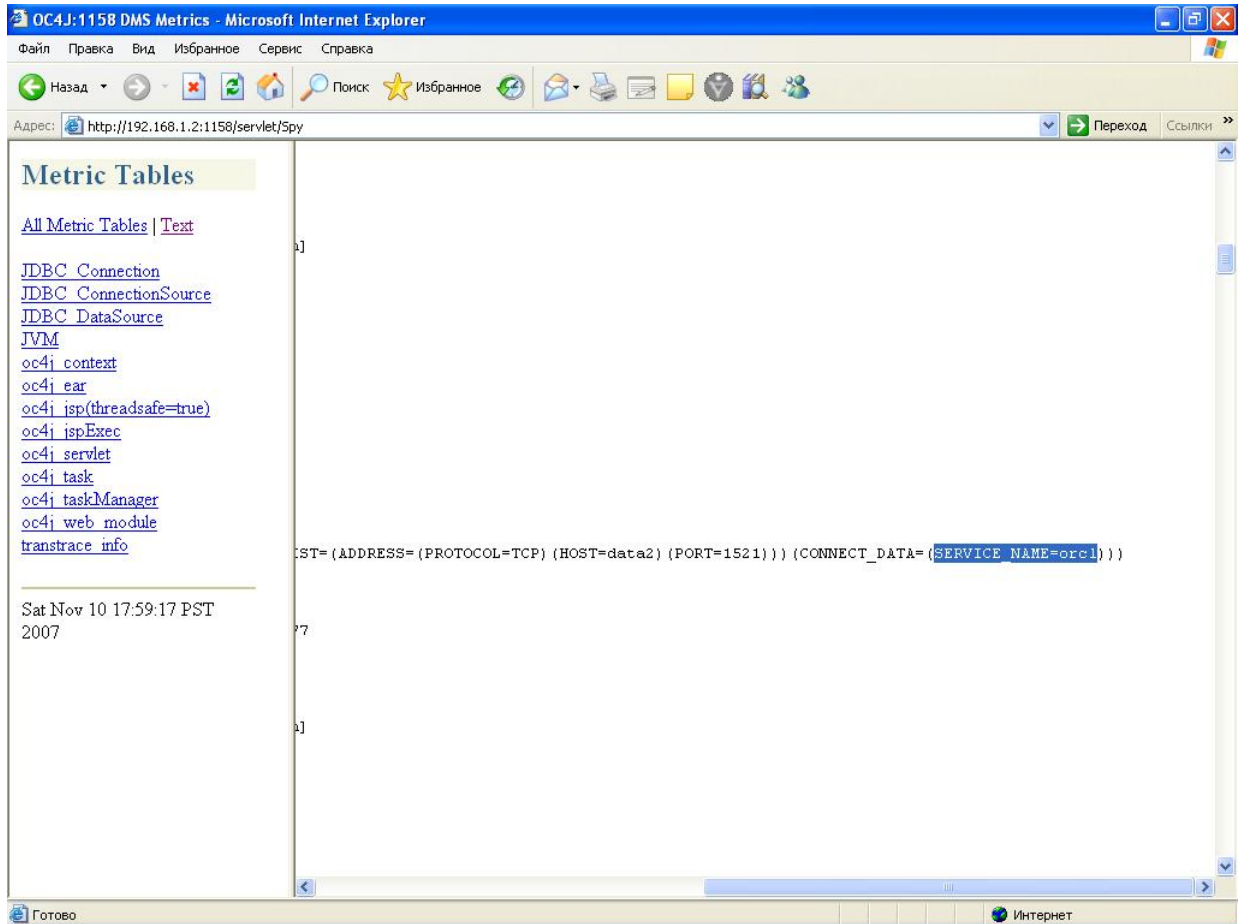
## Oracle Application Server

При установке СУБД Oracle версии 10g по умолчанию устанавливается компонент *Oracle Application Server Containers for J2EE*. Вместе с этим компонентом устанавливается несколько тестовых сервлетов; их список можно получить, обратившись по ссылке <http://hostname:5560/exmples/servlets>.



Список стандартных сервлетов

Существуют также сервлеты, на которые нет ссылок с главной страницы. Один из таких сервлетов – это сервлет `Spy`, который можно использовать для получения `SERVICE_NAME` базы данных. Для этого необходимо обратиться напрямую к этому сервлету по ссылке `http://hostname:5560/servlets/Spy`, в результате чего в одной из вкладок мы можем получить `SERVICE_NAME` базы данных.

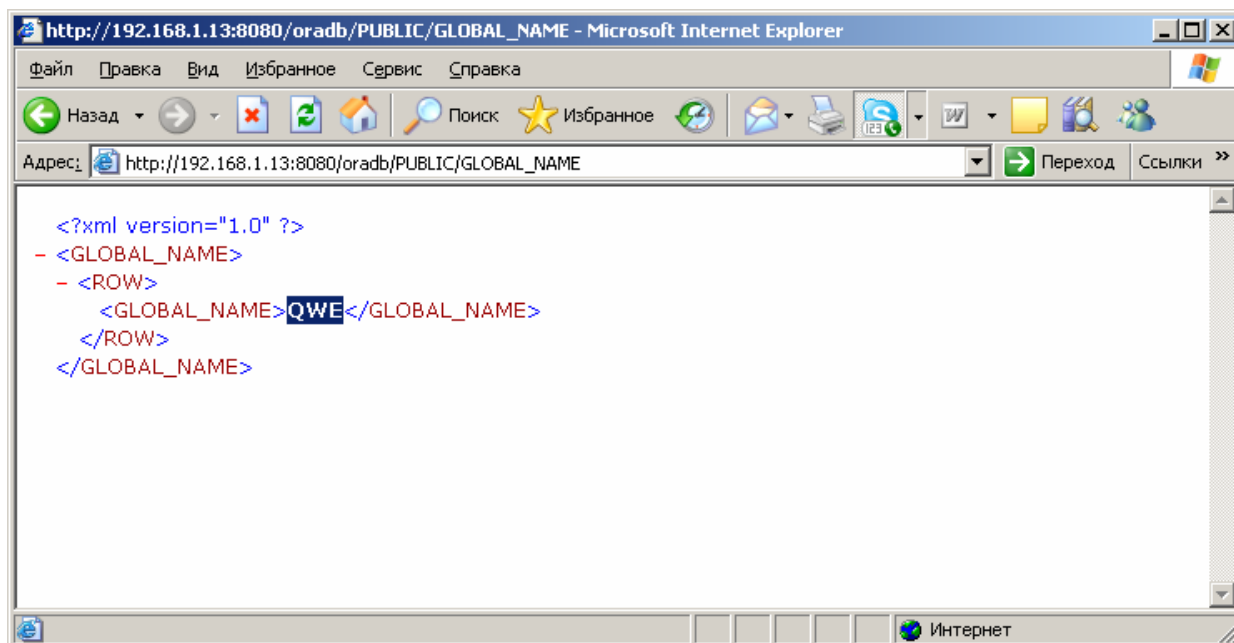


Получение SID через сервлет `Spy`

## Oracle XDB

---

В случае если у нас есть аутентификационные данные для подключения к СУБД, но не известен *SID* или *SERVICE\_NAME*, то можно обратиться к компоненту *Oracle XML DB Enterprise Edition httpd* (устанавливается по умолчанию в версии СУБД Oracle 9-ой и 10-ой ветки), который прослушивает порт *8080/tcp*. Для получения *SERVICE\_NAME* необходимо обратиться по адресу *http://hostname:8080/oradb/PUBLIC/GLOBAL\_NAME*.



Получение *SERVICE\_NAME* через Oracle XML DB

После чего, получив *SERVICE\_NAME* и зная аутентификационные данные пользователя, можно подключаться к СУБД через нормальный интерфейс.

## SAP

---

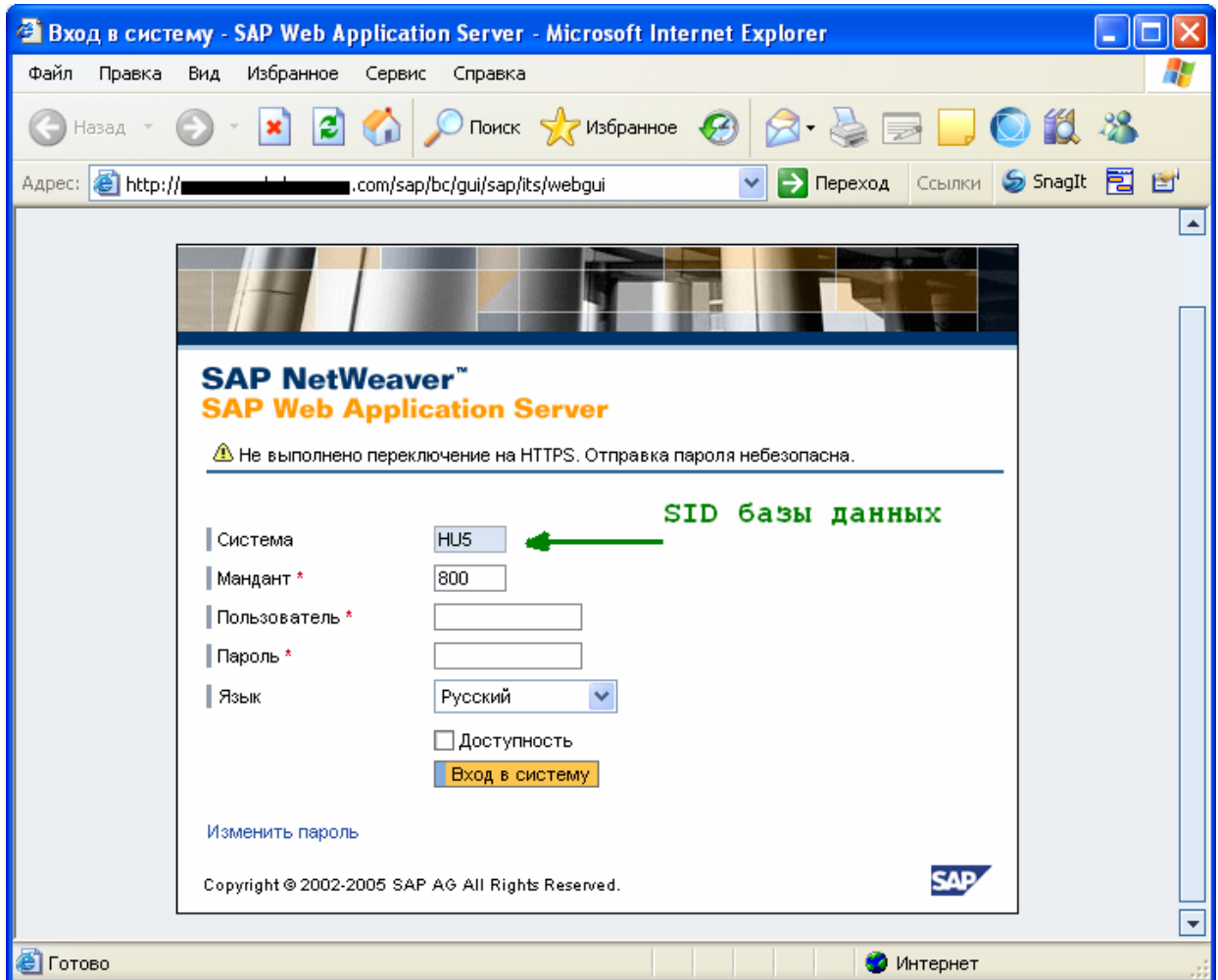
Часто СУБД Oracle устанавливается в связке с системой *SAP/R3*. Во время работ по исследованию системы SAP было обнаружено, что если в качестве базы данных для системы SAP R/3 используется СУБД Oracle то существует несколько способов узнать *SID* базы данных, часть из которых были придуманы и опробованы на реальных системах в процессе работ по анализу защищённости

### Стандартная страница администрирования SAP Web Application Server

---

Первые два способа узнать *SID* базы данных делаются через приложение *SAP Web Application Server*, доступ к которому по умолчанию обеспечивается путем подключения

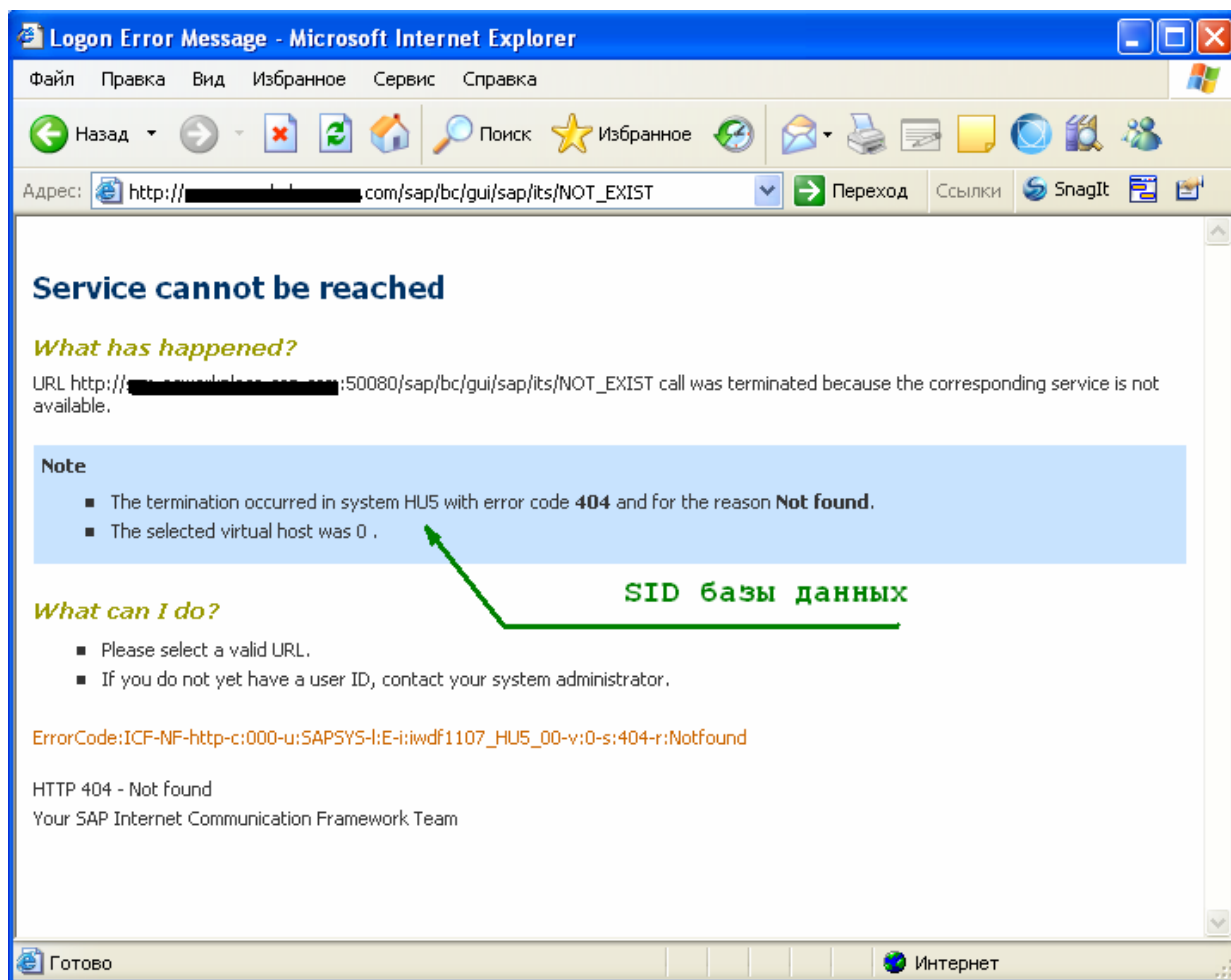
на порт *8000/tcp*. Для того, чтобы получить *SID* СУБД Oracle, необходимо обратиться к стандартной странице для администрирования *SAP* через веб-интерфейс, которая находится по адресу *http://hostname:8000/sap/bc/gui/sap/its/webgui*. При обращении по этому адресу выдается страница с запросом на ввод логина и пароля, на которой также содержится *SID* для подключения к базе данных.



*Получение SID через SAP Web Application Server*

## Запрос несуществующей страницы SAP Web Application Server

Другая возможность получения *SID* – запрос несуществующей страницы в приложении *SAP Web Application Server*. В этом случае сервер выдает страницу ошибки 404, в которой содержится *SID* базы данных.



Получение *SID* через ошибочный запрос к *SAP Web Application Server*

## SAP RFC

Для получения *SID* базы данных, также как и ряда другой полезной информации, можно воспользоваться утилитой *frccping*, которая поставляется с системой *SAP R/3* и используется для проверки работы протокола *RFC*. В случае если *RFC*-интерфейсы не заблокированы, то этот способ сработает.

```
./rfcping ahost=172.16.1.13 sysnr=00
```

#### SAP System Information

```
-----  
Destination          test2_NSP_00  
  
Host                 test2  
System ID            NSP  
Database             NSP  
DB host              test2  
DB system            ORACLE  
  
SAP release          700  
SAP kernel release   700  
  
RFC Protokoll        011  
Characters            1100 (NON UNICODE PCS=1)  
Integers              LIT  
Floating P.          IE3  
SAP machine id       560
```

В выводе утилиты мы видим, что System ID = NSP и база данных - Oracle

### SAP SID Bruteforcing

---

При назначении SID в системе SAP существует одно ограничение, что SID должен состоять из букв латинского алфавита и цифр и быть длиной не более 3х символов. Это означает, что его можно получить простым перебором, и на это уйдёт порядка 9-10 минут максимум. Этим способом можно воспользоваться даже если первые три способа не сработали (к примеру запрещён доступ к серверу приложений и закрыты RFC-интерфейсы).



## Получение SID при использовании дополнительных прав на атакуемом сервере и в сети

---

Выше были рассмотрены способы получения *SID* через сторонние приложения, для доступа к которым нам не требовалось никаких дополнительных прав. Если же ни один из перечисленных способов не дал успешного результата, то обладая определенными правами на атакуемом сервере или на “соседних” серверах сети можно также получить *SID* базы данных. Начнем с ситуации, когда у нас есть права на атакуемом сервере или установленных на нем приложениях.

### Получение SID при использовании дополнительных прав на атакуемом сервере

---

Ниже будут представлены три варианта получения *SID* при наличии доступа к различным сервисам атакуемого сервера:

- Получение *SID*, имея учетную запись в ОС, на которой установлена СУБД;
- Получение *SID*, имея учетную запись на *FTP* сервере в ОС, на которой установлена СУБД;
- Получение *SID*, имея учетную запись в *MsSQL* сервере в ОС, на которой установлена СУБД.

### Получение SID при наличии учетной записи в ОС, на которой установлена СУБД

---

Все предельно просто в случае, если пользователь, под именем которого мы подключились к серверу, имеет права на чтение файлов из директории `$(ORACLE_HOME)/NETWORK/admin`, т.к. *SID* можно получить из конфигурационного файла `tnsnames.ora`. Этот файл предназначен для определения сетевого имени сервиса, по которому можно обращаться к БД, и хранит такие данные, как *SID* или *SERVICE\_NAME* базы данных.

### Получение SID при наличии учетной записи на ftp-сервере

---

В случае если у нас нет аккаунта, предоставляющего удаленный доступ на атакуемый сервер, но есть аккаунт на доступ к *ftp*-сервису, установленному на этот сервер, то это дает возможность получения *SID* в случае, если *ftp*-аккаунт имеет доступ на чтение на директорию `$(ORACLE_HOME)`.

Для получения *SID* мы можем прочитать файл `tnsnames.ora`, как указано в предыдущем разделе. Если доступ на чтение этого файла запрещен, что часто рекомендуется в документах по защите СУБД Oracle, то *SID* можно получить через список директорий. В различных версиях СУБД пути несколько отличаются. Ниже будут

приведены три пути, по которым можно найти *SID* базы данных на примере СУБД Oracle 10g R2.

Первый способ – это вывести список директорий папки  $\$ORACLE\_HOME\..\admin\$ :

```
C:\oracle\product\10.2.0\oradata >dir
```

Том в устройстве C не имеет метки.

Серийный номер тома: 8CFF-37FB

Содержимое папки C:\oracle\product\10.2.0\admin

```
21.09.2008  12:55    <DIR>          .
21.09.2008  12:55    <DIR>          ..
21.09.2008  12:55    <DIR>          ORCL102
```

Название директории *ORCL102* в данном случае является *SID*-ом базы данных.

Второй способ – это вывести список директорий папки  $\$ORACLE\_HOME\..\oradata\$ :

```
C:\oracle\product\10.2.0\oradata>dir
```

Том в устройстве C не имеет метки.

Серийный номер тома: 8CFF-37FB

Содержимое папки C:\oracle\product\10.2.0\oradata

```
21.09.2008  12:55    <DIR>          .
21.09.2008  12:55    <DIR>          ..
21.09.2008  12:55    <DIR>          ORCL102
```

Название директории *ORCL102* в данном случае является *SID*-ом базы данных.

И третий способ – вывести список директорий папки  $\$ORACLE\_HOME$ , содержащий папку, в названии которой будет фигурировать *IP*-адрес сервера и *SID*, разделенные символом нижнего подчеркивания.

Содержимое папки E:\oracle\product\10.2.0\db\_1

```
28.01.2008  18:07    <DIR>          .
28.01.2008  18:07    <DIR>          ..
28.01.2008  18:07    <DIR>          192.168.40.14_orcl102
28.01.2008  17:30    <DIR>          admin
28.01.2008  17:30    <DIR>          assistants
19.06.2008  16:53    <DIR>          BIN
```

В данном случае *SID*-ом базы данных является строка *ORCL102*.

## Получение SID при наличии учетной записи в СУБД MsSQL

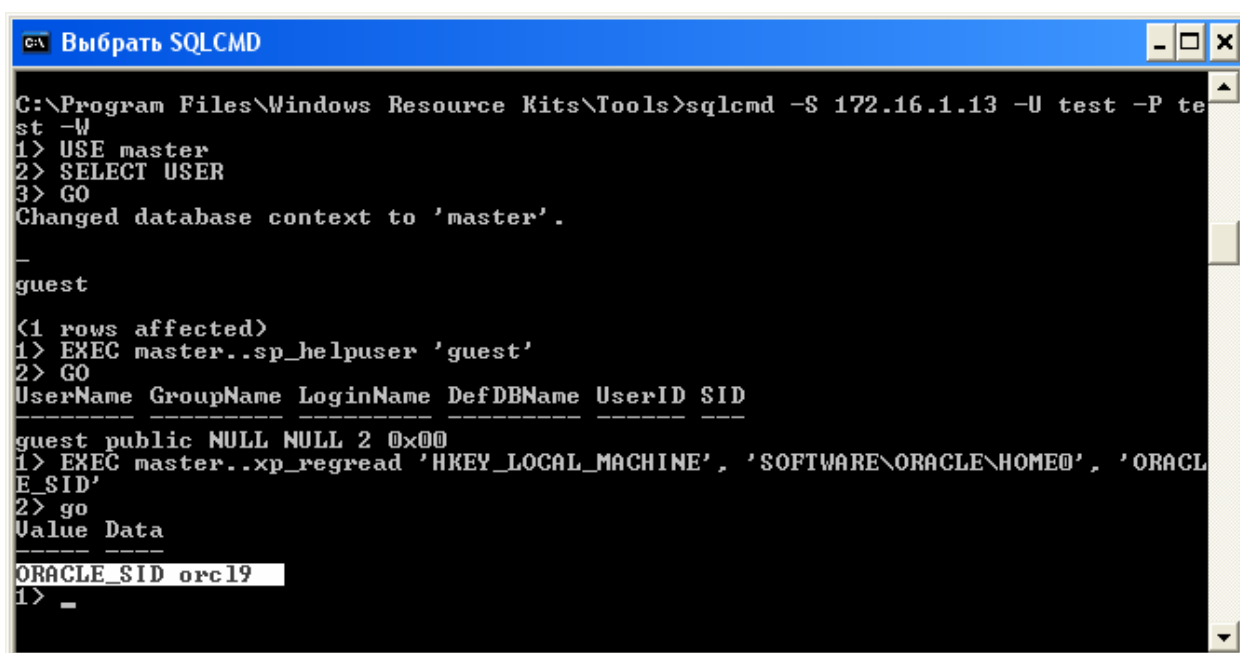
Часто на тестовых серверах и даже на рабочих системах на одном сервере устанавливается СУБД Oracle и СУБД MsSQL. Данная практика, как правило, не считается хорошей, но, тем не менее, такое не редко встречается.

В случае, когда мы имеем хотя бы какой-нибудь аккаунт в СУБД MsSQL (к примеру, мы удаленно перебрали пароль, или перехватили его по сети), установленной на атакуемом сервере, на котором также есть СУБД Oracle, мы можем получить *SID*, используя внутренние процедуры СУБД MsSQL. Для выполнения этих процедур достаточно иметь роль *public* на таблицу *master*, что по умолчанию имеет каждый созданный пользователь. Способы получения *SID* несколько отличаются для разных версий СУБД Oracle, но все они основаны на двух процедурах:

- *master.xp\_regread* – читает ключи реестра. При помощи нее можно прочитать *SID* СУБД Oracle, хранящийся в ключах реестра.
- *master.xp\_dirtree* – выводит дерево каталогов. При помощи нее можно прочитать название каталога, которое совпадает с *SID* базы данных (см. раздел «Получение *SID* при наличии учетной записи на ftp-сервере»).

К примеру, в версии СУБД Oracle 9g R2 *SID* хранится в реестре с известным ключом, и узнать его это можно следующим запросом:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SOFTWARE\ORACLE\HOME0',  
'ORACLE_SID'  
GO
```



```
C:\Program Files\Windows Resource Kits\Tools>sqlcmd -S 172.16.1.13 -U test -P test -W  
1> USE master  
2> SELECT USER  
3> GO  
Changed database context to 'master'.  
-  
guest  
<1 rows affected>  
1> EXEC master..sp_helpuser 'guest'  
2> GO  
UserName GroupName LoginName DefDBName UserID SID  
-----  
guest public NULL NULL 2 0x00  
1> EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SOFTWARE\ORACLE\HOME0', 'ORACLE_SID'  
2> go  
Value Data  
-----  
ORACLE_SID orcl9  
1> -
```

Получение *SID* из реестра через процедуры MsSQL

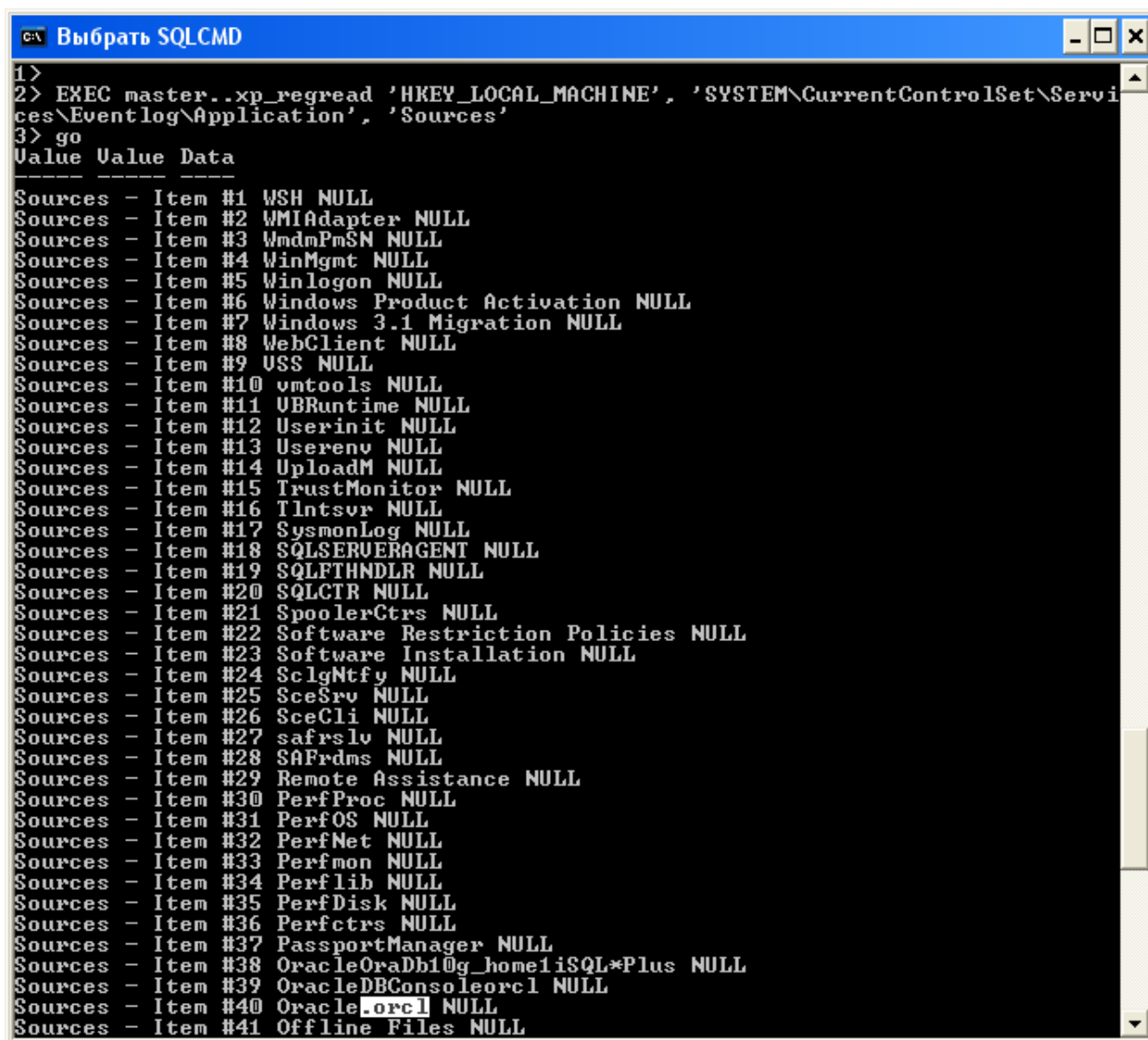
Для того чтобы получить *SID* в более поздних версиях СУБД Oracle, нам понадобятся более нестандартные способы.

## Получение *SID* через список сервисов в ОС

Главный сервис СУБД Oracle содержит в своем названии *SID* базы данных. Для получения списка сервисов можно выполнить следующую команду:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE',  
'SYSTEM\CurrentControlSet\Services\Eventlog\Application', 'Sources'  
GO
```

Ниже показан снимок экрана, на котором виден список сервисов.



```
1>  
2> EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SYSTEM\CurrentControlSet\Servi  
ces\Eventlog\Application', 'Sources'  
3> go  
Value Value Data  
-----  
Sources - Item #1 WSH NULL  
Sources - Item #2 WMIAdapter NULL  
Sources - Item #3 WdmPmSN NULL  
Sources - Item #4 WinMgmt NULL  
Sources - Item #5 Winlogon NULL  
Sources - Item #6 Windows Product Activation NULL  
Sources - Item #7 Windows 3.1 Migration NULL  
Sources - Item #8 WebClient NULL  
Sources - Item #9 USS NULL  
Sources - Item #10 vmtools NULL  
Sources - Item #11 UBRuntime NULL  
Sources - Item #12 Userinit NULL  
Sources - Item #13 Userenv NULL  
Sources - Item #14 UploadM NULL  
Sources - Item #15 TrustMonitor NULL  
Sources - Item #16 Tlntsvr NULL  
Sources - Item #17 SysmonLog NULL  
Sources - Item #18 SQLSERVERAGENT NULL  
Sources - Item #19 SQLFTHDLR NULL  
Sources - Item #20 SQLCTR NULL  
Sources - Item #21 SpoolerCtrs NULL  
Sources - Item #22 Software Restriction Policies NULL  
Sources - Item #23 Software Installation NULL  
Sources - Item #24 SclgNtfy NULL  
Sources - Item #25 SceSrv NULL  
Sources - Item #26 SceCli NULL  
Sources - Item #27 safrrslv NULL  
Sources - Item #28 SAFrdms NULL  
Sources - Item #29 Remote Assistance NULL  
Sources - Item #30 PerfProc NULL  
Sources - Item #31 PerfOS NULL  
Sources - Item #32 PerfNet NULL  
Sources - Item #33 Perfmon NULL  
Sources - Item #34 Perflib NULL  
Sources - Item #35 PerfDisk NULL  
Sources - Item #36 Perfctrs NULL  
Sources - Item #37 PassportManager NULL  
Sources - Item #38 OracleOraDb10g_home1iSQL*Plus NULL  
Sources - Item #39 OracleDBConsoleorcl NULL  
Sources - Item #40 OracleORCL NULL  
Sources - Item #41 Offline Files NULL
```

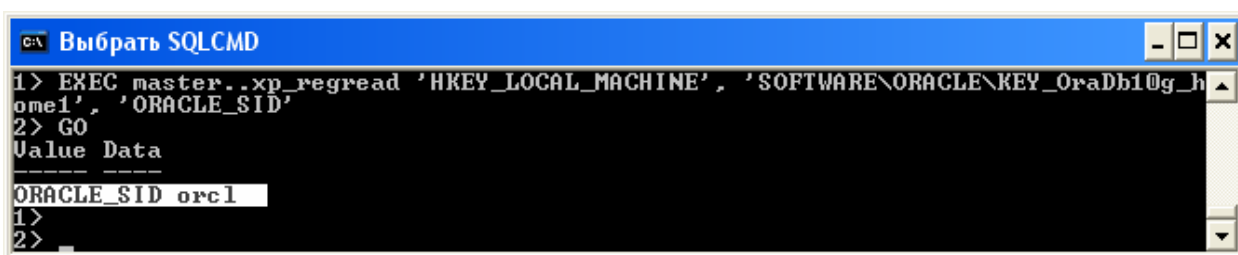
Получение списка сервисов через процедуры *MsSQL*

Под номером 40 указан главный сервис СУБД Oracle, который в своем имени содержит *SID*; в данном случае *SID* – “*ORCL*”. Этот способ действует в СУБД Oracle версии 10g R1, 10g R2 и 11g R1.

## Получение SID из ключа реестра HKLM\SOFTWARE\ORACLE

При установке СУБД Oracle в реестре создается папка с названием, зависящим от версии СУБД. В десятой версии – это *KEY\_Oradb10g\_home1*, в одиннадцатой – *KEY\_Oradb11g\_home1*. Для получения *SID* необходимо обратиться к ключу *ORACLE\_SID*, находящемуся в этой папке:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE',  
'SOFTWARE\ORACLE\KEY_Oradb10g_home1', 'ORACLE_SID'  
GO
```



Получение SID из реестра через процедуры MsSQL

## Получение SID через список директорий

Если приведенными выше способами получить *SID* не удалось, то можно попытаться узнать путь к домашней директории СУБД и вывести список ее поддиректорий, в котором можно обнаружить *SID* в виде *HostName\_SID*. Также можно подняться на уровень выше в папку *oradata* или *admin*, где будет директория, в которой хранятся файлы с базами данных; ее название совпадает с *SID*-ом.

В СУБД Oracle 11 g получить домашнюю директорию можно следующим запросом:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE',  
'SOFTWARE\ORACLE\ODP.NET\1.111.6.0', 'DllPath'  
GO
```

В десятой версии такой возможности нет; можно только попробовать стандартные пути, такие как:

```
C:\oracle\product\10.2.0\  
C:\oracle\product\10.1.0\  

```

## Пример получения SID через список директорий

```
EXEC master..xp_dirtree '$ORACLE_HOME'  
GO  
C:\Program Files\Windows Resource Kits\Tools>sqlcmd -S 192.168.30.102 -U test  
-P  
test -W  
1> EXEC master..xp_dirtree 'C:\oracle\product\10.1.0\oradata\  
2> go  
subdirectory depth  
-----  
1> EXEC master..xp_dirtree 'D:\oracle\product\10.1.0\oradata\  
2> go  
subdirectory depth  
-----  
1> EXEC master..xp_dirtree 'D:\oracle\product\10.2.0\oradata\  
2> go  
subdirectory depth  
-----  
1> EXEC master..xp_dirtree 'C:\oracle\product\10.2.0\oradata\  
2> go  
subdirectory depth  
-----  
orcl 1
```

В результате директория с базой данных была подобрана и найден *SID* – “ORCL”.

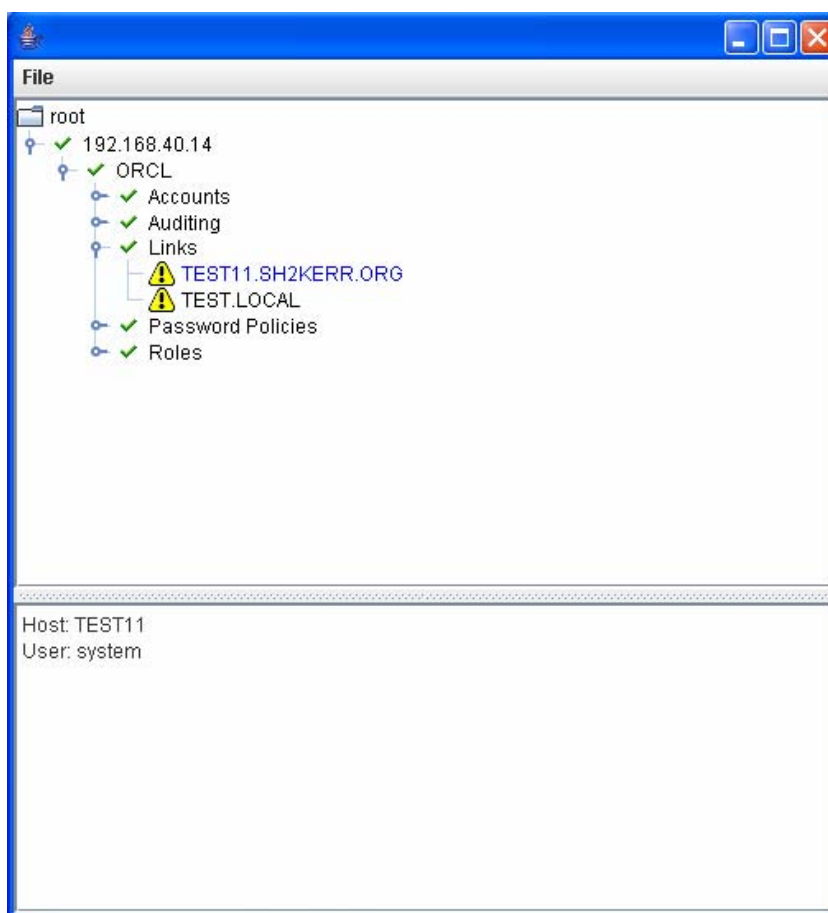
## Получение SID при использовании дополнительных прав в сети

В реальной ситуации приходится иметь дело не с отдельным сервером, а с информационной системой из большого количества серверов, в которой мы можем обладать некими дополнительными привилегиями. В данном разделе будут описаны способы получения *SID* из “соседних” серверов сети или при помощи перехвата сетевого трафика.

## Получение SID при наличии доступа к “соседним” СУБД в сети

Если у нас имеется доступ к какой либо из установленных в компании СУБД Oracle, то есть вероятность обнаружения в ней ссылок на другие СУБД, в которых будет фигурировать *SID*, а также, возможно, имя пользователя и пароль для подключения.

Для того, чтобы посмотреть, на какие СУБД есть ссылки и есть ли они вообще, можно воспользоваться утилитой *Oscanner*. В отчете, создаваемом программой, можно найти ссылки на другие базы данных, в которых будет *SID*, а также имя пользователя и, в некоторых случаях, пароль.



Получение SID через ссылки (Links) на другие СУБД

В нашем примере СУБД содержит две ссылки (Links) на сторонние базы, например, базу с *SID=TEST11*.

По статистике, примерно в 20% установленных СУБД присутствуют ссылки на другие СУБД, нередко с именами пользователей и паролями

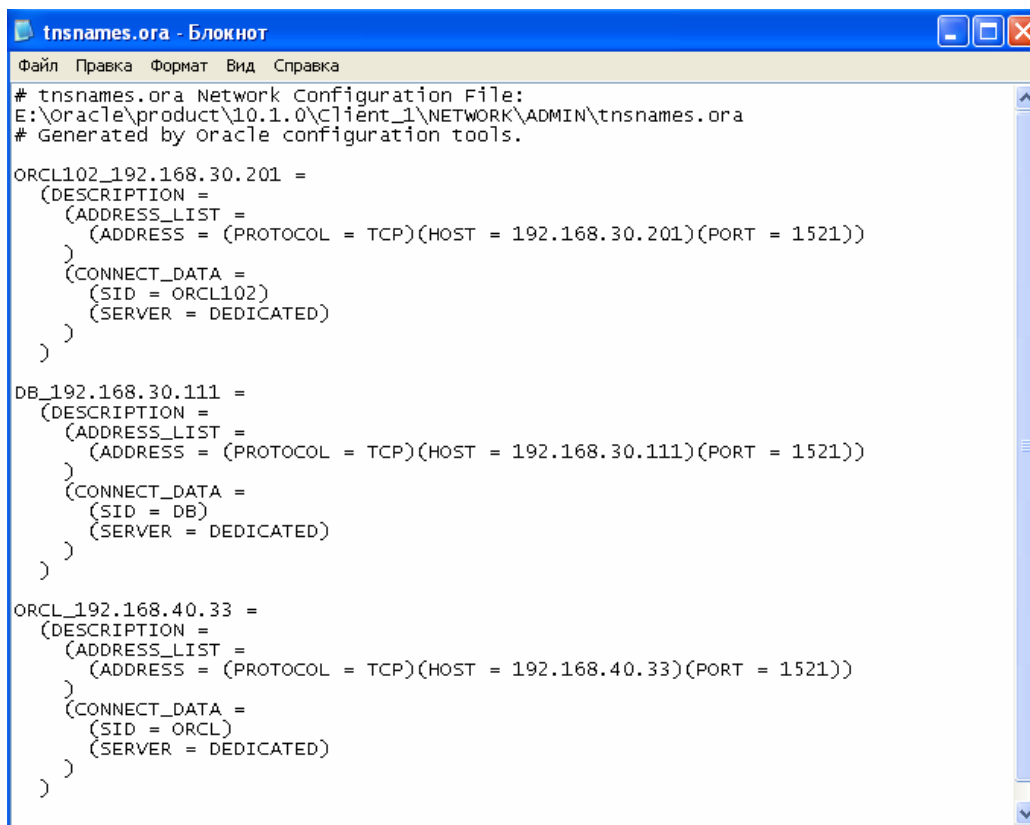
## Получение SID при наличии доступа к “соседним” серверам в сети

Если ранее нами был получен доступ к одному из серверов, находящихся в корпоративной сети, то есть вероятность обнаружить конфигурационные файлы, в которых будут присутствовать ссылки на другие СУБД компании, а в некоторых случаях и аутентификационные данные для подключения.

Обычно ссылки на СУБД, содержащие *SID*, хранятся в конфигурационном файле *tnsnames.ora*. Основной файл *tnsnames.ora* хранится в директории  $\$ORACLE\_HOME/NETWORK/admin$ . Если в главном файле ссылок не обнаружено, то следует поискать его устаревшие копии, возможно, ссылки будут в них. В ОС UNIX для поиска файлов *tnsnames.ora* можно воспользоваться следующей командой:

```
find / -name tnsnames*
```

Пример конфигурационного файла *tnsnames.ora* показан на рисунке ниже.



```
tnsnames.ora - Блокнот
Файл Правка Формат Вид Справка
# tnsnames.ora Network Configuration File:
E:\oracle\product\10.1.0\client_1\NETWORK\ADMIN\tnsnames.ora
# Generated by oracle configuration tools.

ORCL102_192.168.30.201 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.30.201)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = ORCL102)
      (SERVER = DEDICATED)
    )
  )

DB_192.168.30.111 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.30.111)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = DB)
      (SERVER = DEDICATED)
    )
  )

ORCL_192.168.40.33 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.40.33)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = ORCL)
      (SERVER = DEDICATED)
    )
  )
```

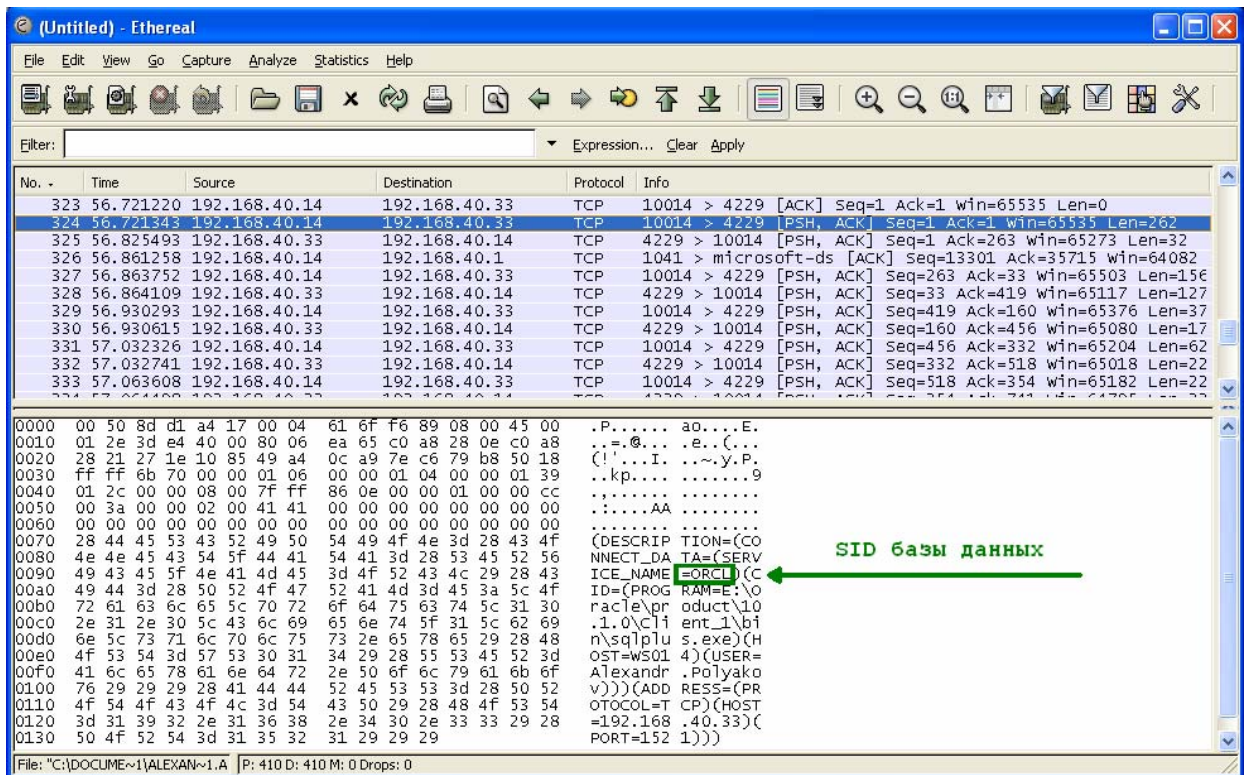
Конфигурационный файл *tnsnames.ora* с *SID*-ами

В приведенном примере мы видим в конфигурационном файле информацию о трех серверах с тремя различными *SID*. Тем самым, получив доступ к серверу, на котором стоит СУБД Oracle, имеем большой шанс получить *IP*-адреса и *SID* других СУБД, находящихся в информационной сети компании.

По статистике, примерно в 60 процентах случаев в файлах tnsnames.ora хранятся ссылки на другие СУБД

## Получение SID или SERVICE\_NAME прослушиванием сетевого трафика

Если в локальной сети, в которой находится сервер СУБД, есть возможность прослушать сетевой трафик между клиентами СУБД и сервером, мы можем перехватить SID в момент его передачи по сети, так как он передается в открытом виде. Для прослушивания данных, передаваемых по сети, можно воспользоваться любым доступным сетевым анализатором пакетов. На рисунке ниже можно наблюдать перехваченный пакет подключения к СУБД с IP-адресом 192.168.40.33 от клиента с IP-адресом 192.168.40.14. Он содержит в себе SID базы данных.



Перехват сетевого пакета в котором передается SERVICE\_NAME

## Заключение

---

В этом документе были собраны известные на данный момент способы получения *SID* базы данных, начиная от обычного перебора, и заканчивая поиском *SID* в сторонних приложениях. Как уже говорилось, этот шаг очень важен для получения доступа к СУБД.

Теперь, получив тем или иным способом *SID*, мы можем перейти к следующему этапу проникновения в СУБД – подбору паролей.

## Дополнительные материалы

---

1. Список стандартных SID

[http://www.red-database-security.com/whitepaper/oracle\\_default\\_sid.html](http://www.red-database-security.com/whitepaper/oracle_default_sid.html)

3. Backtrack Oracle Tutorial

[http://www.red-database-security.com/wp/backtrack\\_oracle\\_tutorial.pdf](http://www.red-database-security.com/wp/backtrack_oracle_tutorial.pdf)

3. Pentesting / Hacking Oracle databases with

<http://www.red-database-security.com/wp/itu2007.pdf>

4. Утилиты для подбора SID

<http://www.red-database-security.com/software/sidguess.zip>

[http://www.cqure.net/tools/osscanner\\_bin\\_1\\_0\\_6.zip](http://www.cqure.net/tools/osscanner_bin_1_0_6.zip)

<http://www.vulnerabilityassessment.co.uk/oak.htm>

[http://www.cqure.net/tools/SIDGuesser\\_win32\\_1\\_0\\_5.zip](http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip)

<http://inguma.sourceforge.net/index.php>