

UKOUG Windows SIG, September 25<sup>th</sup> 2007

# Oracle Security on Windows

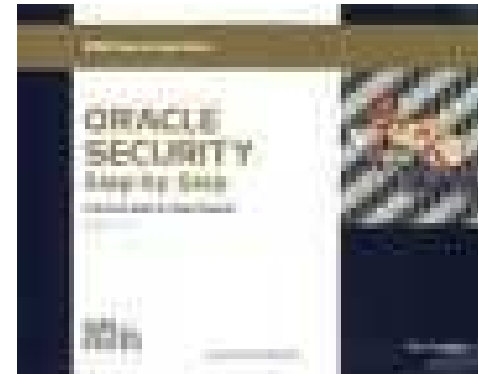
By

**Pete Finnigan**

Written Friday, 07 September 2007

# Introduction - commercial slide. ☹️

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases
- <http://www.petefinnigan.com>
- Consultancy and training available
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA)



# Agenda

- What is Oracle Security?
- Common security issues
- Windows / Unix differences issues
- Windows security
  - Information, bugs
- Windows security differences
- Auditing a database
- Hardening a database

# What is Oracle Security

- Performing a security audit of an Oracle database?
- Securely configuring an Oracle database?
- Designing a secure Oracle system before implementation?
- Using some of the key security features
  - Audit, encryption, RBAC, FGA, VPD...
- Oracle security is all of these
  - It is about creating a secure database
  - Storing critical / valuable data securely

# What's involved in securing data?

- Perform an Oracle Security health audit
- Design a secure installation
- Perform database hardening
  - New database or existing
- Choose and use Security features where relevant e.g.
  - encryption in the database for credit cards
  - TDE for secure data on disk
  - VPD to enable secure access to critical data

# Common Security Issues

- Installation issues
- Feature overload
- Functionality not needed in the database
- Configuration issues
- Operating system - Some real horrors often found
- Network issues – usually not much security
- Bugs / vulnerabilities - no easy fix

Some examples from real life!!

# Unix and Windows

- Is there a difference for securing Oracle on Windows or Unix? – anyone?
- In the database – very small differences in configuration
- Oracle networking – small differences
- Operating system – yes, biggest area but the issues are not dissimilar to Unix
- We will highlight some of the differences shortly

# Windows Oracle Security Info

- There is a lack of Windows specific information on Oracle security - example:
- SANS SCORE – 5 Windows from hundreds (<http://www.sans.org/score/oraclechecklist.php?portal=06e42a60647bfcf9d1afc5b9bdf932b3>)
- CIS Benchmark (v1.2 and 2.0.1) – 21 Windows from hundreds in 10g version - (<http://www.cisecurity.org/>)
- SANS Step-By-Step guide v2 – 4 from hundreds
- Oracle hackers Handbook – 2 pages from @120
- Oracle Privacy Security Auditing – no specific Windows issues



# General Oracle Security Info

- All is not lost; most Oracle security guidelines, information and tools are useful also for Windows
- Tools – <http://www.petefinnigan.com/tools.htm>
  - Who\_has scripts, CIS benchmark, Scuba, Metacortex, cquire, many more
- Papers, blogs, forums
- Checklists
  - CIS, SCORE, DoD Stig, Oracles hardening document
- Websites – petefinnigan, cquire, RDS, Argeniss, databasesecurity.com

# Windows Oracle Bugs

- As with Oracle security information specific Oracle security bugs on Windows are a small percentage of the whole
- Unlike the lack of information where the positive effect is that 95% of other information is still relevant with bugs most are still exploitable against Windows hosted Oracle ..☹
- ORA\_DBA / AcceptSecurityContex / share bug – see OHH
- Windows privilege escalation – NULL DACL bug  
<http://securityvulns.com/news/Oracle/Windows/PE.html>
- Windows directory traversal – extension of previous generic bugs
- 35 bugs on Securiteam – only 1 (possibly 2) are Windows specific
- Milw0rm.com – 4 Windows specific (?) from 27
- BugTraq – Hundreds of issues, difficult to check, possibly 1 in 20/30
- RDS – approx 40 exploits – only one confirmed for just Windows

# Windows Oracle bugs

- As with any exploit / bug; patching is generally the only solution – very few have workarounds
- The action for the DBA is therefore to
  - Be on a supported version of the database
  - Be on a supported platform – i.e. no Windows home edition
  - Be on the latest patch release
  - Ensure CPU's are applied as promptly as possible

# Windows Differences

- Don't install on domain controller (install on domain member/stand alone)
  - If domain services required use RSA and should it be a domain user account not domain admin
  - Create global group, remove from domain group
  - Remove domain users from Users group
- Windows has default Administrator account – rename it
- Oracle must be installed as Local Admin or SYSTEM (No) – Unix doesn't require admin – deny Logon

# Windows Differences (2)

- Limit AT jobs
- Oracle provides Windows Native Authentication
- Audit goes to the event viewer – use SQL to archive and purge and to filter and monitor
- File permissions
  - Remove Everyone group from ORACLE\_HOME  
ORACLE\_BASE
  - Allow Local Administrator full control
  - Remove Users permissions on Program Files\Oracle
  - Do not allow Oracle owner access to system tools

# Windows Differences (3)

- Possibility to stop port redirection in Windows –  
use\_shared\_socket=TRUE
- Set OSAUTH\_PREFIX\_DOMAIN= TRUE in registry to prevent OS account spoofing
- Don't allow Everyone group access to registry and limit access to Oracle keys/ hives to owner
- Windows tends to include additional protocol stacks
- Limited Possibility to rename ORA\_DBA
  - Don't allow any OS user membership of ORA\_DBA except Oracle DBA

# Windows Differences (Subtle)

- Excessive services enabled by default
  - Net meeting, messenger, auto update,
  - Web servers, fax, DHCP etc
  - Ensure OS is hardened first
- Shares – authentication bug
- virus software needed on Windows (Unix usually not a major issue)
- Maintenance access is usually harder
  - Local access or terminal services
  - SSH shell access (Unix) not available

# Auditing Oracle Databases

- We cannot cover a complete security audit here
- Default passwords, weak passwords, password management
- Audit settings
- Configuration settings
- File system – passwords exposed, ad hoc maintenance
- Shares – check for existence
- Confirm accounts used for software, Admin, Application / privileges
- Tendency for remote ops\$ to be used on Windows – check into this

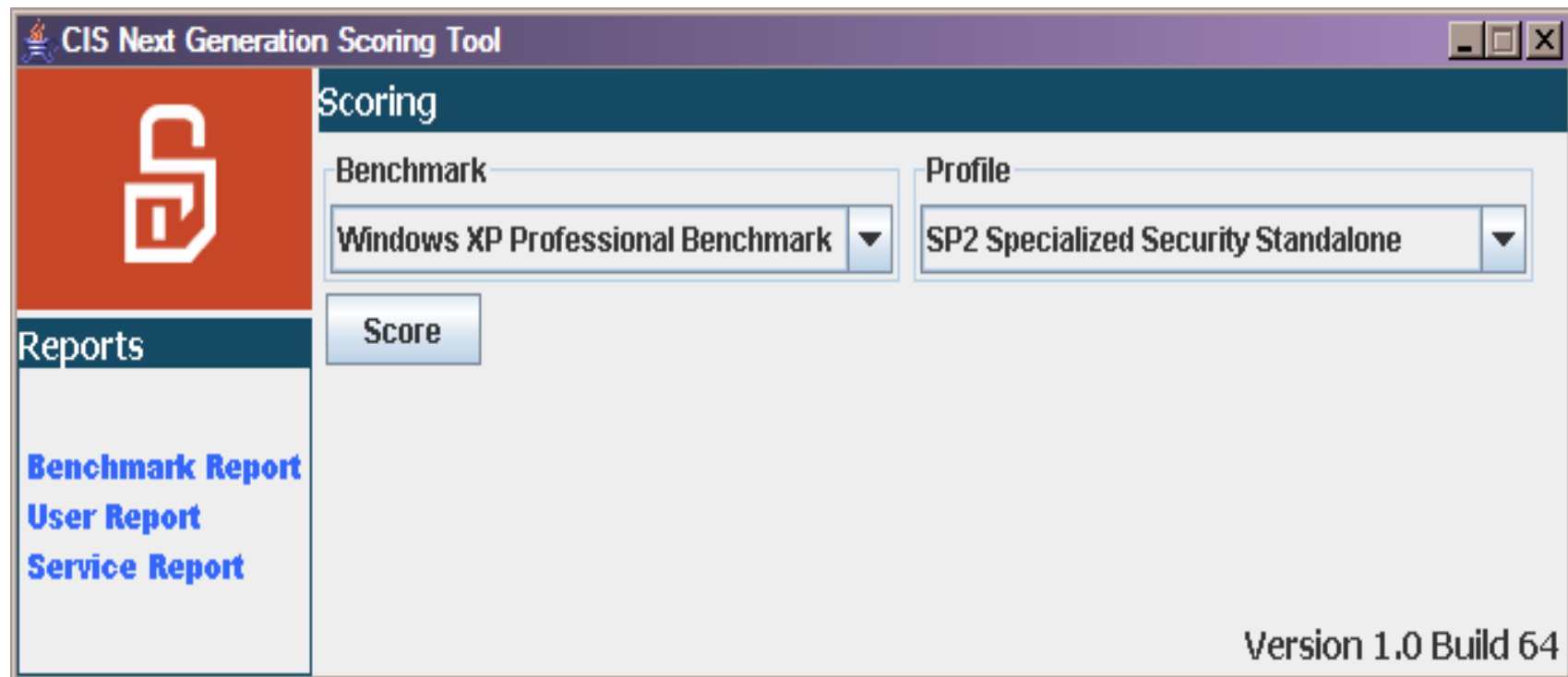


# Auditing an Oracle Database

- Windows security Checklists
  - CIS benchmarks for XP-SP1/2, Server 2003, Win 2000 (Std, Prof, server), NT
  - Windows tools – The CIS benchmarks are useful – others are available
- Oracle security checks
  - Most tools are windows centric – don't install them on the prod
  - Audit by hand
  - Audit using a free or commercial tool
  - Get professional help
- Oracle security checklists
  - use and work through
  - these are great resources to start with

# Windows OS Security Audit (1)

<http://www.cisecurity.org/>



# Windows OS Security Audit (2)

Compliance Validation Report - Microsoft Internet Explorer

Address: C:\Program Files\The Center for Internet Security\CIS NG Scoring Tool\results\20070921082001734+0100\reports\html\benchmark-report.html

Scan Time: 09/21/2007 08:20:39

Description	Items		Score	
	Passed	Failed	Actual	Max
<b>1 Service Packs and Security Updates</b>	1	0	20.000	20.000
1.1 Major Service Pack and Security Update Requirements	1	0	20.000	20.000
1.2 Minor Service Pack and Security Update Requirements	0	0	0.000	0.000
<b>2 Auditing and Account Policies</b>	8	14	8.125	20.000
2.1 Major Auditing and Account Policies Requirements	1	1	5.000	10.000
2.2 Minor Auditing and Account Policies Requirements	7	13	3.125	10.000
2.2.1 Audit Policy (minimums)	0	7	0.000	2.500
2.2.2 Account Policy	1	3	0.625	2.500
2.2.3 Account Lockout Policy	0	3	0.000	2.500
2.2.4 Event Log Settings – Application, Security, and System Logs	6	0	2.500	2.500
2.2.4.1 Application Log	2	0	0.833	0.833
2.2.4.2 Security Log	2	0	0.833	0.833
2.2.4.3 System Log	2	0	0.833	0.833
<b>3 Security Settings</b>	28	44	6.280	20.000
3.1 Major Security Settings	1	2	3.333	10.000
3.2 Minor Security Settings	27	42	2.946	10.000
3.2.1 Security Options	26	22	2.708	5.000
3.2.2 Additional Registry Settings	1	20	0.238	5.000
<b>4 Additional Security Protection</b>	29	42	8.991	20.000
4.1 Available Services	12	7	3.158	5.000

# Windows OS Security Audit (3)

Compliance Validation Report - Microsoft Internet Explorer

Address: file:///C:/Program%20Files/The%20Center%20for%20Internet%20Security/CIS%20NG%20Scoring%20Tool/results/20070921082001734+0100/reports/html/benchmark-report.html#Group3

3 Security Settings

**3.1 Major Security Settings**

3.1.1 Network Access: Allow Anonymous SID/Name Translation:	Unknown
3.1.2 Network Access: Do not allow Anonymous Enumeration of SAM Accounts	Passed
3.1.3 Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares	Failed
3.1.4 Data Execution Protection	Failed

**3.2 Minor Security Settings**

**3.2.1 Security Options**

3.2.1.1 Accounts: Administrator Account Status	Not Tested
3.2.1.2 Accounts: Guest Account Status	Passed
3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only	Passed
3.2.1.4 Accounts: Rename Administrator Account	Failed
3.2.1.5 Accounts: Rename Guest Account	Failed
3.2.1.6 Audit: Audit the access of global system objects	Passed
3.2.1.7 Audit: Audit the use of backup and restore privilege	Passed
3.2.1.8 Audit: Shut Down system immediately if unable to log security alerts	Not Tested
3.2.1.9 DCOM: Machine Access Restrictions	Not Tested
3.2.1.10 DCOM: Machine Launch Restrictions	Not Tested
3.2.1.11 Devices: Allow undock without having to log on	Failed
3.2.1.12 Devices: Allowed to format and eject removable media	Passed
3.2.1.13 Devices: Prevent users from installing printer drivers	Failed
3.2.1.14 Devices: Restrict CD-ROM Access to Locally Logged-On User Only	Passed
3.2.1.15 Devices: Restrict Floppy Access to Locally Logged-On User Only	Passed
3.2.1.16 Devices: Unsigned Driver Installation Behavior	Passed
3.2.1.17 Domain Controller: Allow Server Operators to Schedule Tasks	Not Tested
3.2.1.18 Domain Controller: LDAP Server Signing Requirements	Not Tested
3.2.1.19 Domain Controller: Refuse machine account password changes	Not Tested

# What to audit (First?)

- Perform a password audit – use a tool such as orabf – <http://www.toolcrypt.org/index.html?orabf>
- File system
  - look for passwords
  - permissions
- Audit basic configuration
  - Parameters
  - User accounts that exist
  - Privileges on objects
  - Privileges assigned to users
- Use one of the free tools – CIS, OScanner, Scuba

# Sample Audit Checks using SCUBA

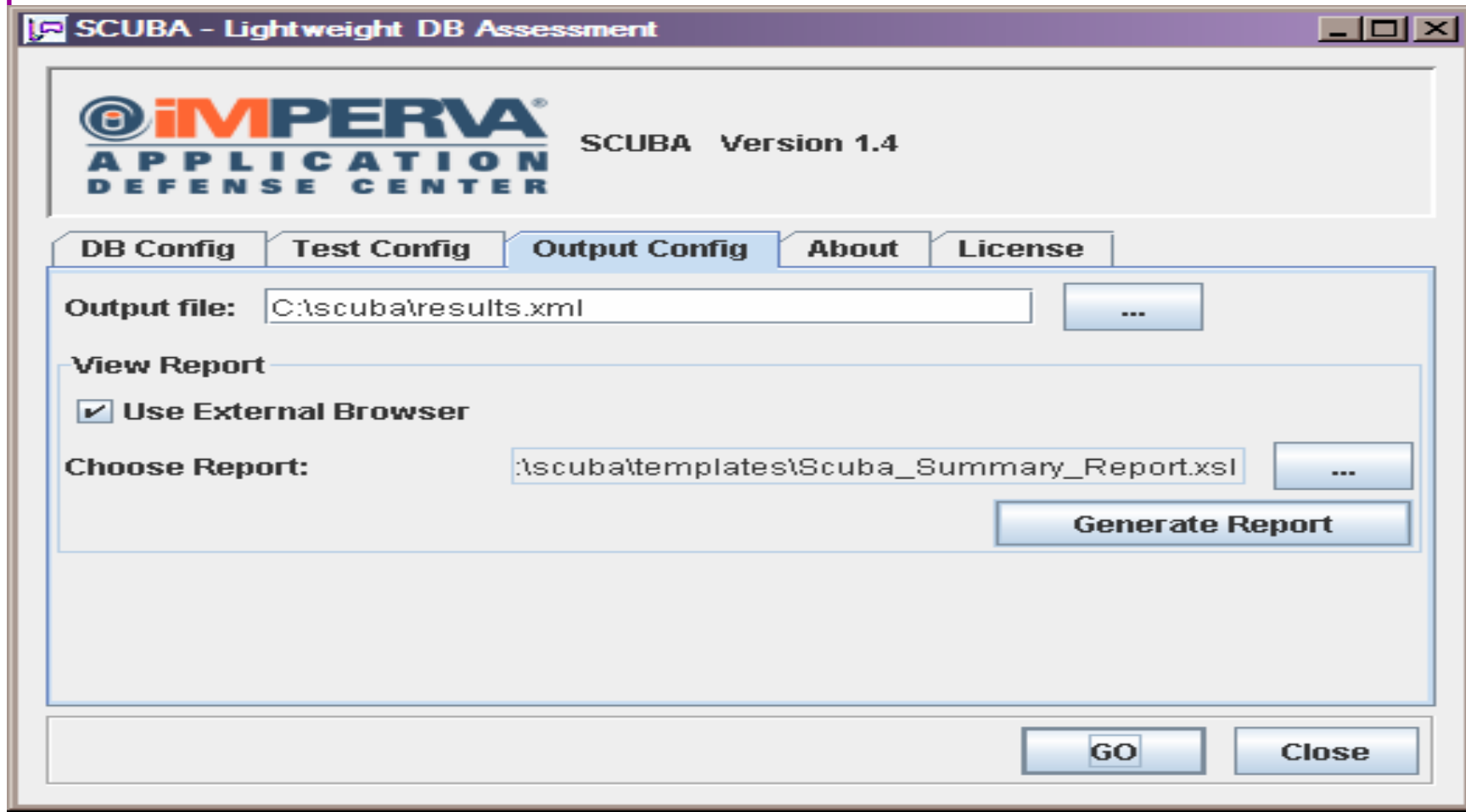
[http://www.imperva.com/application\\_defense\\_center/scuba/](http://www.imperva.com/application_defense_center/scuba/)

The screenshot shows the SCUBA - Lightweight DB Assessment application window. The title bar reads "SCUBA - Lightweight DB Assessment". The main area features the IMPERVA APPLICATION DEFENSE CENTER logo and "SCUBA Version 1.4". Below the logo are five tabs: "DB Config", "Test Config", "Output Config", "About", and "License". The "DB Config" tab is active, showing the following fields:

- DB Type: Oracle (dropdown menu)
- Host: oracle\_hack\_box
- Port: 1522
- DB Name: ora10gr2
- Windows Authentication
- User: system
- Password: \*\*\*\*\*

At the bottom of the "DB Config" section is a "Test Connectivity" button. A tooltip is visible over the "Test Connectivity" button, displaying the text "Type account number to be used for databas". At the bottom of the window are two buttons: "GO" and "Close".

# Sample Audit Checks using SCUBA



# Sample Audit Checks using SCUBA

Scuba by Imperva Database Assessment Report

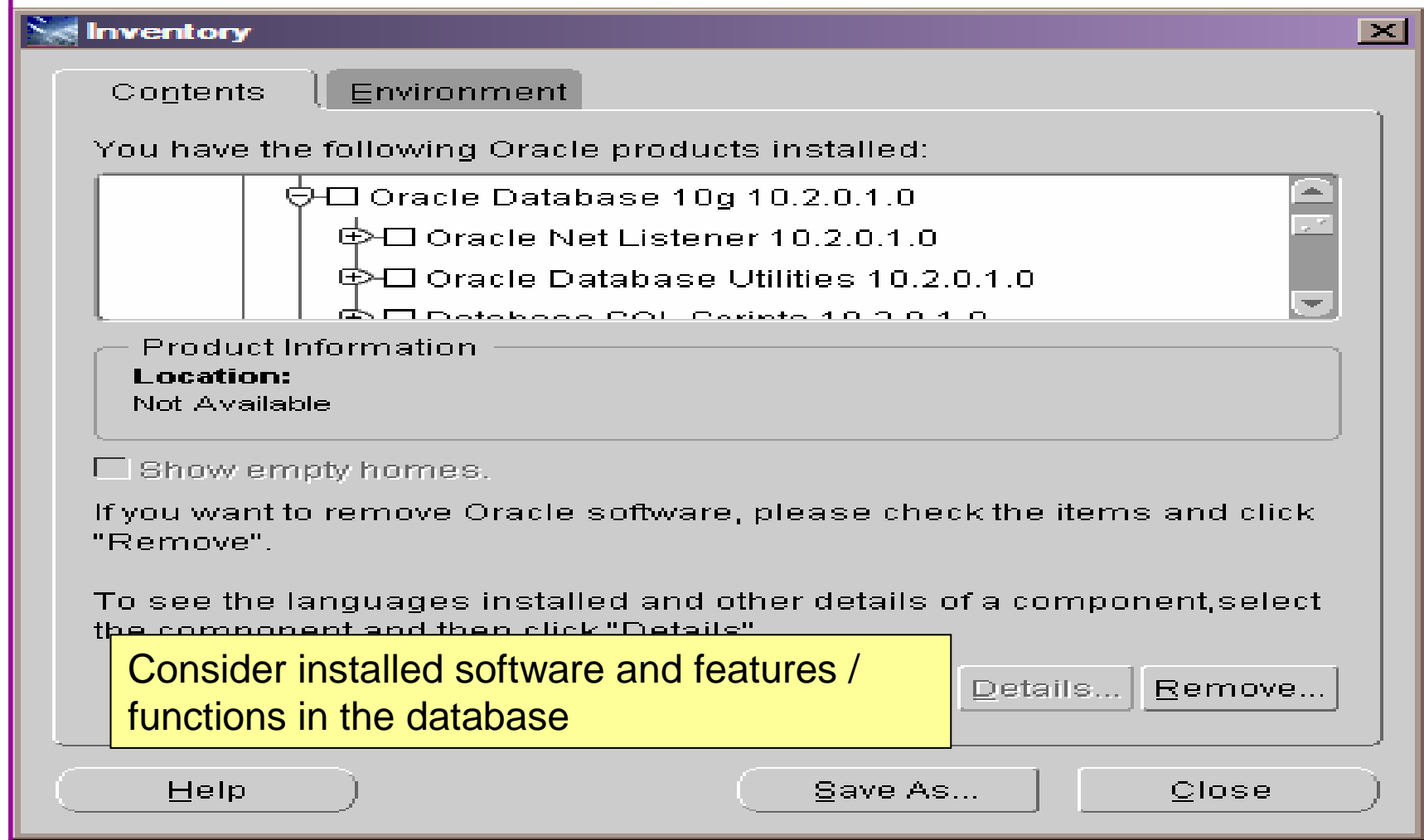
Test	Severity	Result
Package Privilege: Execute UTL_FILE granted to PUBLIC role	High	Failed
Unrestricted access to listener	High	Failed
Profile resource value doesn't meet security policy: FAILED_LOGIN_ATTEMPTS	High	Failed
Remote login password file not disabled	High	Failed
Package Privilege: Execute SYS.DBMS_EXPORT_EXTENSION granted to PUBLIC role	High	Failed
Latest Oracle database patch set not applied	High	Passed
BFILENAME buffer overflow	High	Passed
Critical Patch Update - January 2005	High	Passed
Database link buffer overflow	High	Passed
EXTPROC buffer overflow	High	Passed
FROM_TZ buffer overflow	High	Passed
NSPTCN buffer overflow	High	Passed
NUMTODSINTERVAL buffer overflow	High	Passed
NUMTOYMINTERVAL buffer overflow	High	Passed
Alert #68	High	Passed
SERVICE_NAME buffer overflow	High	Passed
SSL vulnerabilities	High	Passed
TIME_ZONE buffer overflow	High	Passed



# Hardening

- Reduce the features and functions installed – OS and DB
- Harden the OS – covered above
- Review RBAC for all users
- Remove defaults – settings, users, passwords
- Decide on secure configuration settings
- Clean up
- Create processes and policies to ensure secure data going forward

# Features



# RBAC

- Review the complete RBAC model
- Understand default schemas installed and why
- Understand the application schemas
  - Privileges, objects, resources
- Understand which accounts are Admin / user / Application Admin etc
  - Consider privileges, objects, resources
- lock accounts if possible
  - reduce attack surface

# Defaults

- Defaults are one of the biggest issues in Oracle
- Most default accounts in existence
- Tens of thousands of public privileges granted
- Many default roles and privileges
  - Many application developers use default Roles unfortunately
- Reduce the Public privileges as much as possible
- Do not use default accounts
- Do not use default roles including DBA
- Do not use default passwords

# Database Configuration

- Default database installations cause some weak configurations
- Review all
  - configuration parameters
  - File permissions
- Some examples
  - No audit configuration by default (fixed in 10gR2 for new installs)
  - No password management (fixed in 10gR2 new installs)

# Clean Up

- This is the security killer in most systems I see
- Often file systems include
  - Scripts with passwords
  - Use tools such as
    - Oracle Password Repository
    - Mkstore from Oracle
    - DBMS\_JOBS, DBMS\_SCHEDULER
    - OS authenticated users under certain circumstances
- Clean up
  - ad-hoc scripts
  - Maintenance evidence
  - Trace files
  - Audit logs.....

# Create a Policy

- Perform an Oracle database audit
- Define what the key/critical issues are
- Determine / decide what to fix
- Work on a top 20 basis and cycle (This is effective for new hardening)
- Create a baseline standard
  - A document
  - Scripts – maybe for BMC
  - Commercial tool such as AppDetective

# Decide what to fix

- My extensive experience of auditing Oracle databases is that there are
  - Usually a lot of security issues
  - Usually a lot are serious – i.e. server access could be gained if the issue is not plugged
  - There are constraints on the applications, working practice, practicality of fixing
- The best approach is to classify issues
  - Must fix now (really serious), fix as soon as possible, fix when convenient, maybe more
- Create a top ten / twenty approach



# Enable Database Auditing

- Every database I have ever audited has no database audit enabled – ok a small number do, but usually the purpose is for management / work / ??? but not for audit purposes.
- Core audit doesn't kill performance
  - Oracle have recommended 24 core system audit settings since 10gR2 – these can be enabled and added to in earlier databases
  - Avoid object audit unless you analyse access trends then its Ok
- On Windows audit directed to the OS goes to the event Log
- By default all SYSDBA connections are audited – also to the event log on Windows
- VBScript / SQL can be used to access the event log

# Conclusions

- Securing Oracle on Windows is not drastically different to Unix
- Most documentation / checklists / tools are valid for Windows
- Most Oracle security tools are available on Windows – don't install them on prod!
- The key techniques are the same
- Database security is about the data and Oracle isolates the OS quite well
- Don't forget to harden the OS though!

```
create or replace function log_start(fv_path
return utl_file.file_type is
  lv_fptr utl_file.file_type:=null;
  lv_module varchar2(100):='log_start';
begin
  Oracle Security Expertise
dbms_output.disable;
```

## Any Questions?

## Contact - Pete Finnigan

PeteFinnigan.com Limited

9 Beech Grove, Acomb

York, YO26 5LD

Phone: +44 (0) 1904 791188

Mobile: +44 (0) 7742 114223

Email: [pete@petefinnigan.com](mailto:pete@petefinnigan.com)