PeteFinnigan.com Limited

Oracle Security Expertise

White-Hats 2008, London, September 26th 2008

Oracle Security Masterclass

By

Pete Finnigan

Written Friday, 25th September 2008

Why Am I Qualified To Speak

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases providing consultancy and training
- http://www.petefinnigan.com
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland and more)
- Member of the Oak Table Network

Agenda

- Part 1 - Overview of oracle security
  - How and why do hackers steal data
  - What are the issues
  - How are databases compromised
- Part 2 - Main body of the master class
  - Conducting a security audit of a database
  - What to look for
  - Examples
  - How to look
  - What tools
- Part 3 - Conclusions
  - What to do when you have a list of problems to fix
  - Deciding what to fix, how to fix, can you fix
  - Basic hardening – i.e. these are the things you should really fix

Overview

- What do I want to achieve today
- Its high level, an audit can take days so we cannot cover it all in around in the short time we have
- Anyone can perform an audit but be realistic at what level
- I want to teach basic ideas
- **Ask questions any time you would like to**
- Try out some of the tools and techniques yourself later on

What Is Oracle Security?

- **It is about creating a secure database and storing critical / valuable data securely**
- To do this Oracle security is about all of these:
  - 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…

Internal Or External Attacks

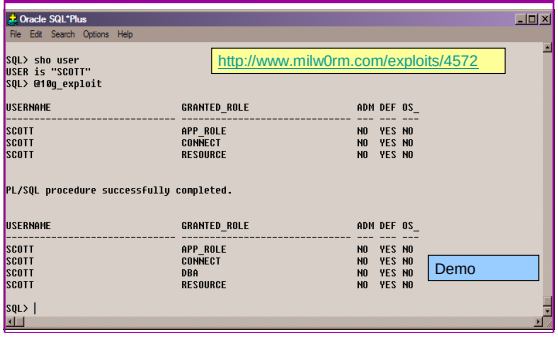
- Internal attacks are shown to exceed external attacks in many recent surveys, Delloite surveys the top 100 finance institutes
- The reality is likely to be worse as surveys do not capture all details or all companies
- Data is often the target now not system access; this could be for identity theft to clone identities
- With Oracle databases external attacks are harder and are likely to involve
  - application injection or
  - Buffer Overflow or
  - Protocol attacks
- Internal attacks could use any method for exploitation. The issues are why:
  - True hackers gain access logically or physically
  - Power users have too many privileges
  - Development staff, DBA's
  - **Internal staff have access already!!**

How Easy Is It To Attack?

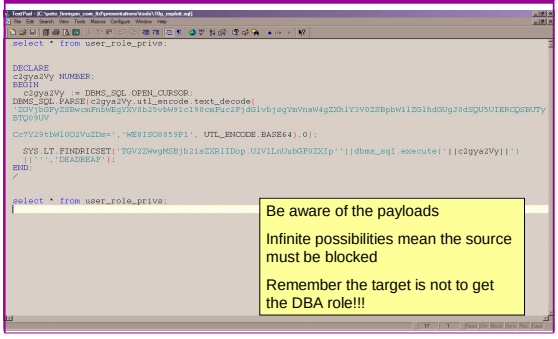
- Many and varied attack vectors
- Passwords are the simplest – find, guess, crack
- Bugs that can be exploited
- SQL injection
- Denial of Service
- Exploit poor configuration – access OS files, services
- Network protocol attacks
- Buffer overflows, SQL buffer overflows
- Cursor injection
- More ?

Most sites are here not below (well below as well but that doesn't matter if they are at the top of the list)

Example Exploit



Example Exploit (2)



Realistic Hacking Of Databases

- The target is data not the DBA role
- The exploits we have just seen work but stealing data is much more "real"
- Its easy
- It doesn't involve complex techniques
- What do you think happens?

Demonstration

- Hacking an Oracle database to "steal"
- 15 minutes or so

Demo

What Are The Problems Here?

- Access is available to the database
- Credentials are guessable
- Default accounts have access to critical data
- Critical data is easy to find
- Poor, weak encryption and protection used
- This is reality, this is what Oracle database security REALLY looks like!!

Stay Ahead Of The Hackers

- When deciding what to audit and how to audit a database you must know what to look for:
  - Existing configuration issues and security vulnerabilities are a target
  - Remember hackers don't follow rules
  - Combination attacks (multi-stage / blended) are common
- The solution: Try and think like a hacker – be suspicious

The Basic Tenets Of Oracle Security

- Reduce the version / installed product to that necessary
- Reduce the users / schemas
- Reduce and design privileges to least privilege principal
- Lock down direct access
- Lock down basic configurations
- Audit
- Clean up

The Access Issue

- A database can only be accessed if you have three pieces of information
  - The IP Address or hostname
  - The Service name / SID of the database
  - A valid username / password

11gR1 has broken this!!

- Lots of sites I see:
  - Deploy tnsnames to all servers and desktops
  - Allow access to servers (no IP blocking)
  - Create guessable SID/Service name
  - Don't change default passwords or set weak ones
  - No form of IP blocking and filtering
- Do not do any of these!

Part 2 – Conducting A Database Audit

- Planning and setting up for An Audit
- Selecting a target
- Interview key staff
- Versions, patches and software
- Enumerate users and find passwords
- File system analysis
- Network analysis
- Database configuration

Planning An Audit

- Create a simple plan, include
  - The environments to test
  - The tools to use
  - Decide what to test and how "deep"
  - The results to expect
  - Looking forward
  - What are you going to do with the results?
- Don't create "war and peace" but provide due diligence, repeatability

The Environment To Be Audited

- This is a key decision
- Which environment should be tested?
- A live production system **MUST** be chosen
- Some elements can be tested in other systems
  - i.e. a complete clone (standby / DR) can be used to assess configuration
  - The file system and networking and key elements such as passwords / users must be tested in production
- Choose carefully

Building A Toolkit

- There are a few standalone tools available
- I would start with manual queries and simple scripts such as:
  - www.petefinnigan.com/find_all_privs.sql
  - www.petefinnigan.com/who_has_priv.sql
  - www.petefinnigan.com/who_can_access.sql
  - www.petefinnigan.com/who_has_role.sql
  - www.petefinnigan.com/check_parameter.sql
- Hand code simple queries as well

Checklists – Basis For The Audit

- There are a number of good checklists to define what to check:
- CIS Benchmark - http://www.cisecurity.org/bench_oracle.html
- SANS S.C.O.R.E - http://www.sans.org/score/oraclechecklist.php
- Oracle's own checklist - http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database_20071108.pdf
- DoD STIG - http://iase.disa.mil/stigs/stig/database-stig-v8r1.zip
- Oracle Database security, audit and control features – ISBN 1-893209-58-X

Keep It Neutral

- All actions must be read only
- Don't stop / start the database
- Don't affect the business
- Read only must also not be heavy queries
- Hands-on and not automated is better
- Remember some things cannot be automated well
- Automated tools have issues

Decide The Scope Of The Test

- What is to be tested (what checks to use)?
- The checklists provide extensive lists of checks
- My advice: keep it simple to start with
  - Concentrate on the "LOW FRUIT"
  - Key issues
    - Passwords
    - Simple configuration issues
    - RBAC issues

Results?

- Before you start you should asses what you expect as results
- This drives two things:
  - The scale of the test
  - What you can do with the results
- It should help derive
  - What to test for
  - What to expect
- If you decide in advance its easier to cope with the output (example: if you do a test in isolation and find 200 issues, its highly unlikely anyone will deal with them)

An interesting concept!

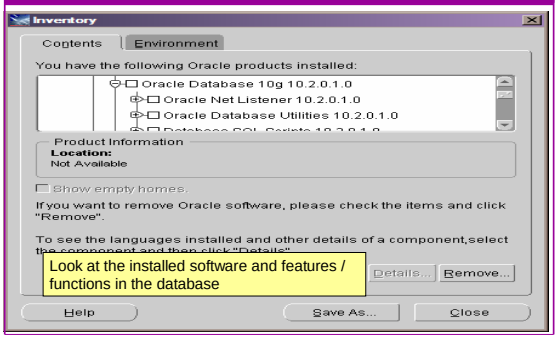
Interview Key Staff

- Perform interviews with key staff
  - DBA
  - Security
  - Applications
- Understand
  - Policies
  - Backups
  - How different groups of staff use and access the database
- The checklists include interview questions
- Prepare an interview list to work to (see the CIS benchmark for examples -

Line up the key people in advance

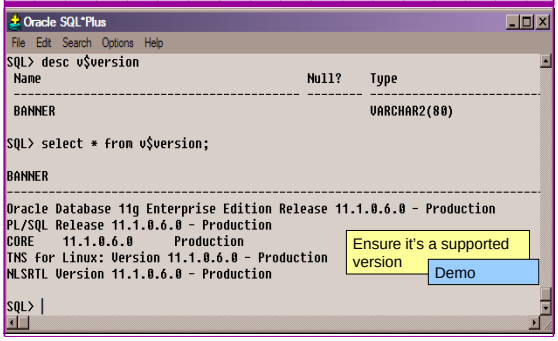
Don't base only on internal policies

Software Installed



Look at the installed software and features / functions in the database

Database Version



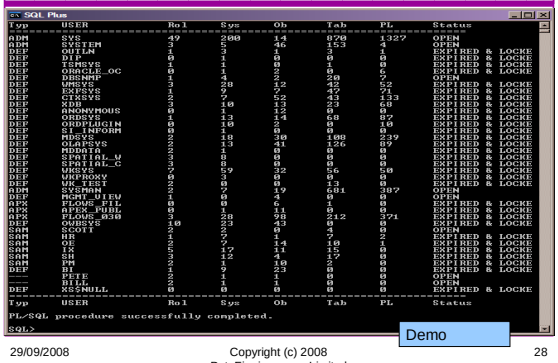
Ensure it's a supported version

Demo

Patch Status

- DBA_REGISTRY_HISTORY (should work now since Jan 2006 CPU)
- Opatch –lsinventory
- Checksum packages, functions, procedures, libraries, views
  - Rorascanner has example code
  - Some Commercial tools do this
  - Problems – if PL/SQL is not updated in CPU
  - Time based approaches with last_ddl_time
- Ask the DBA we are not trying to break in

User Enumeration

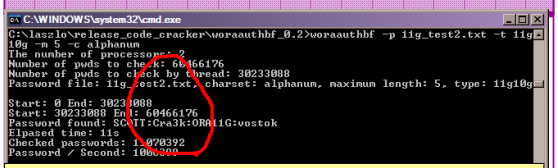


Demo

Auditing Passwords

- Three types of checks (ok 4)
  - Password=username
  - Password=default password
  - Password=dictionary word
  - Password is too short
- Default check tools or password cracker?
- Password cracker
  - http://www.petefinnigan.com/oracle_password_cracker.htm
  - http://sooneror later.hu/index.khtml?article_id=513
  - http://www.red-database-security.com/software/checkpwd.html
  - http://www.toolcrypt.org/tools/orabf/orabf-v0.7.6.zip

Password Cracker



Run in SQL*Plus

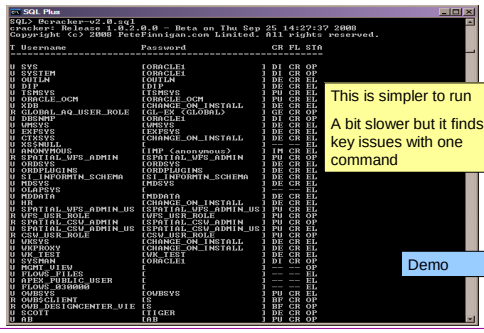
```
Select u.name||':'||u.password
         ||':'||substr(u.spare4,3,63)
         ||':'||d.name||':'
         ||sys_context('USERENV','SERVER_HOST')||':'
from sys.user$ u, sys.V_$DATABASE d where u.type#=1;
```

Create a text file with the results – mine is called 11g_test.txt

```
SCOTT:9B5981663723A979:71C46D7FD2AB8A607A93489E899C08FFDA75B147030761978E6
40EF57C35:ORA11G:vostok:
```

Demo

An Alternate Approach



This is simpler to run

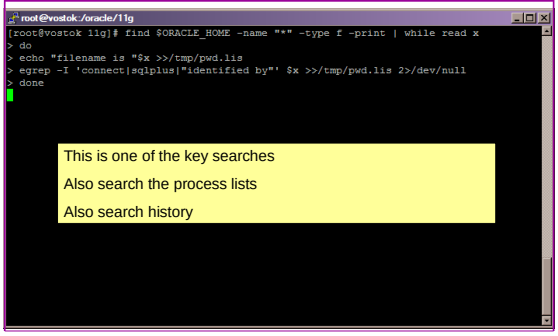
A bit slower but it finds the key issues with one command

Demo

File System Audit

- Finding passwords
- Permissions on the file system
- Suid issues
- Umask settings
- Lock down Key binaries and files
- Look for data held outside the database
- OSDBA membership
- These are a starter for 10: Much more can be done (e.g. I check for @80 separate issues at the OS level); see the checklists for ideas

Finding Passwords

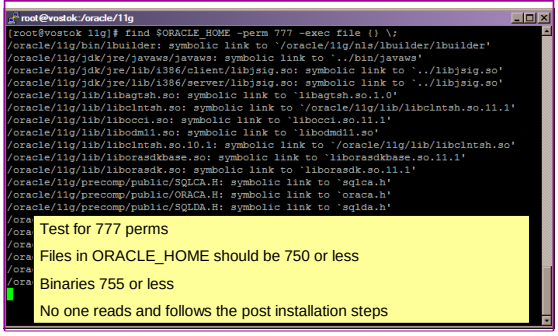


This is one of the key searches

Also search the process lists

Also search history

File Permissions



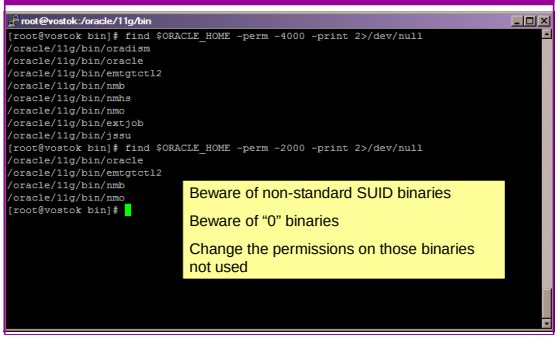
Test for 777 perms

Files in ORACLE_HOME should be 750 or less

Binaries 755 or less

No one reads and follows the post installation steps

SUID and SGID

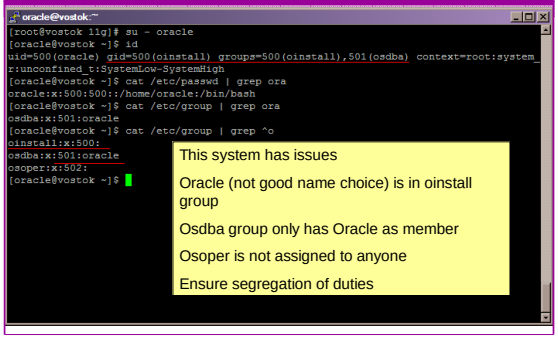


Beware of non-standard SUID binaries

Beware of "0" binaries

Change the permissions on those binaries not used

OSDBA Membership



This system has issues

Oracle (not good name choice) is in oinstall group

Osdba group only has Oracle as member

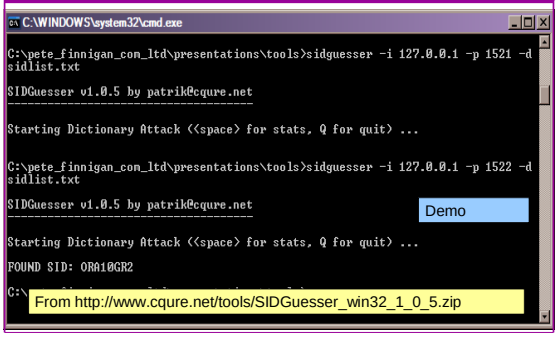
Osoper is not assigned to anyone

Ensure segregation of duties

Network Audit

- Listener
  - port
  - listener name
  - service name
- Listener password or local authentication
- Admin restrictions
- Extproc and services
- Logging on
- Valid node checking

SIDGuesser



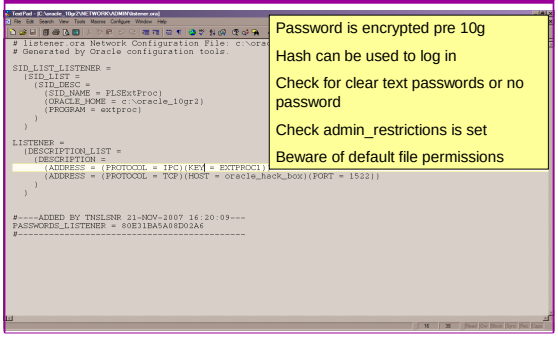
Port, Name and Services

```
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Versi
    Production
Start Date                31-OCT-2007 09:06:14
Uptime                    0 days 4 hr. 56 min. 27 s
Trace Level               off
Security                  ON: Local OS Authenticati
SNMP                      OFF
Listener Parameter File   /oracle/11g/network/admin/listener.ora
Listener Log File
   /oracle/diag/tnslsnr/vostok/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=vostok)(PORT=1521)))
Services Summary...
Service "ORA11G" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
Service "ORA11GXDB" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
Service "ORA11G_XPT" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
```

Sidguesser can guess a SID and cannot be blocked easily

Duplicate services

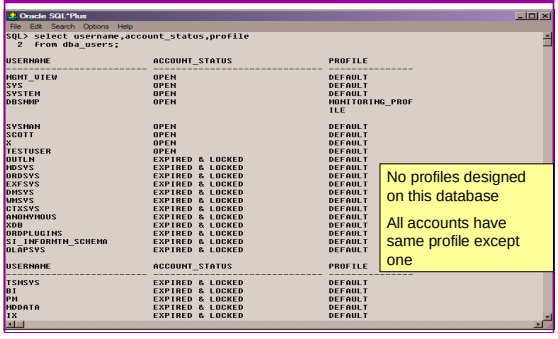
Listener password



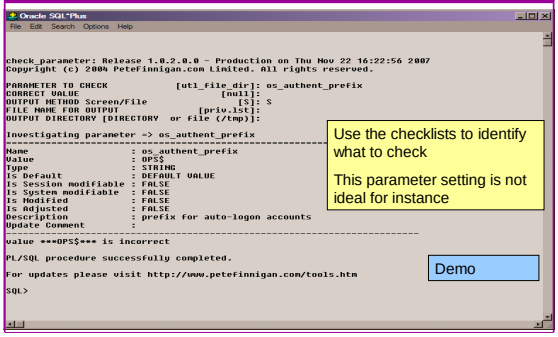
Database Configuration Audit

- Use simple scripts or hand coded commands
- This section can only highlight; use the checklists for a complete list of things to audit
- Check profiles and profile assignment
- Check initialisation Parameters
- Privilege and role assignments
- Much more – see checklists

Users => Profiles



Check Parameters



Use the checklists to identify what to check

This parameter setting is not ideal for instance

Demo

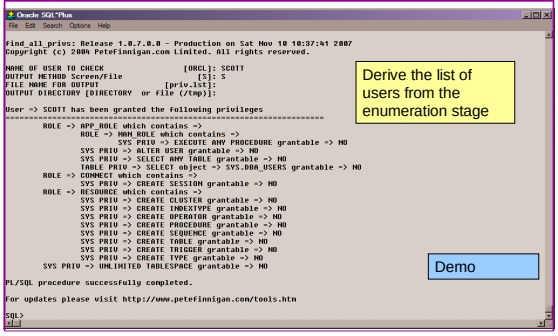
RBAC

- Review the complete RBAC model implemented
- 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 – check for open accounts
  - reduce attack surface

Defaults

- Defaults are one of the biggest issues in Oracle
- Oracle has the most default accounts for any software
- 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

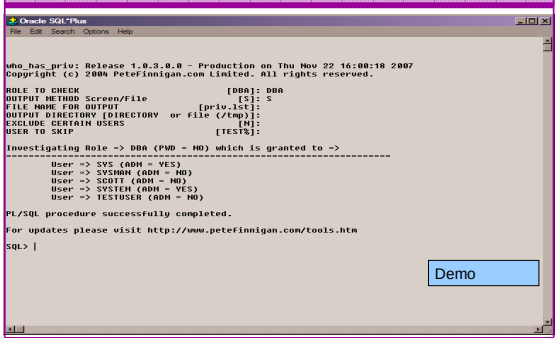
Test Users Privileges (SCOTT)



Derive the list of users from the enumeration stage

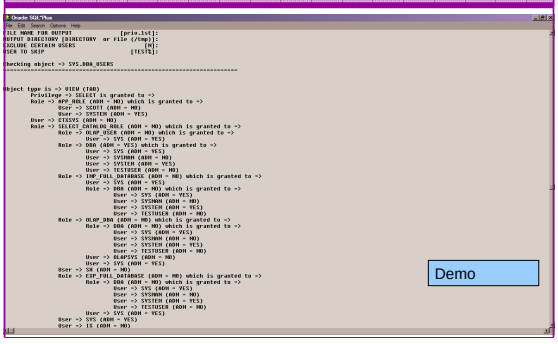
Demo

Who Has Key Roles



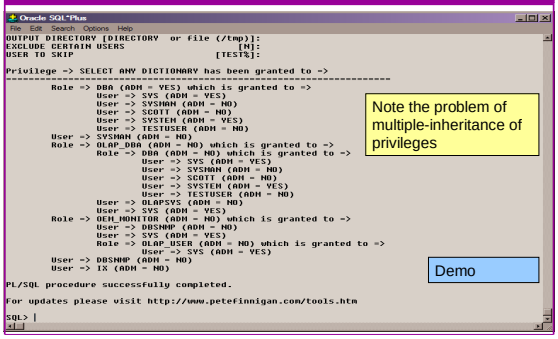
Demo

Access To Key Data (DBA_USERS)



Demo

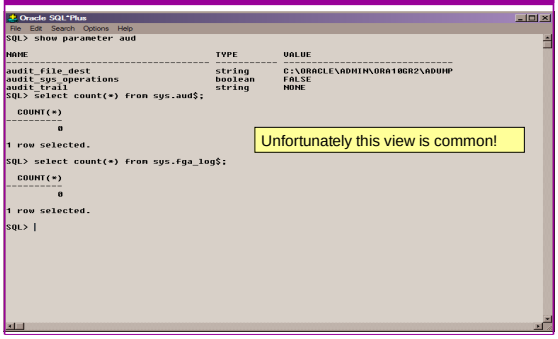
Key System Privileges



Note the problem of multiple-inheritance of privileges

Demo

Audit Checks



Unfortunately this view is common!

Stage 3 - What To Do Next?

- Write up the audit formally
- Prioritise the findings – Severity 1 – 3?
- Use internal procedures as a guide
- Other platforms can help (e.g. use your OS experience if you have it)
- Assess risk
- This is the hardest part of the audit process

Next Step - Create A Policy

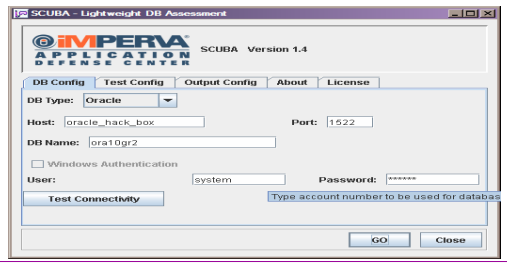
- Perform an Oracle database audit
- Define what the key/critical issues are
- Determine / decide what to fix
- Include best practice
- Work on a top 20 basis and cycle (This is effective for new hardening)
- Create a baseline standard
  - A document
  - Scripts – maybe for BMC
  - Commercial tool such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

Automate Scanning Tools

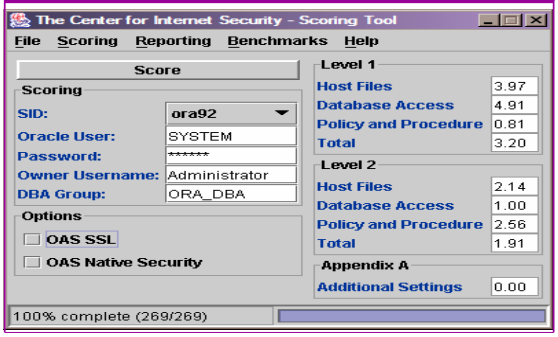
- Commercial
  - AppDetective - http://www.appsecinc.com/products/appdetective/
  - NGS Squirrel - http://www.ngssoftware.com/products/database-security/ngs-squirrel-oracle.php
  - AuditPro - http://www.niiconsulting.com/products/auditpro.html
  - IPLocks - http://www.iplocks.com/products/vulnerability_assessment.html
- Free
  - CIS benchmark - http://www.cisecurity.org/bench_oracle.html
  - Scuba from Imperva - http://www.imperva.com/scuba/
  - RoraScanner - http://rorascanner.rubyforge.org/
  - OScanner - http://www.cqure.net/wp/?page_id=3
  - Inguma - http://sourceforge.net/projects/inguma

Sample Audit Checks Using SCUBA

http://www.imperva.com/application_defense_center/scuba/



CIS Benchmark



Conclusions

- We didn't mention CPU's – Apply them – they are only part of the problem
- Think like a hacker
- Get the basics right first –
  - Reduce the version / installed product to that necessary
  - Reduce the users / schemas
  - Reduce and design privileges to least privilege principal
  - Lock down basic configurations
  - Audit
  - Clean up
- Use a top 10 approach in fixing, it works!

PeteFinnigan.com Limited
Oracle Security Expertise

Any Questions?

PeteFinnigan.com Limited
Oracle Security Expertise

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