**Oracle Security Masterclass**

By Pete Finnigan

Written Tuesday, 9th September 2008

---

**Introduction - Commercial Slide**

- 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](http://www.petefinnigan.com)
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA, Slovenia, Holland, Norway, Iceland, more)
- Member of the Oak Table Network
- I have been doing only Oracle security for 8 years

---

**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 to**
- Try out some of the tools and techniques yourself

---

**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...
  - What is the state of the industry?

---

**Why Do Hackers Steal Data?**

- Data is often the target now not system access; this can be for
- Identity theft to clone identities
- Theft of data to access money / banks
- [http://www.petefinnigan.com/weblog/archives/0001129.htm](http://www.petefinnigan.com/weblog/archives/0001129.htm) - 25 million child benefit identities lost on two discs (not stolen but lost)
Why Can They Steal Data?

- What are the main categories
  - Security bugs where – (this is simple, patch!!)
    - there are exploits and
    - Where there are no current exploits
  - Configuration issues – (complex, depends on apps)
  - Feature overload – attack surface increase
    - Software installed
    - Schemas installed
  - Defaults – (reduce)
    - Passwords
    - privileges

How Easy Is It To Attack?

- Many and varied attack vectors
- Bugs 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?

Example Exploit (1)

Example Exploit 1

Second Example Exploit

Second Example Exploit (2)
Internal Or External Attacks

- Internal attacks are shown to exceed external attacks in many recent surveys.
- The reality is likely to be worse as surveys do not capture all details or all companies.
- 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

Major Issue Is Excessive Privileges / Features

- Just some examples not everything!
- Public gets bigger – (figures can vary based on install):
  - 9iR2 – 12,132
  - 10gR2 – 21,530 – 77.4% more than 9iR2
  - 11gR1 – 27,461 – 27.5% more than 10gR2
- Many schemas are installed by default:
  - 9iR2 @ 30 by default
  - 10gR2 @ 27 by default
  - 11g @ 35 by default

Main Issues To Look For

- Core security issues with the database include:
  - Leaked password hashes
  - Weak passwords and default users
  - Too many features enabled by default
  - Excessive user / schema privileges often
  - No audit enabled to detect issues
  - TNS is an easy target
  - More?

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 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
- 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!

Tools And Info?

- Vulnerabilities and exploits:
  - SecurityFocus – www.securityfocus.com
  - Milw0rm – www.milw0rm.com
  - PacketStorm – www.packetstorm.org
  - FrSirt – www.frsirt.com
  - CERT – www.kb.cert.org/vuls
- Tools – we will cover tools later but some include:
  - Scuba
  - CIS Benchmark
  - RoraScanner
Part 2 – Performing A Database Audit (1)

• Planning and setting up for An Audit
• Starting the audit
• Versions, patches and software
• Enumerate users and find passwords
• File system analysis

Part 2 – Performing A Database Audit (2)

Cont’d…

• Network analysis
• Database configuration
• RBAC and access
• Specialist treatment
• Audit trail analysis

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

• There are a number of good checklists:
  _security_checklist_db_database_20071108.pdf
  – DoD STIG - http://ia.se.disa.mil/stigs/stig/database-stig-
v8r1.zip
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?
- 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

Sorting Access

- Ensure you use a clean PC / Laptop
- Direct SQL*Net access is required
- Direct ssh access to the server is required
- Install a local firewall on the PC
- Virus scan
- Store the data retrieved in an encrypted drive
- Open access only for the audit

Lining Up The Right People

- Before you start the audit you need the right people available to take part
- You also need the right people to give access permissions and assign rights:
  - DBA for account creation
  - DBA for interview
  - Systems admin to allow server access
  - Security manager for policies
  - Applications / DBA team for application knowledge

Results?

- Before you start you should assess 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)

Starting The Audit

- Get the laptop
- Install tools
- Lock down the laptop
- Connect to the database
  - Test the connection
  - Test some simple queries to establish the correct levels of access
  - I ask for CREATE SESSION, SELECT ANY TABLE, SELECT ANY DICTIONARY only
- Test ssh access to the server
  - Check the require file systems can be accessed
- This is an important step, not being prepared can waste half a day – tell people in advance
Interview Key Staff

- 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

- Oracle SQL: The
  - SQL dump (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

CPU Patch Status

- DBA_REGISTRY_HISTROY
- Ask the DBA we are not trying to break in

User Enumeration

- From: http://www.databasesecurity.com/dbsec/OAK.zip
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=dictionary word
  - Password=default password

Password Cracker (1)

Run in SQL*Plus

http://soonerorlater.hu/download/worrauthft_0.2.zip
http://soonerorlater.hu/download/worrauthft_0.3.zip

Select u.name || ' ' || u.password
| ' ' || substr(u.password,3,63)
| ' ' || u.password
| ' ' || u.name
| ' ' || user_name || USER40
| ' ' || SERVER_HOST || ' ' || t'
from sys.user$ u, sys.v$DATABASE d where u.type##=2;

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

SCOTT:9B59811663723A979:71C46D7FD2AB8A607A93489E899C0
8FDAB75B14703D761978640EF57C35:OAK11G:voastok:

Then run the cracker

Password Cracker (2)

As you can see the password is found – running at over 1 million hashes per second
Use a default password list or dictionary file
Worrauthft can also be used to crack from authentication sessions
Worrauthft can be used in dictionary or brute force mode

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
Vary the checks
Be careful on check size

File Permissions

Test for 777 perms
Files should be 750 or less
Binaries 755 or less
SUID and SGID

Beware of non-standard SUID binaries
Beware of "0" binaries
Change the permissions on those binaries not used

Network Audit

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

SIDGuesser

From http://www.csique.net/tools/SIDGuesser_x86_32_1_0_5.zip

OSDBA Membership

This system has issues
Oracle (not good name choice) is in oinstall group
No dba group only has Oracle as member
Chopin is not assigned to anyone
Ensure segregation of duties

Port, Name and Services

<table>
<thead>
<tr>
<th>Status of the Listener</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSTNRS</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td>TLLSNR for Linux: Version 11.1.0.4.0 -</td>
</tr>
<tr>
<td>Start date</td>
</tr>
<tr>
<td>Options</td>
</tr>
<tr>
<td>3 days 34 hr. 28 min. 27 sec.</td>
</tr>
<tr>
<td>Trace level</td>
</tr>
<tr>
<td>off</td>
</tr>
<tr>
<td>Secure ON/Off</td>
</tr>
<tr>
<td>ON</td>
</tr>
<tr>
<td>Listener Parameter File</td>
</tr>
<tr>
<td>/oracle/log/network/admin/listener.ora</td>
</tr>
<tr>
<td>Listener Log File</td>
</tr>
<tr>
<td>/oracle/log/network/admin/listener.log</td>
</tr>
<tr>
<td>Listener Pathname:</td>
</tr>
<tr>
<td>/oracle/log/network/admin/listener.ora</td>
</tr>
<tr>
<td>Listener昤 Pathname:</td>
</tr>
<tr>
<td>/oracle/log/network/admin/listener.log</td>
</tr>
<tr>
<td>Services Summary:</td>
</tr>
</tbody>
</table>
| Service "ORCL"
| has 1 instance(s)
| Instance "ORCL@IN" status READY, has 1 handler(s) for this service... |
| Service "OSI"
| has 1 instance(s)
| Instance "OSI@IN" status READY, has 1 handler(s) for this service... |
| Service "OSI2"
| has 1 instance(s)
| Instance "OSI2@IN" status READY, has 1 handler(s) for this service... |

Listener Password

10g and 11g password must not be set
Listener password

Password is encrypted pre 10g
Hash can be used to log in
Check for clear text passwords or no password
Check admin restrictions is set

Valid Node Checking

My favourite free feature
Unfortunately no one ever uses it

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

Default profile

<table>
<thead>
<tr>
<th>PROFILE</th>
<th>RESOURCE_NAME</th>
<th>LIMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>CONNECT_TIME</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CPQ_MEM</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CPQ_MEM_REGION</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>FAILED_0360ATTEMPTS</td>
<td>10</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>ISSUE_TIME</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>LOGICAL_MAXS_PER_CALL</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD__USAGE_TIME</td>
<td>1</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_MAX</td>
<td>150</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_MIN</td>
<td>1</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_VERIFY_FUNCTION</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PRIVATE_DATA</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>RESOURCE_PFX_USER</td>
<td>UNLIMITED</td>
</tr>
</tbody>
</table>

- All other users have DEFAULT profile by default
- no password reuse set?
- Life time is too long
- no pwd verify function
- It's a good start but not enough

Users -> Profiles

No profiles designed
All accounts have same profile except one
Check Parameters

Use the checklists to identify what to check. This parameter setting is not ideal for instance.

RBAC And Access

- Test RBAC assigned to all users
- Discussed in next slide
- Again this section is a sample — use the checklists
- Assess Default privileges
- Assess access to key roles
- Assess access to key packages
- Assess access to key data
- Access to Key privileges

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
- 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)

Who Has Key Roles
Specialist Considerations

- Look for key data – Data that has value for the organisation or should be protected due to regulatory requirements
  - Identify the data
  - Identify the storage
  - Identify access paths – DBA_DEPENDENCIES
    - Views, procedures
    - Test RBAC on these objects
  - Test is encryption is present if necessary

Automate Scanning Tools

- Commercial

- Free
  - CIS benchmark - http://www.cisecurity.org/bench_oracle.html
  - Scuba from Impera - http://www.impera.com/scuba/
  - RoraScanner - http://rorascanner.rubyforge.org/
  - OSScanner - http://www.cgure.net/wp/?page_id=3
  - Inguma - http://sourceforge.net/projects/inguma

Sample Audit Checks Using SCUBA

http://www.impera.com/application_defense_center/scuba/
Sample Audit Checks Using SCUBA

Review The Audit Trails
- Test what core audit is enabled
- Test if sys is being audited
- Test if FGA is in use
- Examine the core audit trail
- Check failed logins / errors – review the audit data held
- Check the listener log for 1169, 1190 and 1189 errors
- Test RBAC on audit objects and also test audit system privileges

Test Core Audit Settings
This SQL shows the statement and privilege audit settings

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
- 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
### 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
- Perform a risk assessment
- 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

### Perform A Risk Assessment
- To understand what to fix and to what level you must understand risk.
- What is the “cost” to your company / organisation if:
  - A breach occurred
  - A total system loss
- Cost can include media embarrassment
- Frameworks and tools available – CRAMM, CobiT
- Do it as a simple meeting with the right people

### Top 10 Approach
- Pick out the top 10 highest severity issues
- Devise solutions that work for all of them
- Roll out the solutions
  - Test
  - Regression test
  - Make live
- Devise automated checks for these ten – could be simple scripts
- Start on the next ten!

### Basic Hardening
- Harden the operating system first
- Reduce the features and functions installed – on the operating system and in the database
- Review RBAC for all users and group users
- Test all user accounts for weak passwords and set strong complex ones

### Hardening (2)
- Devise profiles for all user groups and implement
- Remove defaults – privileges, users, passwords
- Decide on secure configuration settings
- Clean up – remove ad-hoc files, scripts, examples
- Create processes and policies to ensure secure data going forward
Enable Database Auditing

- Every database I have ever audited has no database audit enabled – ok a small number do, but usually the purpose if 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

- 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!

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