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

- What is Oracle Security?
- Basic Oracle security tenets / ideas
- Why a database must be secured
- How can a database be breached?
- Key security issues
  - Discussion of problems
  - Discussion of high level fixes
- What to do next
What Is Oracle Security?

- Securely configuring an existing Oracle database?
- Designing a secure Oracle database system before implementation?
- Using some of the key security features
  - Audit facilities, encryption functions, RBAC, FGA, VPD...
- Oracle security is about all of these BUT
  - It is about securely storing critical / valuable data in an Oracle database. In other words its about securing DATA not securing the software!
The Basic Tenets Of Oracle Security

- Reduce the version / installed product to that necessary
- Reduce the users / schemas installed
- Reduce and design privileges to least privilege principal
- Lock down basic configurations
- Enable audit trails in the database
- Clean up

Reduction is the key

12/12/2008

Copyright (c) 2008 PeteFinnigan.com Limited
Why The Data Must Be Secured

- 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 traditional 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 have access to data
  - DBA’s use excessive privileges
- Data is often the target now not system access
Breaching The Database?

```
SQL> show user
USER is "SCOTT"
SQL> @10g_exploit

USERNAME       GRANTED_ROLE   ADM DEF OS_
--------------- ----------- ------- ------
SCOTT           APP_ROLE      NO YES NO
SCOTT           CONNECT      NO YES NO
SCOTT           RESOURCE     NO YES NO

PL/SQL procedure successfully completed.

USERNAME       GRANTED_ROLE   ADM DEF OS_
--------------- ----------- ------- ------
SCOTT           APP_ROLE      NO YES NO
SCOTT           CONNECT      NO YES NO
SCOTT           DBA          NO YES NO
SCOTT           RESOURCE     NO YES NO
```

http://www.milw0rm.com/exploits/4572
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 but concentrate on key areas and outside access
General Oracle Security Info

- **Vulnerabilities and exploits:**
  - SecurityFocus – [www.securityfocus.com](http://www.securityfocus.com)
  - Milw0rm – [www.milw0rm.com](http://www.milw0rm.com)
  - PacketStorm – [www.packetstorm.org](http://www.packetstorm.org)
  - FrSirt – [www.frスirt.com](http://www.frスirt.com)
  - CERT – [www.kb.cert.org/vulns](http://www.kb.cert.org/vulns)

- **Tools** – [http://www.petefinnigan.com/tools.htm](http://www.petefinnigan.com/tools.htm)
  - Who_has scripts, CIS benchmark, Scuba, rorascanner, Metacortex, cquare, many more

- **Papers, blogs, forums, books**

- **Checklists**
  - CIS Benchmark - [http://www.cisecurity.org/bench_oracle.html](http://www.cisecurity.org/bench_oracle.html)

- **Websites** – petefinnigan.com, cquare, RDS, Argeniss, databasesecurity.com
• 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

• **Do not do any of these!**
What to audit (First?)

- Perform a password audit – use a tool such as woraauthbf – http://www.soonerorlater.hu/index.khtml?article_id=513
- Reduce network access and leakage
- Review the listener
- File system
  - look for passwords
  - permissions
- Audit basic configuration
  - Parameters
  - User accounts that exist
  - Privileges on objects
  - Privileges assigned to users
- Use one of my scripts, who_can_access.sql, find_all_privs.sql, who_has_role.sql, who_has_priv.sql – see http://www.petefinnigan.com/tools.htm
Password Cracking (Easy way)

For this example run
INFO: Number of crack attempts = [61791]
INFO: Elapsed time = [4.36 Seconds]
INFO: Cracks per second = [14170]

53 out of 60 accounts cracked in 4.3 seconds

We are not trying to break in BUT trying to assess the “real security level”

See
http://www.petefinnigan.com/oracle_password_cracker.htm

Access Issue
As you can see the password is found – running at over 1 million hashes per second on this laptop.

Woraauthbf can also be used to crack from authentication sessions.

Woraauthbf can be used in dictionary or brute force mode.

Use it to supplement the PL/SQL based cracker.

http://www.soonerorlater.hu/download/woraauthbf_src_0.22.zip
http://www.soonerorlater.hu/download/woraauthbf_0.22.zip
SIDGuesser

From http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip

This is not an audit tool BUT you should understand what it does

A better approach is to use the dictionary list in a text editor and check if your service name/SID is listed

Access Issue
User Enumeration

SYS and SYSTEM always exist so passwords guesses can be attempted.

Other users can “almost” certainly be there as well – DBSNMP / OUTLN for instance.

This is not an audit tool; for an audit reduce the number of default schemas.

From [http://www.databasesecurity.com/dbsec/OAK.zip](http://www.databasesecurity.com/dbsec/OAK.zip)
RBAC

• Review the complete RBAC model
• Understand default schemas / features 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

Use.sql demo
## Secure Listener by Default?

### STATUS of the LISTENER

<table>
<thead>
<tr>
<th>Alias</th>
<th>LISTENER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>TNSLSNR for Linux: Version 11.1.0.6.0 – Production</td>
</tr>
<tr>
<td>Start Date</td>
<td>31-OCT-2007 09:06:14</td>
</tr>
<tr>
<td>Uptime</td>
<td>0 days 4 hr. 56 min. 27 sec</td>
</tr>
<tr>
<td>Trace Level</td>
<td>off</td>
</tr>
<tr>
<td>Security</td>
<td>ON: Local OS Authentication</td>
</tr>
<tr>
<td>SNMP</td>
<td>OFF</td>
</tr>
<tr>
<td>Listener Parameter File</td>
<td>/oracle/11g/network/admin/listener.ora</td>
</tr>
<tr>
<td>Listener Log File</td>
<td>/oracle/diag/tnslsnr/vostok/listener/alert/log.xml</td>
</tr>
</tbody>
</table>

**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.

---

**Turn on admin restrictions**

**Ensure no password in >10g**

**Use valid node checking / Firewall – {Access Issue}**
Finding Passwords

This is one of the key searches
Also search the process lists
Also search history
Search each area separately
Extend for exp, imp, expdp, impdp, sqlldr.....
Clean Up

- This is the security killer in most systems I see
- Often file systems include
  - Scripts with passwords or
  - worse rules to change passwords
  - Evidence of password changes...
  - Use tools such as
    - Oracle Password Repository, mkstore, database jobs, OS external users
- Clean up
  - ad-hoc scripts
  - Maintenance evidence
  - Trace files
  - Data files, exports..
  - Audit logs....
- All are evidence of lack of controls!
Default database installations cause some weak configurations

Review all
  – configuration parameters – checklists?
  – File permissions

Some examples
  – No audit configuration by default (fixed in 10gR2 for new installs)
  – No password management (fixed in 10gR2 new installs)

In your own applications and support
  – Do not use default accounts
  – Do not use default roles including DBA
  – Do not use default passwords
Access To Key Data (SYS.USER$)

Checklists can be used
Concentrate on key data, services, OS access

http://www.petefinnigan.com/who_can_access.sql
Who Has Key Roles

The image shows a command line interface with SQL commands executed to check the roles granted to different users and roles. The output indicates the following:

- User SYS has the role DBA with ADM = YES.
- User SYSTEM has the role DBA with ADM = YES.
- Role APPROLE has the role DBA with ADM = NO and PWD = NO.

The PL/SQL procedure is completed successfully.

For updates, please visit http://www.pete finnigan.com.
Check Parameters

Use the checklists to identify what to check

This parameter setting is not ideal for instance

Demo
Check System Privileges

**Demo**

Use the checklists to identify what to check.

Users should not have system privileges.
Who Has What Privileges

Demo

Use to check users and roles
CIS Benchmark

http://www.cisecurity.org/bench_oracle.html

Also look at SCUBA and OScanner as they are free scanners
Get The Basics Right

• OK, we have covered a lot of information
• Concentrate on
  – Checking and strengthening users' passwords
  – Removing default schemas and software not needed
  – Reduce leakage of critical data (passwords and more) from the database and filesystems
Get The Basics Right (2)

- Don’t leak network data to allow connection attempts
- Use firewalls or valid node checking to protect the database [Stop direct connections]
- Review privileges and access to key data
- Confirm key configuration is set securely
What To Do Next

- Fix the basics, then what?
- Use the project lockdown or one of the good checklists to do a more detailed review
- Ensure sound audit plan is in place
- Understand how hackers may steal your data
- This way **YOU** can understand how to protect it
- Monitor the database security for compliance
Audit The Oracle Database

- Operating security Checklists
  - CIS benchmarks for Windows, Linux, Solaris and more
  - OS check tools – The CIS benchmarks are useful – others are available
- Oracle security checks
  - Most tools are windows centric – don’t install them on the prod database servers if you run Windows
  - Audit by hand to gain understanding
  - Audit using a free or commercial tool
  - Get professional help
- Oracle security checklists
  - use and work through
  - these are great resources to start with

Use the tools we have shown
Get the basics right first
Perform Hardening

• Reduce the features and functions installed – OS and DB
• Harden the operating system
• 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
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
Create A Monitoring Process

• Once you are secure or on the way to being secure
• Realise its not a “one-off” process
• Constant monitoring of the database is necessary because
  – New issues arise
  – The database can change shape
  – Your knowledge increases
• Create a monitoring process – this can be a policy, a set of scripts, a commercial tool
Conclusions

• We didn’t mention CPU’s – Apply them – they are only part of the process
• Think like a hacker
• Get the basics right first – stop attempted connections or cracking
• Sort out the RBAC, configuration, installed software and privileges
• Get the basics right first
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