How to Secure Oracle in 20 Minutes
A quick guide to securing an Oracle database

Pete Finnigan, Principal Consultant

SIEMENS

Insight Consulting
Introduction

The premise
Is it realistic to secure Oracle in 20 minutes?
What can be done whilst under fire?
Do you know that you are under fire?
The premise for this presentation

- A game of hackers and security chiefs
- The rules
  - Black hats attacked a single database
  - White hats tried to defend and secure the database
- What happened?
  - Chaos ensued
  - Panicked decisions
  - Loss of the database and server
- What was the result?
  - Attacking is faster than defending
What we learned

What did we learn?

- Attacking a database is easier than defending it, why?
  - Un-hardened database is an easy target
  - Canned exploits, easy to run
  - Attacking does not require excessive expertise
- Database cannot be secured when under fire
- Disconnect from the network, assess the damage
- The database needs to be secured beforehand
- Audit needs to be enabled
The modern Oracle database risks

- Oracle gets bigger and more complex with each version
  - Many database users
  - Many examples
  - Configuration issues
- SQL Injection (Built-in packages and custom code)
- Cross Site Scripting – e.g.
  http://hr:hr@hostnm:8080/oradb<script>alert('Hello')</script>/HR/DEP
- Web facing services
  - Apache
  - XDB – ports 2100, 8080, 443
  - More…
Can you secure Oracle in 20 minutes?

What did we learn from the exercise?
- Attacking is easier than defending
- Securing under fire is pointless
- Knowing where the attacker has been is impossible without proper prior configuration
- You cannot trust an insecure Oracle database

The question again –
- Can you secure Oracle in 20 minutes?

No!
A quick strategy

- Did what we tried to do have real world value?
- Isolation from the network
- Lock down the listener
- Stop all net facing services not needed
- Lock down all schemas
  - Revoke create session, set impossible passwords, password management
A quick strategy

- Lock down paths to the data
  - Valid node checking
  - Firewalls
- Lock down key packages
  - File access, net access, OS access, encryption
- Enable simple audit and logging
  - Connections, use of key privileges
- Re-connect to the network
Shut down services

Some examples…

Apache is often installed and enabled by default
- Disable Apache
- Remove the software installation
- Beware Oracle versions lag

If Apache is needed then it must be hardened
- Remove XDB
  - Many issues, SQL Injection, buffer overflows
  - Edit the init.ora or spfile
Lock down the listener

- The listener is an easy target
- No password management
- No failed login attempts
- No default logging
- Set a password – 10g has local authentication
- Prevent dynamic administration
- Turn on logging
Secure schemas

- Check for password=username
- Check for default passwords
- Brute force or dictionary attack – orabf, checkpwd
- Remove schemas not needed
- Enable profiles
  - Different per user / schema groups
  - Failed logins
  - Password ageing
  - Password complexity
Revoke privileges

- For schemas that have to remain
  - Revoke CREATE SESSION
  - Set an impossible password
  - Lock and expire the account
- Revoke system privileges
- Reduce the attack surface
Lock down key packages

- Revoke public privileges on key packages and views
  - 10G is better
  - UTL_FILE, UTL_HTTP, UTL_TCP and many more
  - How to find them!

- Each version of Oracle increases the number of objects
- Revoking access from PUBLIC is possible
  - Simple process to follow
  - Revoke, check, grant, use!
Lock down the paths to data

- Data can have many access paths
- From clients and application servers
- From DBA workstations
- Inside the database itself
- Use firewalls to block address ranges and services
- Use valid node checking at the database level
  - Applications, DBA’s only
- Review data access duplications – not simple or quick
  - Views, tables, packages
Enable basic audit

- It is essential to audit the database
- Audit all connections
- Audit use of all system privileges
- Audit access to key data tables
- Use FGA for access to critical or regulatory data
- Define an audit procedure
- Create reports
- Purge and archive the data
Sources of information

Oracle security information available is quite good now

Web sites for information

Books
- SANS Oracle security step-by-step – Pete Finnigan
- Effective Oracle database 10g security by design – David Knox
- Oracle privacy security auditing – Arup Nanda

Free tools
- CIS benchmark - http://www.cisecurity.org/bench_oracle.html
- Many tools listed on http://www.petefinnigan.com/tools.htm

Training
- SANS course, also Siemens are preparing a course
Plan for a proper Oracle security audit

- What did we learn – again?
- Build security in when the database and applications are designed and installed
- What if your database exists already?
  - Take some simple basic steps now
  - Plan to conduct a proper database security audit
- Data is often the target
- Firewalls often do not prevent access
- Get professional help to perform an IT health check on your Oracle database
Questions and Answers

Any Questions, please ask Later?

Contact me via email peter.finnigan@insight.co.uk
Or via my website http://www.petefinnigan.com
Insight Consulting
Siemens Communications

Security, Compliance, Continuity and Identity Management

SIEMENS