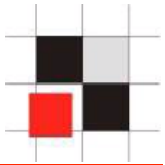
red database security

Troopers - 2008

Hardening Oracle Databases in Corporate Environments

Alexander Kornbrust
23-April-2008

Table of Content



- Introduction
- Theory vs. Real World
- Where to start…
- Useful software for Oracle in Corporate environments

Introduction

Some numbers from a German survey (741 companies) – End of 2007

Damage	2.8 Billion EUR (Germany only!)
Espionage Growth	10% per year
Espionage incidents	18.9%
Assumed incidents	35.1%
Affected Departments	Sales (20%), R&D (16.1%), HR (14.7%), MFG (13.3%)
Attackers	Internal Employees (20%), Competitor (15%)
Police involved	<25%
Offender	Admin. (31.3%), Technician (22.9%), Manager (17.1%)

http://bc1.handelsblatt.com/news/loadbin/ShowImage.aspx?img=1567932&typ=handelsblatt.pdf

Introduction I

Last Tuesday Oracle released their quarterly security patches. One of the bugs fixed with these patches allows ANY user to read ANY table (except SYS).

If your databases are not 11g or 10.2.0.4 your database is affected…

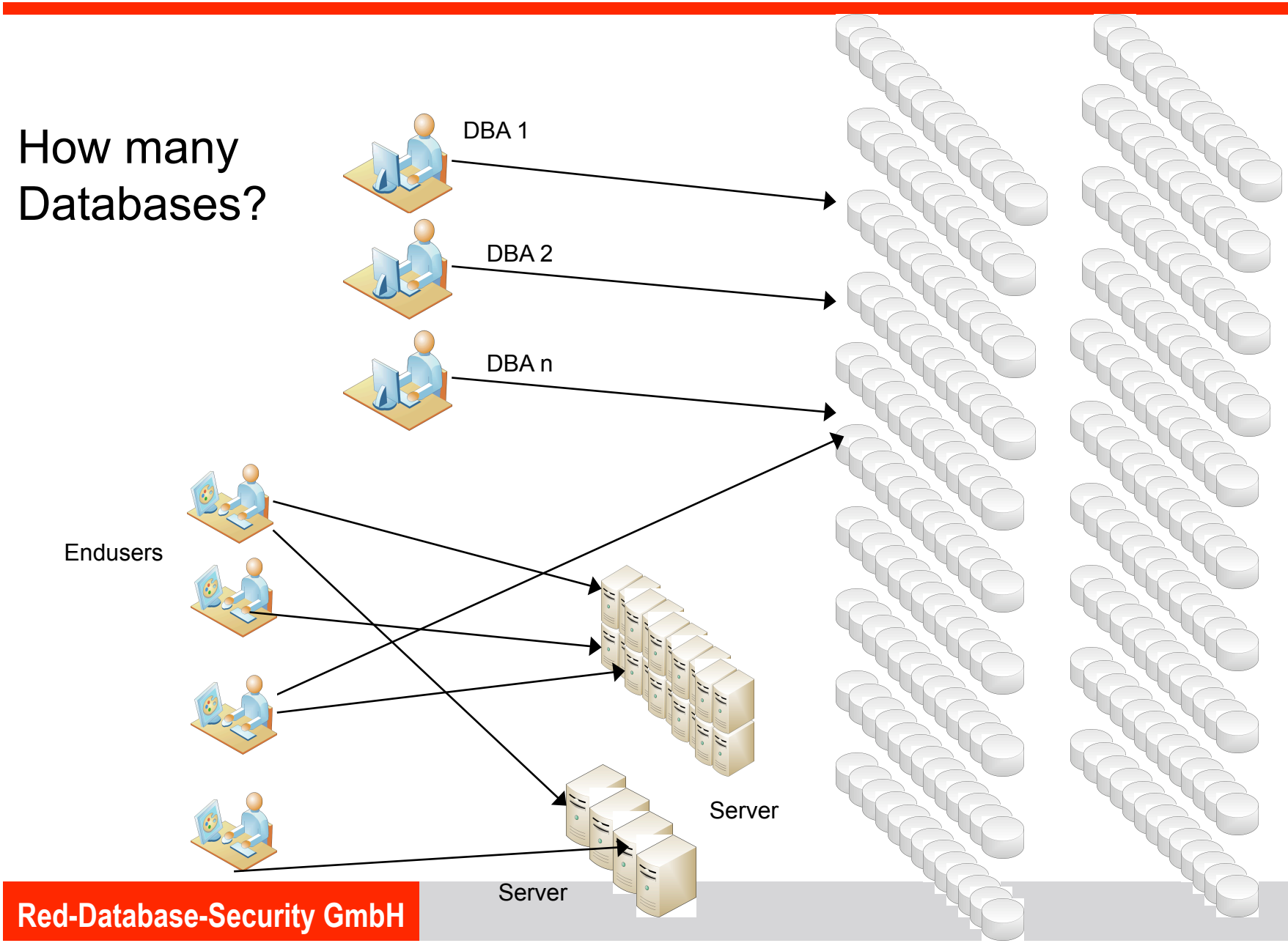
Introduction II

The following talk is about the differences between hardening a single/ few Oracle databases and hundreds or thousands of them.

Non-Oracle-People often have no idea how many databases are existing in huge corporate/government networks. They are often surprised if I talk about 1000+ Oracle Instances.

I know a few German companies with 8000+ Oracle Instances and many companies/organizations with 1000+ Oracle instances. With these huge numbers even simple jobs can become a problem.

Introduction III



Introduction IV – estimated numbers

Do companies really have 1,000 (or 8,000) Oracle databases? Why????

Some figures for 1,000 instances:

1,000 instances ≈ 300 production databases (#inst / 3, DEV, STAGING, PROD)

2-5 % of the databases are important (6-15 production instances)

On average a DBA is responsible for 30-100 databases.

1,000 Instances ≈ 10-15 DBA's

80-90 % of the databases are running the same version

10-20 % are running outdated or customized installations

Oracle Database Security in Theory I

- Buy a database scanner for Oracle
- Run the scanner
- Read the report and fix the problems

➔ That's it. Not really difficult ?!

Oracle Database Security in the real world I

- A typical database scanner can produce up to 200 pages per database, even if the database is patched.
- Let's do a little bit math:
  - 200 pages * 8000 Instances = 1,600,000 pages
  - 1.6 Mio pages = 7,600 kg paper
  - 8000 hours (4 year) to read everything (200 pages per hour)

  - 1,000 instances – 200,000 pages – 950 kg – 1,000 hours

Oracle Database Security in Theory II

- Download a security patch (CPU – Critical Patch Update) from security patch from Oracle, e.g. the April CPU
- Just apply the patch.

➔ That's it. Not applying security patches is bad and only lazy DBA's are not doing it.

Oracle Database Security in the real world II

- Applying a security patch cost approx. 4 hours
- 1 hour to apply the patch, 3 hours for coordinating the downtime. Sometimes more, sometimes less.
- Let's do a little bit math:
  - 8000 Instances * 4 hours * 4 CPU/yr= 128,000 hours
  - 128,000 hours = 64 person years

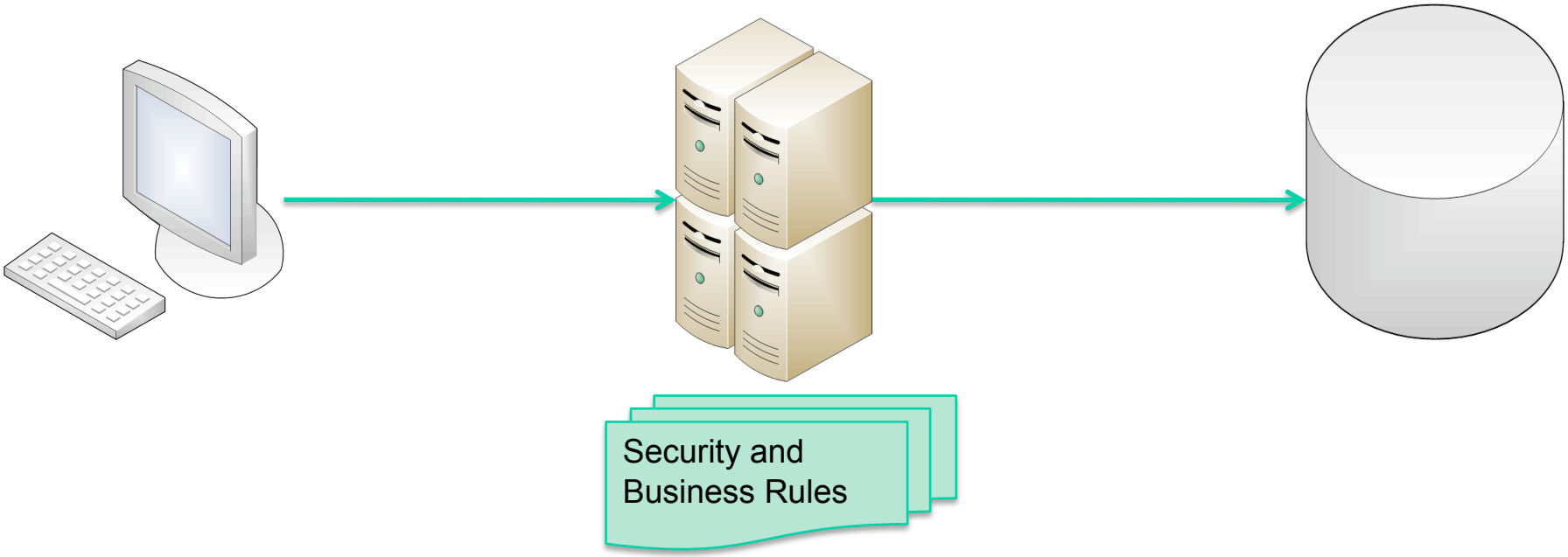
➔ 64 DBA' are doing nothing else than patching Oracle databases

➔ Is this realistic? No

➔ That's why many companies are skipping the process of applying patches

➔ Patches are sometimes breaking the DB

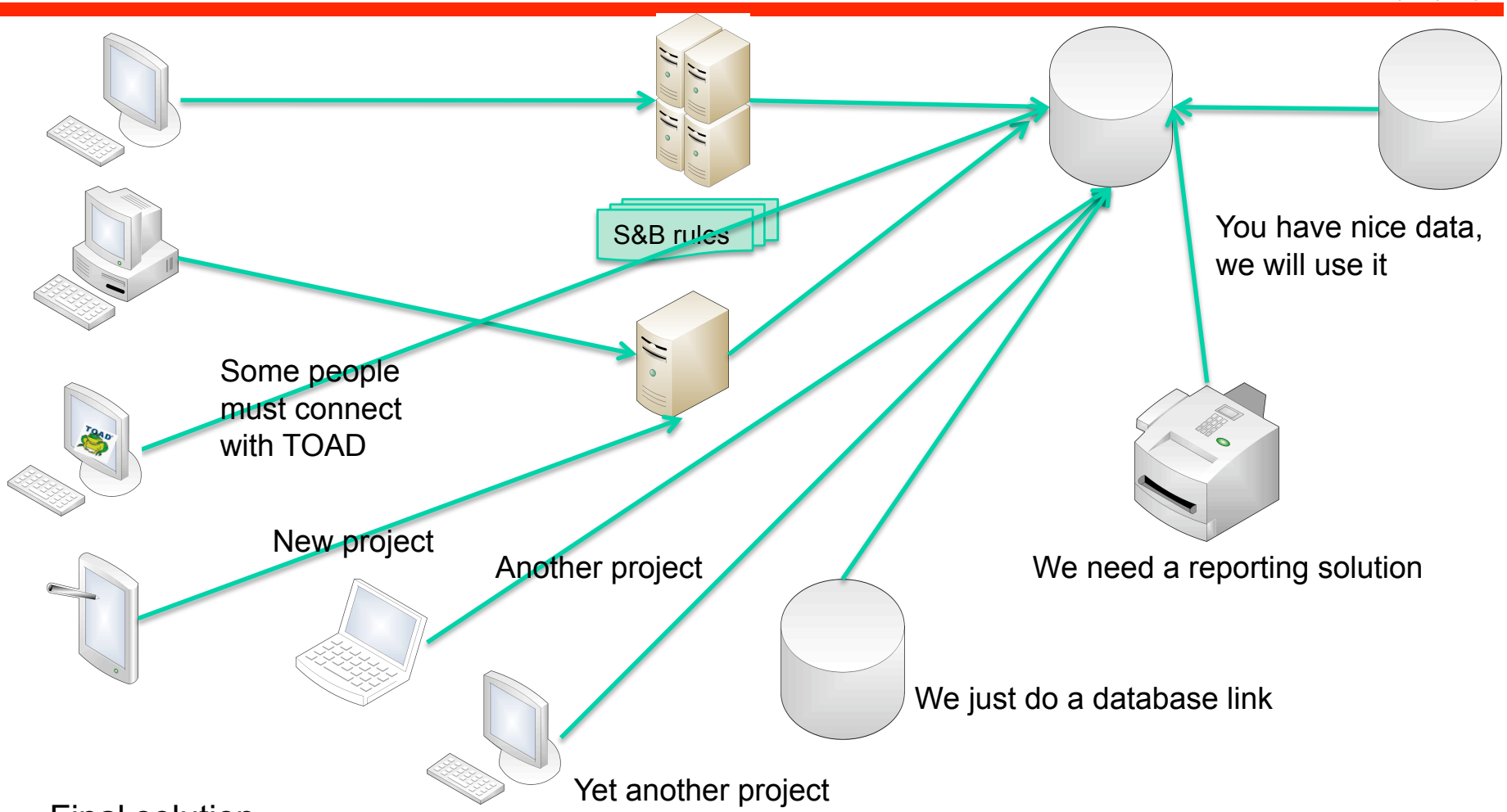
Oracle Architecture in Theory III



Classic solution:

- Clients accessing a database via application server
- No direct access to the database
- Security and business rules are enforced in the application server

Oracle Database Security in the real world III



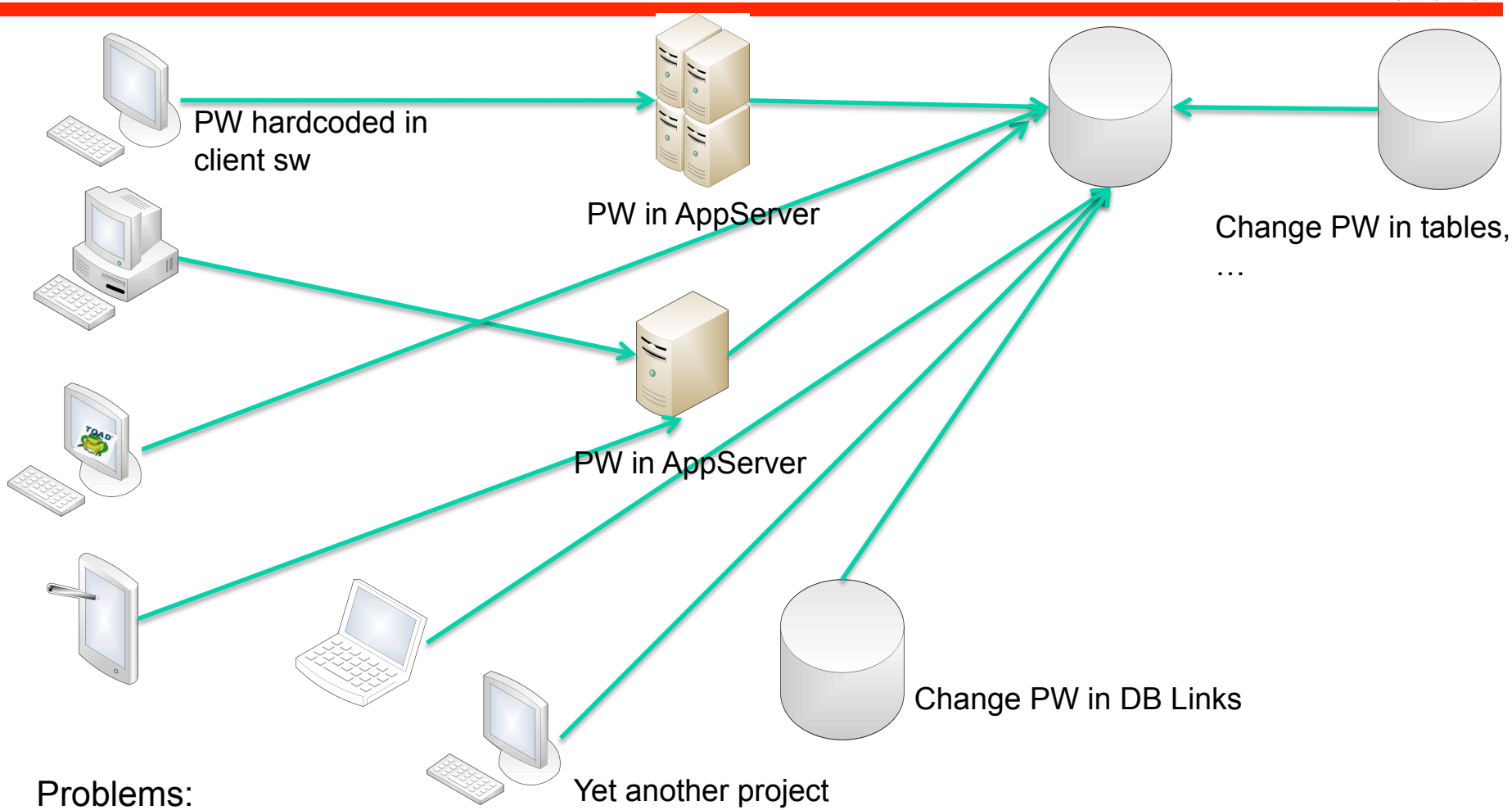
Final solution

- Complex architecture
- All types of clients are accessing the database
- Security and business rules still enforced in the first application server

Oracle Database Security in Theory IV

- The check of the database has revealed some weak and/or default passwords.
- Just change the password with the "`alter user`" command
  alter user app identified by "`!pw!comp!343234`"
- ➔Again an easy job…

Oracle Database Security in the real world IV



Problems:

- Complex architecture (Where must I change my passwords)
- Password change requires downtime !!!
- Hardcoded passwords (e.g. Oracle)
- Often Reverse Engineering is needed to find out what/when to change

Other real world problems which are often ignored

- Certification of systems
  ➔ Applying a patch requires the re-certification of a system (e.g. in Pharma business required by the FDA)
- No downtime for patching (business is against the downtime)
- No Budget (No time/no money). How much money do you spend for anti-virus/anti-spyware software
- Missing database security knowledge of the people

Problems? You always have problems…

Where are the solutions?

Where should we start?

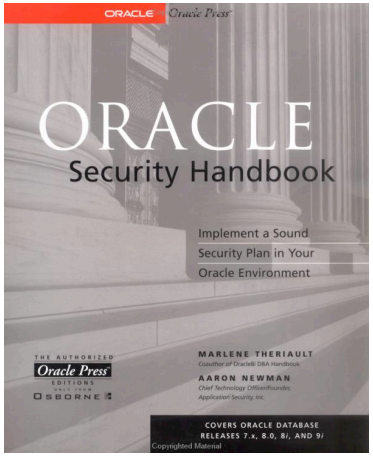
Knowledge & Awareness

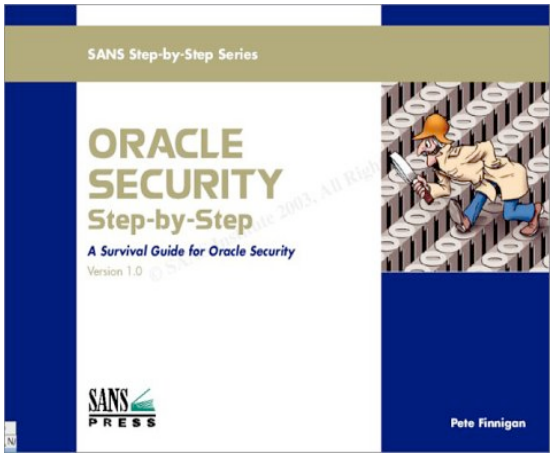
- Oracle DBA's have normally deep Oracle Know-How but less/little Security Know-How.
- Often surprised what a hacker could do (SQL Injection, XSS, …)
- Problems to see the justification for Oracle security (Why should I…? Abusing this issue is really, really difficult)
- In the Oracle CTP competition of our Oracle Anti-Hacker-Training 95% of the attackers won over the DBA's

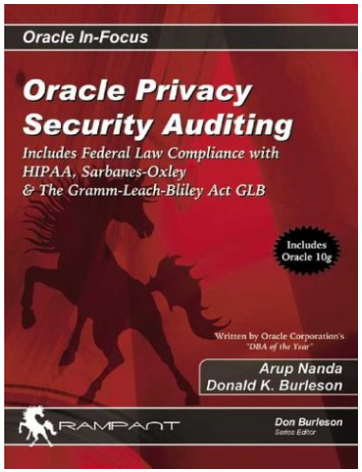
Knowledge & Awareness

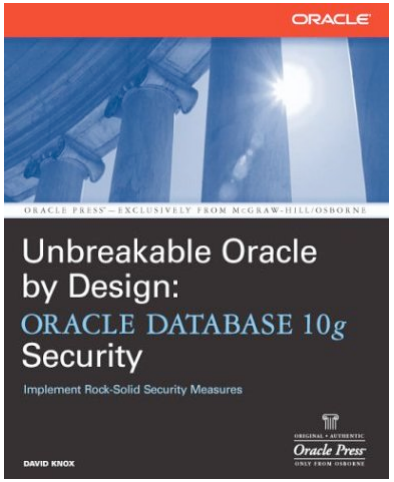
- Learn from the resources in the internet (www.petefinnigan.com, www.red-database-security.com)
- Buy and read some Oracle security books
- To build up Oracle Security Know-How your DBA's/Security Managers can go to a special Oracle security training.

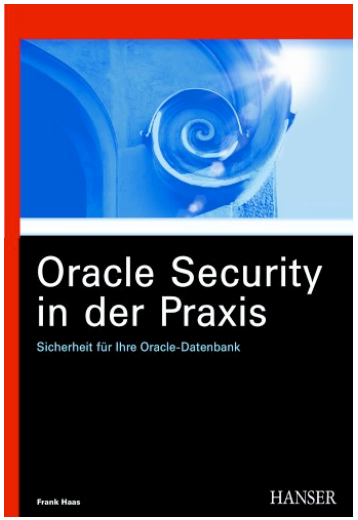
Knowledge & Awareness - Books

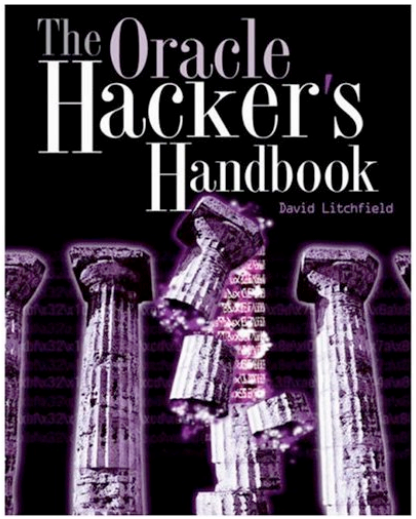


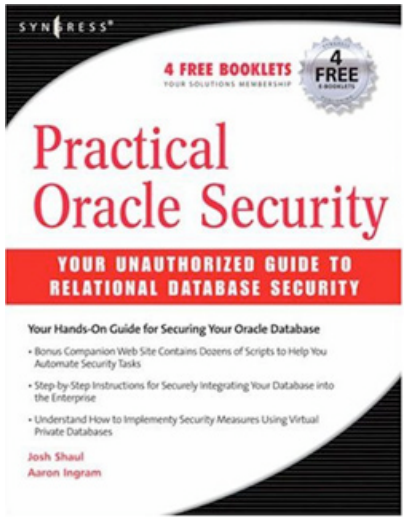












Starting…

1. Start with 2-3 typical databases

2. Try to identify generic problems (PW, Listener, ...)

3.Fix the problems

4. Setup/ Modify Policy

5. Scan more DBs

Where to start – Identify 2 or 3 databases

- Most databases (80-90%) in an organization have the identical setup. They are created with the same setup scripts and vary only in the application running on that database or some components (e.g. XMLDB, …).
- If you find issues in the configuration of 1 database these issues will be available in all other databases with the same setup
- An analysis of 2-3 typical databases gives a good impression about the over-all security level.

Where to start – Identify 2 or 3 databases – Typical Issues

- Insecure TNS-Listener configuration
  (no password in 8i/9i), (password in 10g)
- Weak / Default passwords with checkpwd
  (no default passwords in 10g, application password is often identical with the username: APP/APP)
- Dangerous packages granted to public
  (Oracle's default settings: UTL_TCP, UTL_HTTP, HTTPURITYPE, DBMS_SQL)
- Latest (non-security) patchset is missing (e.g. 10.2.0.4)
- No Oracle Security Patch (CPU) applied
- Unsecure application code
  (SQL Injection in custom PL/SQL code)

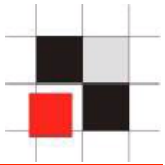
Where to start – Identify 2 or 3 databases – Resolution

- 8i/9i: Set a listener password and change the listener shutdown scripts
  10g/11g: Remove the listener password
  TIME: less than 5 min per DB

- Weak / default passwords
  Try to change weak passwords, Analyze the application, …
  TIME: 1-6 months per DB

- Dangerous packages granted to public
  (Oracle's default setting: UTL_TCP, UTL_HTTP, HTTPURITYPE, DBMS_SQL)
  TIME: less than 5 min per DB)

Where to start – Identify 2 or 3 databases – Resolution



- Apply at least the latest, supported patchset (e.g. 10.2.0.4)
  TIME: at least 8 hours per DB
- No Oracle Security Patch (CPU) applied
  TIME: at least 4 hours per DB
- Unsecure application code
  (Find and fix SQL Injection in custom PL/SQL code)
  TIME: 1 month til 3 years per DB

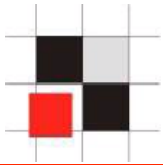
Where to start – Listener.log

The Oracle listener.log should be analyzed on a regular basis to find out:

- Who is accessing the database when
- Programs used to access the DB (e.g. TOAD on a production database, licensing issues)
- Database links accessing the DB
- D.O.S. attempts (stop TNS listener, rare)
- What remote apps must be changed during a password change

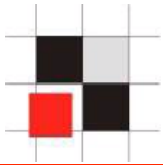
Keep in mind that most of the entries in the TNS protocol (like program, username, …) can be forged but most attackers are not doing this

Monitor Listener.log with external table



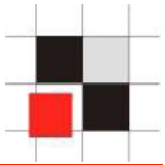
```
create table listener_log (
   log_date date,
   connect_string varchar2(300),
   protocol_info varchar2(300),
   action varchar2(15),
   service_name varchar2(15),
   return_code number(10)
)
organization external (
   type oracle_loader
   default directory LISTENER_LOG_DIR
   access parameters   (
      records delimited by newline
      nobadfile
      nologfile
      nodiscardfile
      fields terminated by "*" lrtrim
      missing field values are null  (
          log_date char(30) date_format
          date mask "DD-MON-YYYY HH24:MI:SS",
          connect_string,
          protocol_info,
          action,
          service_name,
          return_code      )    )
   location ('listener.log'))
reject limit unlimited
/
```

Monitor Listener.log with external table



```
create or replace function parse_listener_log_line
   (
       p_in varchar2,
       p_param in varchar2
   )
   return varchar2
   as
       l_begin     number(3);
       l_end       number(3);
      l_val       varchar2(2000);
  begin
      if p_param not in (
              'SID', 'SERVICE_NAME','PROGRAM','SERVICE',
              'HOST','USER', 'PROTOCOL','TYPE',
              'METHOD','RETRIES', 'DELAY','PORT','COMMAND'
      ) then
          raise_application_error (-20001,'Invalid Parameter Value '|
|p_param);
      end if;
      l_begin := instr (upper(p_in), '('||p_param||'=');
      l_begin := instr (upper(p_in), '=', l_begin);
      l_end := instr (upper(p_in), ')', l_begin);
      l_val := substr (p_in, l_begin+1, l_end - l_begin - 1);
      return l_val;
  end;
 /
```

Show all programs accessing the DB



```
select parse_listener_log_line(connect_string,'PROGRAM') program,
       count(1) cnt
from listener_log
group by parse_listener_log_line(connect_string,'PROGRAM');
-----------------------------------------------------------------------
C:\InstalledPrograms\Quest Software\TOAD\TOAD.exe                     1
C:\Program Files\Actuate7\Server\operation\fctsrvr7.exe          25,796
C:\Program Files\Embarcadero\DBA700\DBArt700.exe                     53
C:\Program Files\Informatica PowerCenter 7.1\Client\pmdesign.exe      1
C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE                 20
C:\Program Files\Microsoft Office\Office10\MSACCESS.EXE               4
C:\Program Files\Oracle\jre\1.1.8\bin\jrew.exe                        9
C:\Program Files\Quest Software\TOAD\TOAD.exe                       846
c:\9I_CLIENT\bin\sqlplus.exe                                          5
exp@odsddb01                                                          2
oracle                                                               31
oracle@stcdwhdd                                                       4
sqlplus                                                              20
```

Where to start – Oracle Policy

- Based on the results from the previous scan, a policy with the recommendations could be useful (especially for new installations).
- Smaller is better…
- Do not use the SANS list from the internet.
  This list contains 300+ more or less useful recommendations (e.g. revoke all privileges from public)
- A policy should have less than 10 pages and 40 settings.

Where to start – Identify the critical databases

- Many companies are not aware about their critical databases
- Identifying the most important assets
  - Grid Control Instances (contain all passwords for all databases)
  - Research Results
  - Company secrets (formulas, patents, …)
  - Merger & Acquisition
  - …

Where to start – Check the critical databases

- Every critical database should be check separately
- Plan 1 or 2 days per database (e.g. 6-15 DB in our 1,000 instance example)
- Develop a plan how to harden these databases

Where to start – Analyze 3rd party applications/DB

- 3rd party applications are often the most unsecure databases in a corporation because the 3rd party vendor often installs the entire system including database. This installation is different from the corporate standard.
- 3rd party vendor are supporting multiple different databases (Oracle, MSSQL, MySQL, DB2) and their knowledge in Oracle is normally poor.
- Typical quotes from 3rd party vendors are: "If you change this setting we are no longer supporting the application", "Our app requires DBA privileges", "The app must be installed in the SYSTEM tablespace"

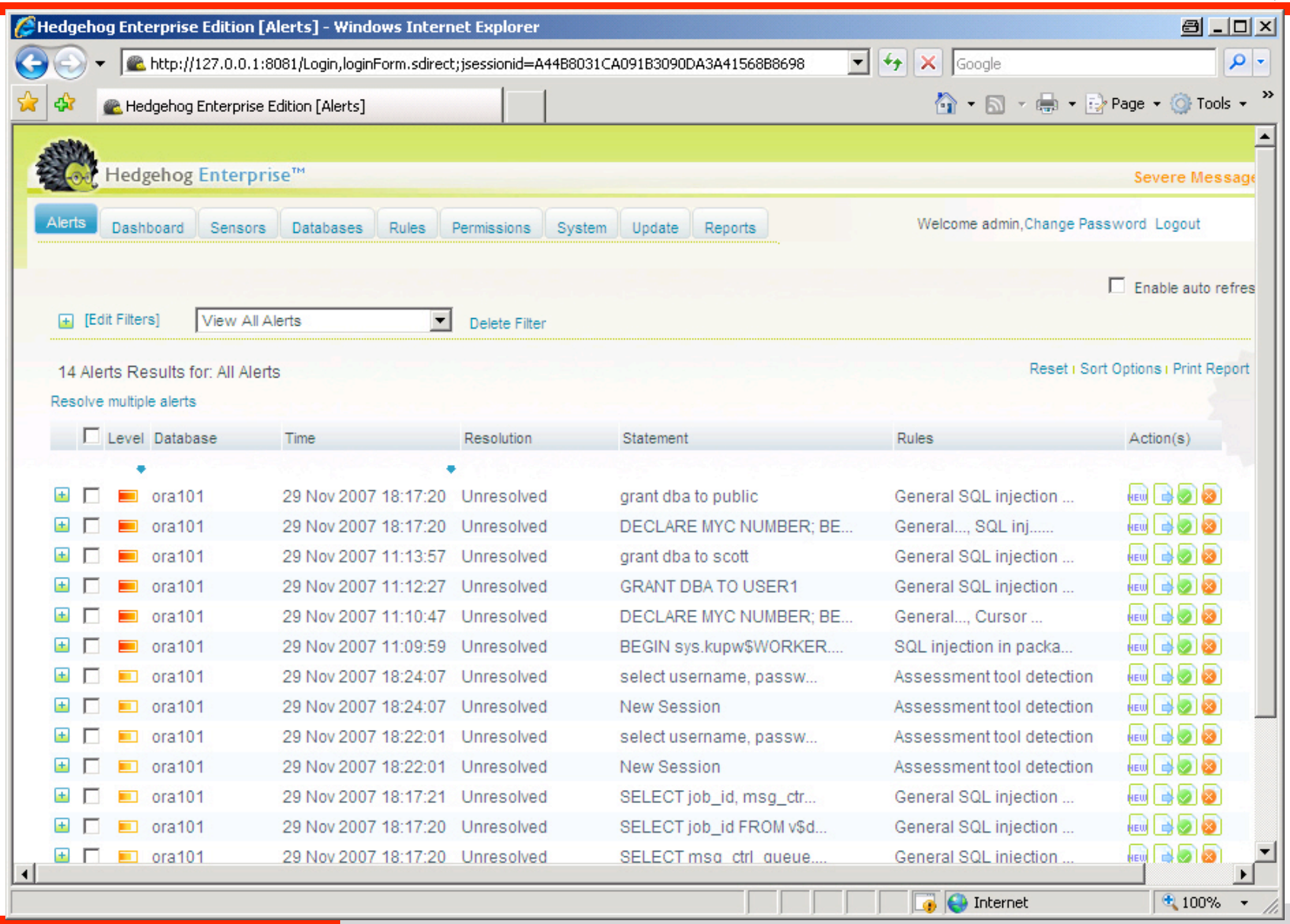
Useful Software for Oracle in company environments

- Special software could help you to deal with the problems mentioned in this presentation
  - Monitoring / Patching Solution
    (e.g. Sentrigo Hedgehog)
  - Database Scanner for companies
    (e.g. Repscan from Red-Database-Security)

Useful Software – Sentrigo Hedgehog

- Hedgehog is a real-time database activity monitoring, auditing and breach prevention software
- Little performance impact (less than 5%)
- Allows to monitor DBA access. Important because hackers often become DBA
- Virtual patching. Protect against a known vulnerabilities

Useful Software – Sentrigo Hedgehog



Useful Software – Sentrigo Hedgehog

Resolution	Statement	Rules	Action(s)
Unresolved	grant dba to public	General SQL injection ...	
Unresolved	DECLARE MYC NUMBER; BE...	General..., SQL inj.....	
Unresolved	grant dba to scott	General SQL injection ...	
Unresolved	GRANT DBA TO USER1	General SQL injection ...	
Unresolved	DECLARE MYC NUMBER; BE...	General..., Cursor ...	
Unresolved	BEGIN sys.kupw$WORKER....	SQL injection in packa...	

Useful Software – RDS Repscan

- Repscan was designed to scan large amount of databases with a small reports
- Fast and easy to use
- Command line interface

Summary

- Oracle Security is a process. It takes time to fix the biggest issues
- Start with listener-security and passwords first.
- Raise the bar for the attacker.
- Fix the biggest holes first.

Links

- Listener.log analysis:
  http://www.red-database-security.com/scripts/analistener.sql
- Checkpwd:
  http://www.red-database-security.com/software/checkpwd.html
- Repscan:
  http://www.red-database-security.com/software/repscan.html
- Sentrigo Hedgehog:
  http://www.sentrigo.com/

red database security

Contact

Red-Database-Security GmbH
Bliesstraße 16
66538 Neunkirchen
Germany

Phone: +49 - 174 - 98 78 118
Fax: +49 – 6821 – 91 27 354
E-Mail: training at red-database-security.com