



# Hacking & Defending Databases

Todd DeSantis

Technical Pre-Sales Consultant

[todd@sentrigo.com](mailto:todd@sentrigo.com)

# Agenda

- Database hacking in 2007
  - Why, Who, What, How
- Google Hacking
- SQL Injection
- General Security Recommendations
- The Best Security Recommendation
  - (Proactive Real-Time DB Monitoring, Alerting, Prevention)



# What happened in the last 3 years?

- February 2005: ChoicePoint Breach
  - Credit history information
  - Classic social engineering attack
  - Result: 163k consumer records stolen, \$15M in penalties and charges, security audits until 2026...
- December 2005: Guidance Software Inc. Breach
  - 3,800 Credit cards, names and more of professionals from NSA, FBI, CIA...
  - Probably SQL injection attack via the web
- Also in 2005 - -- University of Southern California, Boston College, California State University, Chico and the University of Georgia, Lexis Nexis, PayMaxx, San Jose medical, DSW all suffered high profile data breaches ...



# This Year



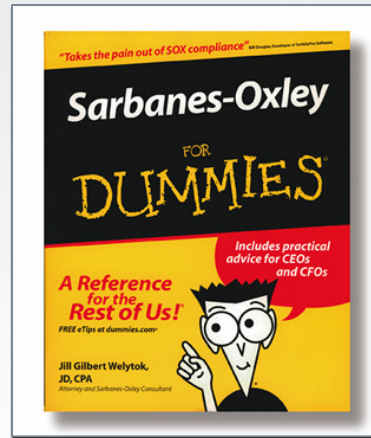
- July 2005 - January 2007: TJX
  - 45.7M+ credit/debit card records stolen
  - Sophisticated attack (WiFi -> Internal Network -> DB)
  - Result: data sold to data brokers and used in many scams, TJX faces lawsuits and losses of \$25M until May 07 (will grow considerably)
- July 2007 - Fidelity National Information Services
  - Bank and credit data of 2.3M customers
  - Stolen by a DBA
- And many more breaches... not only in the U.S. (e.g. Home Office breach in the U.K.)
- Many breaches are unknown or not made public
- Many breaches remain undetected



# What else happened during these years?

- Regulations kicking in:

- SB 1386
- Sarbanes Oxley
- PCI-DSS
- SAS 70
- and more...

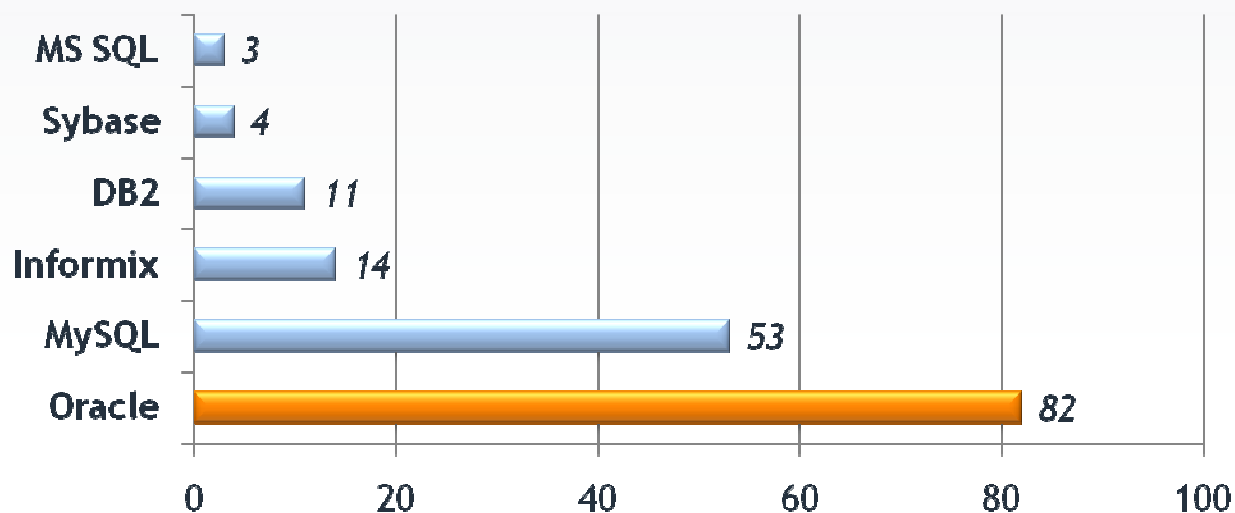


- Bad guys are getting more "professional"
- Perimeter firewalls are doing a better job at protecting databases from external threats
- Insider threat continues to grow
  - Outsourcing IT is the norm
- Database vendors begin to acknowledge vulnerabilities



# Vulnerabilities abound

- The most widely used, diverse and complicated DBMS - Oracle is the center of attention as regards DBMS security threats
- CVE (*Common Vulnerabilities and Exposures, an independent security website*) lists the no. of vulnerabilities for DBMSs as follows:

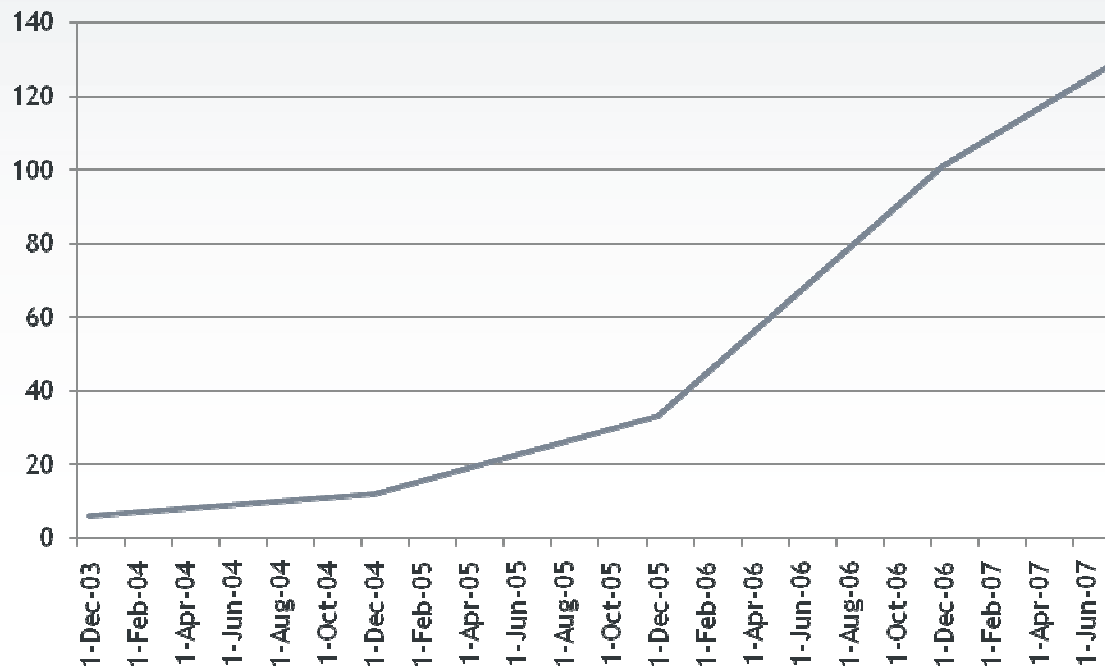


*No. of vulnerabilities reported since Jan 2006*



# Oracle database CVEs (Common Vulnerabilities and Exposures)

Total Number of CVEs from 2003  
(accumulated)



# Why Protect The Database?

- Databases hold sensitive information - and lots of it:
  - Customer data, accounts, transactions, payroll, investor data
- When a breach occurs, damage is significant:
  - Direct damages and costs
  - Bad publicity
  - Regulatory penalties
- What is more important to protect than the database?



# Know Your Enemy

- Unauthorized access - not just hackers
  - Too many privileges
- Internal attacks
  - Disgruntled employees
  - Just trying to get the job done
  - Industrial espionage, Identity theft, etc.
  - Look around you!!!
- External attacks



# The Database: Exposed

- Does a hacker need DBA access?
- Myriads of privileges
  - System level, Application level, Data access
  - Any privilege in the right circumstances can be an issue
- Other issues
  - Incorrect configuration
  - Too many features - large attack surface



# Available Exploits

- Have someone grant you DBA or ALL PRIVILEGES or ALTER USER
- Default passwords
- Password hashes
- Vulnerable code
- Built-in package exploits
  - `dbms_metadata.get_ddl`
  - `ctxsys.driload.validate_stmt`
  - Many more



# To Protect your DB... Become a Hacker

- Hackers are trying:
  - To cause damage
  - Steal
  - Gain access to host systems
- Think like a hacker
  - Learn exploits
  - Look for security issues
    - ◆ Configuration, permissions, bugs



# Finding Available Services

- Google Hacking
  - <http://johnny.ihackstuff.com/ghdb.php>
  - ora tnsnames, iSQL isqlplus
  - 0-Day Database Hacks - Become a DBA
- Use tools for:
  - Brute force password cracking
  - Guessing service names and versions
  - <http://www.petefinnigan.com/tools.htm>



# Google Hacking

filetype:ora tnsnames - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help BlinkList

http://www.google.co.il/search?num=100&hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=kIs&q=filetype:ora tnsnames

Google Hacking Database filetype:ora tnsnames

Google Web Images Groups News Scholar more »

filetype:ora tnsnames Search Advanced Search Preferences

Web Results 1 - 100 of about 236 for filetype:ora tnsnames. (0.24 seconds)

[3.6 Configure TNSNAMES.ORA - Interagency Electronic Reporting ...](#)  
tnsnames.ora Network Configuration File: /home/oracle/product/10g/network/admin/  
tnsnames.ora # Generated by Oracle configuration tools. ...  
elandingstest.alaska.gov/confluence/display/ERS/3.6+Configure+TNSNAMES.ORA - 17k -  
Cached - Similar pages

[Tnsnames.ora - Oracle FAQ](#)  
TNSNAMES.ORA is a SQL\*Net configuration file that defines databases addresses for  
establishing connections to them. This file normally resides in the ...  
orafaq.com/wiki/Tnsnames.ora - 11k - Cached - Similar pages

[TNSNAMES.ORA Network Configuration File: C:\oracle\ora92\network ...](#)  
ORA Network Configuration File: C:\oracle\ora92\network\admin\tnsnames.ora # Generated  
by Oracle configuration tools. KEN = (DESCRIPTION = (ADDRESS\_LIST ...  
www.orafaq.com/maillist/oracle-l/2002/08/att-1668/tnsnames.ora - 2k - Supplemental Result -  
Cached - Similar pages  
[ More results from www.orafaq.com ]

[TNSNAMES.ORA Configuration File /oracle/OraHome1/network/admin ...](#)  
ORA Configuration File: /oracle/OraHome1/network/admin/tnsnames.ora # Generated by  
Oracle configuration tools. DARE EXZILLA ...  
www.exzilla.net/docs/sampleFiles/viper/admin/tnsnames.ora - 2k - Cached - Similar pages

[CVS log for ORACLE/admin/tnsnames.ora](#)  
CVS log for ORACLE/admin/tnsnames.ora. [BACK] Up to [Harp Software Repository] /  
ORACLE / admin. Request diff between arbitrary revisions ...  
harp.web.cern.ch/harp/cgi-bin/cvsweb/cvsweb.cgi/ORACLE/admin/tnsnames.ora - 12k -  
Supplemental Result - Cached - Similar pages

[Akadia AG, Arvenweg 4, CH-3604 Thun tnsnames.ora ...](#)  
ORA ###----- # NetService in TNSNAMES.ORA replaces SID  
Parameter used # in Oracle7 and Oracle8 Releases. ...  
www.akadia.com/services/linux/ora817/tnsnames.ora - 2k - Cached - Similar pages

[Akadia AG, Arvenweg 4, CH-3604 Thun, Switzerland tnsnames.ora ...](#)  
Akadia AG, Arvenweg 4, CH-3604 Thun, Switzerland tnsnames.ora ... ORA ###  
----- # NetService in TNSNAMES. ...  
www.akadia.com/services/win-nt/ora816/tnsnames.ora - 2k - Cached - Similar pages  
[ More results from www.akadia.com ]

newidconnect(uffl\_inufltk\_#nsnames.ora - view\_4\_4

Scripts Currently Forbidden [<SCRIPT>: 2] [<OBJECT> (Java, Flash, Plugin): 0]

Done

start Search Desktop EN 100% 2:36 PM

# Google Hacking

```
oracle@slavik-vm1:~  
)  
SYNTAX =  
  (DESCRIPTION =  
    (ADDRESS = (PROTOCOL = TCP) (HOST =          ) (PORT = 1521))  
    (CONNECT_DATA = (SID = T))  
  )  
  
EXTPROC_CONNECTION_DATA =  
  (DESCRIPTION =  
    (ADDRESS_LIST =  
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1))  
    )  
    (CONNECT_DATA =  
      (SID = PLSExtProc)  
      (PRESENTATION = RO)  
    )  
  )  
)  
  
[oracle@slavik-vm1 ~]$ tns ping syntax  
  
TNS Ping Utility for Linux: Version 10.2.0.1.0 - Production on 10-JUL-2007 14:48  
Copyright (c) 1997, 2005, Oracle. All rights reserved.  
  
Used parameter files:  
/u01/app/oracle/product/10.2.0/db_1/network/admin/sqlnet.ora  
  
Used TNSNAMES adapter to resolve the alias  
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST =  
OK (2040 msec)
```



# Google Hacking

```
oracle@slavik-vm1:~  
Used TNSNAMES adapter to resolve the alias  
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = .  
OK (2040 msec)  
[oracle@slavik-vm1 ~]$ lsnrctl status systax  
  
LSNRCTL for Linux: Version 10.2.0.1.0 - Production on 10-JUL-2007 14:50:21  
  
Copyright (c) 1991, 2005, Oracle. All rights reserved.  
  
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST= . ) (PORT=1521)  
) (CONNECT_DATA=(SID=T)))  
STATUS of the LISTENER  
-----  
Alias                LSNR  
Version              TNSLSNR for Solaris: Version 8.1.7.4.0 - Production  
Start Date           24-MAY-2007 14:44:03  
Uptime               46 days 23 hr. 9 min. 45 sec  
Trace Level          off  
Security             OFF  
SNMP                 OFF  
Listener Parameter File /home/oracle/ora817home/network/admin/LSNR/listener.or  
a  
Listener Log File    /home/oracle/ora817home/network/log/lsnr.log  
Listening Endpoints Summary...  
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST= . ) (PORT=1521)))  
Services Summary...  
Service "S_TEST.world" has 2 instance(s).  
  Instance "S_TEST", status READY, has 1 handler(s) for this service...  
  Instance "S_TEST", status READY, has 1 handler(s) for this service...  
Service "T.world" has 2 instance(s).  
  Instance "T", status READY, has 1 handler(s) for this service...  
  Instance "T", status READY, has 2 handler(s) for this service...  
Service "TMP.world" has 1 instance(s).  
  Instance "TMP", status READY, has 1 handler(s) for this service...  
The command completed successfully  
[oracle@slavik-vm1 ~]$
```

# SQL Injection

- Wikipedia -
  - is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.



# SQL Injection

- Exists in
  - Applications
  - Stored program units
    - ◆ Built in
    - ◆ User created
- Several types
  - Inject SQL, Inject Functions
  - Anonymous blocks of code



# SQL Injection - Web Application

- Username = ' or 1=1 --

The original statement looked like:

```
'select * from users where username = ''' + username +  
''' and password = ''' + password + '''
```

The result =

```
select * from users where username = " or 1=1 --" and  
password = "
```



# SQL Injection - Built-In Packages

- Every time Oracle patches, several are for SQL Injection vulnerabilities
  - Oct '07 CPU has 27 DB specific vulnerabilities
    - ◆ 5 of these can be exploited without user authentication
- Hacker boards - New ways to hack into Oracle are coming out all the time
- Oracle CPUs and hacking forums - Roadmaps to your data



# Protecting Your Database

- Apply patch sets, upgrades and CPUs
  - Easier said than done
- Check for default and weak passwords regularly
- Secure the network
  - Listener passwords
  - Valid node checking + firewall
  - Use encryption



# Protecting Your Database

- Install only what you use, remove all else
  - Reduce your attack vector
- The least privilege principle
  - Lock down packages
    - ◆ System access, file access, network access
- Encrypt critical data
- Use secure coding techniques
  - Bind variables, ownership



# Protecting Your Database

- Try out the Hedgehog -  
FREE TRIAL
- <http://www.sentrigo.com>
  - Virtual patching
  - SQL Injection protection
  - Fine grain auditing
  - Centralized management
  - Terminate rogue sessions
  - More



# Questions?

