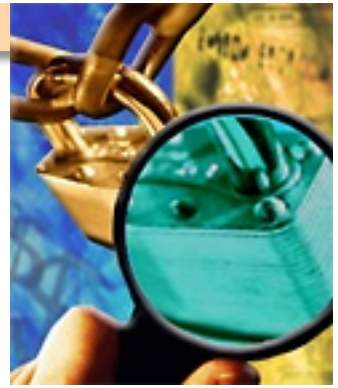
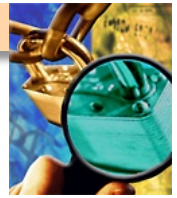


Database Assessment

Vulnerability Assessment Course

All materials are licensed under a Creative Commons “Share Alike” license.



- **http://creativecommons.org/licenses/by-sa/3.0/**

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Agenda

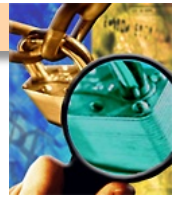
- Introduction
- Configuration Guidance
- Operating System Configuration
- Database Installation
- Default Database Configurations
- Identification and Authentication
- Auditing and Monitoring
- Overview of Oracle Testing
- Overview of SQL Server Testing

Introduction

- Database Security focuses on the use of database management systems to protect systems and data from unauthorized:
  - Access
  - Creates
  - Reads
  - Updates
  - Deletes

Relational Database Management Systems

- Sublanguages
  - Data Definition Language (DDL) defines structure
  - Data Control Language (DCL) defines security/access controls
  - Data Manipulation Language (DML) for data query/updates
- Interface drivers – code libraries for prepare statements, execute statements, and fetch results
  - SQL*Net/Net8
  - Open Database Connectivity (ODBC)
  - Java Database Connectivity (JDBC)
- SQL Engine interprets/executes DDL, DCL, and DML
- Other Engines
  - Transaction – statements either succeed or fail as a group
  - Relational – integrity constraints
  - Storage – data modification, commit/rollback, and backup/recovery



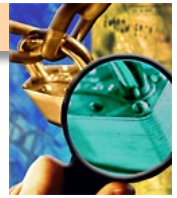
Breadth of Technology

- **Examples of Databases**
  - Oracle
  - Microsoft SQL
  - MySQL
  - DB2
  - Informix
  - TeraData
  - Sybase
- **Examples of Database Applications**
  - Oracle Financials
  - SAP
  - SAS

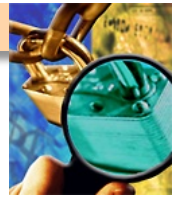
Considerations

- Majority of tests performed on live production systems
  - Limit to non-destructive testing
  - Penetration testing vs. Vulnerability Assessment/Compliance
- Database similarities allow for similar tests
  - Different products use different commands/procedures
  - Features are similar yet different between products
- Must be very familiar with the product and add-ons to
  - Eliminate false positives
  - Be taken seriously by administrators
  - Know most important product add-ons
  - Where is the database within the system architecture
  - Understand the database purpose

Security Configuration Guidance

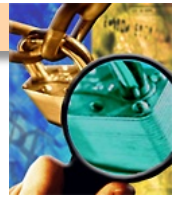


- DISA Guidance – Secure Technical Implementation Guides (STIGS) and Checklists
- NSA Security Configuration Guidance
- NIST Security Configuration Checklists
- Center for Internet Security (CIS) Benchmarks
- Vendor Database Security Guidance



What is a STIG?

- What is a Database STIG?
  - Guidance on technical security policy, requirements, and implementation details
  - Covers major vendors' database product
  - Provides classification guidance for weaknesses found
- What it is not?
  - Step by step implementation guide
  - Guidance to be taken literally
  - Always consistent and up to date
  - Always applicable to commercial or non-DoD environments



What Else Is It Not?

Hackers

- highly-skilled, but few in numbers, break mostly into "challenging" systems, publish/trade weaknesses

➢Hackers look for new security weaknesses

Not Addressed

Script Kiddies

- low-skilled, but numerous, use other peoples' tools to break into systems
- goal is to "OWN" as many machines as possible

➢Script Kiddies look for systems vulnerable to known exploits

Addressed

Social Engineers

- very good technical as well as social skills
- attacks are primarily directed against humans ('wetware')

➢Social Engineers look for clues on which they can base their attacks.

Partially Addressed

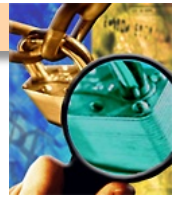
(Disgruntled) Employees

- use insider knowledge to gain system access
- motivated by curiosity or anger
- Disgruntled employees will try to damage the IT infrastructure

➢Employees usually look for HR information (e.g. salary) or want to enrich themselves

Partially Addressed

Common Pitfalls

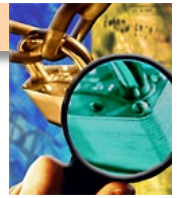


- Guidance can be out-of-date
  - Covers only the “core” product
  - What about add-on options?
  - Some add-on options are not so optional
  - Infrastructure and system architecture in which the DB operates not taken into account
- Familiarity with a variety of vendor add-on products or 3rd party tools used to
  - Manage the database
  - Monitor the database
  - Backup the database
  - Perform ETL operations on the database
  - Authentication constraints imposed by tools
  - Permissions required to run tools
  - Constraints imposed by application using DB

Operating System Configuration

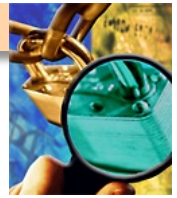
- Permissions on the OS directories and on the binary files
  - Why bother to break into the database if you can just take the database files
- Permissions of critical configuration files
- Permissions of installation, log, trace, and files

Database Installation



- Root of many problems
  - "All or nothing" option when installing some products
- Removal of options difficult if not impossible
  - If at all possible, vendor technical services needed in some cases
- Demonstration code in the database and on the binary install base
- Java Virtual Machines (JVM) and Java Runtime Environments (JRE) inside the database and in the binary install base
- Fully functioning, unsecured J2EE containers
- DBMS version maintenance
- Updated patch and fix installation

When Your Database Looks Like The Web



Methods for HttpSoap11 - Microsoft Internet Explorer provided by MITRE

File Edit View Favorites Tools Help

Back Search Favorites

Address http://sternschnuppe:8888/javacallout/javacallout?HelloServiceEJBHttpSoap11stub.html

Google Go Bookmarks 195 blocked Check AutoLink AutoFill Send to Settings

Method Summary

HttpSoap11_getProperties ()
Synchronous invocation of operation: getProperties

HttpSoap11_getProperty ()
Synchronous invocation of operation: getProperty

HttpSoap11_propertyNames ()
Synchronous invocation of operation: propertyNames

HttpSoap11_sayHello ()
Synchronous invocation of operation: sayHello

HttpSoap11_getPropertiesAsync ()
Asynchronous invocation of Operation: getProperties

HttpSoap11_getPropertyAsync ()
Asynchronous invocation of Operation: getProperty

HttpSoap11_propertyNamesAsync ()
Asynchronous invocation of Operation: propertyNames

HttpSoap11_sayHelloAsync ()
Asynchronous invocation of Operation: sayHello

HttpSoap11_getProperties

```
string[] HttpSoap11_getProperties (string[] arrayOfString_1);
```

HttpSoap11_getProperty

```
string HttpSoap11_getProperty (string String_1);
```

HttpSoap11_propertyNames

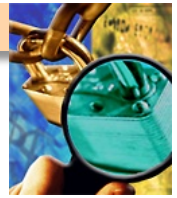
```
string[] HttpSoap11_propertyNames ();
```

HttpSoap11_sayHello

```
string HttpSoap11_sayHello (string String_1);
```

Local intranet

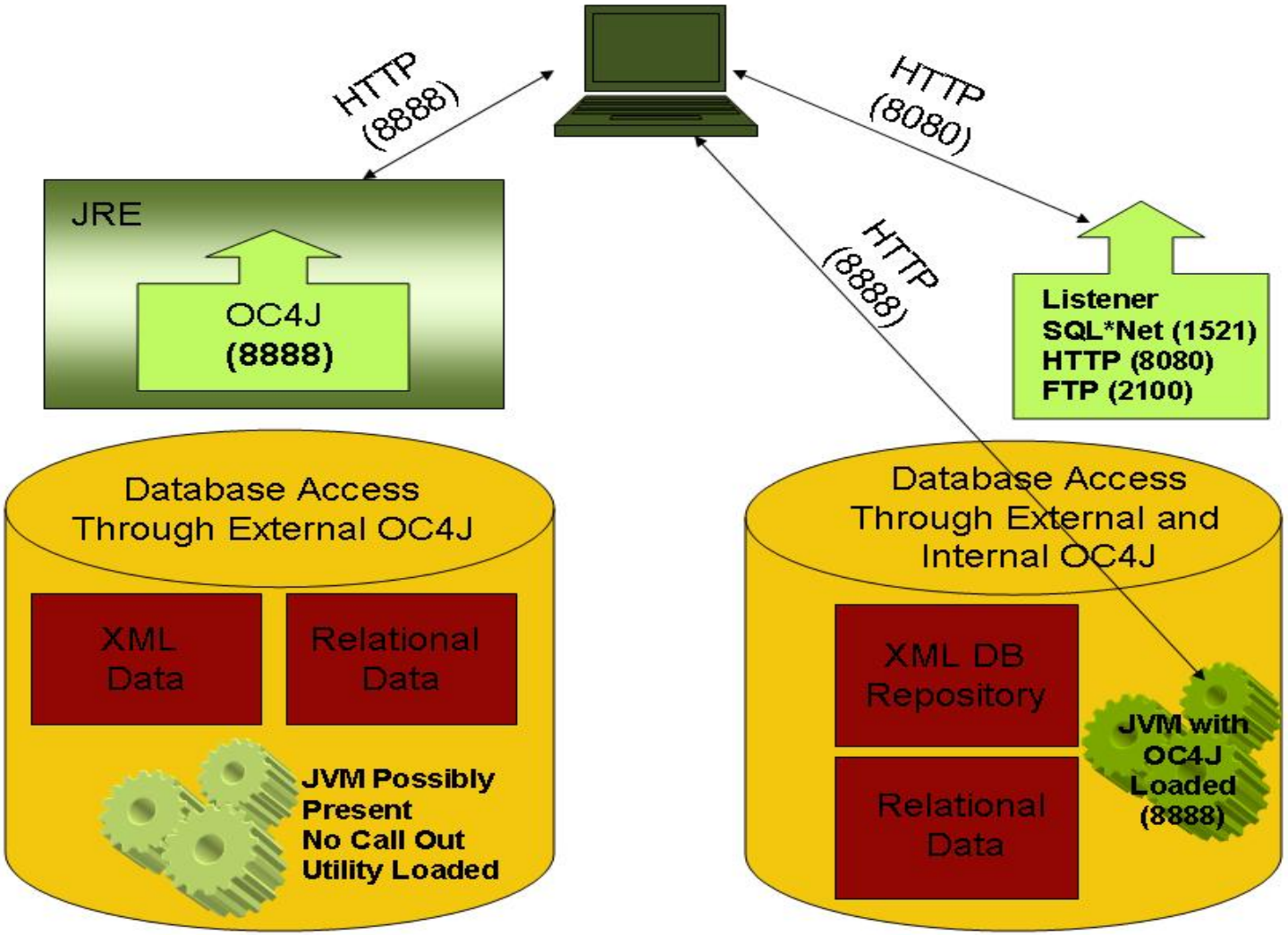
Default Oracle LISTENER Configuration 10g



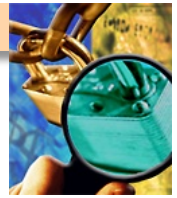
Telnet

```
$ lsnrctl status

LSNRCTL for Solaris: Version 10.2.0.1.0 - Production on 01-MAR-2007 11:45:56

Copyright (c) 1991, 2005, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC2)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Solaris: Version 10.2.0.1.0 - Production
Start Date                01-MAR-2007 11:05:35
Uptime                    0 days 0 hr. 40 min. 21 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /export/oracle/10g/network/admin/listener.ora
Listener Log File         /export/oracle/10g/network/log/listener.log
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC2)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=s[illegible])(PORT=1522)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=[illegible])(PORT=8080))(Presentat
ion=HTTP)(Session=RAW))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=[illegible])(PORT=2100))(Presentat
ion=FTP)(Session=RAW))
Services Summary...
Service "PLSExtProc" has 1 instance(s).
  Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
Service "V880" has 1 instance(s).
  Instance "V880", status READY, has 1 handler(s) for this service...
Service "V880XDB" has 1 instance(s).
  Instance "V880", status READY, has 1 handler(s) for this service...
Service "V880_XPT" has 1 instance(s).
  Instance "V880", status READY, has 1 handler(s) for this service...
The command completed successfully
$
```

Default Oracle 11g Database Access

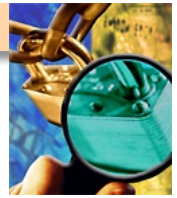


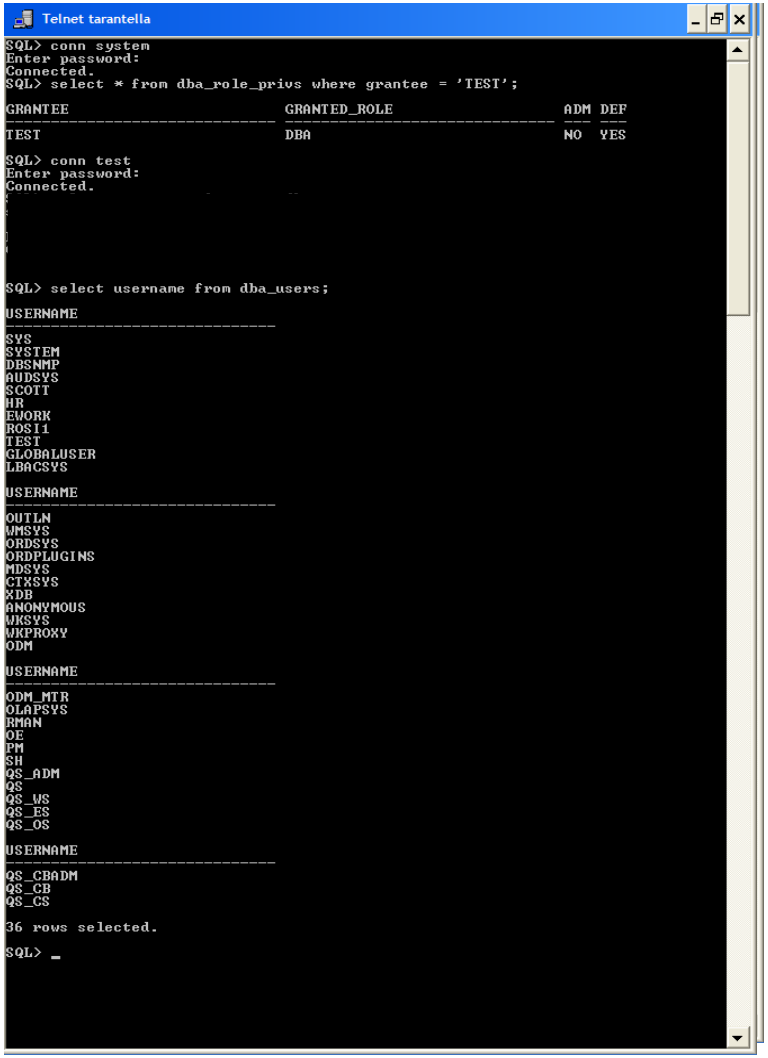
More Exploits, No Checklists



- Previous examples showed default installation issues
  - Database is no longer accessible with SQL*Net only
  - JRE installed as an external component to the database
  - Internal JVM is another potential vulnerability
- Next example demonstrates
  - Behavior of invoker vs. definer rights
  - PUBLIC assignment of privileges
  - Exploit using both to elevate user privileges from next to none to DBA
- What you should take away from these examples
  - Some guidance does not always address vulnerabilities
  - Gap needs to be addressed by manual testing and ad-hoc probing
  - There are no checklists for this!

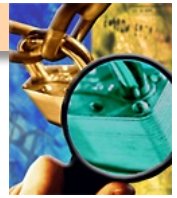
Escalation of privileges





- Unpatched Oracle 9i
- Create user (TEST)
- Minimal privilege (CREATE SESSION and PUBLIC privileges)
- TEST user executes CTXSYS package with rogue command
- TEST user has DBA privileges

DBA Role

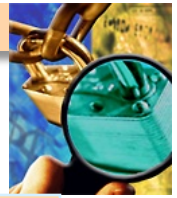


- DBA role is very powerful and access to it should be restricted
- Verify that any database account granted the DBA role is explicitly authorized
- Individual DBA accounts should be created for each DBA
- DBA accounts used only for DBA functions

Identification and Authentication

- OS-based authentication mode
  - Different databases, different modes
    - MS SQL Server – Windows or server authentication
    - Oracle – OS authentication or remote authentication
- Default or blank passwords
  - Oracle accounts…too many!!!
    - 483 unique default accounts
    - 46 accounts have multiple default passwords, depending on version
    - 597 total default password possibilities
- Oracle LISTENER security
  - Local OS authentication is used for listener security in Oracle 10g and higher version
  - Prior to 10g, password did not follow best practices
    - Age, strength, history, and lockout

Oracle Connection Security



- listener.ora file
  - Program = extproc

```
# listener.ora Network Configuration File: C:\oracle\product\10.1.0\db_
1\NETWORK\ADMIN\listener.ora
# Generated by Oracle configuration tools.

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = C:\oracle\product\10.1.0\db_1)
      (PROGRAM = extproc)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = IOWACSVRSTLDB)(PORT = 1521))
    )
  )
```

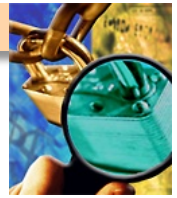
- sqlnet.ora file
  - TCP.VALIDNODE_CHECKING = yes
  - TCP.INVITED_NODES = list of accepted TCP/IP addresses
  - TCP.EXCLUDED_NODES = list of unallowed TCP/IP addresses

```
# sqlnet.ora Network Configuration File: C:\oracle\product\10.1.0\db_1
\NETWORK\ADMIN\sqlnet.ora
# Generated by Oracle configuration tools.

SQLNET.AUTHENTICATION_SERVICES= (NTS)

NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
```

Database Links and Remote Connections

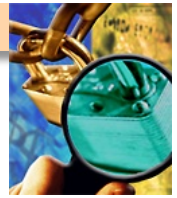
- Available for almost all databases
- Are they required for this database to operate?
- Ensure that the database object containing the link and password information is not accessible

Data Confidentiality



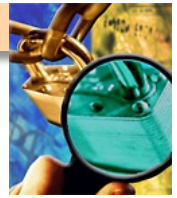
- Data in transit
  - Per default, database connections are not encrypted
  - Some vendors' encryption capabilities are add-on purchases and expensive
  - Consider encrypting JDBC connections
- Data at rest
  - Encryption of Personally Identifiable Information (PII) data in the database
  - Encryption of database data means
    - Examine any custom code used to encrypt data
    - Examine the encryption algorithms used and the implementation details
    - Some use Vormetric or Decru…issues with key management
  - Newer versions of Oracle and SQL Server offer data encryption

Data Integrity



- Assurance that data is consistent throughout various data operations
- Most guidance does not cover this aspect
- Application and business process dependent
- Highest levels of data integrity are in databases with rigid business process frameworks like Oracle Financials and SAP
- Both Oracle and SQL Server allow developers to wrap custom code
  - SQL Server – Encrypted Stored Procedures
  - Oracle – Database Source Code Object Encryption/Encoding

Auditing and Monitoring – A Sore Subject



- Auditing and Monitoring is resource intensive
  - Human resources
  - Computing resources
- Different audit settings for different databases
  - Audit the privileged and database users
  - Various level of audit settings
  - Location of audit data
    - Choice of OS, DB, extended, XML (Oracle)
    - Set audit destination (SQL Server)
  - Permissions on audit data files
- Most guidance is excessive – balance it with resources
- Frequently no auditing is performed at all
- Fine-grained auditing installed 90%, but only used 10% of time

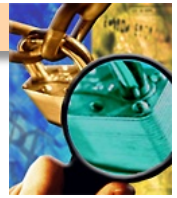
Backup and Recovery

- Main focus is on backup procedures
  - Poor OS permissions
  - “Cold” backup files – entire database at a point in time
  - “Hot” backup or archive log files – incremental data changes written to the redo logs
- Backup can also mean a quick export file, which may have World OS permissions
- Backup procedure usually involves
  - Oracle Recovery Manager (RMAN)
  - SQL Server Management Studio
  - Third-party backup tool

Overview of Oracle Testing

- Built-in users installed with excess privileges
- Default passwords and roles assigned to users
- Demo and sample schemas; well known passwords
- All or most users assigned to default tablespaces
- Users have SYSTEM tablespace assigned
- Every DBA uses SYSTEM or SYS account to manage database
- Database was not patched after installation
- Specific parameters left at default setting
- Default profiles used
- No or inadequate password management
- LISTENER has default port, name, and no security settings
- Audit not enabled

Overview of SQL Server Testing



- Big differences between SQL Server 2000, 2005, and 2008
- Built-in user account name left unchanged
- Guest User account enabled in database
- SA account password left null
- SYSADMIN fixed server role assigned to BUILTIN/ Administrators
- Fixed server and database roles used instead of custom roles
- Xp_cmdshell not removed
- Demo databases installed on the server
- DBMS object permissions granted to PUBLIC role
- SQL Server vs. Windows authentication
- Audit not enabled; audit flags not set

Questions