# Hack-proofing Oracle Databases

Aaron Newman

anewman@appsecinc.com

Application Security, Inc.

www.appsecinc.com

Download updated version of presentation from
http://www.appsecinc.com/news/briefing.html

APPLICATION SECURITY, INC.

www.AppSecInc.com

# Agenda

- State of Oracle Security
- Listener Vulnerabilities
  - Tnscmd demonstration
- Oracle in a Web application
  - SQL Injection Demo
- Database Vulnerabilities
- Resources, Conclusion, and Wrap Up

APPLICATION SECURITY, INC.

www.AppSecInc.com

# State of Oracle Security

APPLICATION SECURITY, INC.

www.AppSecInc.com

# In the media

## “Look what they've done to my database, Ma”

- **By John Leyden, The Register**

**Posted: 23/01/2002 at 17:40 GMT**

- 1 out of 10 corporate databases connected to the Internet had a breach of security last year.
- Taken from a survey of 750 US database developers which also reveals growing concern about security issues.

**http://www.theregister.co.uk/content/55/23800.html**

# Underground Hacking World

- Increasing number of presentations on hacking databases at conferences
  - Blackhat, Defcon
- Exploits being written
- Worms found in the wild using databases
  - Alpha Voyager
  - Spida worm
- Whitepapers on attack Oracle

# Oracle Website – Alerts Web page

http://otn.oracle.com/deploy/security/index2.htm?Info&alerts.htm

- Prior to July 2000
  - One vulnerability acknowledged by Oracle
- From July 2000 to August 2002
  - 41 vulnerability reports on the Oracle website
- Vulnerabilities reported on SecurityFocus.com
  - About 75 vulnerabilities reported about Oracle

# Myth – Oracle is secure behind a firewall

- Is your database secure because it's behind a firewall?
- NO!!!
- Most security compromises are result of inside jobs
- Internal threats are the most dangerous
- Non-privileged users in the database

APPLICATION SECURITY, INC.

www.AppSecInc.com

# What to do about the situation

- The problem exists but it won't be fixed tomorrow
- But we must start plugging these holes
- Become aware of the risks and threat
- Find the right solutions

# Securing the Listener service

APPLICATION SECURITY, INC.

www.AppSecInc.com

# Listener Vulnerabilities

- What is the listener?
  - Proxy between the client and the database
- Why is it important?
  - Separate authentication and auditing
  - Runs as a separate process
  - Accepts commands and performs tasks outside the database
- Vulnerabilities in Listener Service

# Security Issues with the Listener Service

- The listener must be secured with password
  - Default configuration is no password
  - lsnrctl set password
- Must set a strong password
  - Not vulnerable to brute-forcing
- Must protect the listener.ora file
  - Password stored in this file
- Do not remotely manage listener
  - Password is not encrypted over network

# Listener commands

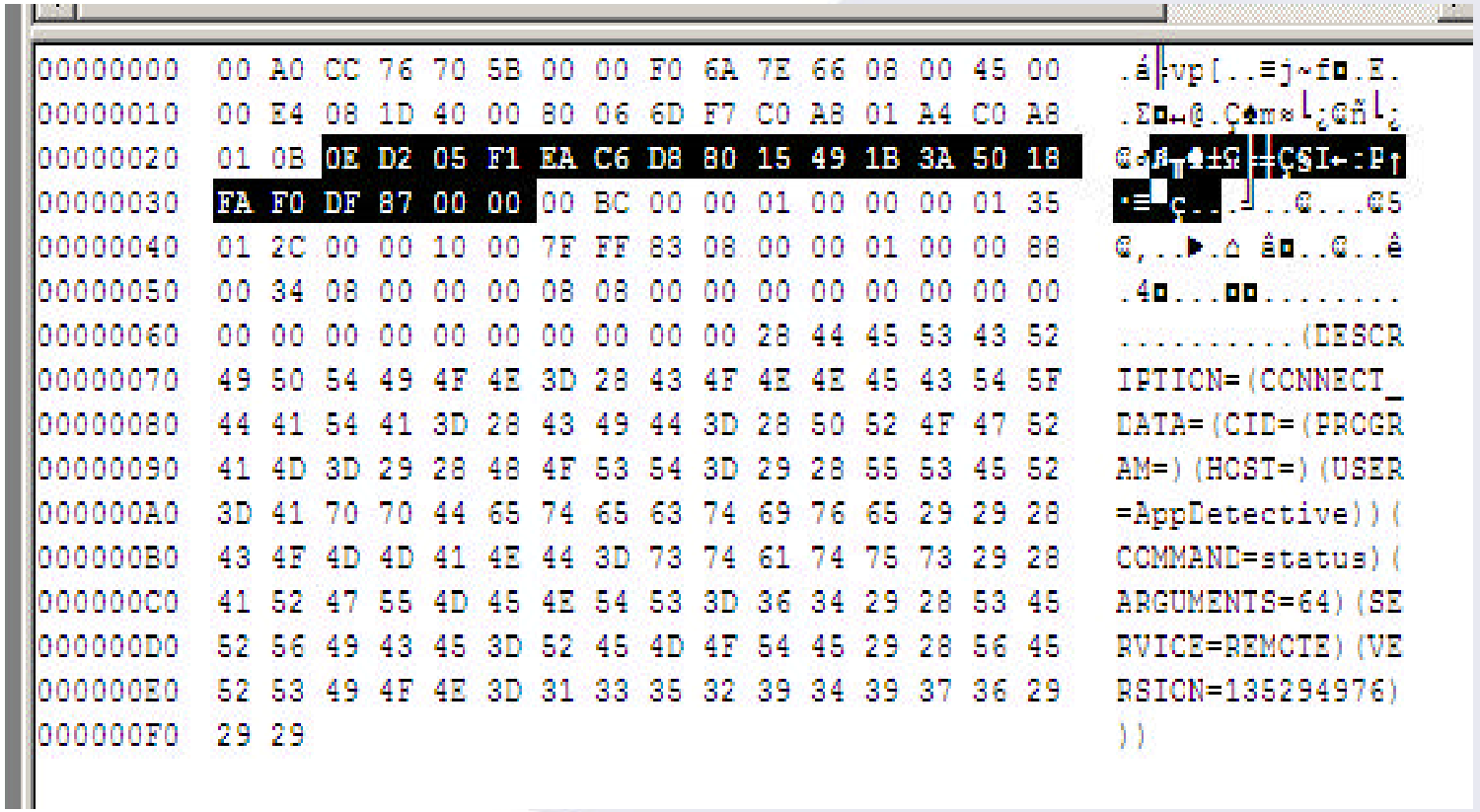
- What are the commands?
  - LSNRCTL> help
    The following operations are available

    start stop status
    quit exit set*
    show*

    password rawmode displaymode
    trc_file trc_directory trc_level
    log_file log_directory log_status
    current_listener connect_timeout startup_waittime
    use_plugandplay save_config_on_stop

# Listener packet

- Below is an example of a command:



```
00000000  00 A0 CC 76 70 5B 00 00 F0 6A 7E 66 08 00 45 00   .á╠vp[..≡j~f◘.E.
00000010  00 E4 08 1D 40 00 80 06 6D F7 C0 A8 01 A4 C0 A8   .Σ◘↔@.Ç♠m≈└¿☺ñ└¿
00000020  01 0B 0E D2 05 F1 EA C6 D8 80 15 49 1B 3A 50 18   ☺♂♫╥♣±Ω╪╪ÇSI←:P↑
00000030  FA F0 DF 87 00 00 00 BC 00 00 01 00 00 00 01 35   ·≡▀ç..┘..☺...☺5
00000040  01 2C 00 00 10 00 7F FF 83 08 00 00 01 00 00 88   ☺,..►.⌂ â◘..☺..ê
00000050  00 34 08 00 00 00 08 08 00 00 00 00 00 00 00 00   .4◘...◘◘........
00000060  00 00 00 00 00 00 00 00 00 00 28 44 45 53 43 52   ..........(DESCR
00000070  49 50 54 49 4F 4E 3D 28 43 4F 4E 4E 45 43 54 5F   IPTION=(CONNECT_
00000080  44 41 54 41 3D 28 43 49 44 3D 28 50 52 4F 47 52   DATA=(CID=(PROGR
00000090  41 4D 3D 29 28 48 4F 53 54 3D 29 28 55 53 45 52   AM=)(HOST=)(USER
000000A0  3D 41 70 70 44 65 74 65 63 74 69 76 65 29 29 28   =AppDetective))(
000000B0  43 4F 4D 4D 41 4E 44 3D 73 74 61 74 75 73 29 28   COMMAND=status)(
000000C0  41 52 47 55 4D 45 4E 54 53 3D 36 34 29 28 53 45   ARGUMENTS=64)(SE
000000D0  52 56 49 43 45 3D 52 45 4D 4F 54 45 29 28 56 45   RVICE=REMOTE)(VE
000000E0  52 53 49 4F 4E 3D 31 33 35 32 39 34 39 37 36 29   RSION=135294976)
000000F0  29 29                                           ))
```

# Listener attack demo

http://www.jammed.com/~jwa/hacks/security/tnscmd/

# What is a buffer overflow

- When a program attempts to write more data into buffer than buffer can hold
- Starts overwriting area of stack memory
  - Can be used maliciously to cause a program to execute code of attackers choose
  - Overwrites stack point

# Buffer overflows in the listener service

- Example of a connection string
  - (DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=)(HOST=)(USER=))(COMMAND=status) (SERVICE=LIST80) (VERSION=135294976)))
- Finding buffer overflows:
  - Try changing this values to see what happens
  - Try USER= with 4,000 Xs after it
  - Try SERVICE= with 4000 Xs after it
  - Etc…

# Buffer overflows in the listener

- Oracle 8.1.7
  - Sending 1 kilobyte of data for COMMAND= caused crash
  - Sending more than 4 kilobytes in the COMMAND= caused core dump
    - Problem in structured-exception handler allows hacker to execute code
- Oracle 9.0.1
  - Sending 1 kilobyte of data for SERVICE=

# Manipulating header field values

- Typical command
  - .T.....6.,.....:.....4.....(CONNECT_DATA=.)
- Garbage characters represent header information
  - Offset to data
  - Size of connection string
  - Size of packet
  - Type of packet

# Stealing Listener Commands

- The following command is sent:
  - .T.....6.,.....:.....4.....(CONNECT_DATA=.)
- Change header to say 40 bytes
  - ....."...(DESCRIPTION=(ERR=1153)(VSNNUM=135290880)(ERROR_STACK=(ERROR=(CODE=1153)(EMFI=4)(ARGS='(CONNECT_DATA=.)ervices))CONNECT'))(ERROR=(CODE=3 03)(EMFI=1))))
- Change header to say 200 bytes
  - ....."..>.H.....@(DESCRIPTION=(ERR=1153)(VSNNUM=135290880)(ERROR_STACK=(ERROR=(CODE=1153)(EMFI=4)(ARGS='(CONNECT_DATA=.)ervices))CONNECT_DATA=(SID=orcl)(global_dbname=test.com)(CID=(PROGRAM=C:\Oracle\bin\sqlplus.exe)(HOST=anewman)(USER=aaron))')) (ERROR=(CODE=303)(EMFI=1))))

# External Procedures

- Functions in DLL and shared libraries
- Can be called from PL/SQL
- Setup by creating libraries and packages:
  - CREATE LIBRARY test AS ‘msvcrt,dll’;
    CREATE PACKAGE test_function IS PROCEDURE exec(command IN CHAR);
    CREATE PACKAGE BODY test_function IS
    PROCEDURE exec(command IN CHAR)
    IS EXTERNAL NAME “system”
    LIBRARY test;

# Remotely calling External Procedures

- Not “officially” support
  - But it works
- ExtProcs are another connection point for listener
  - SID_LIST_LISTENER =
  - (SID_LIST =
  - (SID_DESC =
  - (SID_NAME = PLSExtProc)
  - (ORACLE_HOME = E:\oracle\ora81)
  - (PROGRAM = extproc)
- How does ExtProc authenticate the user
  - IT DOESN’T!!!!!!!!!

# Default setup - External Procedures

- Automatically configured?
  - Oracle 8i – YES
  - Oracle 9i - NO
- How do we fix this?
- Callout listener
  - Do not create ExtProc as another listener endpoint
  - Create its own entry in the listener.ora file
- Can only be called local then

# Oracle in a Web application

APPLICATION SECURITY, INC.

www.AppSecInc.com

# Can attacks go through a firewall?

- YES!!!
- Firewall configuration
  - Block access through port 1521
  - Only allow traffic to port 80
  - Block UDP as well as TCP
- SQL Injection
  - Not specific to Oracle
  - a web programming problem

# How does it work?

- Modify the query
- Change:
  - Select * from my_table where column_x = ‘1’
- To:
  - Select * from my_table where column_x = ‘1’ UNION select password from DBA_USERS where ‘q’=‘q’

APPLICATION SECURITY, INC.
www.AppSecInc.com

# Example JSP page

```
Package myseverlets;
<….>
String sql = new String(“SELECT * FROM
  WebUsers WHERE Username=’” +
  request.getParameter(“username”) + “’
  AND Password=’” +
  request.getParameter(“password”) + “’”
 stmt = Conn.prepareStatement(sql)
Rs = stmt.executeQuery()
```

# Valid Input

- If I set the username and password to:
  - Username: Bob
  - Password: Hardtoguesspassword
- The sql statement is:
  - SELECT * FROM WebUsers WHERE Username='Bob' AND Password='Hardtoguess'

# Hacker Input

- Instead enter the password:
  - Aa’ OR ‘A’=‘A
- The sql statement now becomes:
  - SELECT * FROM WebUsers WHERE Username=’Bob’ AND Password=’Aa’ OR ‘A’=‘A’
- The attacker is now in the database!

# Selecting from other Tables

- To select data other than the rows from the table being selected from.
- UNION the SQL Statement with the DBA_USERS view.

# Sample ASP Page

```
Dim sql
Sql = “SELECT * FROM PRODUCT WHERE
  ProductName=’” & product_name & “’”
Set rs = Conn.OpenRecordset(sql)
‘ return the rows to the browser
```

# Valid Input

- Set the product_name to :
  - DVD Player
- The SQL Statement is now:
  - SELECT * FROM PRODUCT WHERE ProductName='DVD Player'

# Hacker Input

- Set the product_name to :
  - test’ UNION select username, password from dba_users where ‘a’ = ‘a
- The SQL Statement is now:
  - SELECT * FROM PRODUCT WHERE ProductName=’test’ UNION select username, password from dba_users where ‘a’=‘a’

# Preventing SQL Injection

- Validate user input
  - Parse field to escape single quotes to double quotes
- Use the object parameters to set parameters
  - Bind variables

# SQL Injection demo

ASP page, IIS web server

Oracle database

APPLICATION SECURITY, INC.

www.AppSecInc.com

# Database Vulnerabilities

APPLICATION SECURITY, INC.

www.AppSecInc.com

# Database Security Issues

- sqlnet.log
- Popular Oracle Security Issues
- PL/SQL Vulnerabilities
  - Examples
- Host Operating System
  - Known Issues Installing Oracle
  - Lockdown Protection Procedures

# Sqlnet.log

- File is created in a directory when a connection attempt fails from a machine
- Gives too much information – username, IP address, date, etc…
- Have seen many times on public web sites

# Popular Oracle Security Issues

- Default passwords!
  - SYS, SYSTEM, DBSNMP, OUTLN,MDSYS, SCOTT
- Password management features not enabled
  - No password lockout by default
  - No password expiration by default
- Public permissions on ALL_USERS view

# PL/SQL Vulnerabilities

- Problem with dynamic SQL
  - EXECUTE IMMEDIATE
  - DBMS_SQL
- Danger allowing the user to pass parameters that are used in the parsed SQL statement

# Dynamic SQL Example

```
CREATE PROCEDURE BAD_CODING_EXAMPLE ( NEW_PASSWORD
    VARCHAR2 ) AS
TEST VARCHAR2;
BEGIN
-- DO SOME WORK HERE

EXECUTE IMMEDIATE 'UPDATE ' || TABLE_NAME || ' SET ' ||
    COLUMN_NAME || ' = '' || NEW_PASSWORD || ''‘ WHERE USERNAME=
    = '' || CURRENT_USER_NAME || '';

END BAD_CODING_EXAMPLE;
```

APPLICATION SECURITY, INC.

www.AppSecInc.com

# Valid input

- Input
  - EXEC BAD_CODING_EXAMPLE( ‘testabc’ );

- SQL Created
  - UPDATE APPLICATION_USERS SET PASSWORD = ‘testabc’ WHERE USERNAME = ‘aaron’

# Hacker input

- Input
  - EXEC BAD_CODING_EXAMPLE( ‘testabc’’, ADMIN=1, FULL_NAME=‘’TEST’ );

- SQL Created
  - UPDATE APPLICATION_USERS SET PASSWORD = ‘testabc‘, ADMIN=1, FULL_NAME=‘TEST’ WHERE USERNAME = ‘aaron’

# Getting to the operating system

- Oracle on NT typically runs as LocalSystem
  - Act as part of the OS privilege
- Oracle on Unix runs as the oracle user
  - Privilege to all oracle files
- Procedures such as:
  - UTL_FILE, UTL_HTTP
- System privileges such as Create Library

# On the operating system

- Oracle has many setUID files
- Oratclsh was setUID root
  - TCL debugger
  - Allowed you to run a script as root
  - Change setuid immediately, even if you are not using

# Other SetUID files

- Were many until Oracle8i release 2
  - Cmctl, tnslsnr, etc…
- Very important one – oracle
  - Main database engine
- Relies on ORACLE_HOME directory
  - To load the pwdSID.ora file
  - Allows you to load a rogue database

# Installing Oracle

- Oracle trusts the /tmp directory
- If a file is created before the Oracle file is written, it is overwritten but retains the permissions
- Allows backdoors to be injected into installation

# Lockdown the operating system

- Lock all users out of the OS during installation
- Set the TMP_DIR directory to a secured directory
- Lockdown ORACLE_HOME permissions
- Remove setUID from all files
- Rename the UNIX oracle account

# Resources, Conclusion, and Wrap Up

APPLICATION SECURITY, INC.

www.AppSecInc.com

# How to Combat Hackers

- Stay patched –
  - http://metalink.oracle.com
- Security alerts:
  - www.oraclesecurity.net/resources/mailinglist.html
- Security Discussion Board
  - www.oraclesecurity.net/cgi-bin/ubb/ultimatebb.cgi
- Check out security solutions at:
  - www.appsecinc.com

APPLICATION SECURITY, INC.
www.AppSecInc.com

# How to Combat Hackers

- Defense in depth
- Multiple levels of security
  - Perform audits and pen tests on your database on a regular basis
  - Encryption of data-in-motion
  - Encryption of data-at-rest
  - Monitor your log files
  - Implement intrusion detection

# Questions?

- About
  - Oracle security features
  - Vulnerabilities
  - Protecting your database
- Email me at:

**anewman@appsecinc.com**

**www.appsecinc.com**

APPLICATION SECURITY, INC.

www.AppSecInc.com