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:
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

• Cquare – www.cquare.net/tools.jsp?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`

![Image of TNS Ping utility output]

```
C:\Oracle\ora92\bin> tnsping 192.168.1.101
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 (VSNUM) 153092352 = 0x9200100 = 9.2.0.1.0**
Enumeration - TNScmd

- Tns cmd.pl also reveals the SID = “spy”
- Tns cmd.pl also reveals the installation directory and other sensitive Oracle configuration information
• 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
    • Reveals Oracle installation directory
    • Reveals Apache installation directory
    • Reveals Operating System installation directory
    • Reveals system ports
    • Other sensitive information


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=ASPSESSIONIDHQQGFQPCY=PKINKOCBHBABEKDFLHMHGANA
HTTP_HOST=192.168.1.101:7779
HTTP_USER_AGENT=Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.0)
MOD_PERL=mod_perl/1.25
PATH=C:\oracle\ora92\bin;C:\oracle\ora92\Apache\Perl\5.0C03\bin\mswin32-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=y0ur.address
SERVER_NAME=ah
SERVER_PORT=7779
SERVER_PROTOCOL=HTTP/1.1
SERVER_SIGNATURE=
SERVER_SOFTWARE=Oracle HTTP Server Powered by Apache/1.3.22 (Win32) mod_plsql/3.0
SYSTEMROOT=C:\WINNT
WINDIR=C:\WINNT
• Global Gateway Settings -
  http://oracleserver:<port>/pls/simpledad/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

Modify Global Settings

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: SIMPLEDAD

mod_plsql v3.0.9.8.3b Plugin for Oracle HTTP Listener
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 Basic
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: 172.22.10.41  
Launch Console

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: 172.22.10.41  Port: 3340  
Access Reports

Information
- Documentation
- Release Notes
- Quick Tour

Useful Links
- Oracle Home Page
- Enterprise Manager Home Page
- Support Home Page
- Download Plug-in
- Accessibility Setup
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-limited.com)
- [http://www.pentest.co.uk/documents/default-user.htm](http://www.pentest.co.uk/documents/default-user.htm)
Exploitation – Finding weak accounts

- Oracle Password Guesser – [www.cqure.net]
Exploitation – Finding weak accounts

- Oracle Password Guesser
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
• **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
  • Provides command line and GUI.
  • (I prefer command line, therefore the remainder of this presentation will detail the steps using the command line interface.)
**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.

```sql
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@databasename`
  - Remember that this database name is related to the name in the tnsnames.ora file created earlier.
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>
```
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”
We have now effectively escalated our access. This allowed SYSDBA access to the database, thus allowing enumeration of the password file.
• 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...)
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 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
  - Oracle 11g hardening info:
- Signs that your objects/database may have been tampered with…
  - [http://www.pentest.co.uk/documents/tampered_objects.htm](http://www.pentest.co.uk/documents/tampered_objects.htm)
- Other great sites:
  - Pentest Limited [www.pentest.co.uk](http://www.pentest.co.uk)
  - NGSSoftware [www.nextgenss.com](http://www.nextgenss.com)
  - Pete Finnigan [www.petefinnigan.com](http://www.petefinnigan.com)
    - Many links to Oracle Security whitepapers on this site!
References

- Hackproofing Oracle Application Server, David Litchfield
- 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. YEAHHHHHH!!!
- 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
      - 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
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.
### SQL Server Version Database

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 Kraft for helping maintain this area of the site. With the seemingly endless stream of PSS-only releases out there this gets to be really tough!

#### SQL Server 2008 Builds

<table>
<thead>
<tr>
<th>Patch Level</th>
<th>PSS Only</th>
<th>Link</th>
<th>Build</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005 February CTP</td>
<td>NO</td>
<td></td>
<td>1,300</td>
<td>10.00.1300.13</td>
</tr>
<tr>
<td>2005 July CTP</td>
<td>NO</td>
<td></td>
<td>1,049</td>
<td>10.00.1040.14</td>
</tr>
<tr>
<td>2005 June CTP</td>
<td>NO</td>
<td></td>
<td>1,019</td>
<td>10.00.1019.17</td>
</tr>
</tbody>
</table>

#### SQL Server 2005 Builds

<table>
<thead>
<tr>
<th>Patch Level</th>
<th>PSS Only</th>
<th>Link</th>
<th>Build</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005 SP2+Q4949959</td>
<td>YES</td>
<td>GO</td>
<td>3,232</td>
<td>9.00.3232</td>
</tr>
<tr>
<td>2005 SP2+Q49499587</td>
<td>NO</td>
<td></td>
<td>3,231</td>
<td>9.00.3231</td>
</tr>
<tr>
<td>2005 SP2+Q4941700</td>
<td>NO</td>
<td></td>
<td>3,230</td>
<td>9.00.3230</td>
</tr>
<tr>
<td>2005 SP2+Q4946630</td>
<td>NO</td>
<td></td>
<td>3,228</td>
<td>9.00.3228</td>
</tr>
<tr>
<td>2005 SP2+Q4946492</td>
<td>NO</td>
<td></td>
<td>3,225</td>
<td>9.00.3225</td>
</tr>
<tr>
<td>2005 SP2+Q4943976</td>
<td>NO</td>
<td></td>
<td>3,224</td>
<td>9.00.3224</td>
</tr>
<tr>
<td>2005 SP2+Q4942039</td>
<td>NO</td>
<td></td>
<td>3,223</td>
<td>9.00.3223</td>
</tr>
<tr>
<td>2005 SP2+Q4932897</td>
<td>NO</td>
<td></td>
<td>3,222</td>
<td>9.00.3222</td>
</tr>
<tr>
<td>2005 SP2+Q4932809</td>
<td>NO</td>
<td></td>
<td>3,221</td>
<td>9.00.3221</td>
</tr>
<tr>
<td>2005 SP2+Q4931616</td>
<td>NO</td>
<td></td>
<td>3,220</td>
<td>9.00.3220</td>
</tr>
</tbody>
</table>

---

SQL Server Versions Database – sqlsecurity.com
SQL Server Account Acquisition

• SQL Server Account Acquisition
  • Attacks the native SQL Server authentication model
  
  • Password brute force tool

• forceSQL – [www.nii.co.in/tools.html](http://www.nii.co.in/tools.html)
  • Password brute force tool

• SQLPing v3.0 – [www.sqlsecurity.com](http://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

![SQLdict Application]

**SQLdict 2.1 - The SQL Server Dictionary Attacker**

copyright (c) 2000, Arne Vidstrom
arine.vidstrom@ntsecurity.ru - http://ntsecurity.ru

**Target server IP:**

**Target account:**

- [Load Password File]

- [Start]
- [Stop]
- [Exit]
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:

<table>
<thead>
<tr>
<th>Hex</th>
<th>A2</th>
<th>B3</th>
<th>92</th>
<th>92</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swap</td>
<td>2A</td>
<td>3B</td>
<td>29</td>
<td>29</td>
</tr>
<tr>
<td>Digits</td>
<td>0010 1010</td>
<td>0011 1011</td>
<td>0010 1001</td>
<td>0010 1001</td>
</tr>
<tr>
<td>Binary</td>
<td>0101 1010</td>
<td>0101 1010</td>
<td>0101 1010</td>
<td>0101 1010</td>
</tr>
<tr>
<td>5A</td>
<td>0111 0000</td>
<td>0110 0001</td>
<td>0111 0011</td>
<td>0111 0011</td>
</tr>
<tr>
<td>XOR</td>
<td>0111 0000</td>
<td>0110 0001</td>
<td>0111 0011</td>
<td>0111 0011</td>
</tr>
<tr>
<td>Hex</td>
<td>70</td>
<td>61</td>
<td>73</td>
<td>73</td>
</tr>
<tr>
<td>Text</td>
<td>P</td>
<td>a</td>
<td>s</td>
<td>s</td>
</tr>
</tbody>
</table>

- **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](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_spacedused
    - Returns database names, size, and unallocated space
  - sp_who, sp_who2
    - Displays usernames and the hosts they are 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>`
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 common 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
SQL Server Security Whitepapers and Sites

- Hammer of GOD – www.hammerofgod.com
- SQL Magazine – www.sqlmag.com
- SQL Server Security Checklist
  www.securitymap.net/sdm/docs/windows/mssql-checklist.html
- Microsoft SQL Server 2008 Security Checklist
SQL Server Security References

- Special Ops, by Eric Pace Birkholz
- The Database Hacker’s Handbook, David Litchfield, 2005
- 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` command
      - `# mysqladmin -h <localhost> <variables>`
  - Have access to OS?
    - `~/.mysql_history` file stores a history of all SQL commands including passwords!
• **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
Other Databases – DB2

- **DB2** – [www.ibm.com/db2](http://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_ICBM_DB2.pdf
  • DB2 Installation and Security
Q&A

Thank You

mraggo@accuvant.com