**Wgel THM CTF simple writeup**

- CTF Name: Wgel ctf

- CTF Level: Easy

- Date: 6/28/2025

- Platform: THM CTF

- Category: Jeopardy style

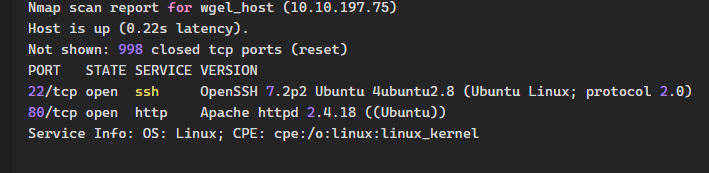
- IP: here I used host “wgel\_host”

- CTF Description: This ctf teaches you about directory broutforcing, remote connection(ssh)..etc.

NB. Before start connect your network!

**Nmap scann result**

* nmap -sV -Pn wgel\_host –vvv

****

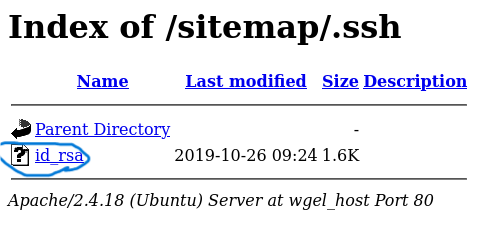
so it has a website(http) and open SSH port(we can connect remotely).

**when I bruteforce directories i found an interesting file .ssh**

* dirb <http://wgel_host>

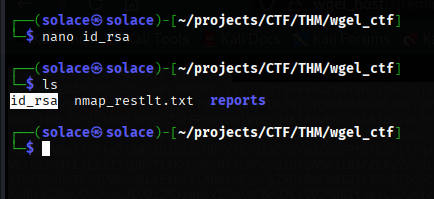


**Then I browse** <http://wgel_host/sitemap/.ssh/> and then **I got a private key**:

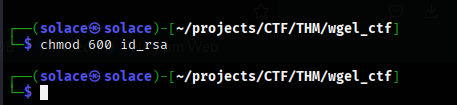




I saved it in txt file(**id\_rsa**).



Then i gave a proper permission for the file:

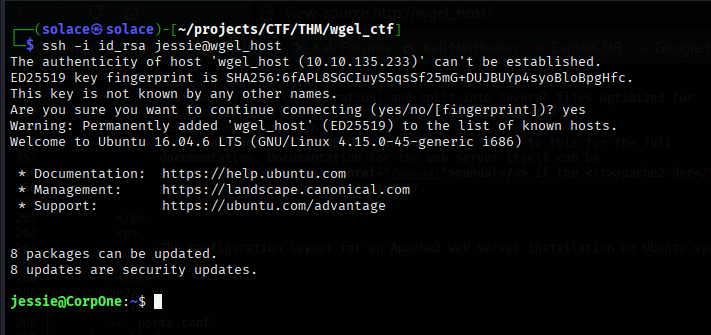


I got the username from the "**view page source**" of wgel\_host

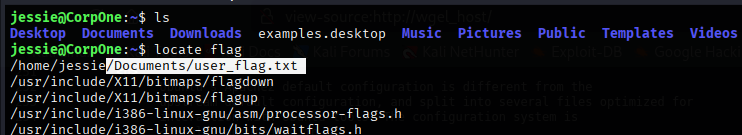


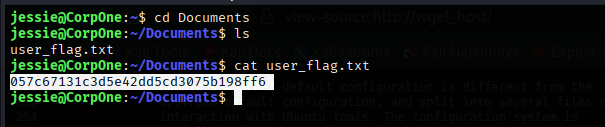
So, **jessie** is the username.

**Now I have connected with ssh**:



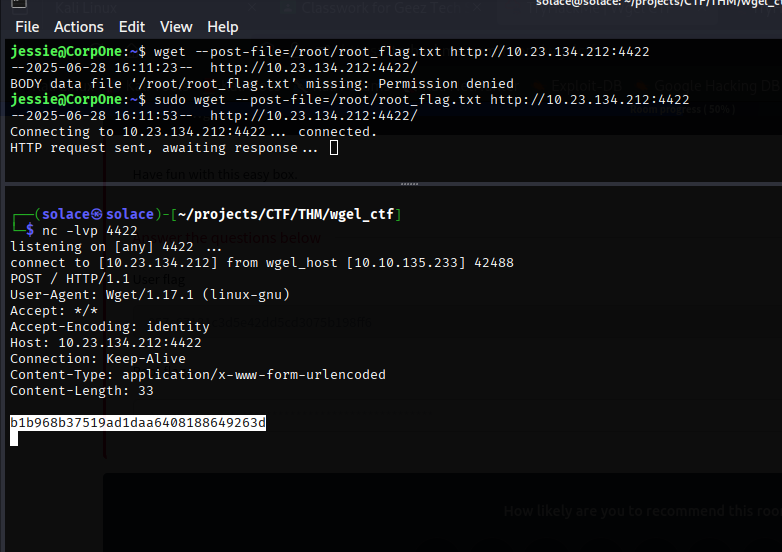
**To get the user flag just locate it:**

****

****

**User Flag =** 057c67131c3d5e42dd5cd3075b198ff6

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

****

**The Root flag =** b1b968b37519ad1daa6408188649263d

**BOOM BOOM BOOM!!**

Finally I did it!



**Name**: Solomon Tesfaye

ETHICAL HACKER