Informatio

- CTF Name: Wgel CTF

- CTF Level: 1

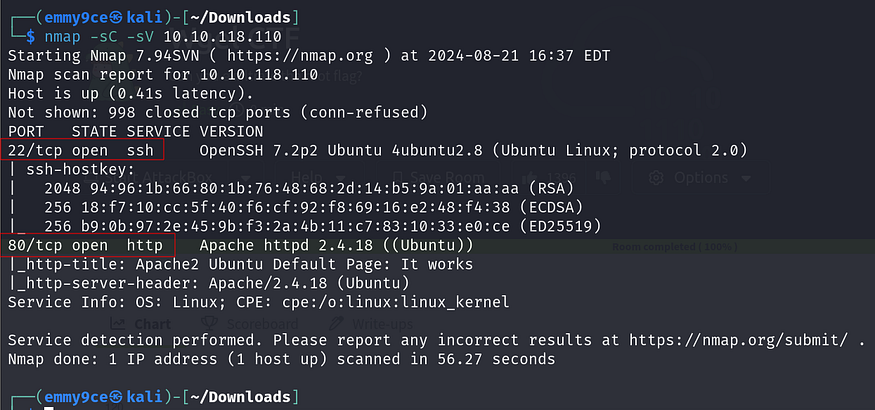
- Description Can you exfiltrate the root flag?

- Date: 8/25/2024

- Platform: tryHackme

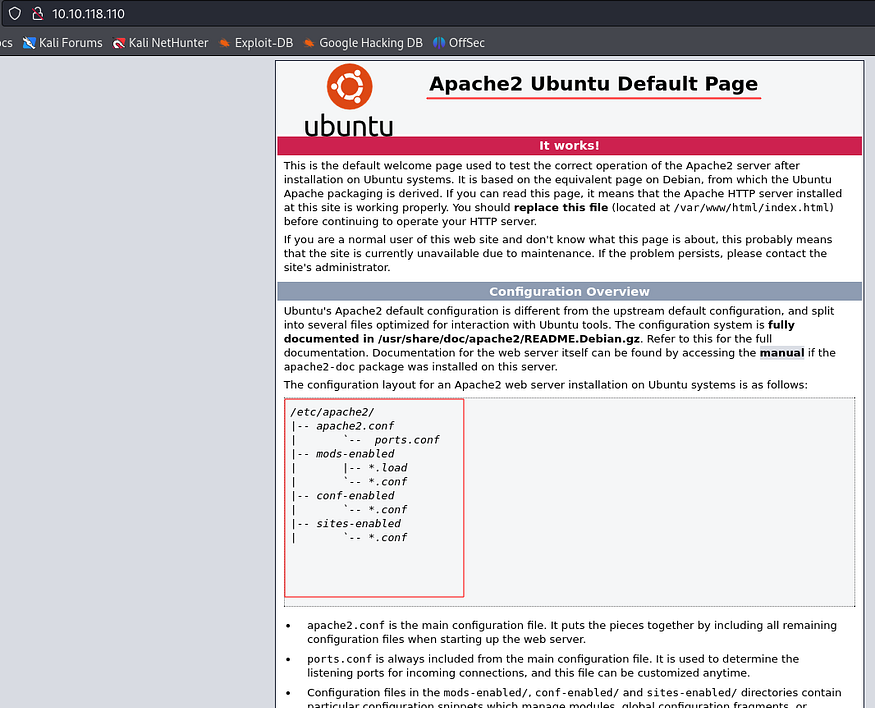
- IP: 10.10.118.110

start by an Nmap scan

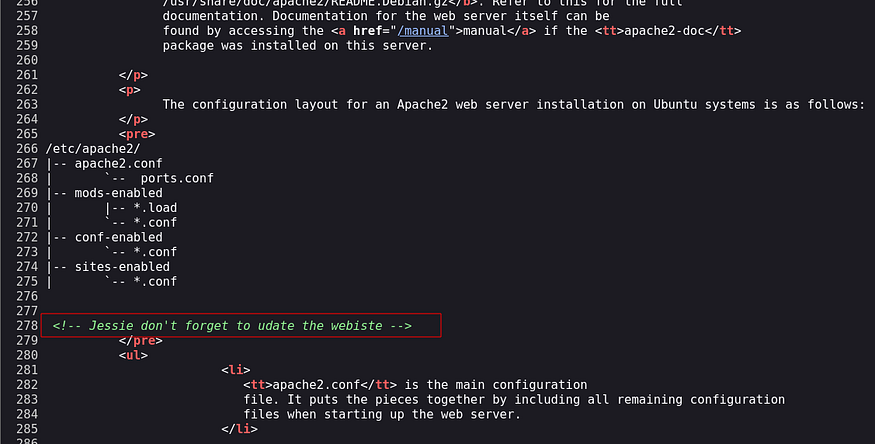


From the above we found two open ports, port 22 and 80.

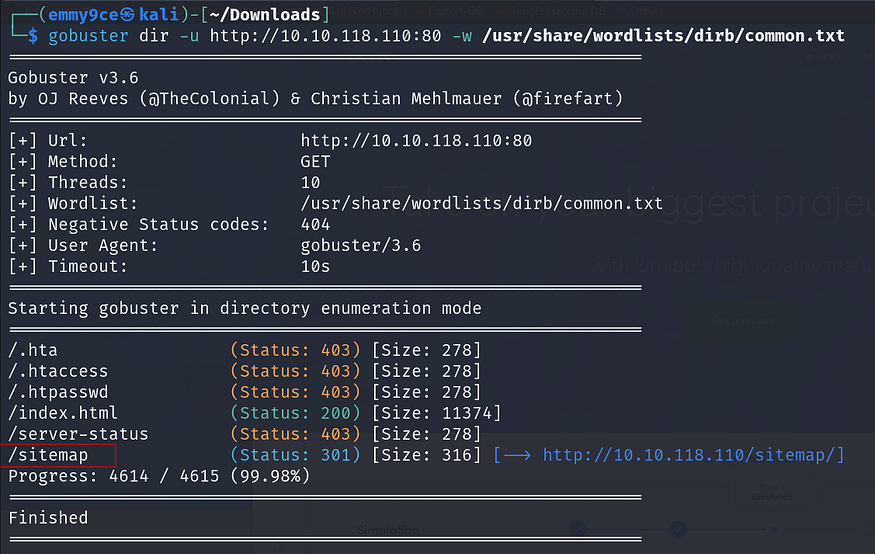
we go ahead and check out port 80 site.



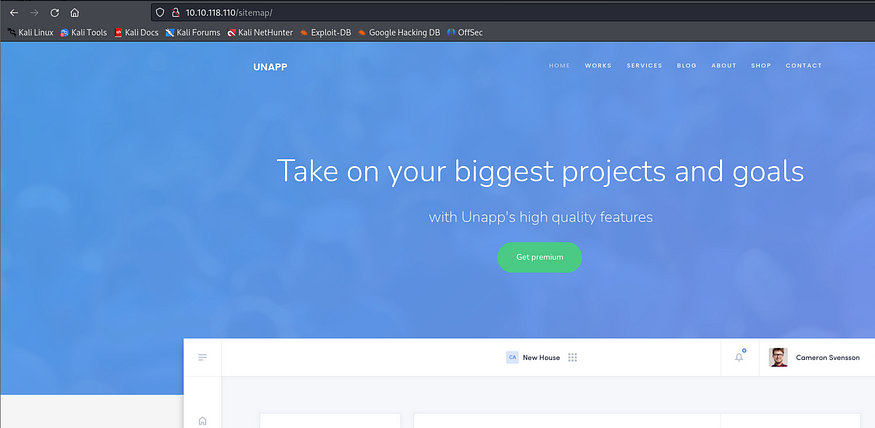
This is a default Apache2 page, I couldn’t find anything here so I checked out the source code and found a very interesting comment



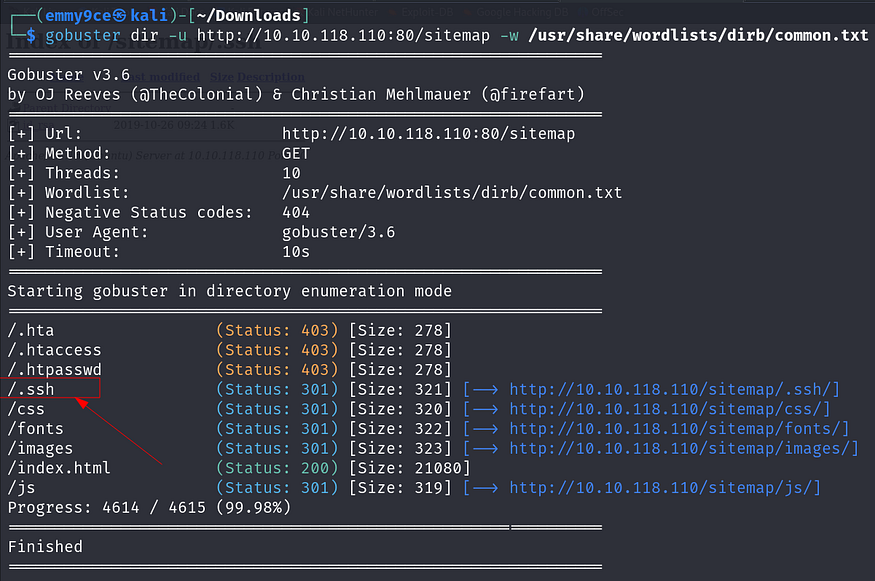
So we possible have found a user with the name “**jessie**”. Now we continue our enumeration by using **Gobuster**to bust directories on the IP address.



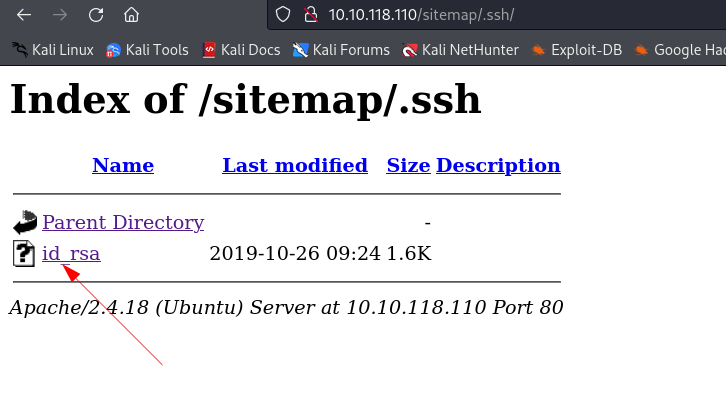
Here we found the **sitemap**directory and we checked it out and found nothing interesting.



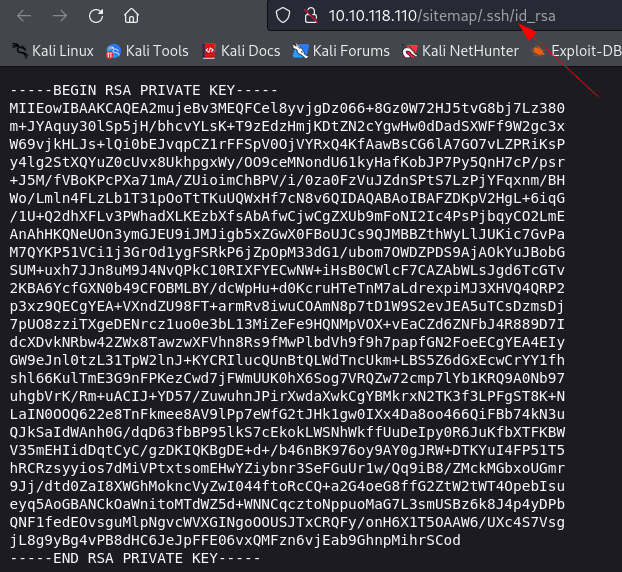
Next we can use **Gobuster**to bust the sitemap directory for hidden directories under it, and we found a hidden **“.ssh”** directory



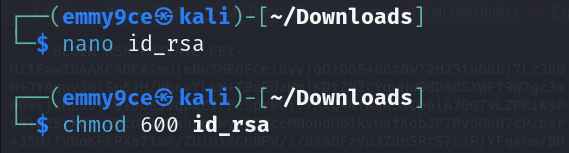
Great! now we can check out that directory and look what we found.

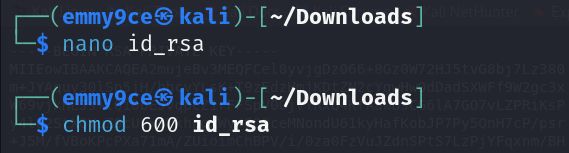


We opened the “**id\_rsa**” file and it’s a private key, looks like we can get our initial access now.

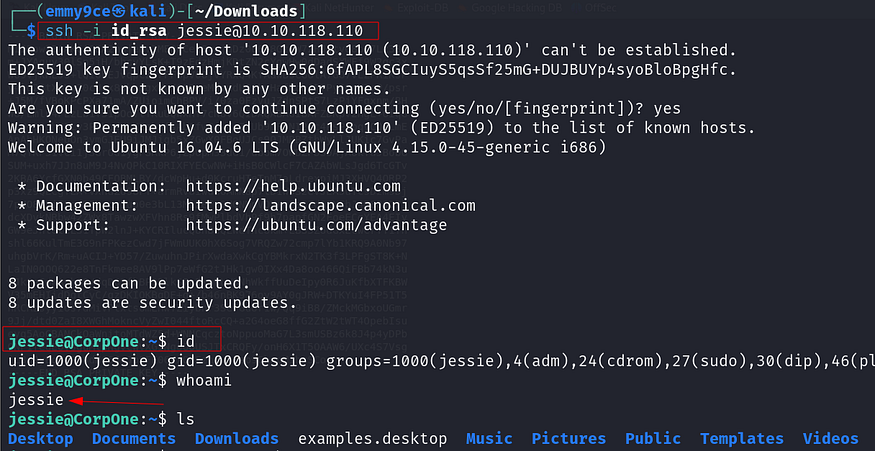


Now we save this file using **nano**or directly copy the id\_rsa link and download with **wget**tool. And next we change the mode and reset the permissions:



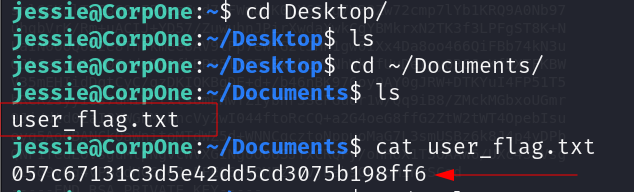


Now let’s recall ssh port is open, so using the jessie user and the Ip address with the private key we found, let try to login and we got the access.



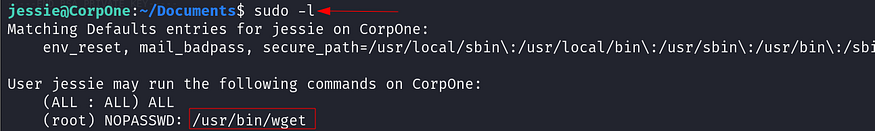
From the above you can see we got a successful login and the **whoami** command confirms the use is **jessie**.

Now let’s get our first flag the user flag — user\_flag.txt



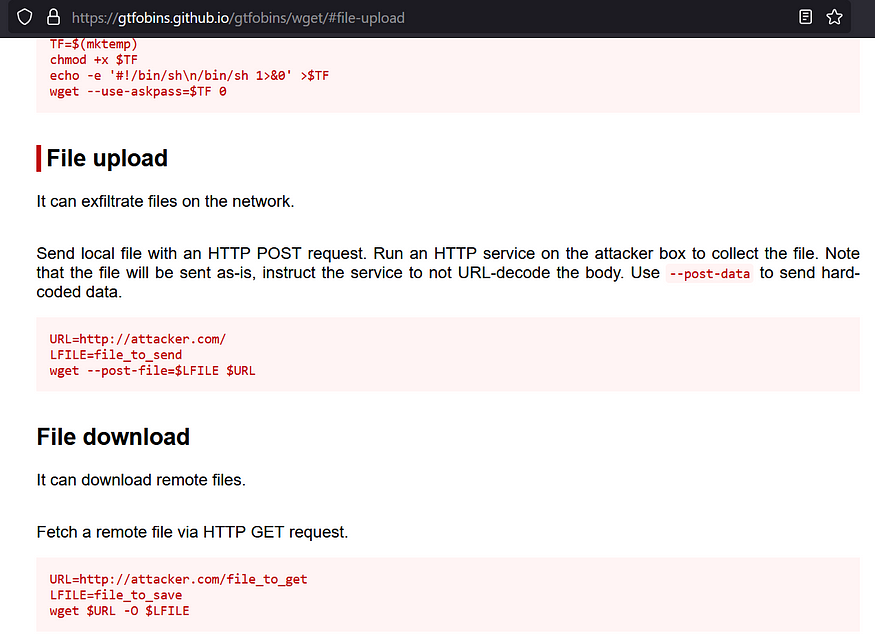
Viola we got the user flag!!!

Next let’s try to excalate privilege and get the root flag. First thing we do here is to check the sudo privileges of the user jessie



Using “sudo -l” we found that the user jessie can run the wget binary as a privileged user. Now we will try to exploit this.

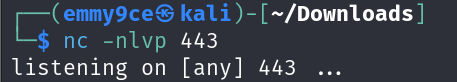
We can check out <https://gtfobins.github.io/> and search “wget” to see how to use it.

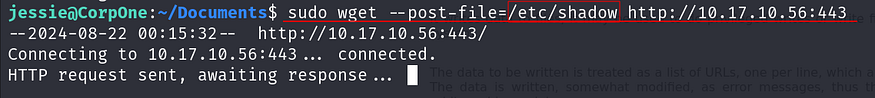


Now there are so many ways to do this, but we just want the flag so we can just use the file upload code to send a file from the machine to the attacker’s machine using an HTTP POST request.

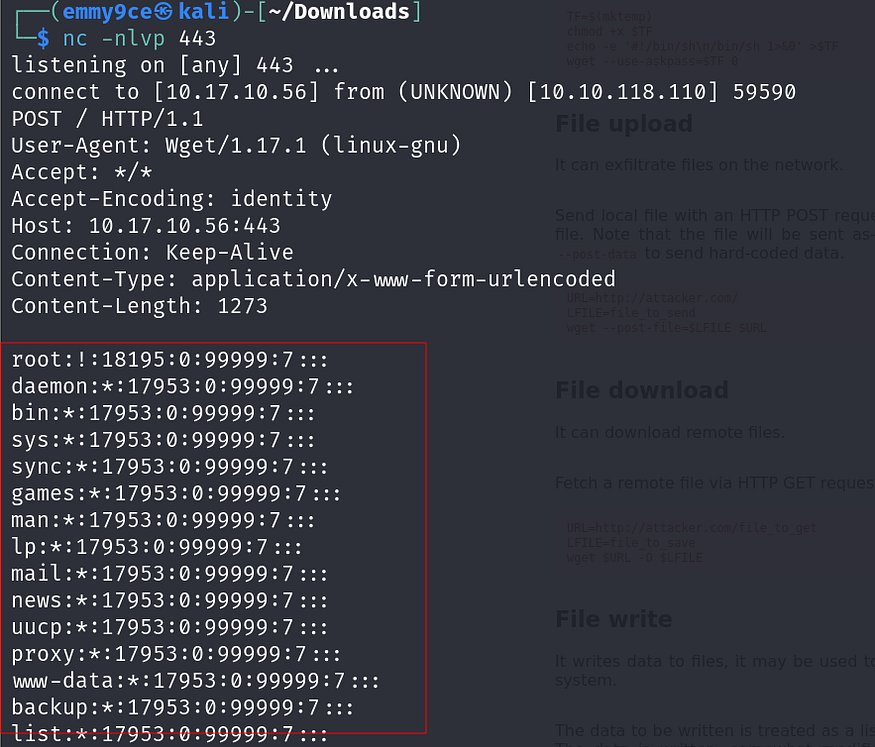
Now turn on a netcat listener and then using the attacker’s IP we can get files from the machine.

First let’s try by getting the shadow files using the line of code below:



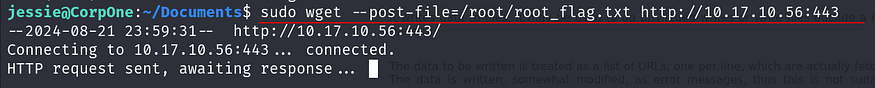


Checking our netcat listener we get the result



Now that we know we can get files an HTTP POST request we can get the root flag, Now the idea is that since the user flag was named “user\_flag.txt” then it’s possible the root flag is going to be “root\_flag.txt” on the root folder.

With out netcat listener on again we using the similar line of code below:



And voila!! we get the root flag!!!

