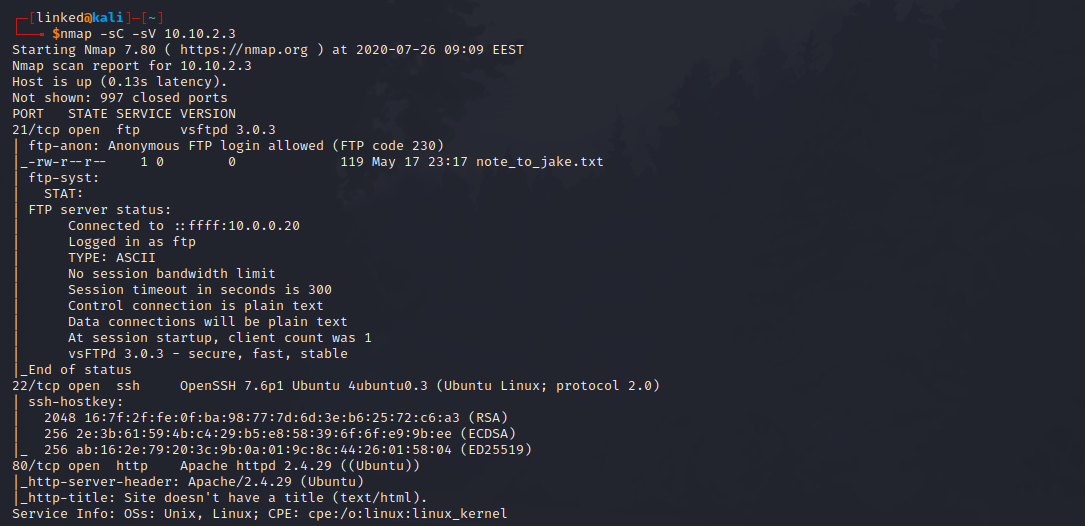
First we start a nmap scan

**Command:** nmap -sC -sV <Target IP>

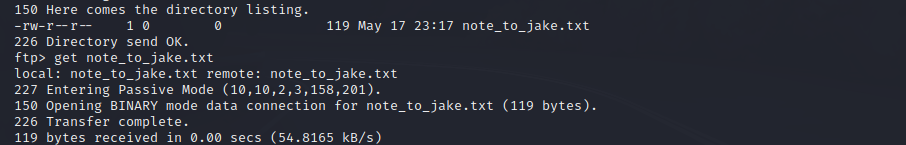


From the nmap result we have 3 open ports

* 21 FTP
* 22 SSH
* 80 HTTP

Let’s acces the FTP because we can anonymous login

The FTP contains a file that I have downloaded it to my machine



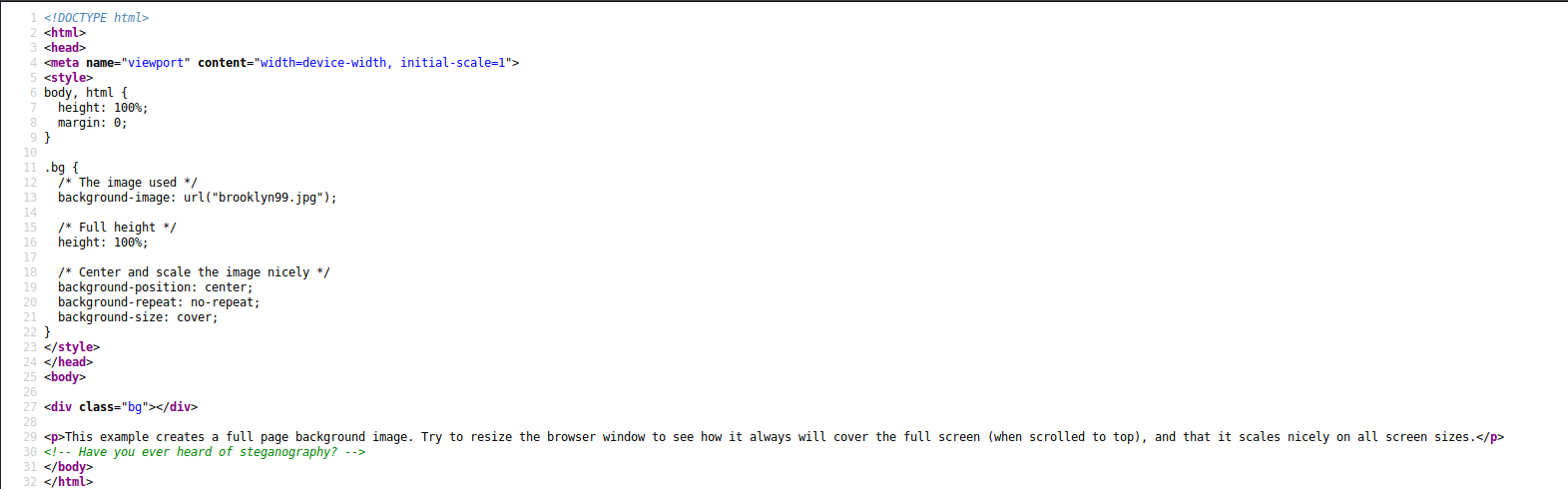
Here is the content of that file:



Now let’s visit the website on port 80



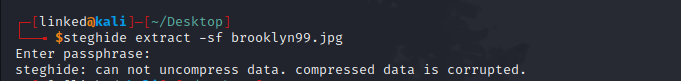
Nothing much here. How about the page source, maybe is something there. Hmmm….. Looks like we have to deal with steganography.



OK. I downloaded the background from the website using wget.

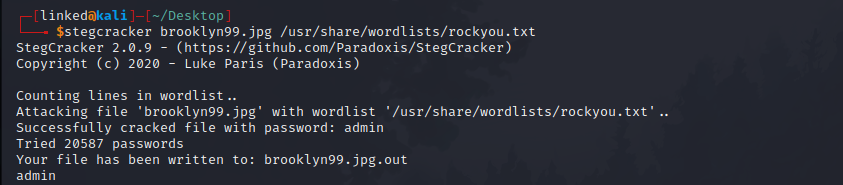
**Command:** wget <Target IP>/brooklyn99.jpg

If I want to extract the content from the image I downloaded it’s asking me for I passphrase, but I don’t have one.

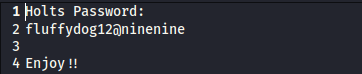


How about I use stegcracker???

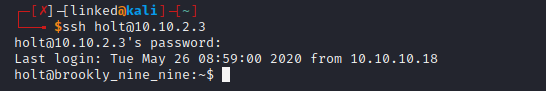
**Command:** stegcracker <image> <wordlist location>



Yep, stegcracker works :D. We have some credentials and only one port to use them at, SSH.



SSH login

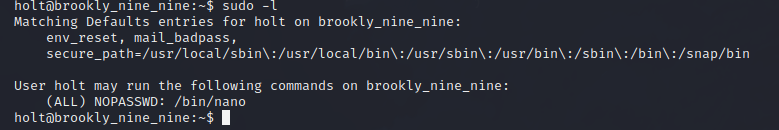


And here is user.txt



Privilege escalation

**Command:** sudo -l



Ok, looks like we can use nano with sudo, nice!

**Command:** sudo nano

You can use GTFObins to check on privilege escalations

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on sudo.

First we open nano with sudo:

sudo nano

Then we execute the key commands as shown below:

^R^X

And finally we write the next command:

reset; sh 1>&0 2>&0

And we are ROOT:



After that we can read root.txt from the root directory