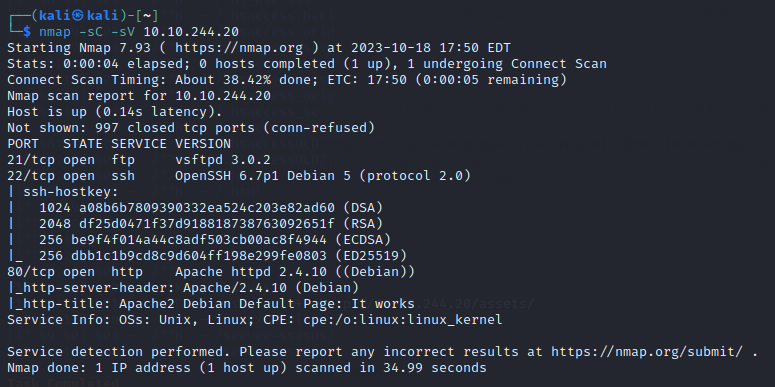
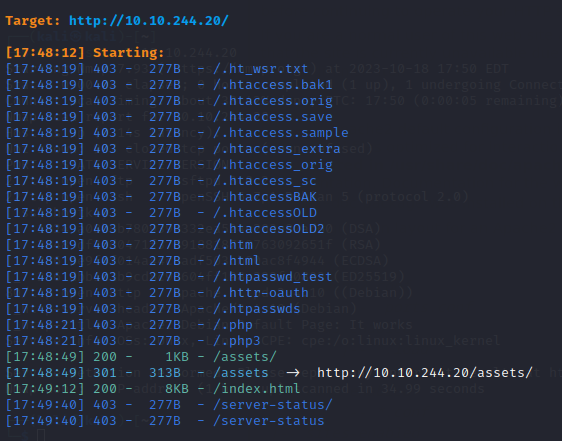
Recon

1. Nmap -sC -sV (ip address)
   1. Enumerate to see services and ports open

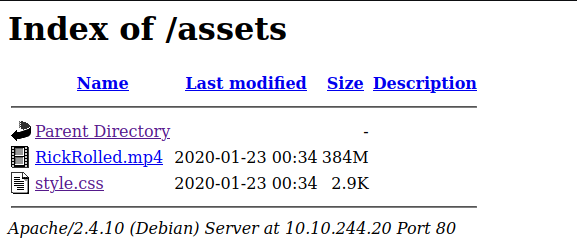


Let’s remember these ports and services open.

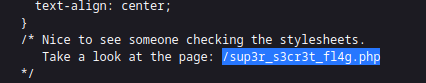
1. Dirsearch -u (ip)
   1. Looks at the directories for the website.



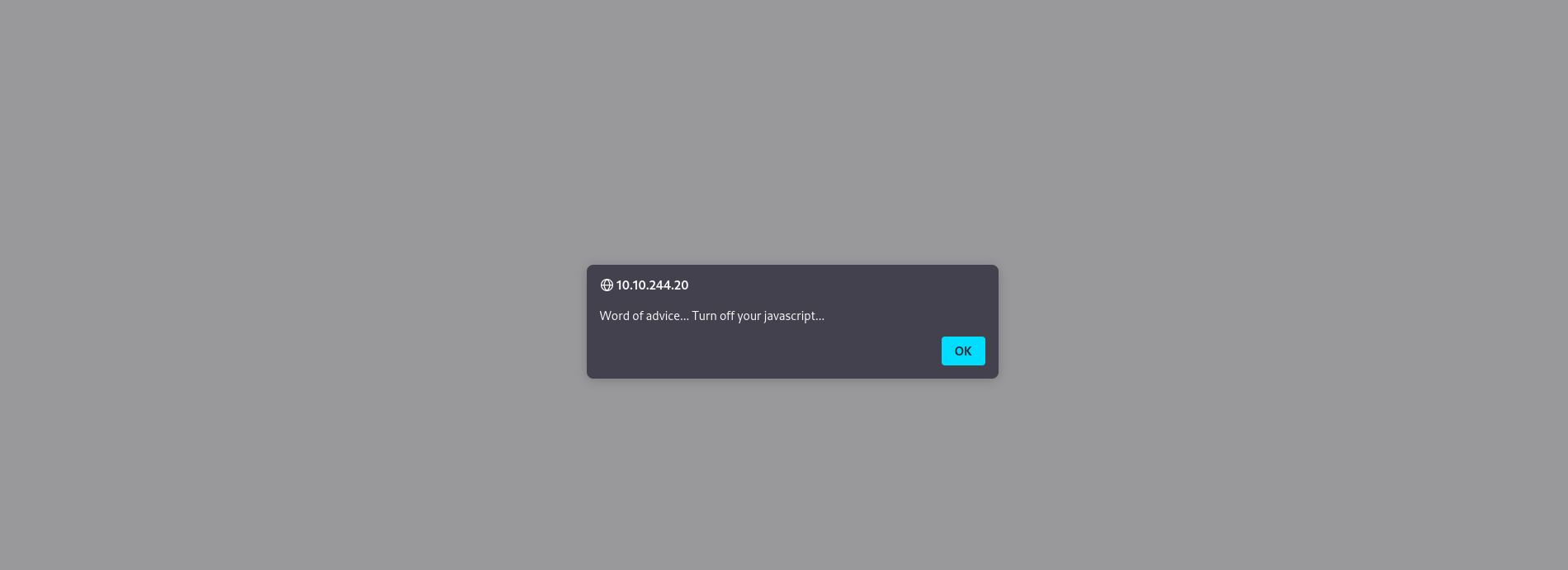
Let’s visit the directories.



Looks like there’s a css file.



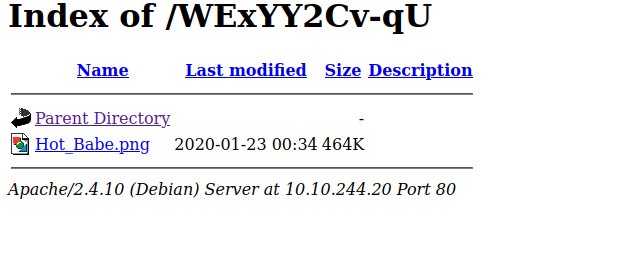
In the css, there’s a comment telling us to check out this page, let’s see it.



So we disable Javascript and see a website. Let’s look at the network requests.



This looks interesting. Let’s try and put that in the search engine.



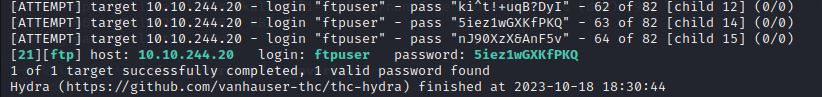
Looks like we’ve got a directory. Let’s see the png file.

1. Strings Hot\_Babe.png
   1. Let’s see the data inside the image



Looks like the user to the FTP is ftpuser but the password seems to be unknown, let’s bruteforce it.

1. hydra -l ftpuser -P Password\_list ftp://10.10.244.20 -V

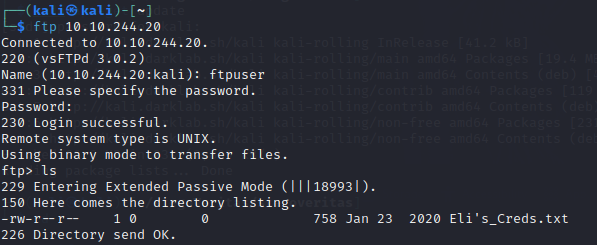


Looks like the password is 5iez1wGXKfPKQ

Exploit

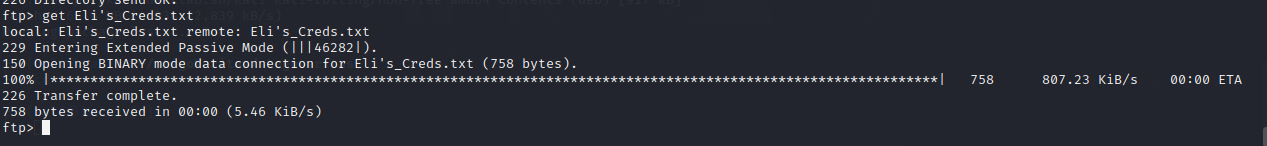
Let’s ftp in now

1. Ftp (ip)

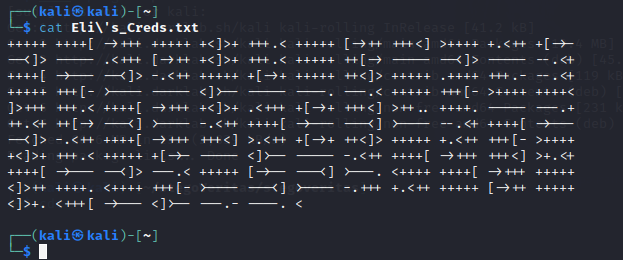


Looks like there’s a text file here, let’s get it.

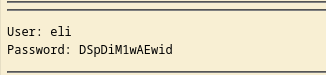
1. Get (file name)



Let’s check what’s inside now.

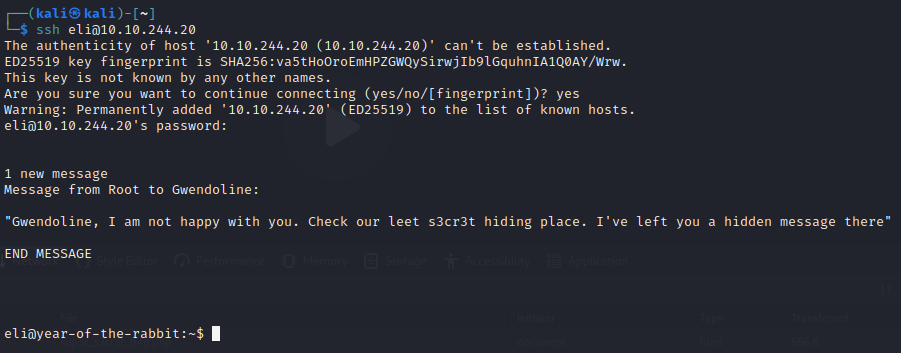


Looks like there’s an encryption. Let’s figure this out.

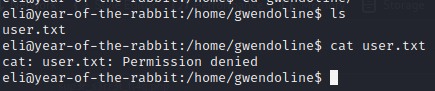


So turns out it was brainfuck encryption. The username here is “eli” while password is DSpDiM1wAEwid. Perhaps this is an ssh?

1. Ssh eli@(ip)



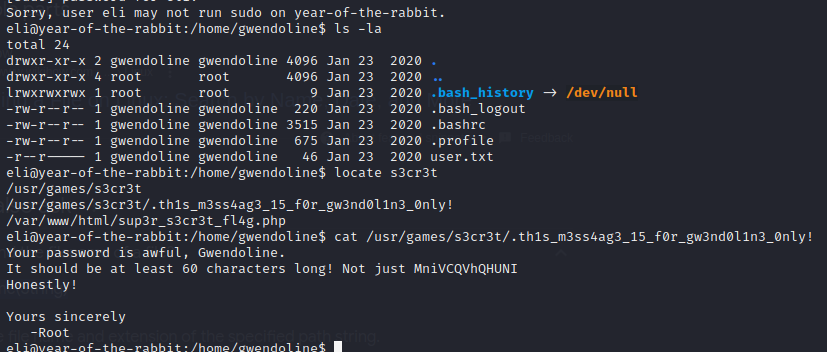
Looks like it worked!



Looks like the user.txt file is in gwendoline, but it’s denying us permission! Let’s try and escalate ourselves.

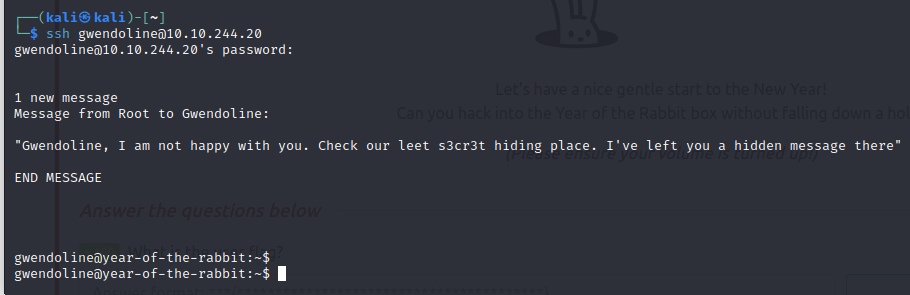
Escalation

At the start it looks like there was a message for Gwendoline from the admin. Let’s find this “s3cr3t”

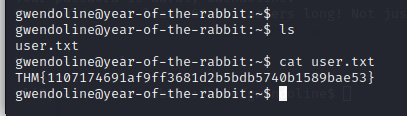


Looks like her password is put in here. Let’s ssh into her account now

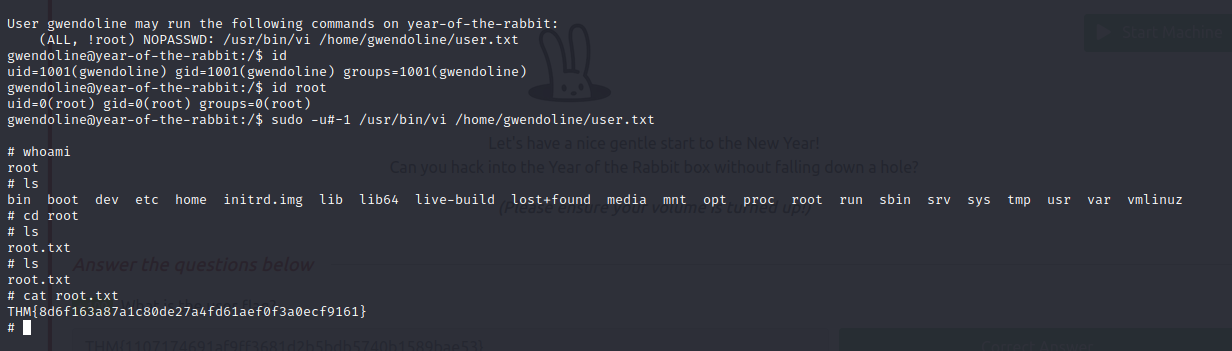
1. Ssh gwendoline@(ip)



1. Cat user.txt



There’s the user.txt.



Now here to escalate, w/ “sudo -l”, we see we can run:

/usr/bin/vi /home/gwendoline/user.txt

This means we can edit the user.txt file here, but not as root as it said (!root). So I googled and saw a bypass to this restriction w/ an id of -1. So we run:

2) sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

Inside the vim, we do “:!/bin/sh” to open a shell

Then we’re in!