First, we will start with our Nmap scan. command would be.

nmap -sC -sV 10.10.153.75

A computer screen shot of a program

Description automatically generated

As we can see from our Nmap scan result we have port 80 is open and running. We also have port 21(FTP) and port 22(SSH) are open. So, we can check out if there is any website running and as we do, we found out that there is and it has only a default Apache page running. When I looked at the source code I thought I might find some interesting thing but no luck.



A screenshot of a computer

Description automatically generated

We will do brute force attack with the help gobuster.

gobuster dir -u http://10.10.153.75 -w /usr/share/wordlists/dirb/common.txt

A computer screen shot of a computer

Description automatically generated

We get some intriguing facts, such as the existence of the "/assets" directory and the status code 301. We'll investigate that.

A screenshot of a computer

Description automatically generated

We were given two files, and when I opened the "style.css" file, I discovered something intriguing.

A screenshot of a computer

Description automatically generated

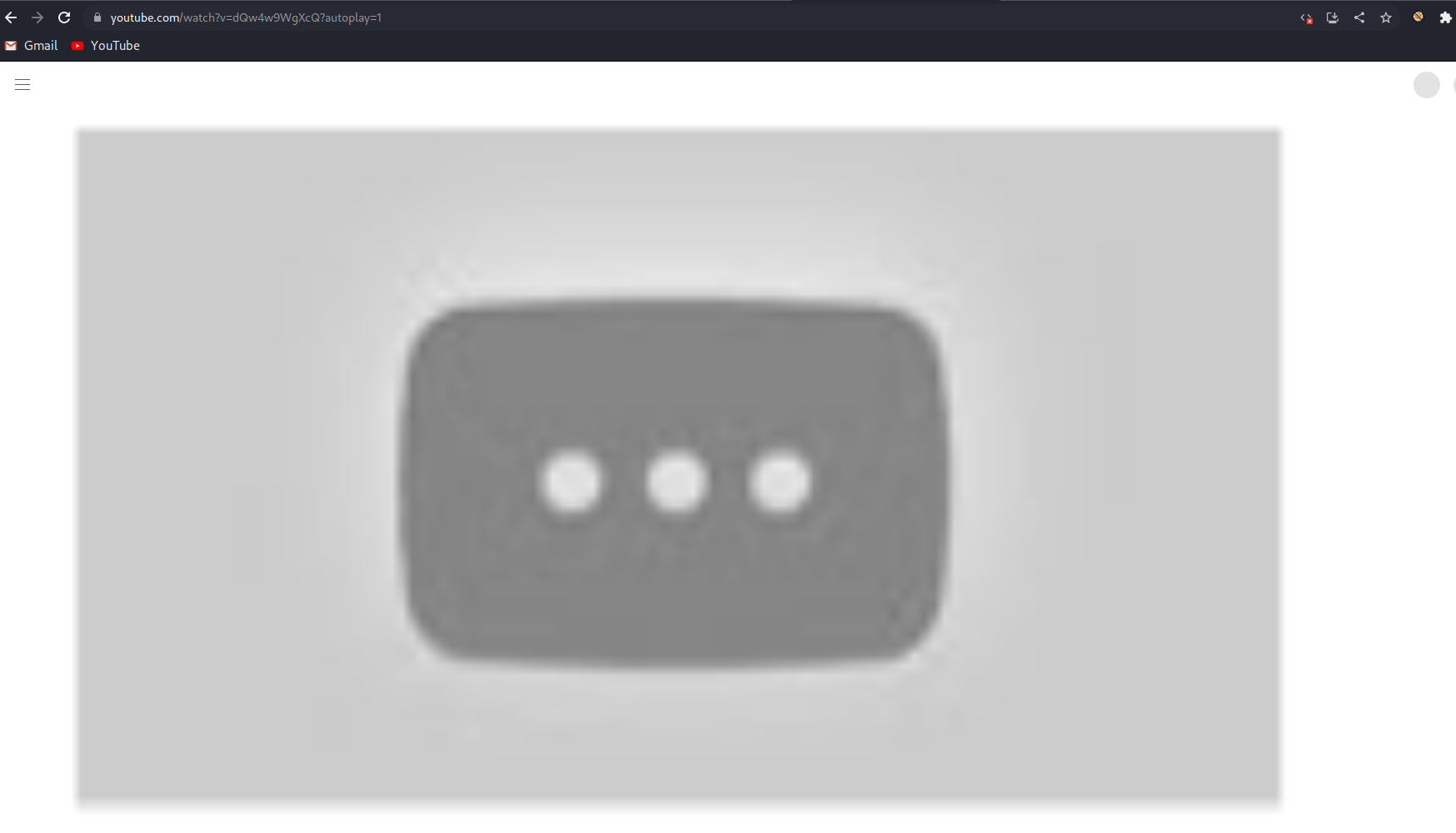
It has a remark that reads, "Nice to see someone checking the stylesheet," as seen in the image above. Visit the following page: /sup3r\_s3cr3t\_fl4g.php.

We then went right to that page and discovered that,

A screen shot of a computer

Description automatically generated

As we can see that it says to disable the java-script. When pressed ok on above alert box it took me to a YouTube page. So, what I thought is if I disable the JavaScript, I might get the information the page /sup3r\_s3cr3t\_fl4g.php.



So, after blocking the JavaScript we again navigate to that page. Once we do we find that,

A screenshot of a computer

Description automatically generated

We have a text document and a video. I tried the video because the text said to do so, but I had no luck. Here, I tried directory brute force, but it didn't work. I also tried a tonne of other stuff, but I was unsuccessful. After racking my brain for a while, I finally concluded that perhaps there is something faulty going on in the back end because the first time I went to reach /sup3r\_s3cr3t\_fl4g.php, it actually redirected me to a YouTube video. So, I decided to launch Burp Suite and record the requests.

Start the burp suite now. select the proxy tab, then enable intercept. Return to /sup3r\_s3cr3t\_fl4g.php now. And as you can see, the burp suite has been used to capture several requests, from which we have learned something really intriguing.

A screenshot of a computer

Description automatically generated

We can now view the "/WExYY2Cv-qU" secret directory that we were missing. Navigate to that directory right away and we'll see,

A screenshot of a computer

Description automatically generated

We can see that the file is a.png. That will be downloaded and counted. On the image, I experimented with several things such as exiftool, file, etc. I discovered some quite intriguing things when I ran strings on it,

strings Hot\_Babe.png

A screenshot of a computer

Description automatically generated

A list of passwords and the username for the FTP were provided to us. The text file with the name "pass.txt" will be used to store these passwords. The username is “ftpuser”.

Use "HYDRA" now that I have a list of usernames and passwords.

hydra -l ftpuser -P pass.txt ftp:// 10.10.153.75 -t 64.

A blurry image of a computer screen

Description automatically generated

We have successfully discovered our password. We are now ftping to that username.

ftp 10.10.153.75

password: 5iez1wGXKfPKQ

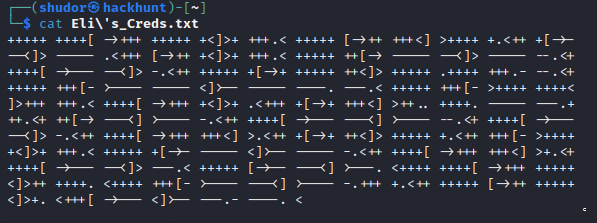
After getting logged in use ls command to view all files and we see Eli’s\_Credit.txt file. With the help of get command we extract the file and logged out from ftp.

A black background with a blue border

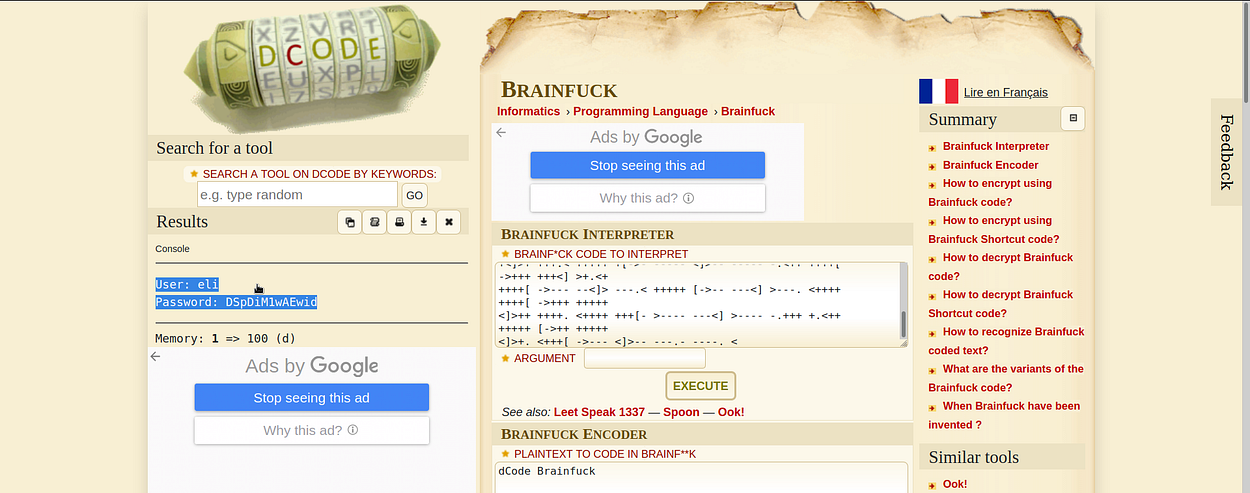
Description automatically generated

We'll cat that text file, and when we do, strange text appears.

cat Eli\’s\_Creds.txt



The "Brain Fuck" programming language is esoteric. Therefore, we must now decipher it. To decode it, I utilised this particular website, <https://www.dcode.fr/brainfuck-language>.



I so obtained the login "eli" and the password after decoding it. Our Nmap scan revealed that there is an open ssh port. So, with these credentials, we attempt ssh.

ssh [eli@10.10.153.75](mailto:eli@10.10.153.75)

password : DSpDiM1wAEwid

A screenshot of a computer program

Description automatically generated

As soon as we log in, we receive a notice telling us to check our leet "s3cr3t" hiding spot, as we can see. We shall search that s3cr3t file or directory, whichever it may be, as I believe this to be the hint. It will take time to perform this manually by going to each directory. The find command will be helpful and very time-saving in this situation.

locate s3cr3t

A computer screen shot of a computer code

Description automatically generated

In above all we open the file /usr/games/s3cr3t/.th1s\_m3ss4ag3\_15\_f0r\_gw3nd0l1n3\_0nly! Using cat command. We find the item is in below screenshot.

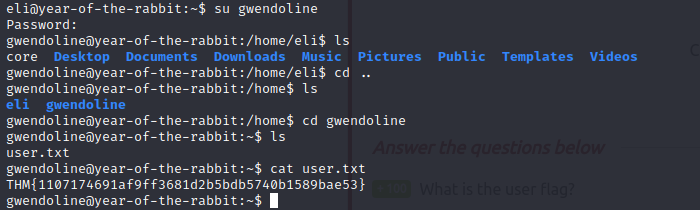
A screen shot of a computer

Description automatically generated

As we can see, a hidden file with the extension “. this\_m3" exists. Once we figure things out, we will receive a message from root. Thus, "gwendoline" is a prospective user, while "MniVCQVhQHUNI" is a list of possible passwords. so, we'll change users by,

su gwendoline

With the password we got and now we are “gwendoline”. So, we will go it’s home directory and we have found our user.txt file.



Now we will find the root flag.

sudo -l

to check if current user can run anything as root.

A computer code with text

Description automatically generated

As seen above, user gwendoline has the ability to modify the file /home/gwendoline/user.txt with sudo privileges using /usr/bin/vi. However, the issue was that we were unable to run sudo as root because we had (ALL,!root) at this location. We could easily escalate the situation if we had (ALL, ALL). What to do next, then.

It appears that sudo has a flaw that permits us to run commands as root in certain configurations. This vulnerability is well understood at https://resources.whitesourcesoftware.com/blog-whitesource/new-vulnerability-in-sudo-cve-2019-14287.However, in sort, if you run a user with id -1, sudo will not be able to recognise it and will reset it to 0, which is root id. Therefore, this is what we're going to do:

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

With the vi editor now open, you may enter the command line by entering ":" and then "!/bin/sh" and pressing enter to get the root shell.

A green rectangle with black text

Description automatically generated