

# ***enumeration***

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/popcorn/nmap_default.txt  
10.10.10.6
```

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-02-16 08:46 EST

Nmap scan report for 10.10.10.6

Host is up (0.18s latency).

Not shown: 998 closed ports

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-server-header: Apache/2.2.12 (Ubuntu)

|\_http-title: Site doesn't have a title (text/html).

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 41.17 seconds

open ports are

22/tcp open ssh OpenSSH 5.1p1 Debian 6ubuntu2

80/tcp open http Apache httpd 2.2.12

and now we are running complete port scan to make sure no other ports are open which went unnoticed

mean time lets go to http port 80

## **It works!**

This is the default web page for this server.

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

```
1 <html><body><h1>It works!</h1>
2 <p>This is the default web page for this server.</p>
3 <p>The web server software is running but no content has been added, yet.</p>
4 </body></html>
5
```

so lets enumerate we will use nikto , searchsploit and gobuster

```
(root@kali)-[/home/kali]
# nikto -h 10.10.10.6
- Nikto v2.1.6

+ Target IP: 10.10.10.6
+ Target Hostname: 10.10.10.6
+ Target Port: 80
+ Start Time: 2021-02-16 09:09:53 (GMT-5)

+ Server: Apache/2.2.12 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 43621, s
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
+ The X-Content-Type-Options header is not set. This could allow the user age
^C
```

nothing special

run searchsploit

nothing interesting

lets run go buster

```
2021/02/16 09:24:46 Starting gobuster
```

```
/index (Status: 200)
/index.html (Status: 200)
/test (Status: 200)
/torrent (Status: 301)
[ERROR] 2021/02/16 09:29:55 [!] Get http://10.10.10.6/h3.html: net/http: request canceled (Client
[ERROR] 2021/02/16 09:31:14 [!] Get http://10.10.10.6/cgi-sys: net/http: request canceled (Clie
[ERROR] 2021/02/16 09:31:14 [!] Get http://10.10.10.6/errata25: net/http: request canceled (Clie
[ERROR] 2021/02/16 09:32:24 [!] Get http://10.10.10.6/oklahoma: net/http: request canceled (Clie
[ERROR] 2021/02/16 09:32:34 [!] Get http://10.10.10.6/bookreviews.txt: net/http: request ca
[ERROR] 2021/02/16 09:34:24 [!] Get http://10.10.10.6/voorwaarden.txt: net/http: request ca
[ERROR] 2021/02/16 09:34:24 [!] Get http://10.10.10.6/galery: net/http: request canceled (Clie
[ERROR] 2021/02/16 09:34:54 [!] Get http://10.10.10.6/d-fy93.html: net/http: request cancel
[ERROR] 2021/02/16 09:35:04 [!] Get http://10.10.10.6/hir9: net/http: request canceled (Clie
/rename (Status: 301)
[ERROR] 2021/02/16 09:37:13 [!] Get http://10.10.10.6/left_arrow.html: net/http: request ca
[ERROR] 2021/02/16 09:37:22 [!] Get http://10.10.10.6/sm_cool: net/http: request canceled (Clie
[ERROR] 2021/02/16 09:37:22 [!] Get http://10.10.10.6/en_GB.html: net/http: request cancel
[ERROR] 2021/02/16 09:37:32 [!] Get http://10.10.10.6/o3: net/http: request canceled (Clie
Progress: 15560 / 220561 (7.05%)^C
[!] Keyboard interrupt detected, terminating.
```

we can see we have

```
/index      -----html page
/index.html-----html page
/test       -----php info page
/torrent
/rename
```

in which torrent and rename are 301 moved permanently

lets see these

/test



<b>System</b>	Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686
<b>Build Date</b>	May 2 2011 22:56:18
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php5/apache2
<b>Loaded Configuration File</b>	/etc/php5/apache2/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php5/apache2/conf.d
<b>additional .ini files parsed</b>	/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
<b>PHP API</b>	20041225
<b>PHP Extension</b>	20060613
<b>Zend Extension</b>	220060519
<b>Debug Build</b>	no
<b>Thread Safety</b>	disabled
<b>Zend Memory Manager</b>	enabled
<b>IPv6 Support</b>	enabled
<b>Registered PHP Streams</b>	https, ftps, compress.zlib, compress.bzip2, php, file, data, http, ftp, zip
<b>Registered Stream Socket Transports</b>	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
<b>Registered Stream Filters</b>	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed

This page is protected with the Subsis Patch 0.0.7

/torrent

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

[About](#)
[Development](#)

## Torrent Hoster

### 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, 2006, µTorrent developer Ludvig Strigeus and BitTorrent, Inc. CEO Bram Cohen announced that BitTorrent, Inc. had acquired µTorrent.

01/06/07 Posted by [Admin](#)

#### Azureus

Azureus (Ah/ZURE/us) is a Java-based BitTorrent client, with support for I2P and Tor anonymous communication protocols. The core developers of Azureus have formed a company called Azureus, Inc. The

[Login](#)

[Login](#)

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

[Search](#)

## /rename

Renamer API Syntax: `index.php?filename=old_file_path_and_name&newfilename=new_file_path_and_name`

here we can see it is using a api which is use to rename something and this is the given format

lets see the other 2 pages

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

[About](#)
[Development](#)

## Torrent Hoster

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

Username:

Password:

Password:(confirm)

Email:

Enter Code:

571d7

[Register](#)

[Login](#)

[Login](#)

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

[Search](#)

5/8

lets register and see whats inside

# Welcome

Thank you for registering to Torrent Hoster Your account information is:

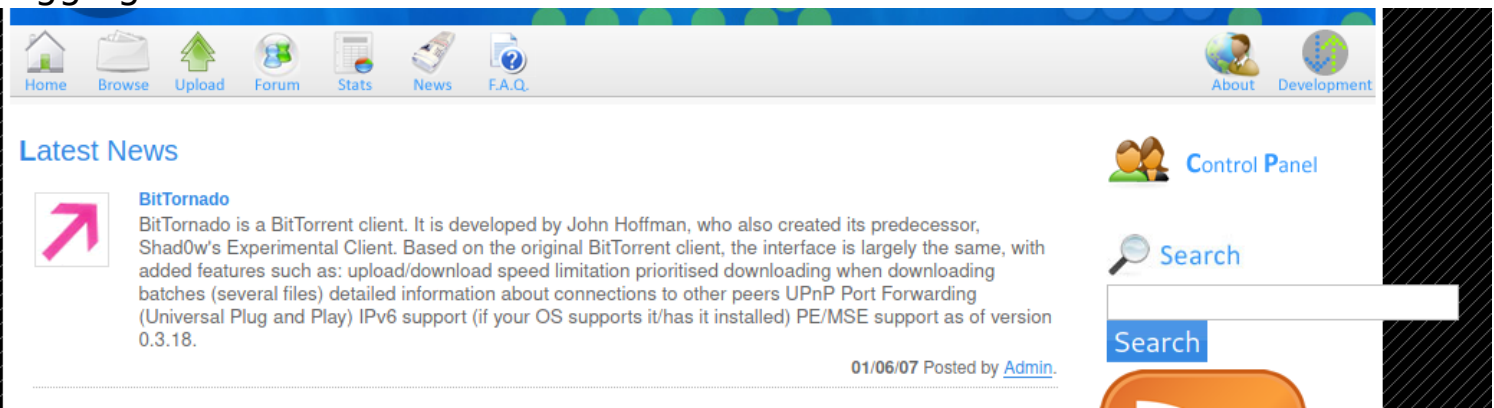
Username: **hack**

Password: **hack**

Please write these down in a safe place and please do not give your password to  
reset it if you forget it on the login page.

To continue using the system, please [login](#) now.

logging in we can see



here we have a upload button and also we can see that something is posted by admin so root name is admin or a username is admin which we can use



## Torrent Hoster 2.0

Modified by DiEg0 based on webtorrent and t-xore.  
visit to <http://www.myanmartorrents.com/>

### Requirements:

- SQL
- php
- GD2

### Installation

1. Create a new database for Torrent Hoster. Then, using phpmyadmin or any mysql administrator script, import /database/th\_database.sql.
2. Open config.php and add the requirements.
4. Upload all the files from Torrent Hoster folder to your website.
5. CHMOD upload folder and torrents folder to 755. if u see error later, change it to 777.
6. go to the url where you uploaded the script and you are good to go. Admin username: admin; password : admin12

### Update

No Update Yet.

### Credit

Torrent Hoster script is based on webtorrents and t-xore. Full credits go to them. Other Credits to:

- Lokesh Dhakar <http://www.huddletogether.com/> for image loading javascript
- Alexandre Moore <http://www.iconsdesigns.com/> for lovely icons.

found this in /torrent/readme/readme.html

we have to upload a torrent file so lets download a kali torrent file and uplaod it

- 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	<input type="button" value="Browse..."/> kali-linux-2020.4-installer-amd64.iso.torrent
Optional name	will use it to uplaod a picture
Category	Other ▾
Subcategory	Other ▾
Description	<div>next we have to upload a picture with malicious code</div>
Tracker requires registration	<input checked="" type="radio"/> Yes <input type="radio"/> No
Post Annoymous	<input checked="" type="radio"/> Yes <input type="radio"/> No
<input type="button" value="Upload Torrent"/>	

we uploaded a normal torrent file

so torrent file got uploaded lets see

will use it to uplaod a picture



Download	will use it to uplaod a picture
Uploaded By	Guest
Category	Other
Size	5.15 MB



Seeds	0
Peers	0
Finished	
Update Stats	<a href="#">Update Stats</a>



Tracked By	http://tracker.kali.org:6969/announce
Added	2021-02-17 16:21:09
Last Update	0000-00-00 00:00:00
Comment	next we have to upload a picture with malicious code



Screenshots



[+ Files](#)

here we can see at the bottom we also have a option to uplaod a picture

and we have a directory in 10.10.10.6/torrent/upload/ in which the uplaoded picture goes and hence we can upload a php reverse shell and run it

but the problem is that we have to add a magic byte to out reverse file and intercept it with burp change it and uplaod id