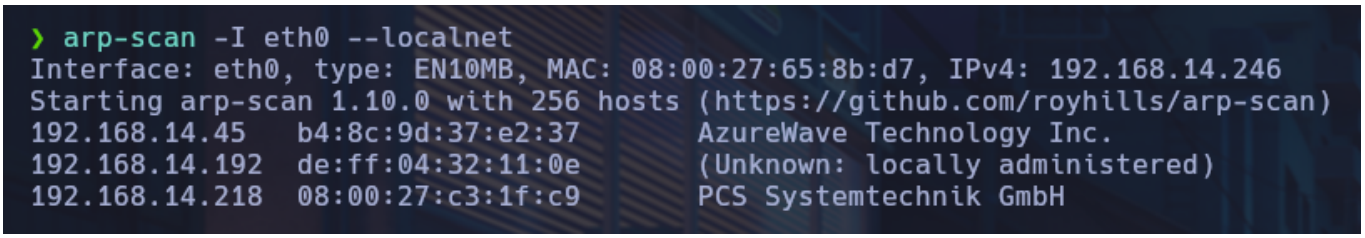
SYMFONOS 1

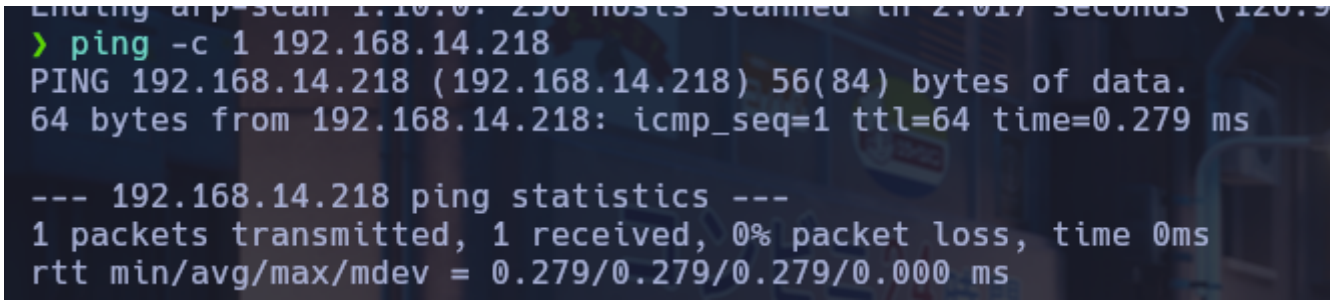
#SYMFONOS

Escaneo de la maquina

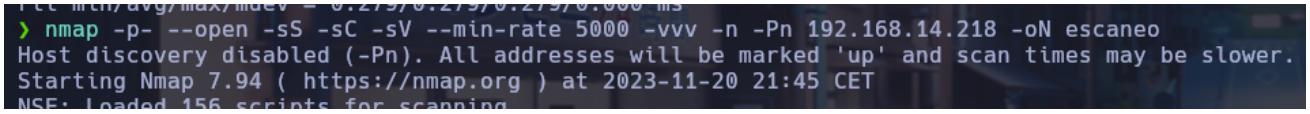
ARP ver que equipos hay en nuestra Red



Al ver la IP 192.168.14.218 y ver la mac ser 08:00 es una maquina virtual esta seria nuestra maquina Symfonos
Hacemos un ping a la maquina y vemos el TTL 64 entonce sabemos que es una maquina linux porque una maquina wind es 128 de TTL



- Primer Escaneo con Nmap




```Bash
nmap -p- --open -sS -sC -sV -vvv -n -Pn IP -oN escaneo
```

Ahora hacemos un **smbmap** para ver que recursos compartidos tenemos

- Esta herramienta la usamos porque vemos que tenemos un puerto que es el 445 que tiene un SAMBA #SAMBA

Ahora vamos a explotar la vulnerabilidad de SAMBA con SMBMAP herramienta de kali linux
#SMBMAP

```bash
smbmap -H +IP
```

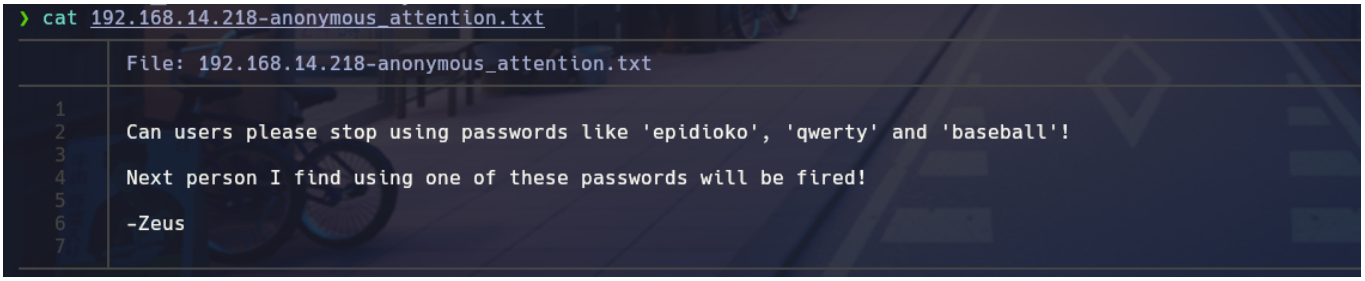
Ahora despues de ver que tenemos anonymous vemos que puede leer y eso lo añadimos en el mismo comando

```bash
smbmap -H +IP -r +usuario
```

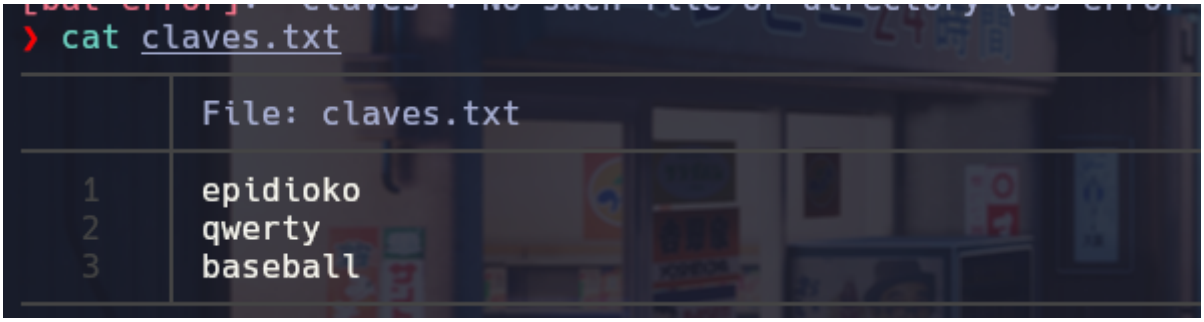
Nos sale un archivo llamado attencion.txt que podemos leer

Una vez visto esto lo descargamos para hacerlo es el mismo comando quitando el -r y añadiendo --download +usuario/ruta

```bash
smbmap -H +IP --download +usuario/ruta.
```



Como vemos tenemos passwords posibles lo guardamos en un archivo claves.txt



Una vez visto esto vamos a utilizar el SMBMAP + usuario y probar las contraseñas

En la primera no hjay suerte como se muestra la imagen

Probamos con otra contraseña

Y en este caso si funciona

Ya comprobado que podemos entrar pues nos intetamos meter en los recursos que hay:

```bash
smbmap -H +IP -u +usuario -p +password -r +usuario
```

Nos bajamos los archivos ya sabeis con --download usuario/rutadelarchivo

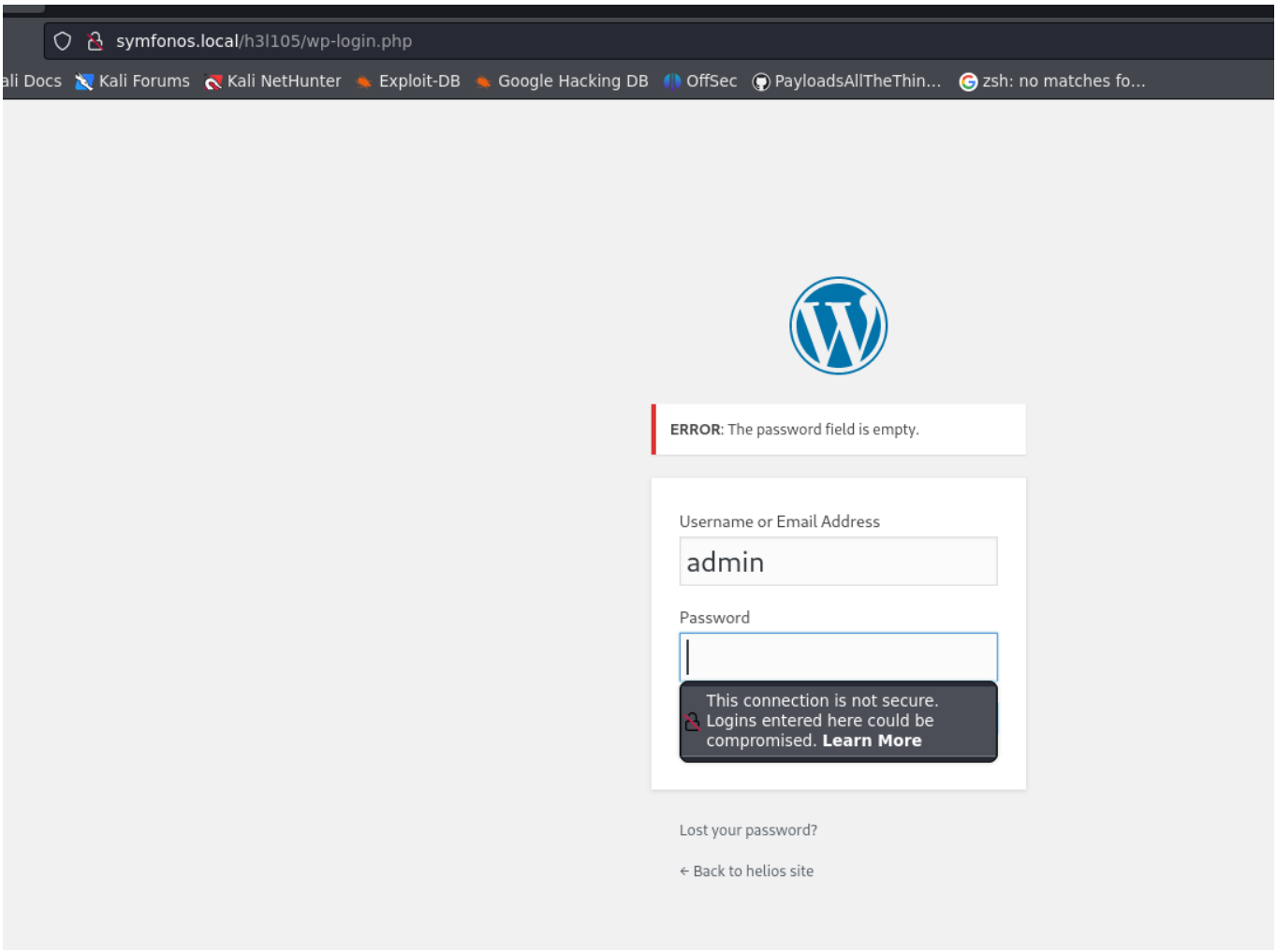
Lo vemos con Cat	Como vemos ternemos un directorio y aqui empieza nos tenemos que dirigir al puerto 80 y ponerlo que deberia salir asi	Y tenemos un Worpress

```
❯ wpscan --url http://192.168.14.218/h3l105/ -e u,p
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

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

[+] URL: http://192.168.14.218/h3l105/ [192.168.14.218]
[+] Started: Wed Nov 22 18:50:44 2023

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://192.168.14.218/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://192.168.14.218/h3l105/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

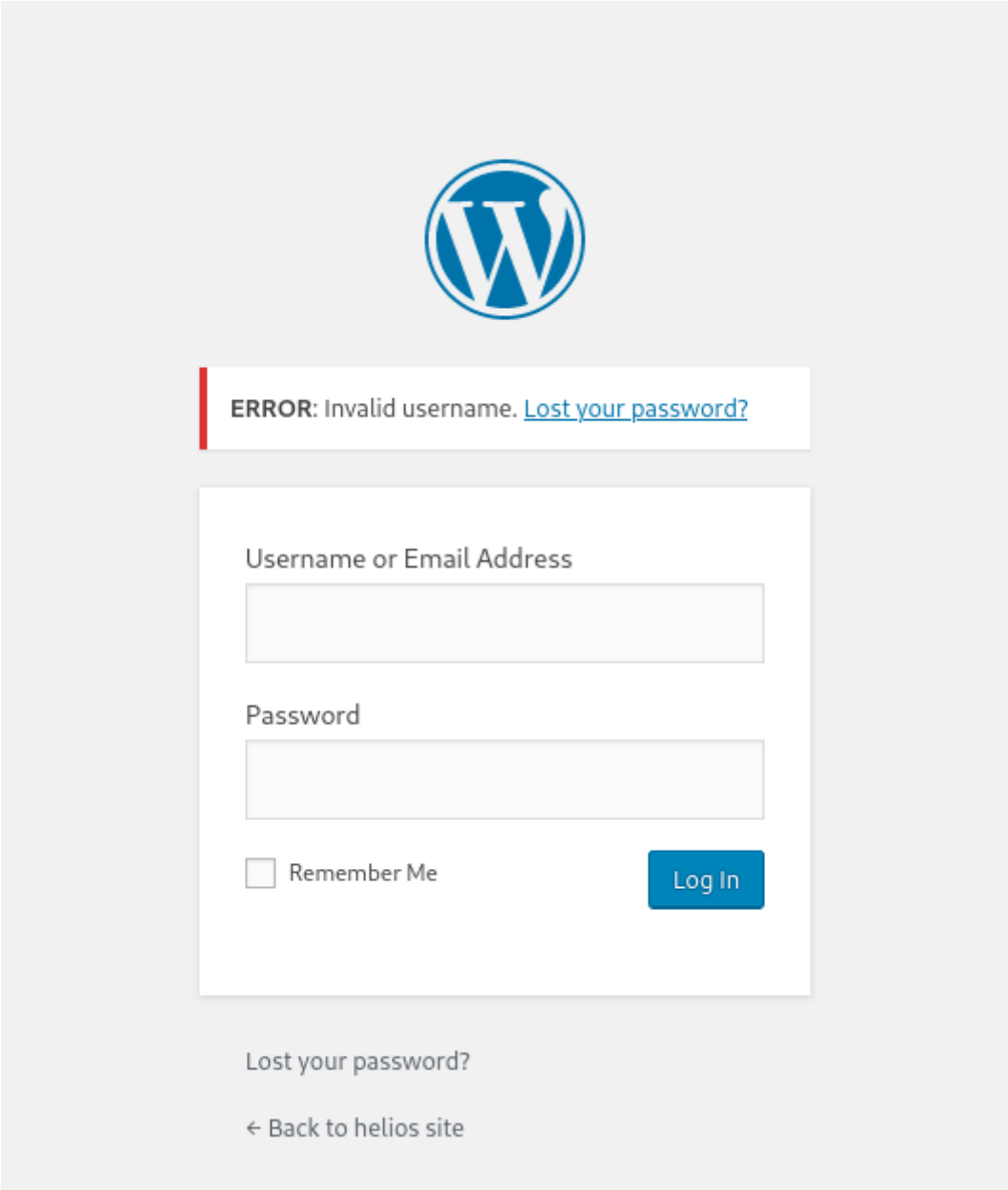
```
[+] WordPress version 5.2.2 identified (Insecure, released on 2019-06-18).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.14.218/h3l105/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.2.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.14.218/h3l105/, Match: 'WordPress 5.2.2'

[i] The main theme could not be detected.

[+] Enumerating Most Popular Plugins (via Passive Methods)
```

Usuarios encontrados

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



Si ponemos Helios



Si una vez visro el WPSCAN no encuentra plugins podemos hacer un CURL tal que asi cin un grep para encontrar la palabra clave wp-content

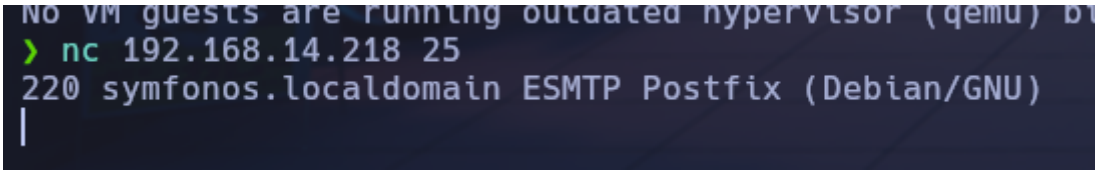
```Bash
curl url | grep "wp-content"
```

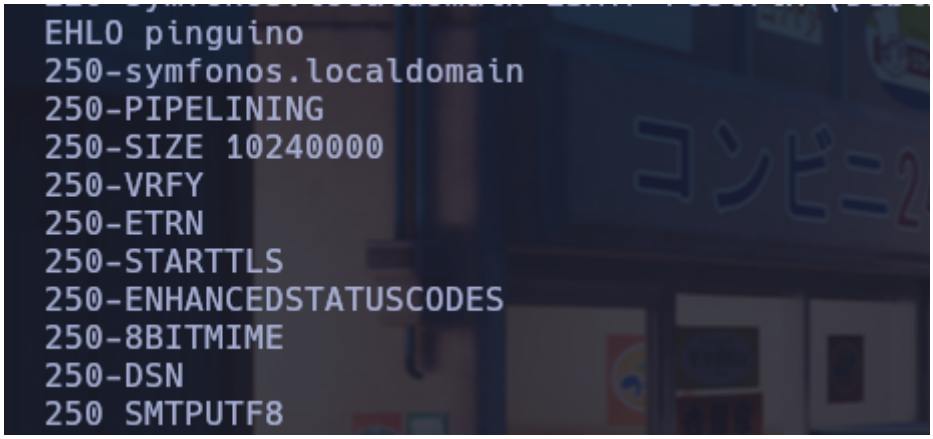
```
❯ curl http://192.168.14.218/h3l105/ | grep "wp-content"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<link rel='stylesheet' id='sed-FontAwesome-css'  href='http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/FontAwesome/FontAwesome.css?ver=4.3' type='text/css' media='all' />
<link rel='stylesheet' id='general-css'  href='http://symfonos.local/h3l105/wp-content/plugins/site-editor/framework/assets/css/general.min.css?ver=1.1.1' type='text/css' media='all' />
<link rel='stylesheet' id='css3-animate-css'  href='http://symfonos.local/h3l105/wp-content/plugins/site-editor/framework/assets/css/animate/animate.min.css?ver=5.2.2' type='text/css' media='all' />
<link rel='stylesheet' id='twentynineteen-style-css'  href='http://symfonos.local/h3l105/wp-content/themes/twentynineteen/style.css?ver=1.4' type='text/css' media='all' />
<link rel='stylesheet' id='twentynineteen-print-style-css'  href='http://symfonos.local/h3l105/wp-content/themes/twentynineteen/print.css?ver=1.4' type='text/css' media='print' />
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/mail-masta/lib/subscriber.js?ver=5.2.2'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/mail-masta/lib/jquery.validationEngine-en.js?ver=5.2.2'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/mail-masta/lib/jquery.validationEngine.js?ver=5.2.2'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/framework/assets/js/sed_app_site.min.js?ver=1.0.0'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/assets/js/livequery/jquery.livequery.min.js?ver=1.0.0'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/assets/js/livequery/sed.livequery.min.js?ver=1.0.0'></script>
                <figure class="wp-block-image"><img src="http://symfonos.local/h3l105/wp-content/uploads/2019/06/image-1.png" alt="" class="wp-image-7"/></figure>
<link rel='stylesheet' id='mm_frontend-css'  href='http://symfonos.local/h3l105/wp-content/plugins/mail-masta/lib/css/mm_frontend.css?ver=5.2.2' type='text/css' media='all' />
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/framework/assets/js/animate/wow.min.js?ver=1.0.2'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/framework/assets/js/parallax/jquery.parallax.min.js?ver=1.1.3'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/framework/assets/js/render.min.js?ver=1.0.0'></script>
<script type='text/javascript' src='http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/js/row.js?ver=1.0.0'></script>
100 16786    0 16786    0     0   779k      0 --:--:-- --:--:-- --:--:--  780k
                var $style_sheet = "<link rel='stylesheet' id='general_home_css-css'  href='http://symfonos.local/h3l105/wp-content/uploads/siteeditor/sed_general_home.css' type='text/css' media='all' />";
```

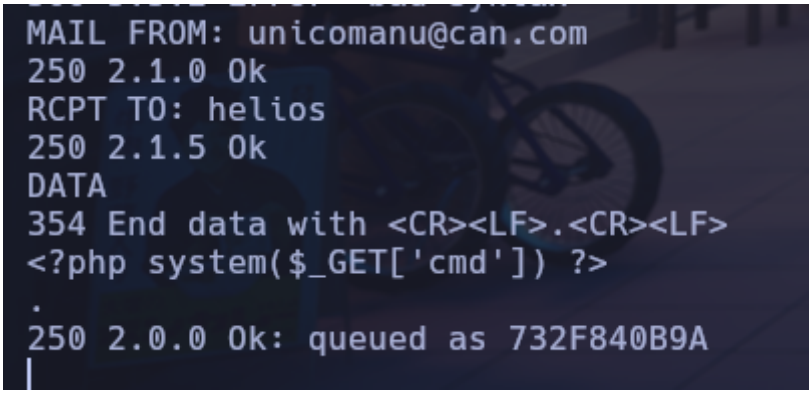
Como vemos el plugin que vamos a sacar
el el wp-mail masta
Lo buscamos en el buscador

Vemos qie nos pone un url y
lo probamos

Al ver que podemos acceder haciendo un LFI tenemos que pensar que podemos hacer un log poisin desde otros protocolos y como hemos visto en el protocolo smtp por el puerto 25 hacemos un netcat







Una vez sabido esto tenemos que saber que directorio donde esta el mensaje es en /var/mail/usuario&cmd=whoami