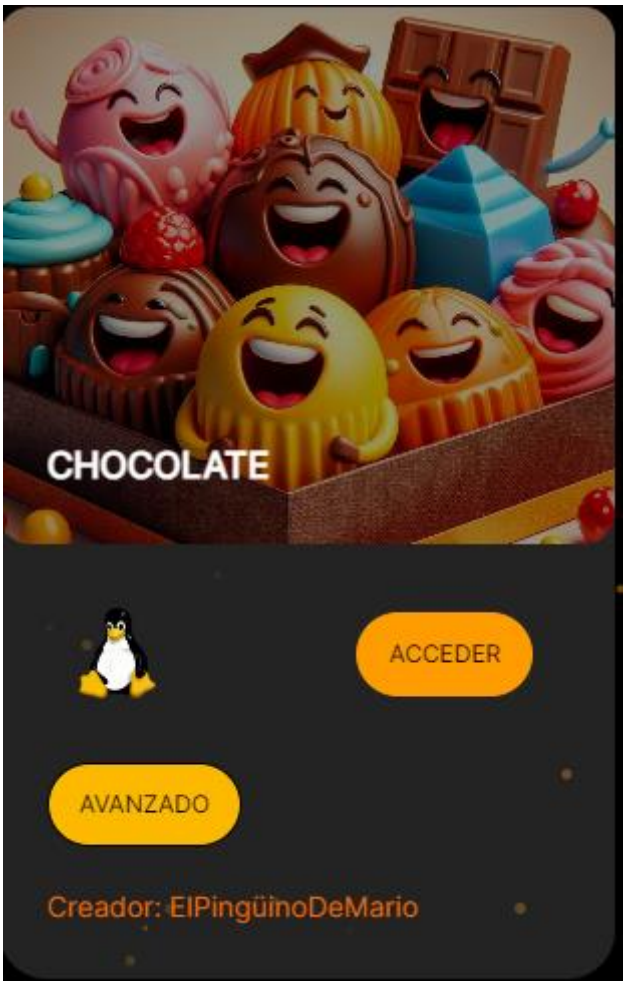
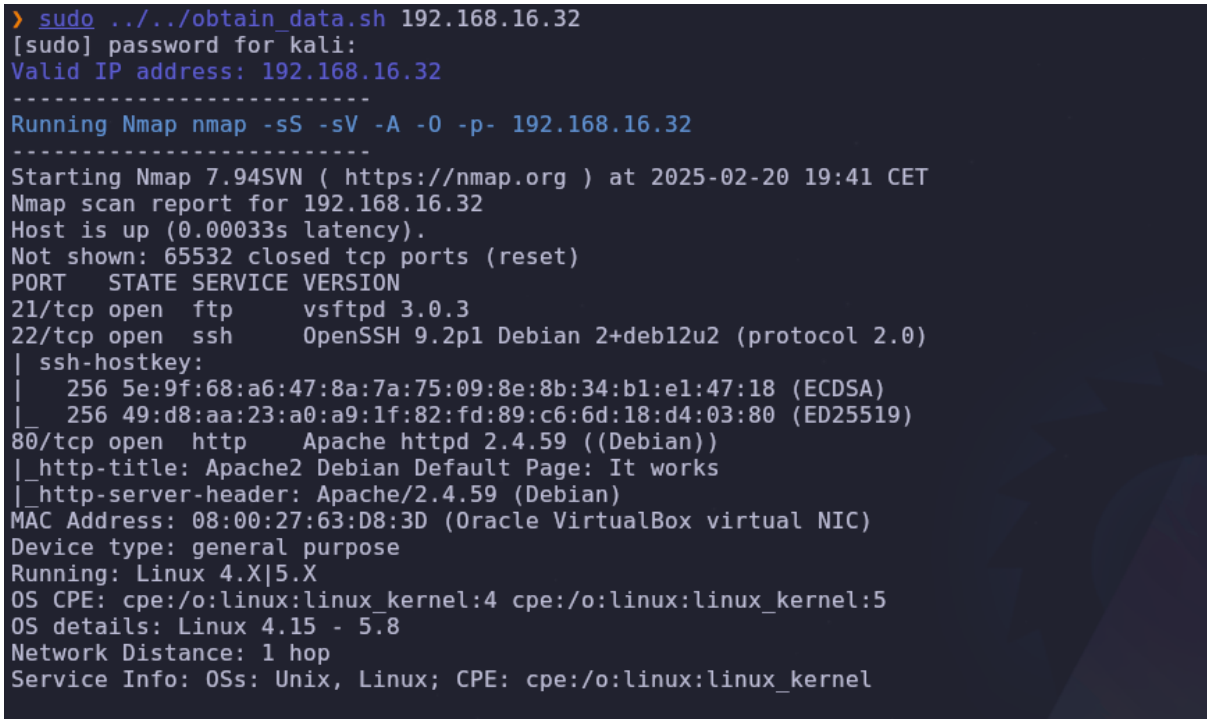
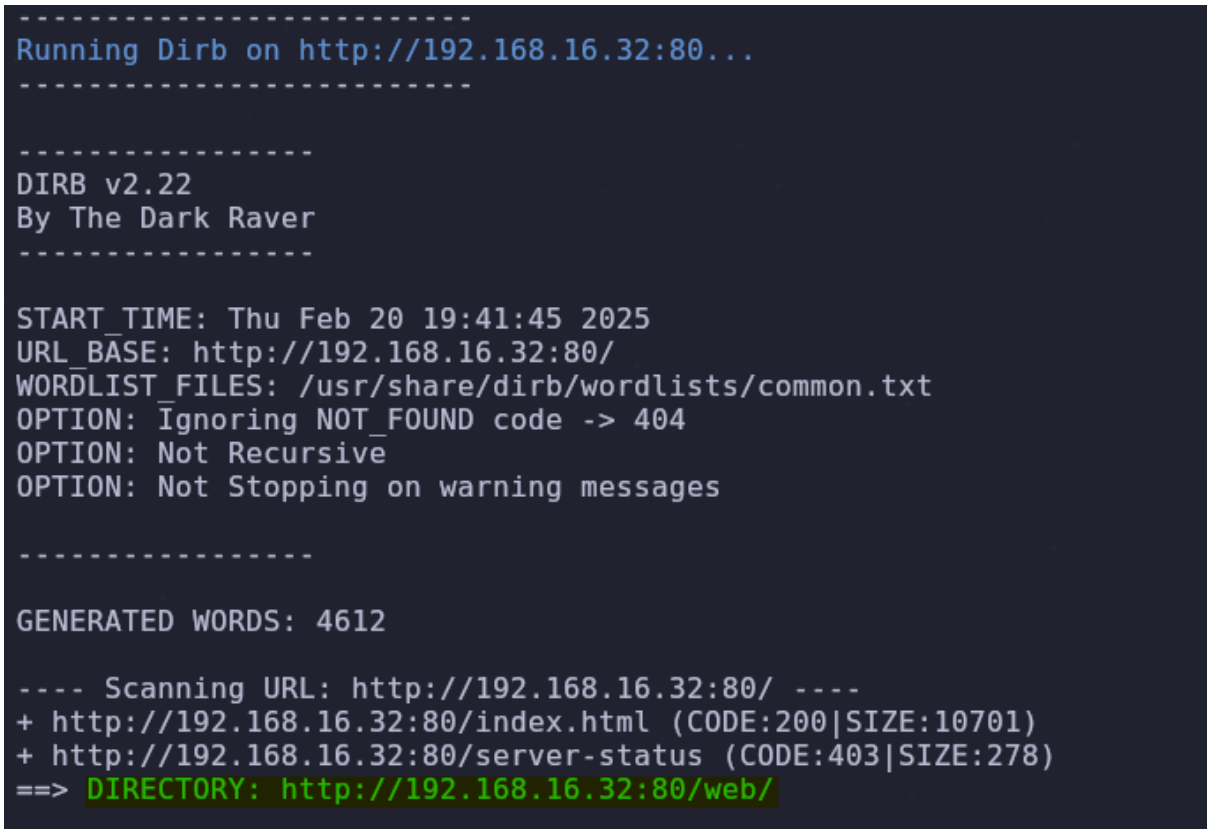
CHOCOLATE



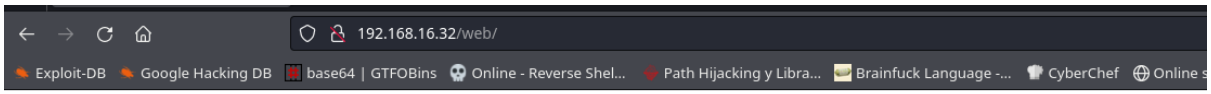
Comenzamos ejecutando nmap para descubrir los puertos abiertos. Encontramos los puertos 21,22 y 80 abiertos.



Usando dirb encontramos la página web.

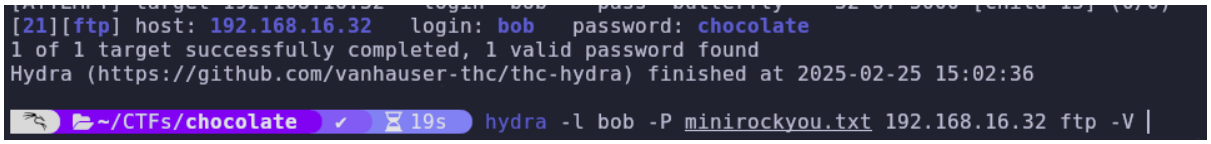


Donde nos encontramos una pequeña pista.

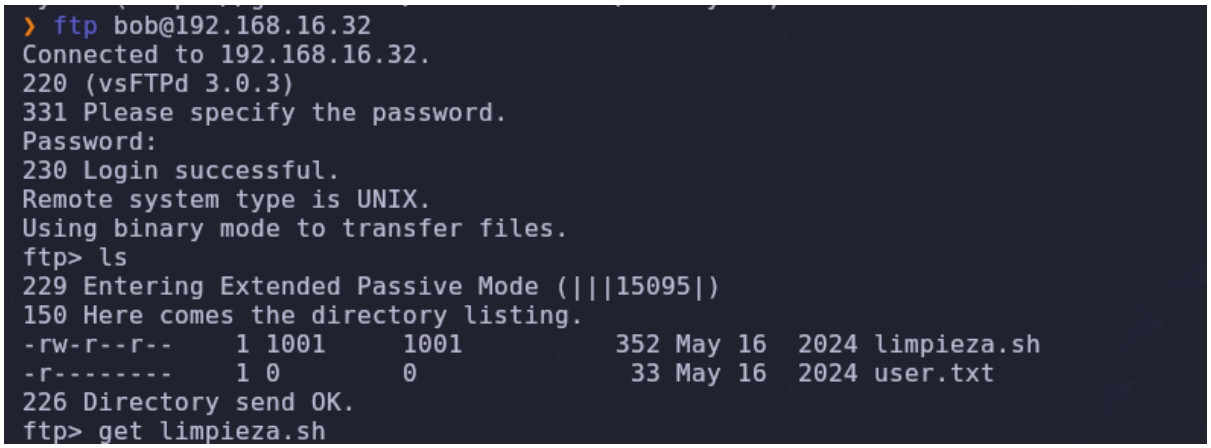


Bob, comprueba que la limpieza se estÃ© ejecutando automÃ¡ticamente en el sistema

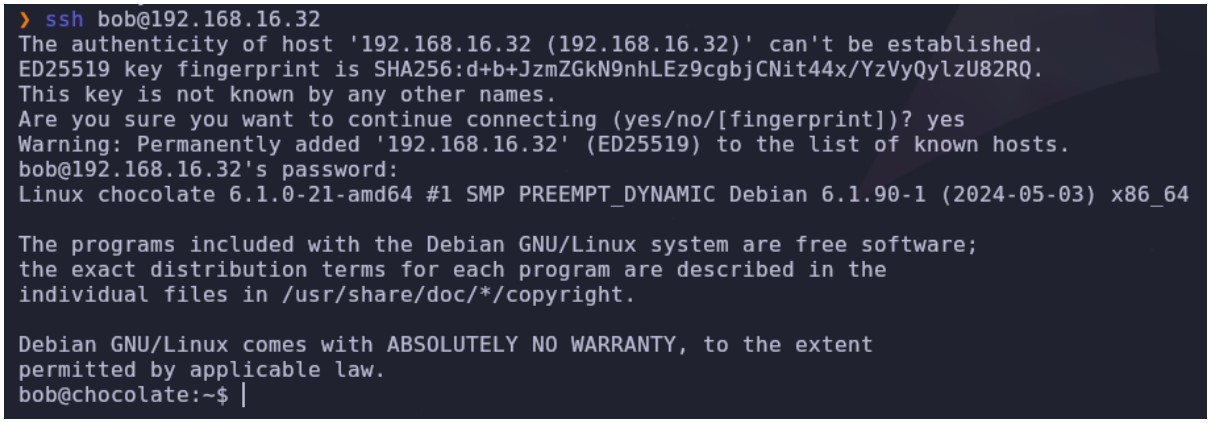
Teniendo el usuario probamos a hacer un ataque de fuerza bruta contra el puerto 21.



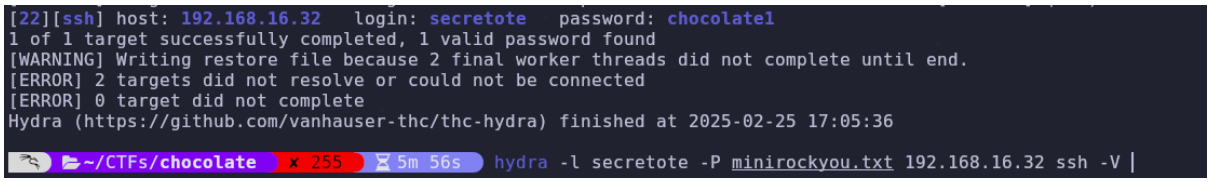
Accedemos al puerto 21 con las credenciales obtenidas donde descargamos un script llamado limpieza.sh.



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

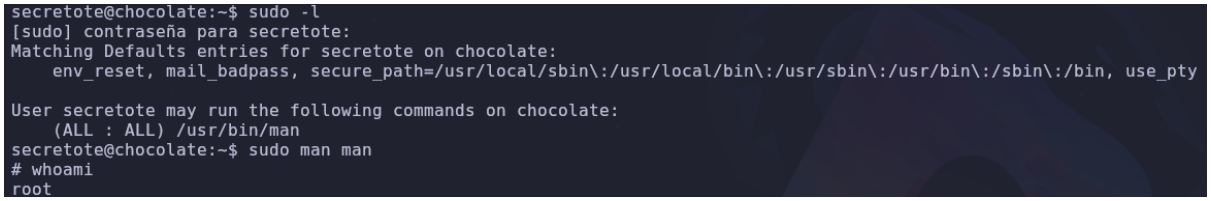


Buscando por el sistema no encontramos nada con el cual escalar con el usuario bob, es por ello que miramos los usuarios existentes en el sistema para realizar una fuerza bruta.



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
```



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
[redacted]
```

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

```
# 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.