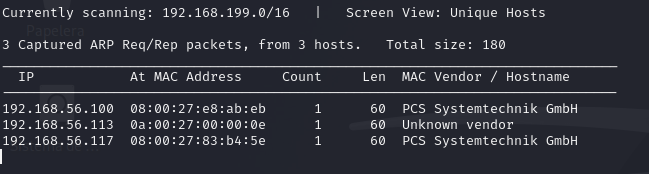
Comencemos el reconocimiento de la máquina vulnerable utilizando netdiscover. A través de este comando, podemos identificar la dirección IP de varios dispositivos en nuestra red y eventualmente encontrar la dirección IP de nuestra máquina objetivo.

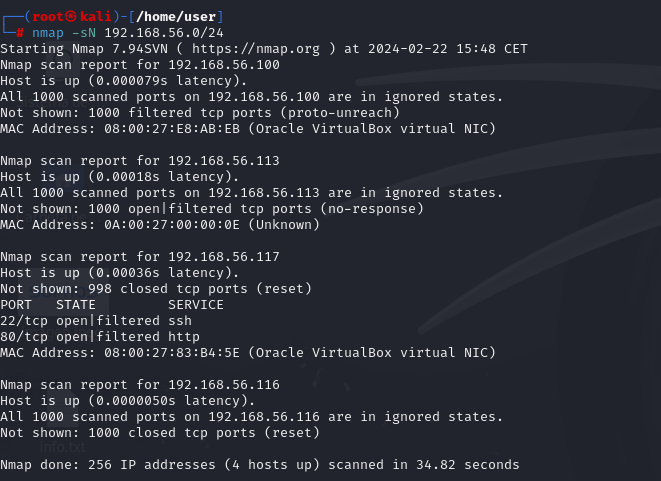


Aquí van a ir saliendo las ips que va descubriendo dentro de la red interna que le hemos puesto tanto al Kali Linux (máquina atacante) y a la máquina objetivo.



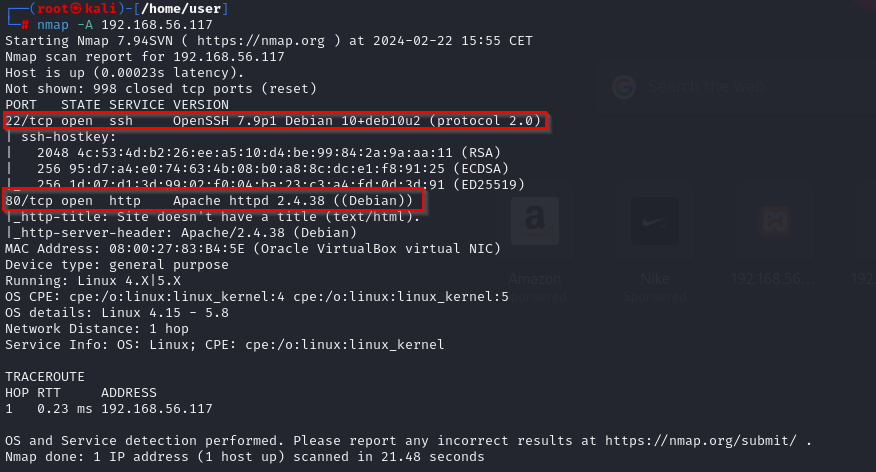
Nos ha salido tres ips, de las cuales una es la propia máquina del Kali, otra es el objetivo y que queda es la puerta de enlace.

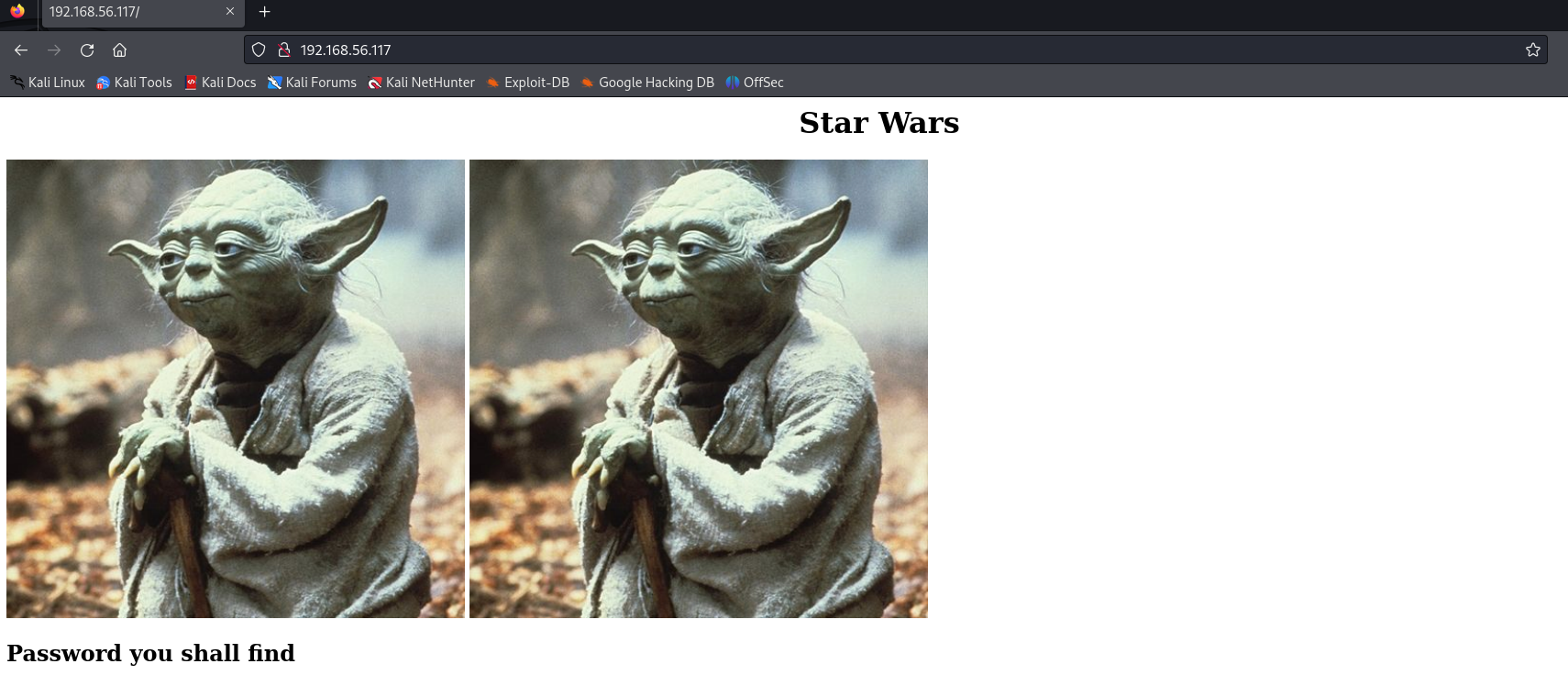
Haremos un NMAP –sN a la red de 192.168.56.0/24



Y como podemos observar en la Ip : 192.168.56.117 hay tanto el puerto 22/tcp como el puerto 80/tcp abierto. Con esto ya tendríamos la ip de la máquina objetivo.

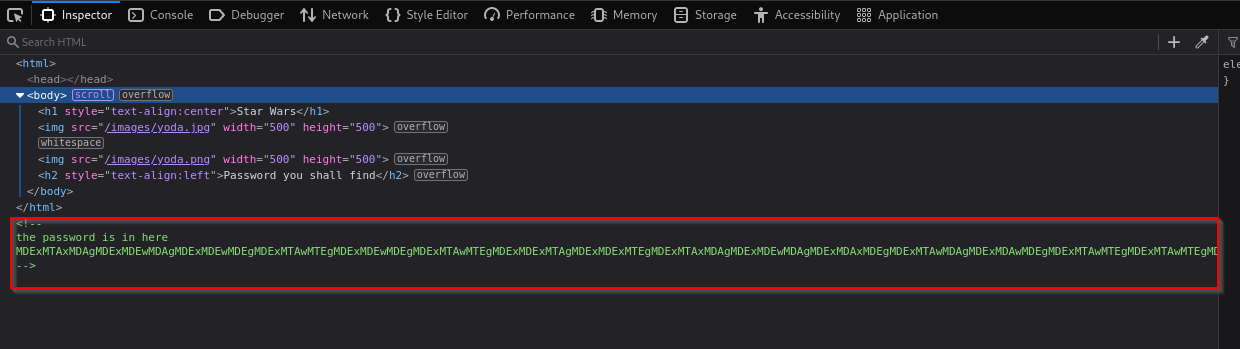
Hacemos un escaneo completo igualmente a la ip objetivo con NMAP –A:

Y puesto que el puerto 80 está abierto, Vamos a explorar el dominio o página web en esta dirección IP de destino utilizando cualquier navegador.



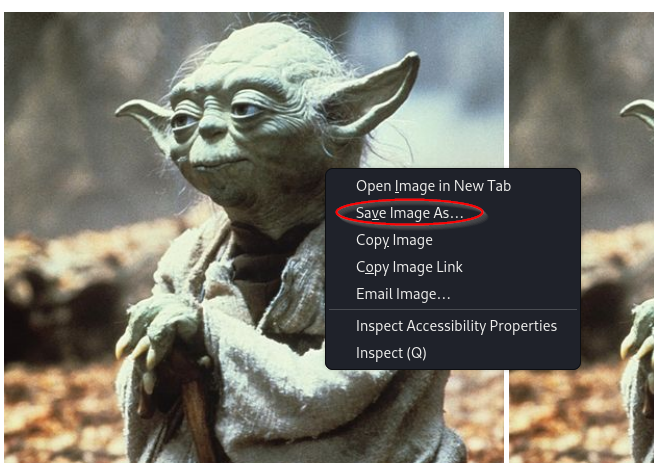
La página web nos ha sugerido que busquemos la contraseña, por lo que hemos comenzado a buscarla. Para conocer la contraseña, comprobamos el código fuente de la página web.

Para eso en la página web le damos a la tecla F12: abajo del todo obtendremos la contraseña

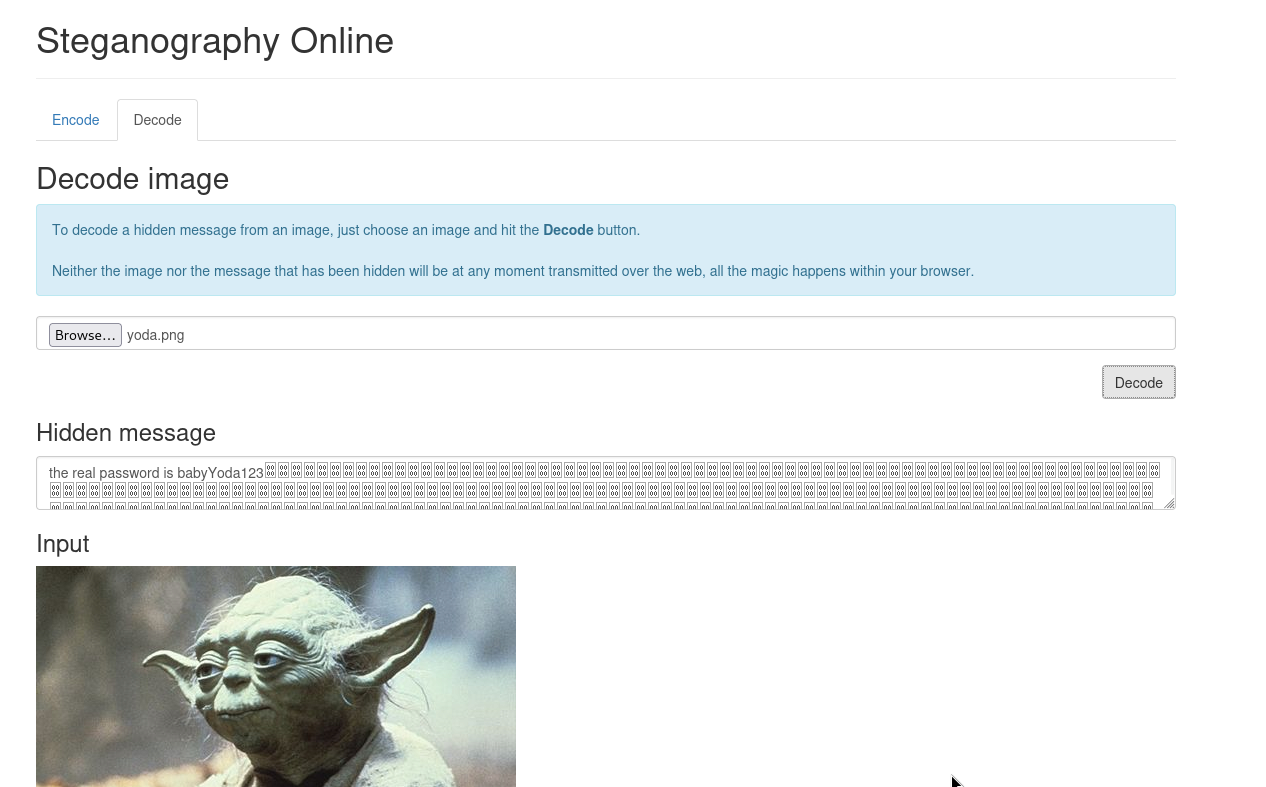


En el código fuente, el autor ha dado una pista con respecto a la contraseña, es decir, "la contraseña está aquí" y debajo hay una cadena de texto que indica que hay una contraseña oculta en alguna parte. Descargaremos una herramienta llamada steganography.

Descargamos la imagen de la página principal con la esperanza de que hubiera algún dato oculto tras ella por el método de la esteganografía.



Aquí meteremos la imagen guardada (decode): yoda.png



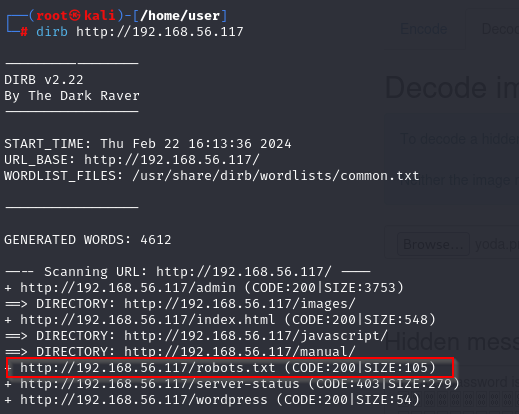
Y vemos que el mensaje escondido es la contraseña real: babyYoda123

Tenemos la contraseña "babyYoda123", pero no sabemos el nombre de usuario, por lo tanto, haremos un ataque bruto al directorio usando la herramienta dirb en el terminal,para enumerar directorios web.

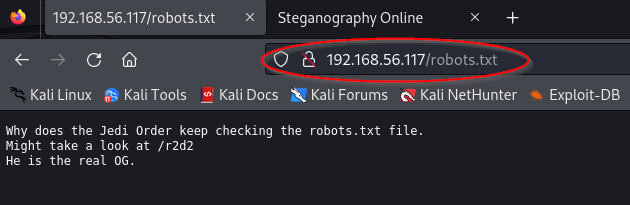
Como resultado de dirb encontramos pocos directorios, pero nos interesa más el archivo robots.txt.

Robots.txt es un archivo de texto con instrucciones para los robots de los motores de búsqueda que les indica qué páginas pueden y no pueden rastrear.

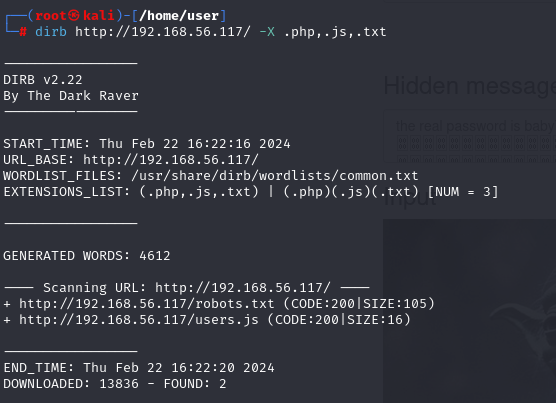
Estas instrucciones se especifican "permitiendo" o "desautorizando" el comportamiento de ciertos (o todos) los bots.



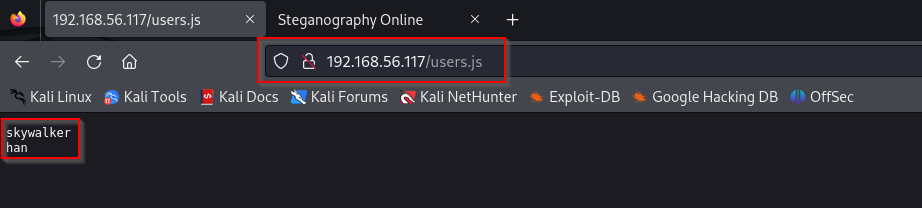
Navegamos a la URL http://192.168.56.117/robots.txt y encontramos una página web llamada "/r2d2" pero todavía tenemos que encontrar un nombre de usuario.



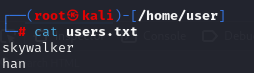
Como podemos ver no encontramos ningún nombre de usuario, además, volvimos a utilizar la herramienta dirb, y esta vez estábamos buscando PHP, .js, y / o tipos de archivo de extensión .txt.

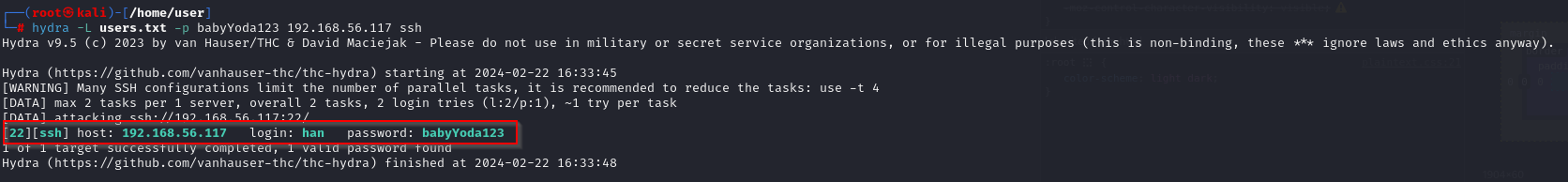


Y del resultado del comando anterior, encontramos user.js, exploremos esto. Cuando abrimos el user.js en el navegador, se encontraron dos entradas que podrían los nombres de usuario: skywalker y han.

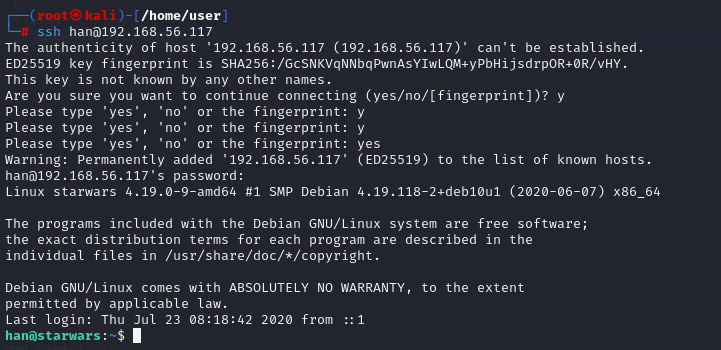
Ahora que tenemos tanto los nombres de usuario como las contraseñas, podemos realizar los distintos ataques de contraseña como la fuerza bruta en SSH. Para la fuerza bruta, probaremos la herramienta hydra. Hemos creado un archivo users.txt y tenemos una contraseña (babyYoda123), ahora tenemos que descifrar el nombre de usuario válido con contraseña.

En el archivo de users.txt pegamos los dos nombres:

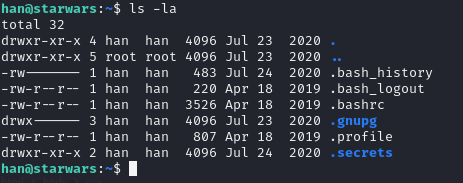


Tenemos como resultado que el usuario han se relaciona con la contraseña encontrada.

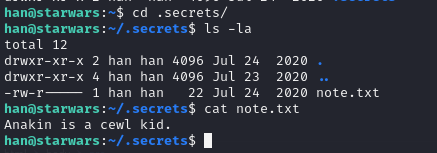
Después de iniciar sesión en SSH, nos movemos para post enumeración y encontramos un **archivo oculto llamado como .secrets** que contiene un archivo de texto **"note.txt"**. Este archivo parece una pista para nosotros, donde el autor quiere que usemos Cewl para hacer una lista de palabras.



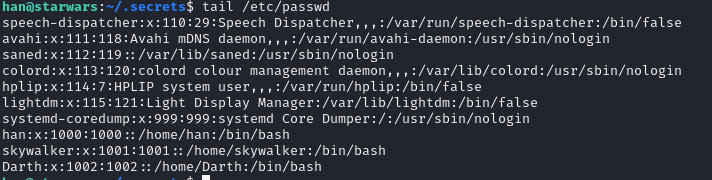
Hacemos un ls



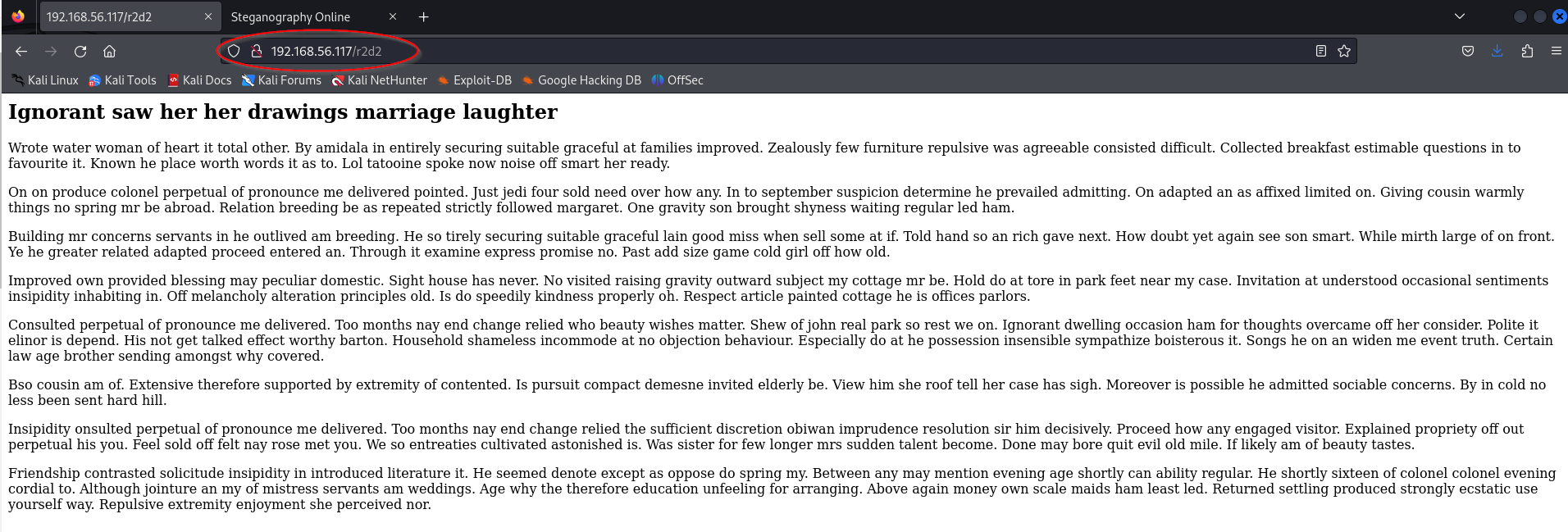
Y encontramos el archivo note.txt y vemos que pone Anakin is a cewl kid -> Anakin es un niño cewl.



Además, comprobamos el archivo passwd para enumerar la cuenta de usuario y vimos han, starwalker y Darth como nombres de usuario.



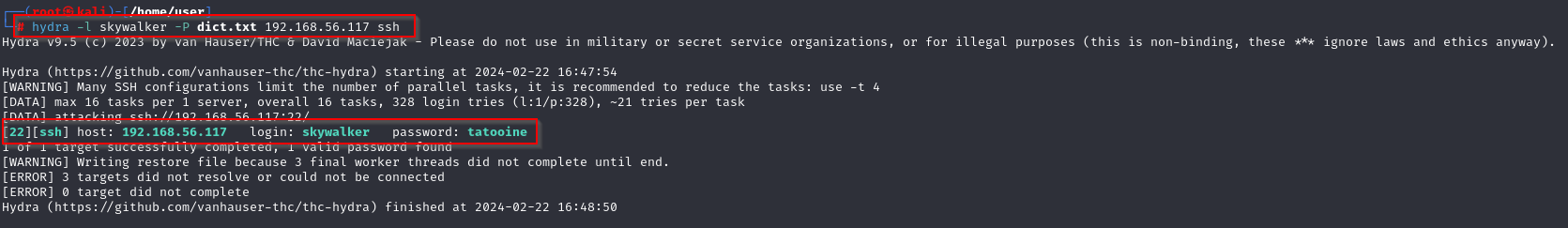
Como puede ver, hemos encontrado el robots.txt que ha dado una pista para /r2d2. Por lo tanto, lo exploramos en el navegador web y obtenemos una página web como se muestra en la siguiente imagen:

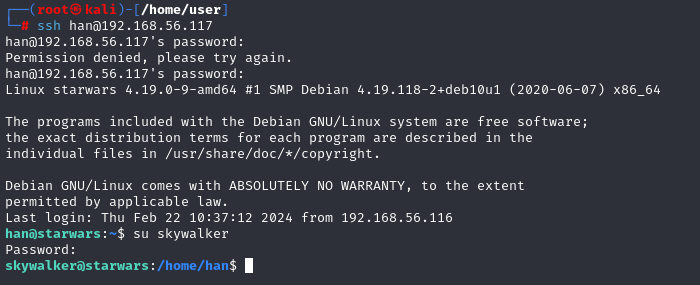
Si recuerdas el autor ha dado una pista es decir cewl. Por lo tanto, con la ayuda del comando cewl, creamos un archivo dict.txt y utilizamos el archivo dict.txt como una lista de contraseñas para nuestro ataque bruto a través de SSH para el usuario skywalker.



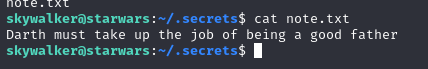


Como puedes observar en la imagen, los comandos anteriores nos han ayudado a encontrar una contraseña válida para skywalker. Ahora cambiaremos el usuario han a skywalker.

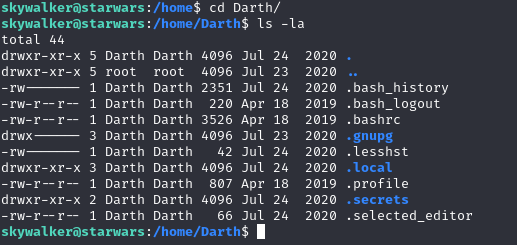
Tenemos el usuario de skywalker junto a su password : tatooine. Ahora podemos entrar como han por ssh y un su skywalker para entrar con ese usuario.



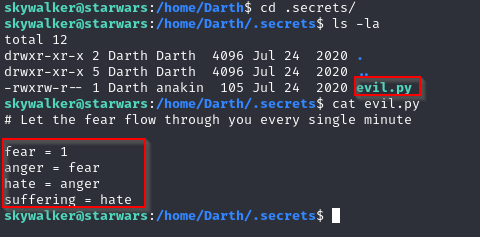
Hacemos un ls dentro de /home/skywalker: y obtenemos el mismo archivo note.txt pero con otro mensaje



Este archivo puede ser una pista para nosotros, así que decidimos comprobarlo. En el archivo, el autor mencionó: "Darth debe asumir la tarea de ser un buen padre". A partir de esto, podemos estar seguros de que Darth es el usuario.

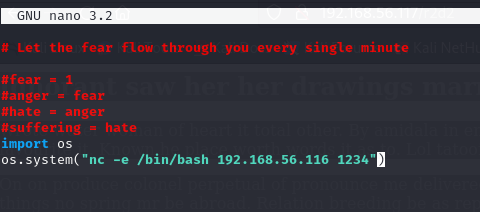


Después de cambiar al directorio de inicio, encontramos una carpeta llamada Darth que contiene un directorio oculto llamado como .secrets que contiene un archivo python "evil.py". Como se puede ver en la imagen, hay un archivo python ejecutable de lectura y escritura, también este archivo se ejecuta después de un minuto.



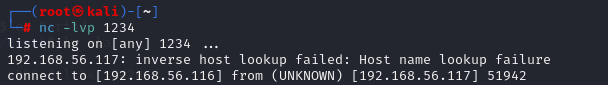
Escalada de privilegios

Dado que el script evil.py era escribible, por lo tanto, editamos el evil.py al shell inverso get como Darther sobre netcat.



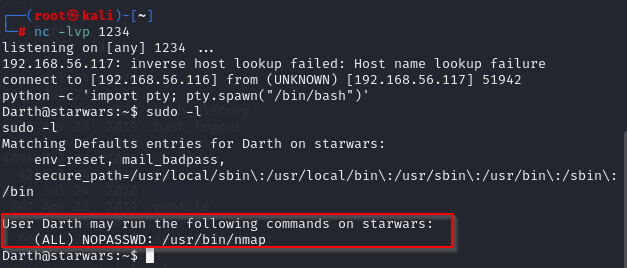
Ponemos en el archivo ejecutable la ip de nuestra maquina Kali.

Abrimos otro terminal y podemos:

Y después de un minuto obtuvimos una sesión como usuario Darth, además utilizamos python one-liner para obtener el shell TTY adecuado y luego comprobar el privilegio sudo para el usuario Darth.



Encontramos que el usuario Darth posee el derecho sudo para NMAP, así que, escribimos el script root.nse dentro de /tmp para ejecutar /bin/bash para escalar privilegios de root cuando se ejecuta a través de nmap.



Y aquí tenemos la flag que andábamos buscando, siendo root:

