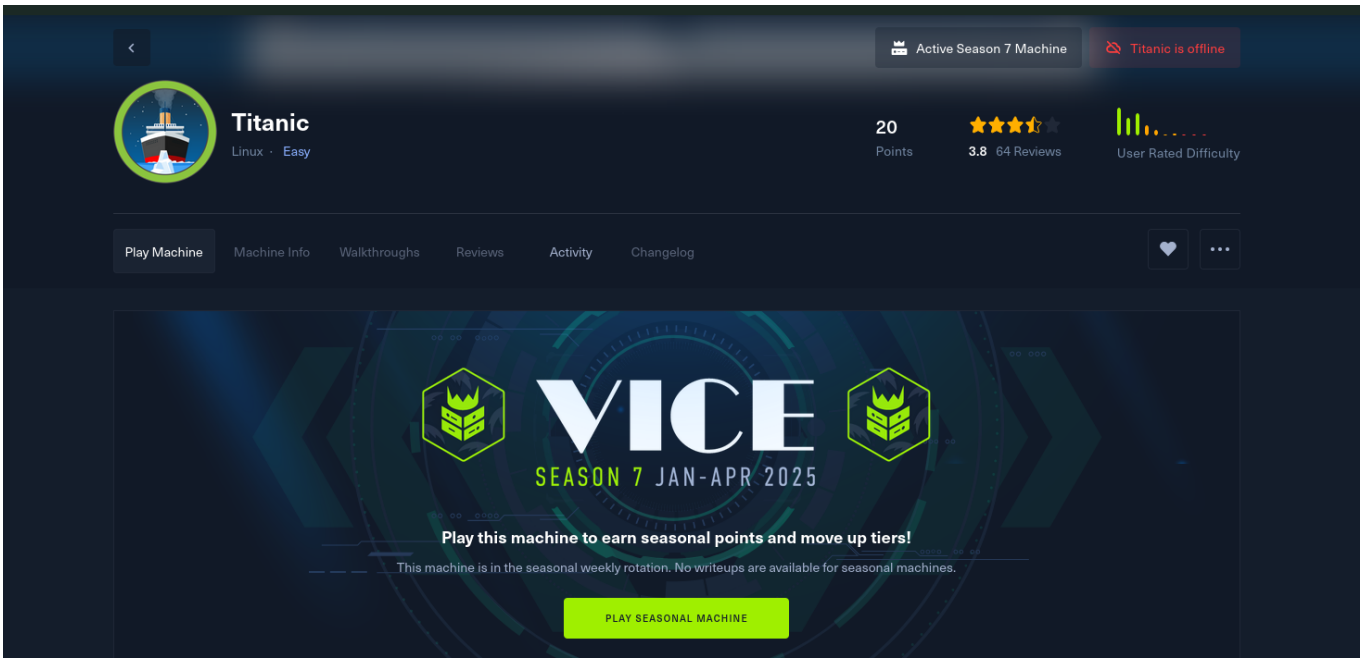
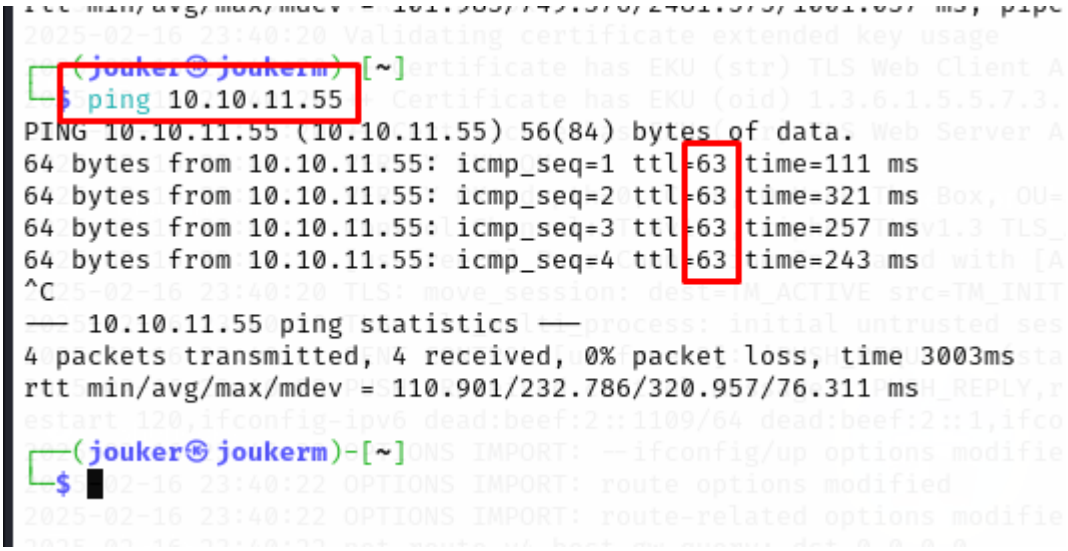
Imagen de la máquina seasonal de hack the box



ping inicial de reconocimiento, ya sabemos que es linux por la imagen pero aún así vamos a identificarlo por el ttl del ping que vamos a realizar a la máquina atacante.

Ping cercano a TTL 64.



Hacemos un escáner completo de puertos y en dicho escáner vemos como se nos lista el puerto 22 y 80 habituales dentro de un CTF en

linux.

```
└─$ sudo nmap -p- -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.11.55 -oN target.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 23:43 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:43
Completed NSE at 23:43, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:43
Completed NSE at 23:43, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:43
Completed NSE at 23:43, 0.01s elapsed
Initiating SYN Stealth Scan at 23:43
Scanning 10.10.11.55 [65535 ports]
Discovered open port 22/tcp on 10.10.11.55
Discovered open port 80/tcp on 10.10.11.55
```

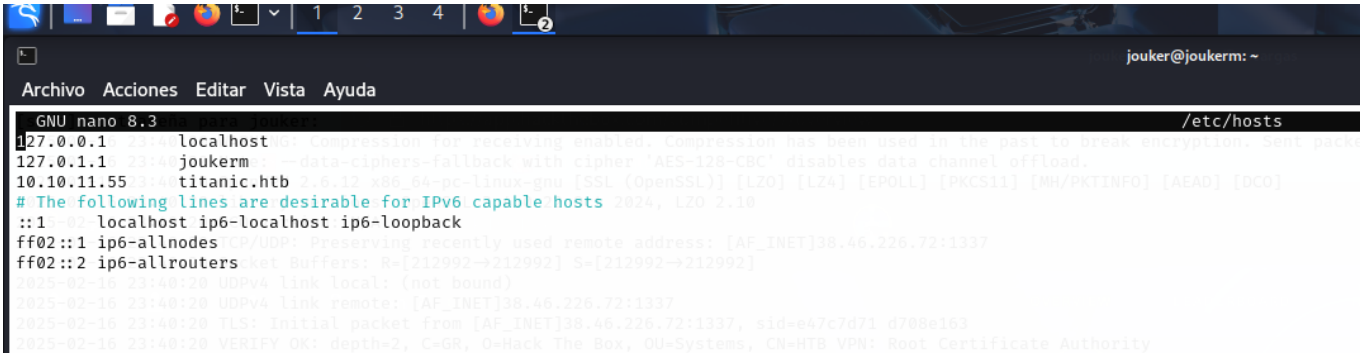
Responde a titanic.htb por lo que voy a editar el archivo /eyc/hosts para que incluya titanic.htb con la IP que me han dado.

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 73:03:9c:76:eb:04:f1:fe:c9:e9:80:44:9c:7f:13:46 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGZG4yHYcDPrtn7U0l+ertBhGBgjIeH9vWnZcmqH0cvmCNvdcDY/ItR3tdB4yMJp0ZTth5itUVtlJJGHRYAZ8Wg=
|   256 d5:bd:1d:5e:9a:86:1c:eb:88:63:4d:5f:88:4b:7e:04 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDT1btWpkcbHWpNEEqICTtbAcQQitzOiPOmc3ZE0A69Z
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.52
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://titanic.htb/
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: titanic.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Tenemos ping correcto tambien

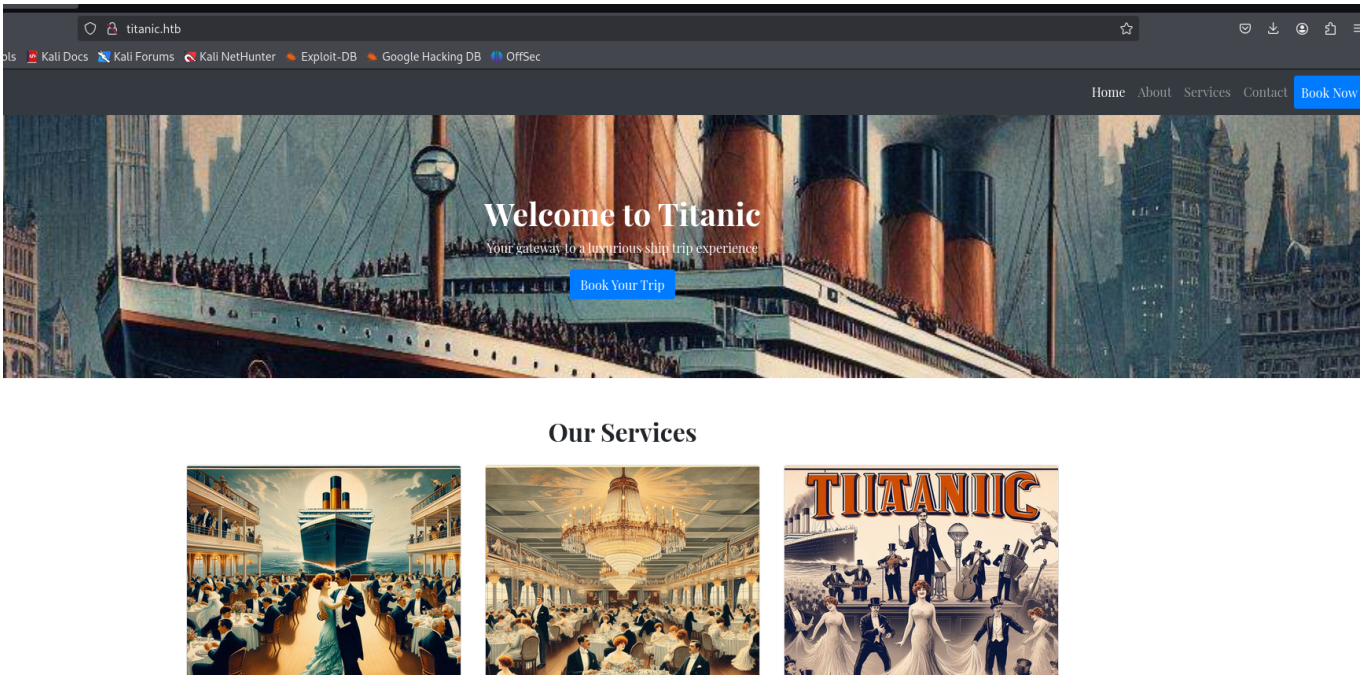
```
┌──(jouker㉿joukerm)-[~]
└─$ ping titanic.htb
PING titanic.htb (10.10.11.55) 56(84) bytes of data.
64 bytes from titanic.htb (10.10.11.55): icmp_seq=1 ttl=63 time=104 ms
64 bytes from titanic.htb (10.10.11.55): icmp_seq=2 ttl=63 time=103 ms
^C
--- titanic.htb ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 103.152/103.476/103.800/0.324 ms

┌──(jouker㉿joukerm)-[~]
└─$
```

Dejo captura del /etc/hosts



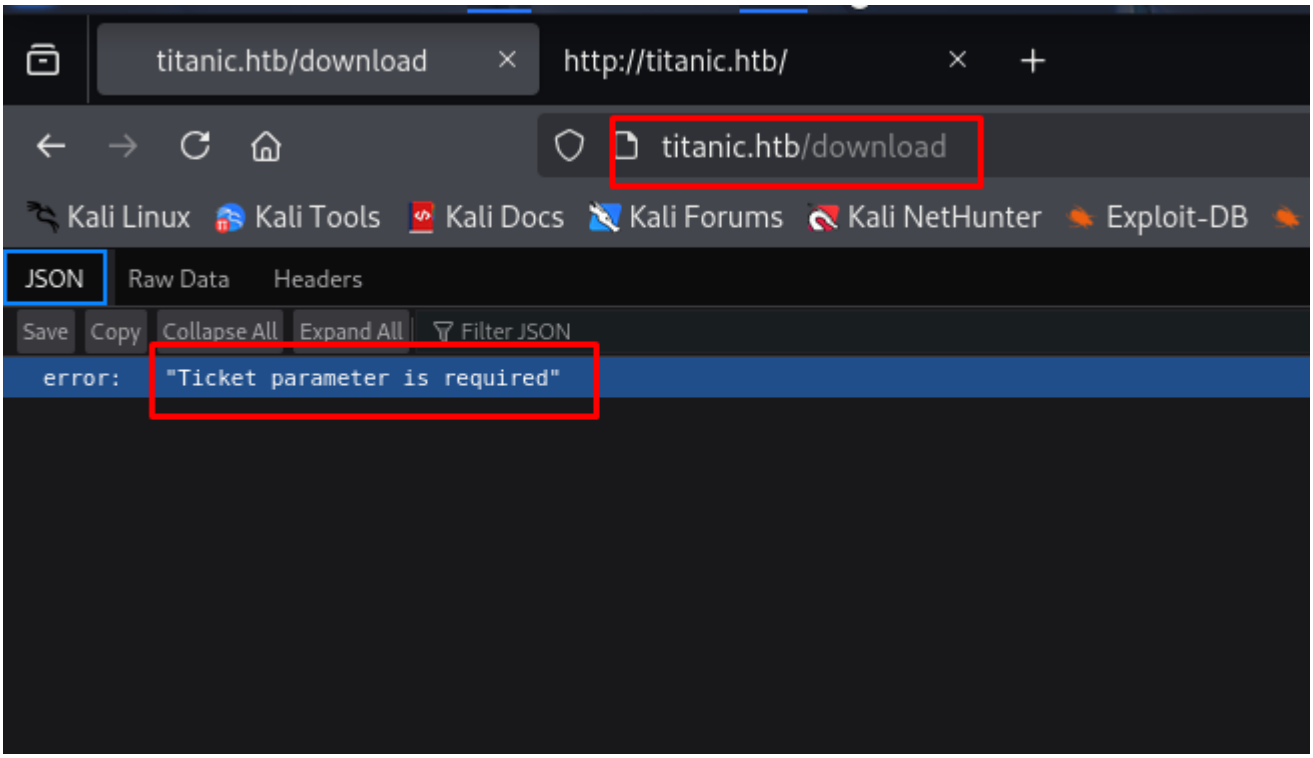
Captura del whatweb que corre en el servicio del puerto 80:

página titanic.

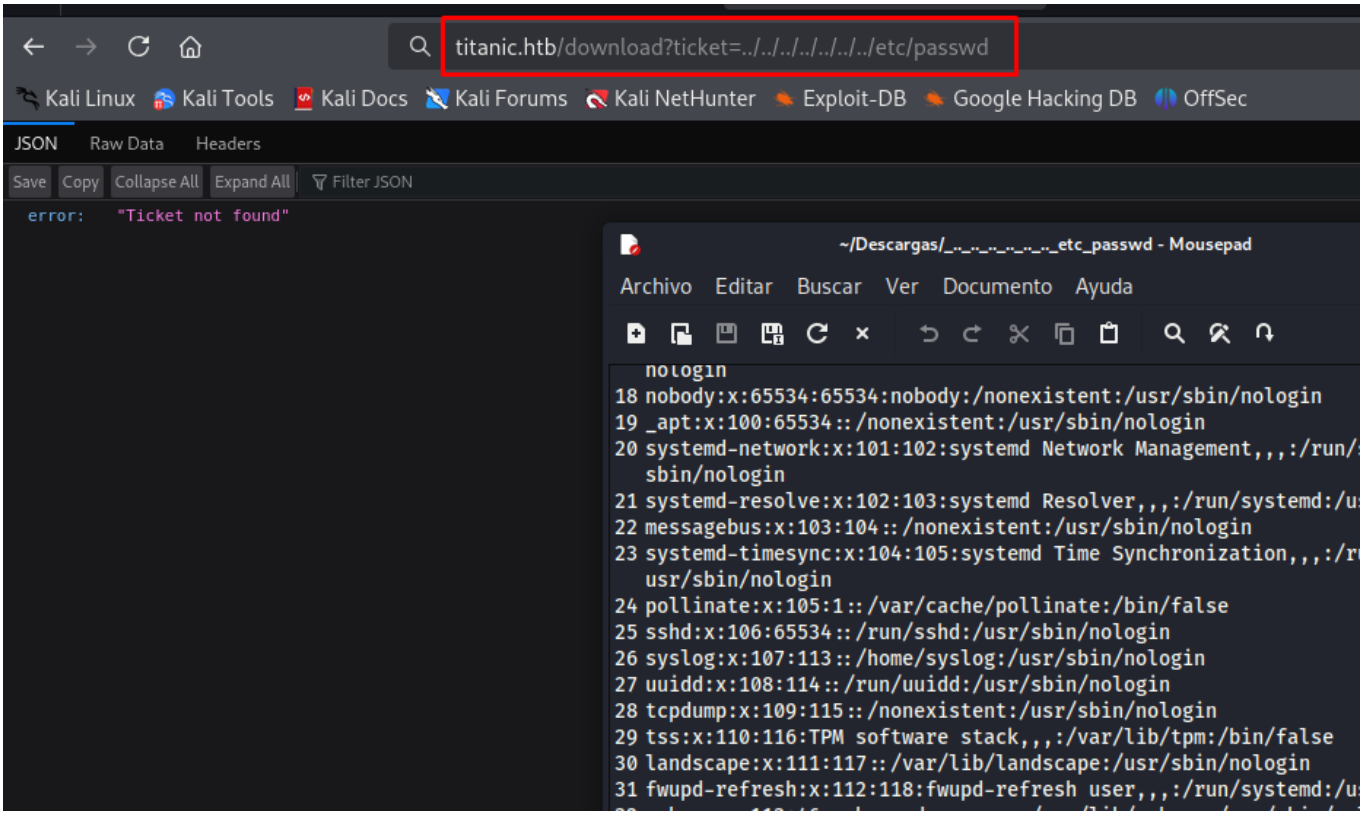


Todo el resto de botones e imágenes son inútiles, te redirigen a ninguna parte. Lo único que tiene algo dentro es la misma opción con diferente nombre BOOK YOUR TRIP y BOOK NOW que podría ser una ruta de entrada para una vulnerabilidad XSS.

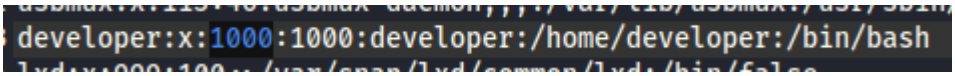
En la pestaña titanic.htb/download, que he conseguido listar gracias a gobuster, veo que hay un error dond pide ticket parameter is required.



Sin ir mucho más lejos obtengo el /etc/passwd a traves de un LFI

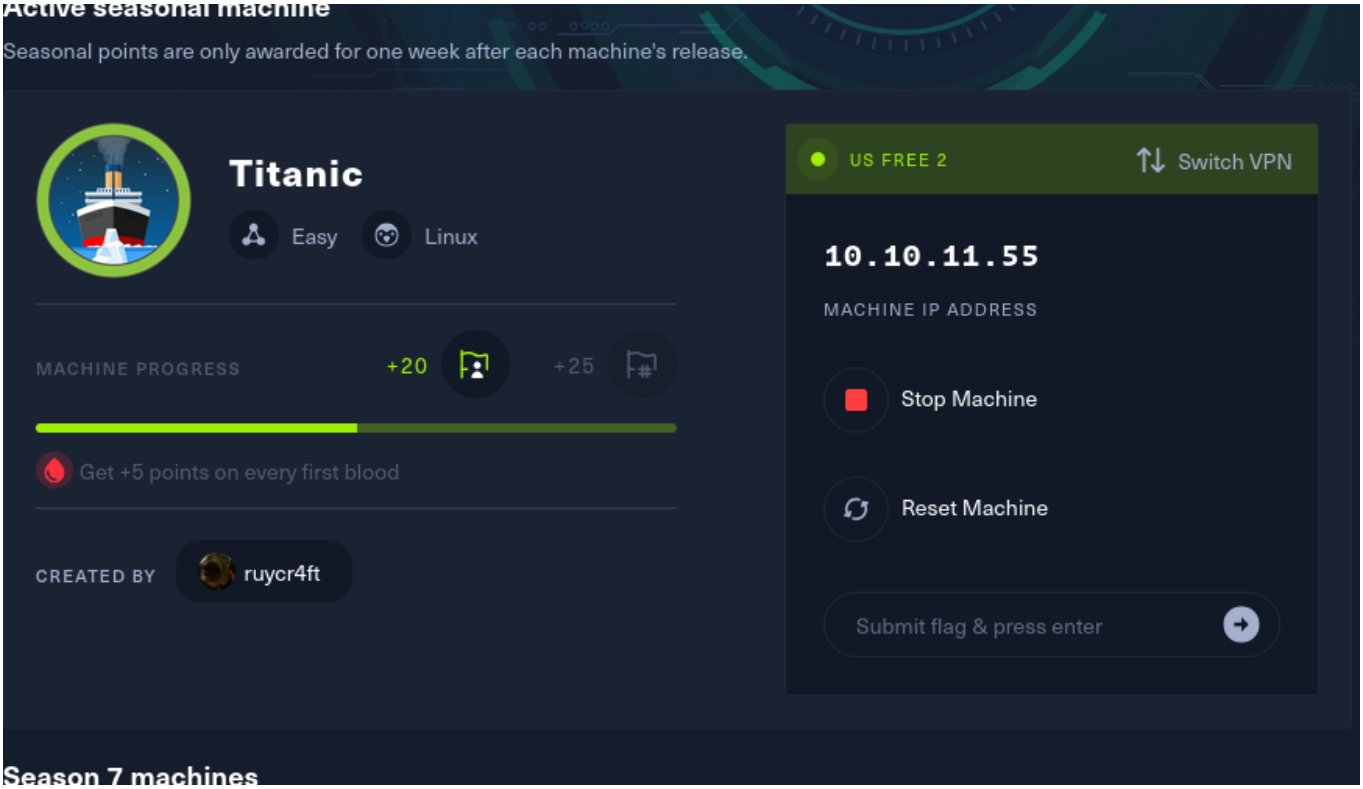


Me he quedado aquí porque hydra se cuelga, imagino que será por compartir VPN con 70 personas que se cuelga fácil. El usuario es developer, és el único que tiene una /bin/bash



Al igual que hemos conseguido el /etc/passwd y hemos listado los usuarios a base de conocer el lugar donde se suele almacenar el user.txt, hemos hecho lo mismo pero en este caso lo hemos hecho para ../../../home/developer/user.txt

Y hasta aquí he llegado, solo he conseguido vulnerar la primera flag en esta ocasión


Active seasonal machine
Seasonal points are only awarded for one week after each machine's release.
Titanic
Easy
Linux
MACHINE PROGRESS
+20
+25
Get +5 points on every first blood
CREATED BY
ruycr4ft
US FREE 2
Switch VPN
10.10.11.55
MACHINE IP ADDRESS
Stop Machine
Reset Machine
Submit flag & press enter
Season 7 machines