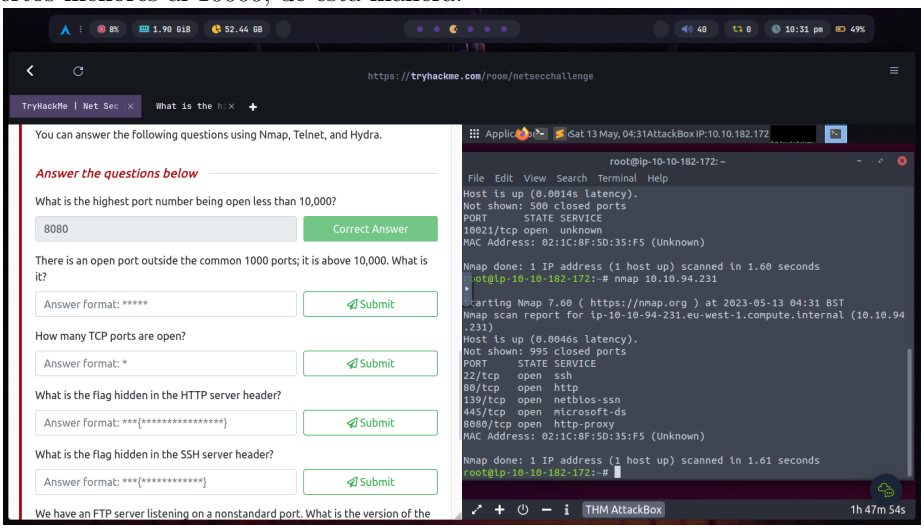
Resolución del reto NetSecChallenge de TryHackMe

Daniel Valdivieso

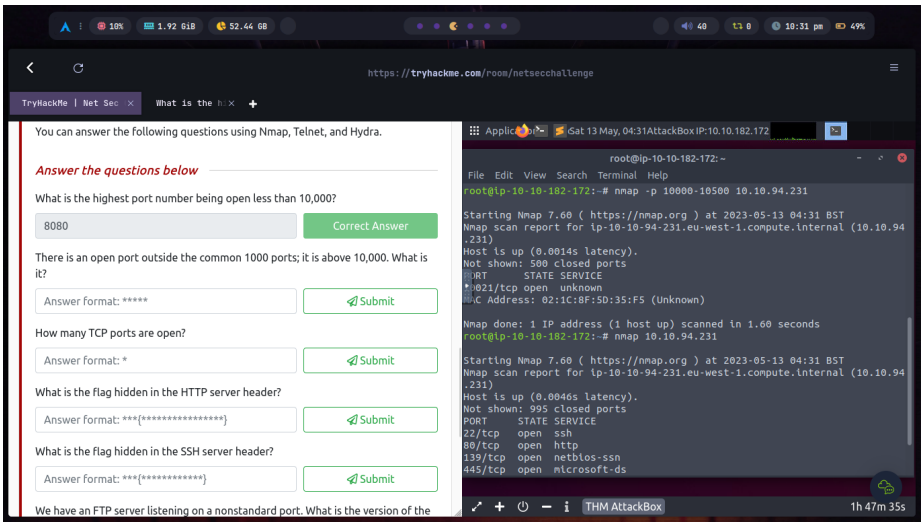
May 14, 2023

1 Reconocimiento y solucion

El primer paso es realizar el escaneo basico con nmap para ver los puertos abiertos menores al 10000, de esta manera:

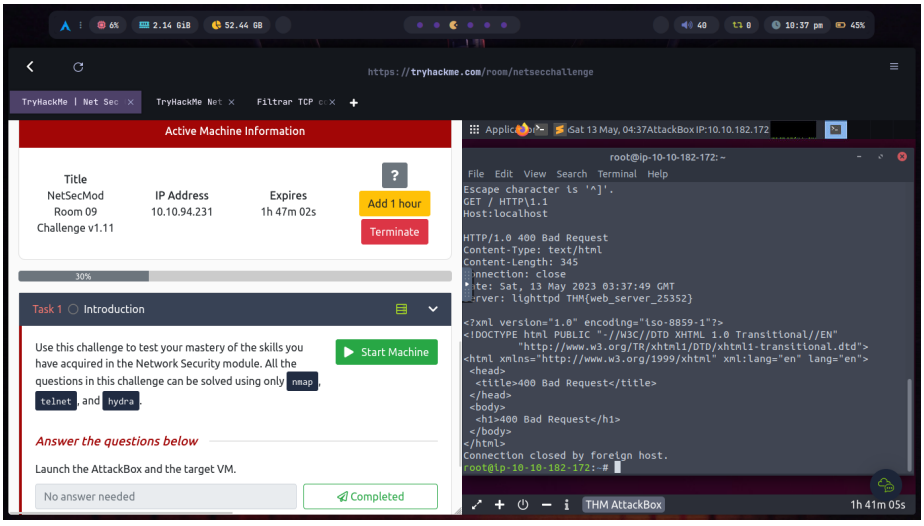


La salida indica que el puerto 8080 esta abierto, por lo que es el puerto comun mas cercano a 10000. Luego se realiza una busqueda con nmap para encontrar el puerto abierto no comun mayor a 10000:



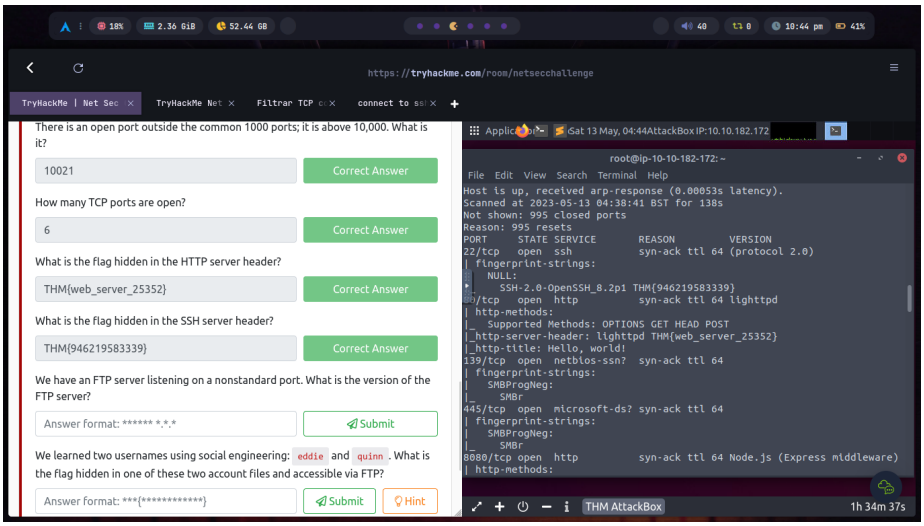
Posteriormente se obtiene el header del servicio HTTP que esta corriendo bajo el puerto 80 con el siguiente comando:

```
nc $ip_maquina 80
```

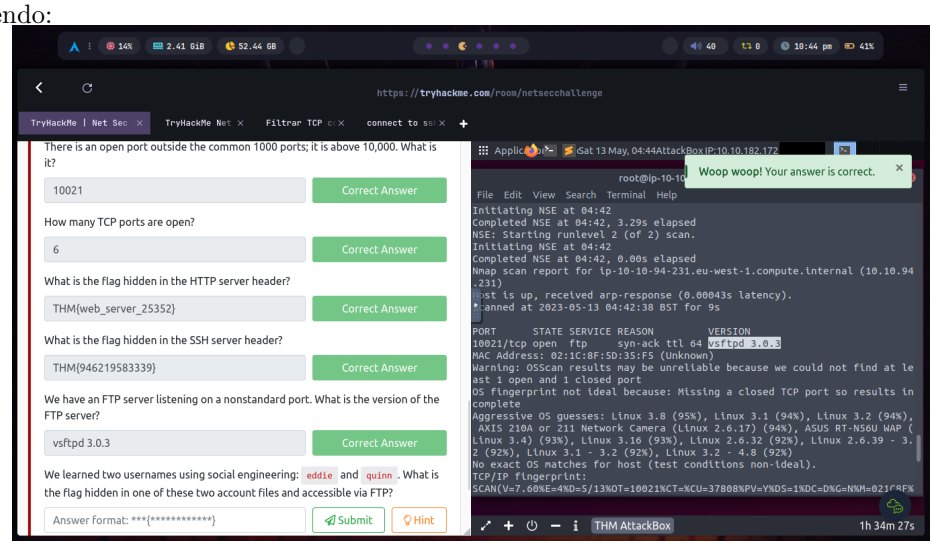


Para obtener el header SSH se decide realizar un escaneo a los puertos abiertos con nmap de la siguiente manera:

```
nmap -A -vv $ip_maquina
```



Con el mismo comando se obtiene la version del servicio fpt que esta corriendo:



2 Explotación

Para comenzar con la explotación de los dos usuarios que realiza un crackeo de sus contraseñas con la herramienta hydra y la wordlist "rockyou":

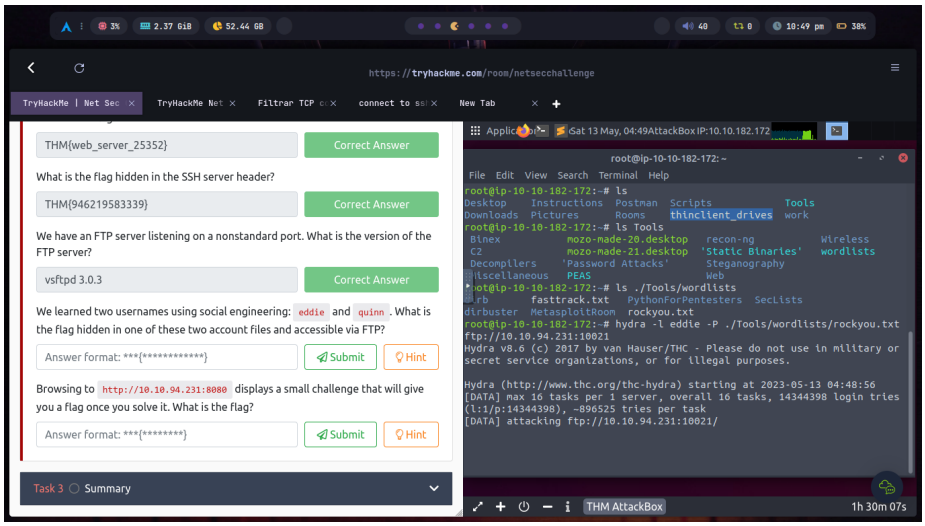
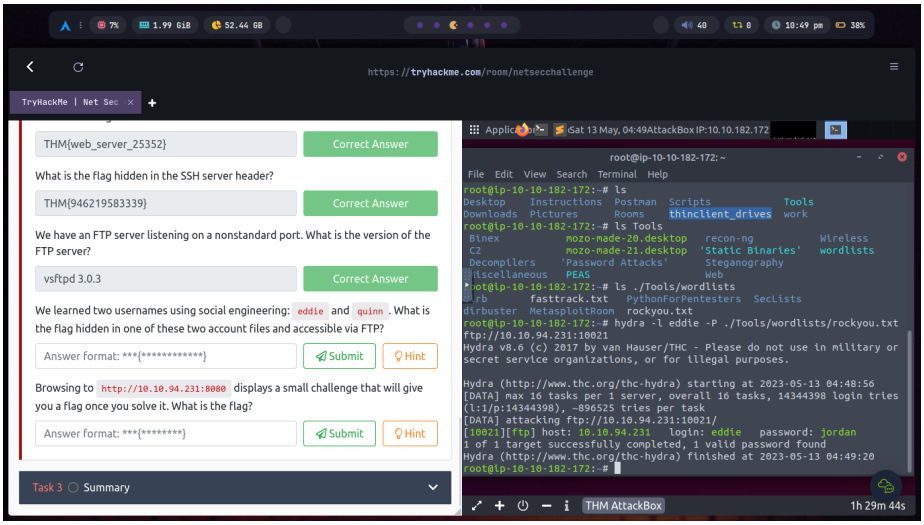
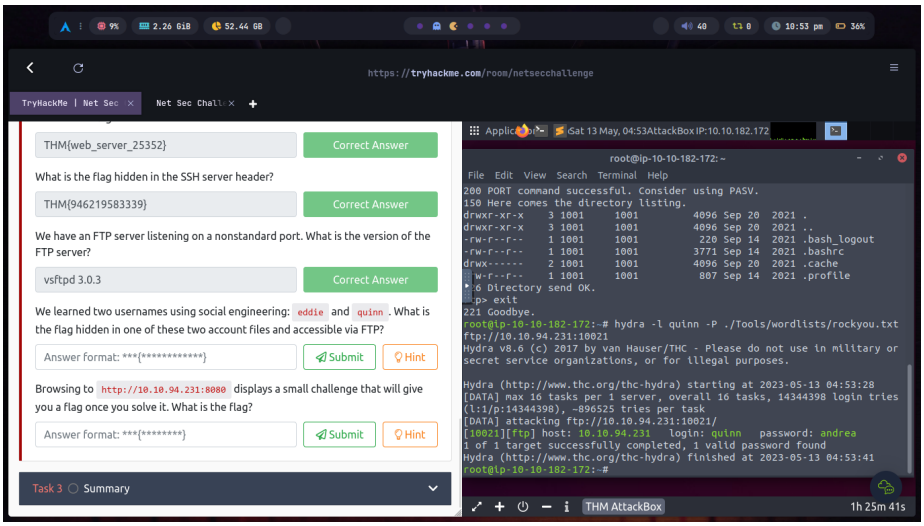
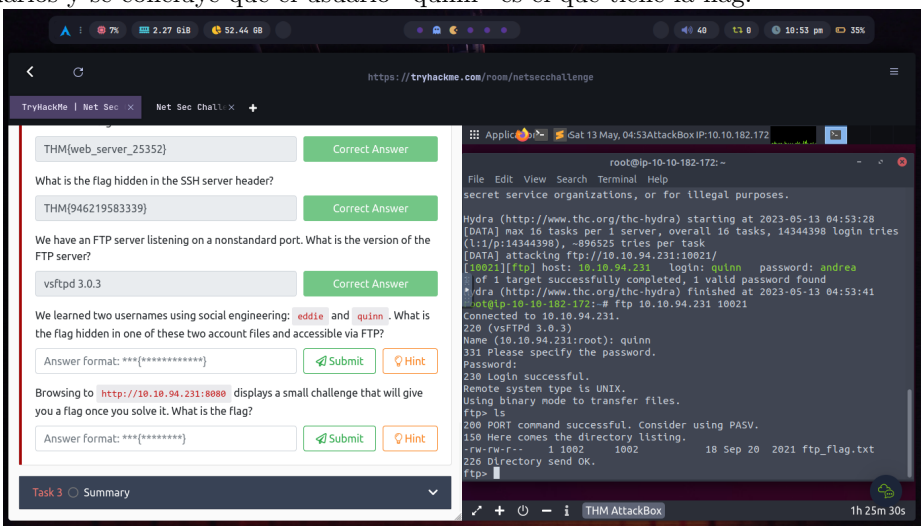


Figure 1: Hydra 1





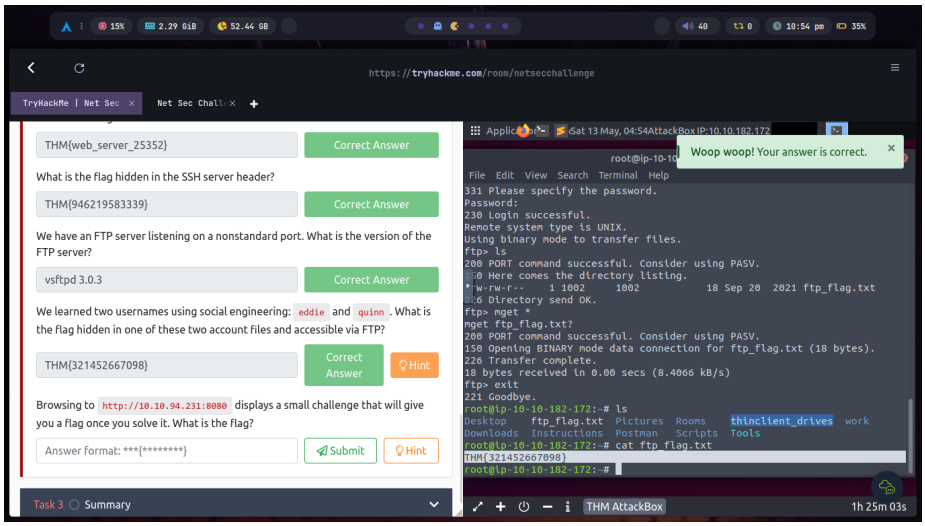
Tras tener las contraseñas se intenta acceder al ftp con cada uno de estos usuarios y se concluye que el usuario "quinn" es el que tiene la flag:



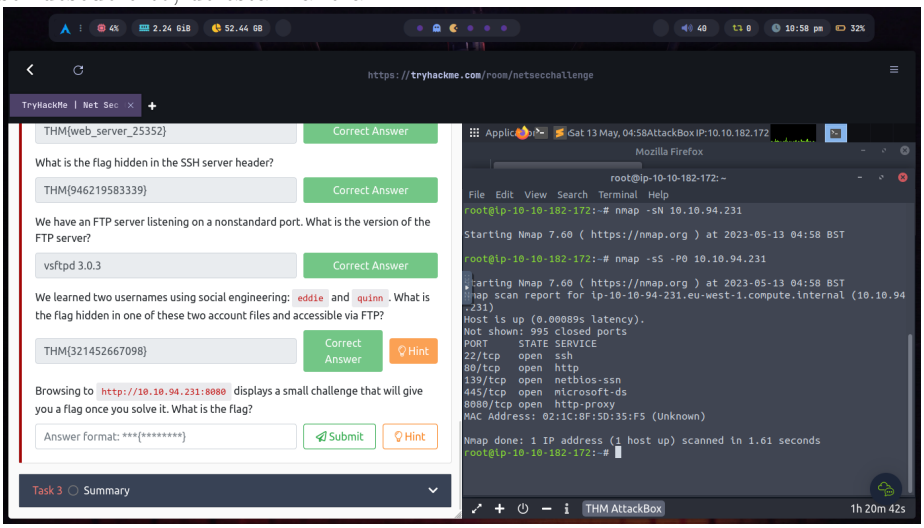
Este archivo se copia a mi maquina local con el comando:

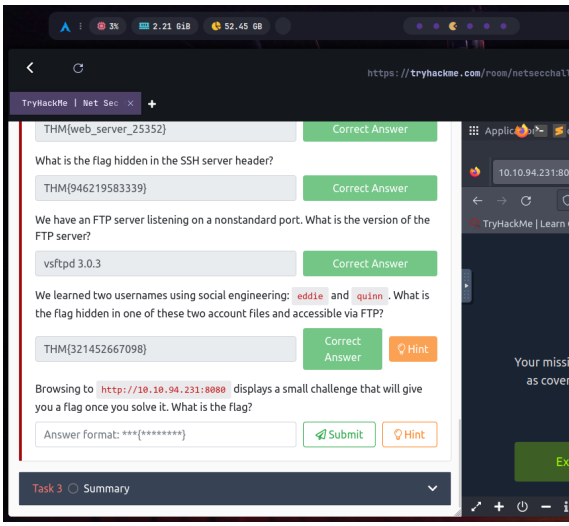
```
mget *
```

Y posteriormente la abro

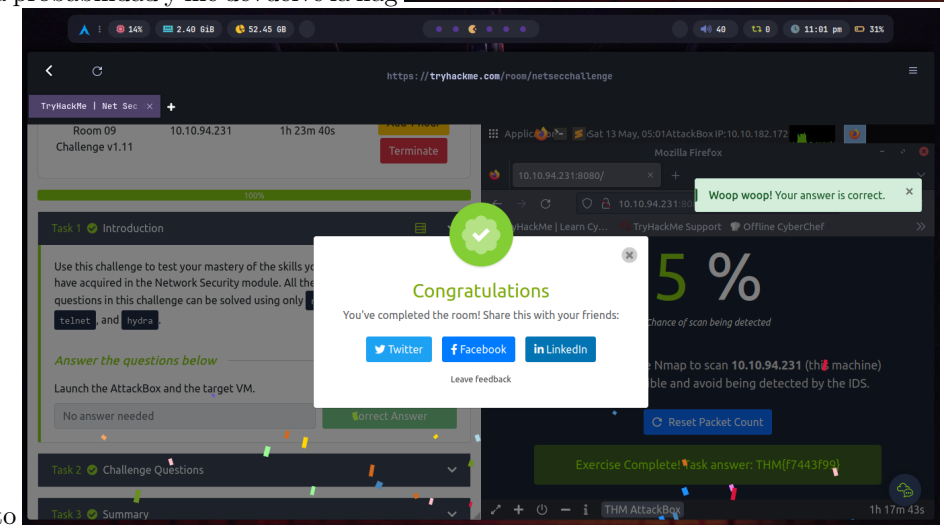


Para el ultimo paso debo realizar un escaneo con nmap con poca probabilidad de ser descubierto, de esta manera





Que me otorga una baja probabilidad y me devuelve la flag



Con esto concluyo el reto