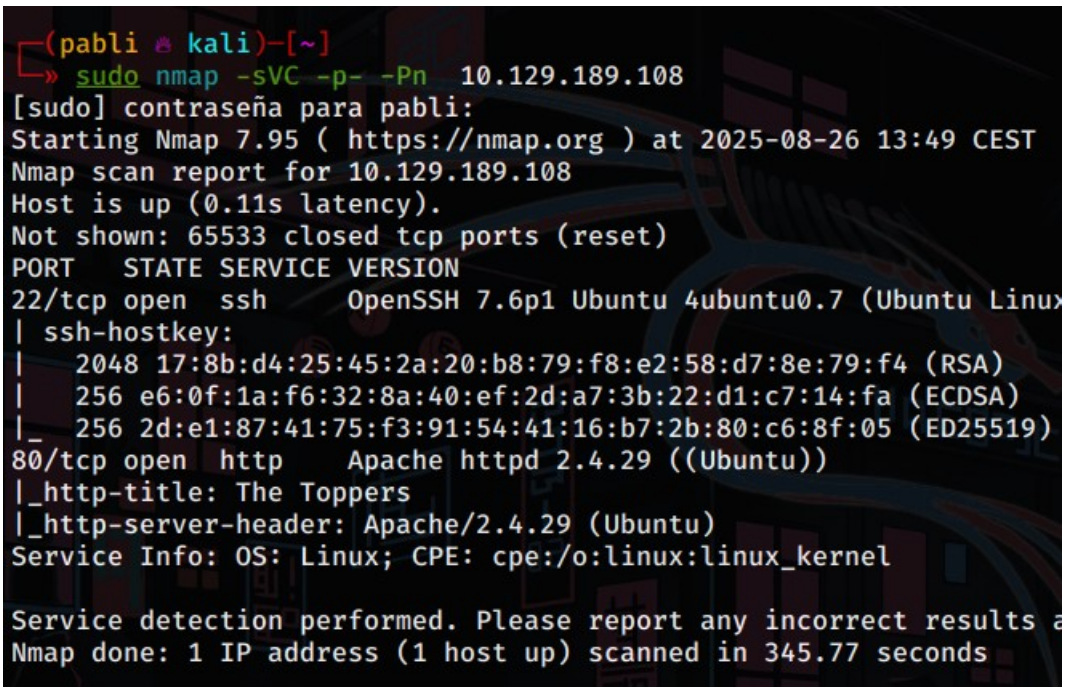
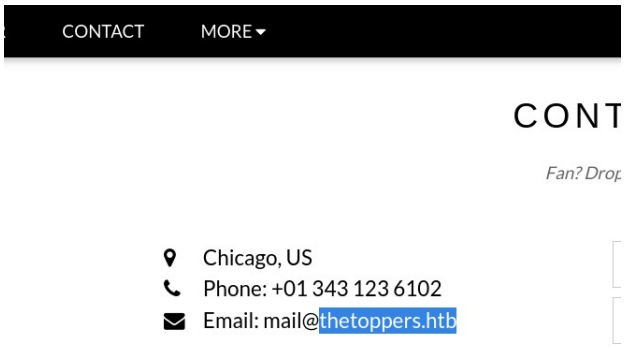
HackTheBox

Máquina: Three
Pablo José Pérez Díez

Escaneo Inicial:

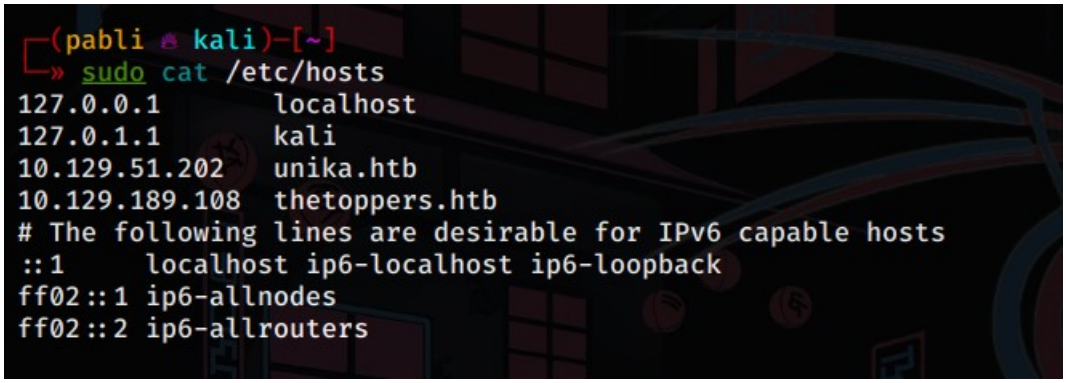


Analizando la web encontramos un dominio:



Los dominios y subdominios pueden ser puntos de entrada clave.

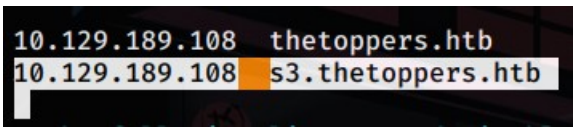
Para poder buscar subdominios con gobuster añadimos al archivo /etc/hosts el dominio que queremos analizar (en este caso es thehoppers.htb):



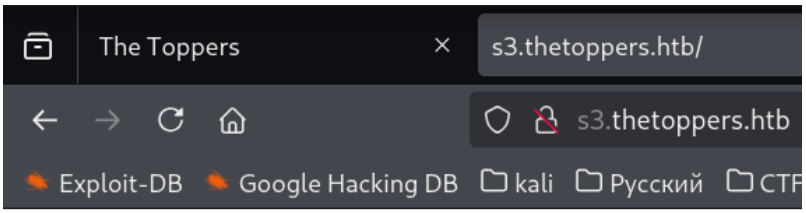
Una vez hecho esto analizamos los subdominios con GoBuster:

Como podemos ver encontramos 2 subdominios

Añadimos a /etc/hosts el nuevo subdominio



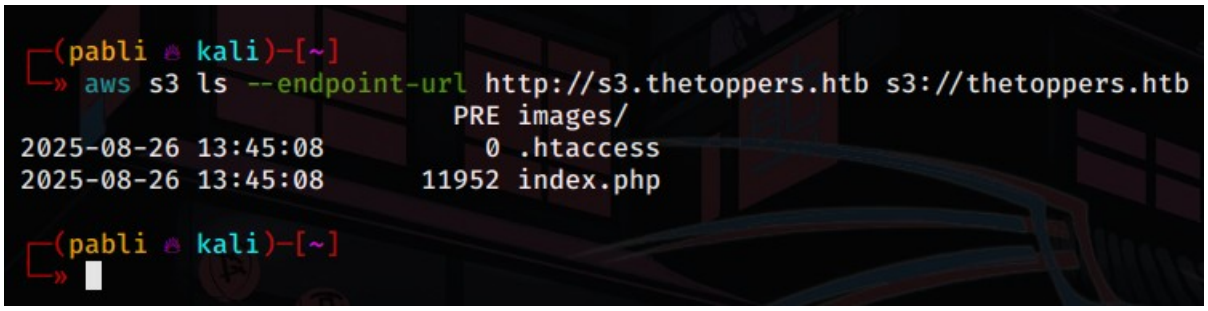
Si lo analizamos en el navegador vemos lo siguiente:



{"status": "running"}

Se esta utilizando Amazon S3.

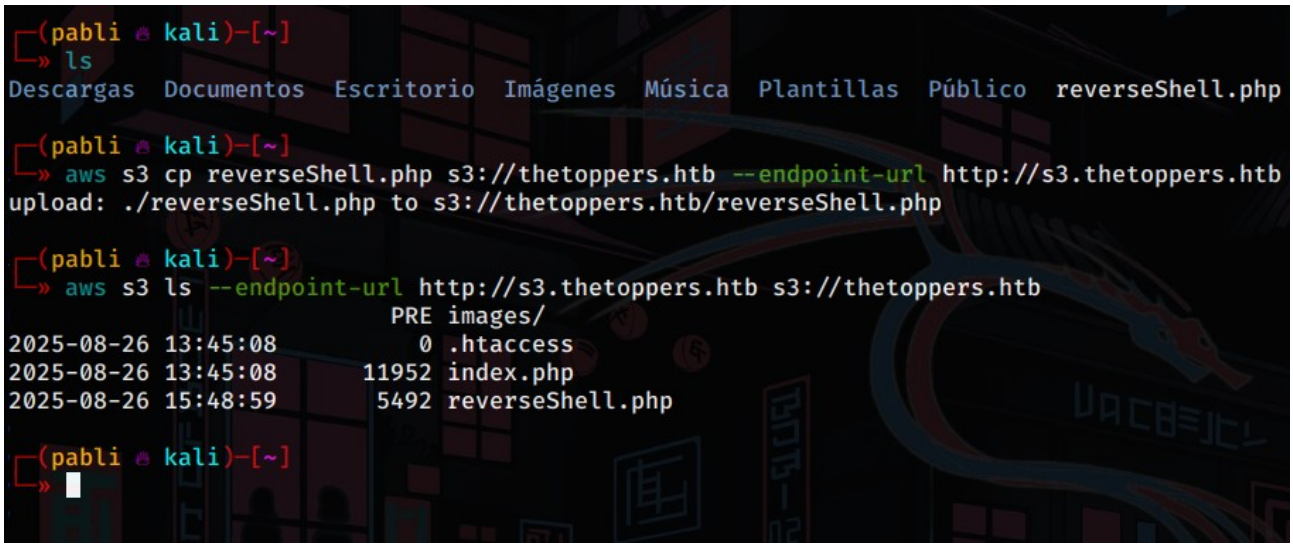
Listamos los Buckets:



Intentaremos subir un archivo y realizar un reverse shell.

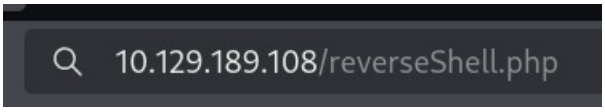
Creamos un archivo reverseShell en php y adaptamos los parametros de Puerto e IP:

subimos el archivo mediante aws:



Escuchamos desde nuestra máquina atacante con netcat en el puerto 8080.

Accedemos desde la url al recurso que acabamos de subir:



observamos que ya tenemos acceso con el netcat:

Una vez dentro encontramos la flag: