# Desplegar maquina

Lo que haremos será desplegar la máquina obsession, tenemos que instalarnos previamente Docker.io y descargarnos la maquina de la web.



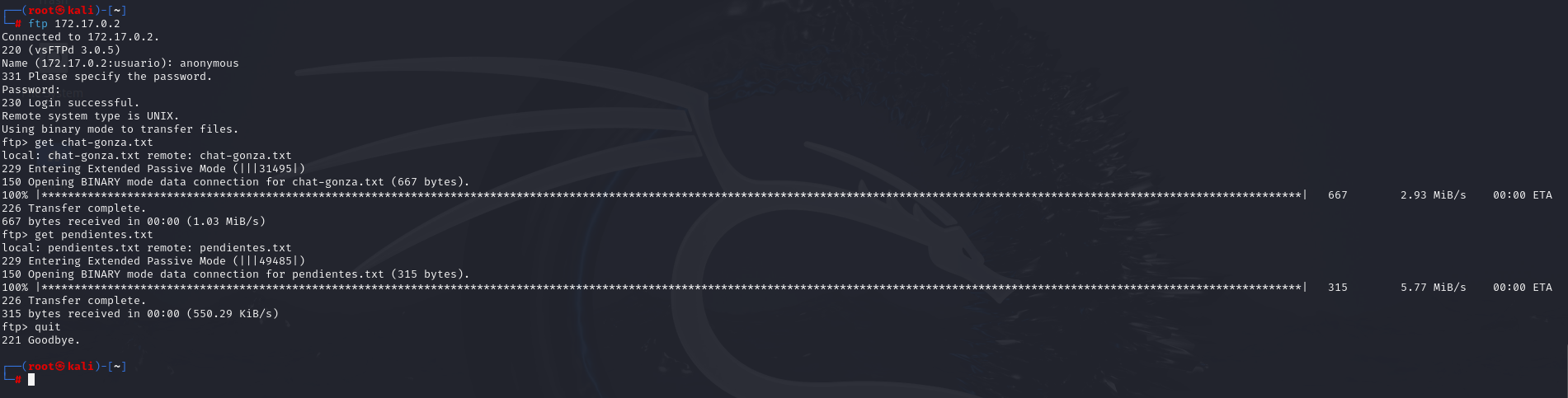
# Búsqueda de puertos

Ahora lo que haremos será ver que servicios y que puertos hay abiertos y que versión tiene

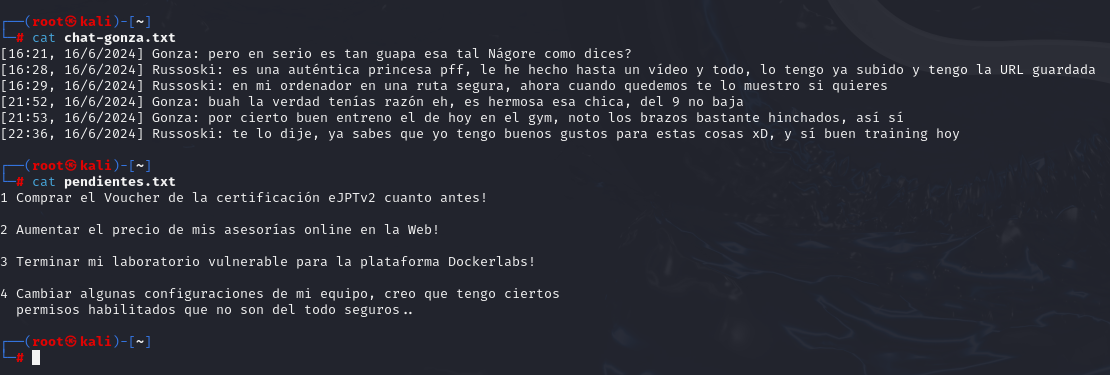


# Conexión mediante ftp

Vemos que hay un puerto ftp, vamos a probar si podemos conectarnos mediante usuario anónimo y descargarnos los archivos que nmap nos ha proporcionado

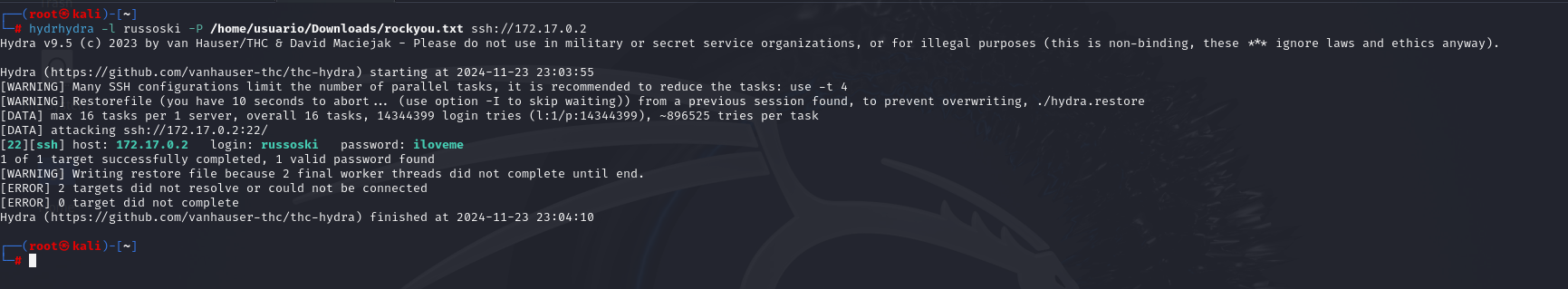


Una vez que hemos descargado los archivos, vemos que contienen los archivos



# Ataque contraseña fuerza bruta

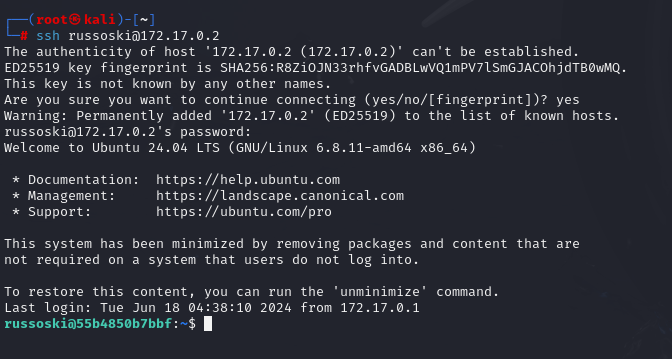
Vemos que hay un usuario llamado russoski, vamos a probar con hydra un ataque de fuerza bruta mediante el archivo rockyou.txt que es un fichero de contraseñas.



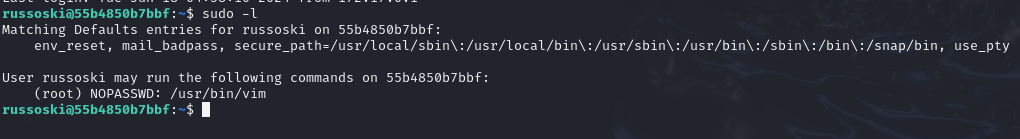
Vemos que hay un usuario llamado russoski y su contraseña es iloveme

# Conexión mediante ssh

Como vimos en nmap que tiene un servicio ssh y un ftp, vamos a conectarnos mediante el usuario russoski y la contraseña iloveme.

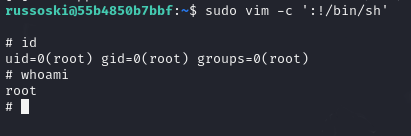


Una vez que nos hemos conectado miraremos como podemos escalar privilegios



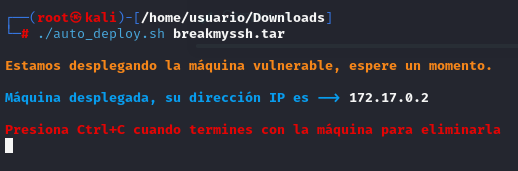
# Escalada de privilegios

Mediante el comando vim cambiaremos a sudo ya que tiene una Shell distinta a la de bash



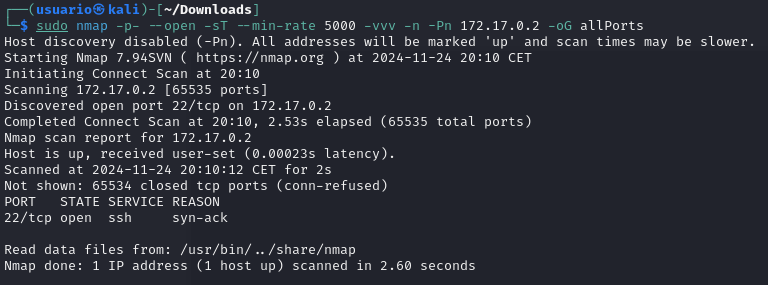
# Despliegue de maquina

Vamos a usar la maquina break my ssh, desplegaremos la maquina, importante hacer esto con root, si no nos daría fallo



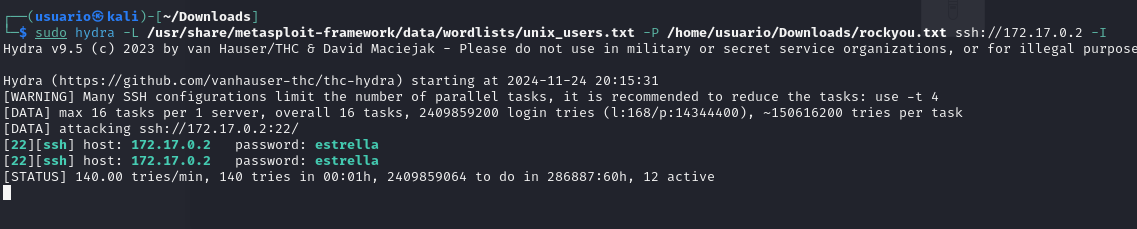
# Búsqueda de puertos

Mediante el comando nmap haremos un escaneo general de los puertos habilitados

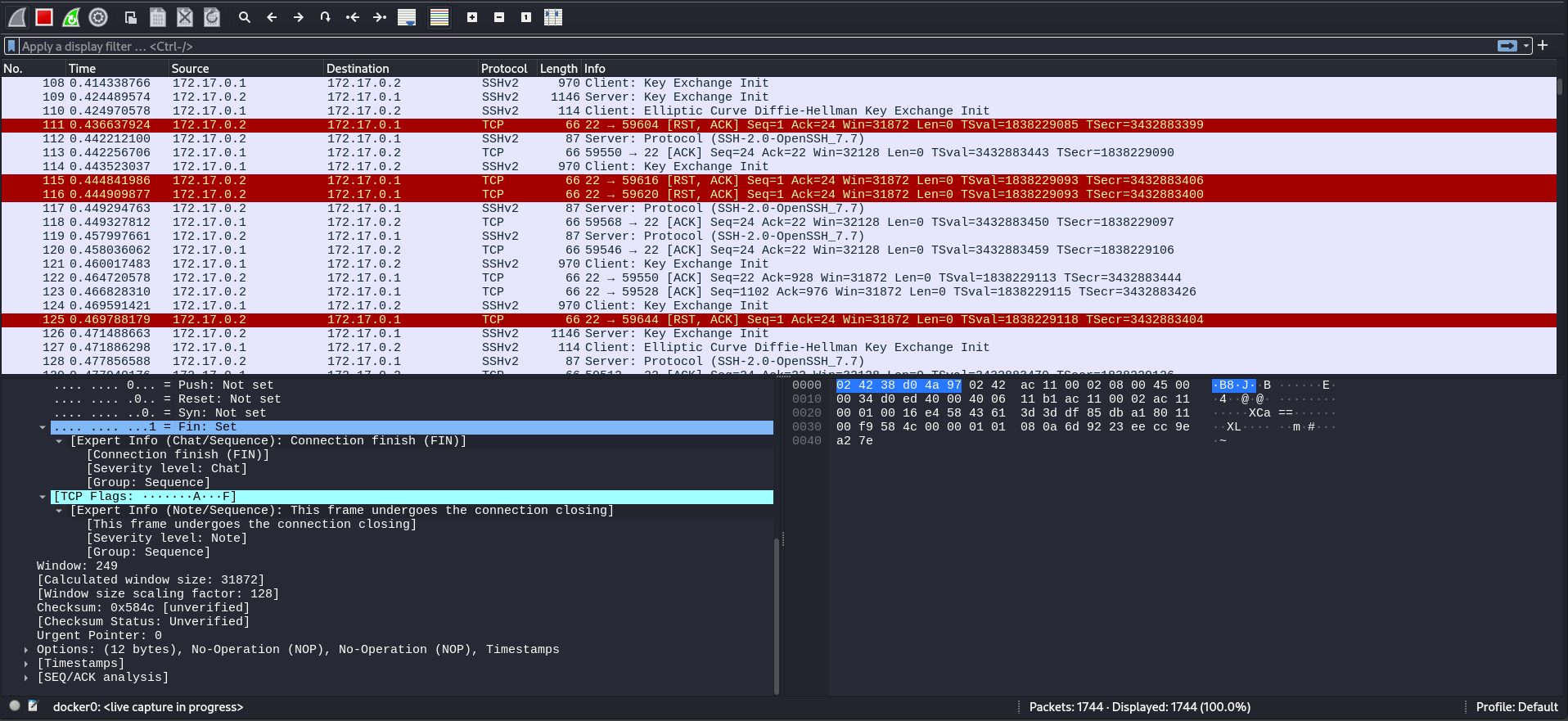


# Conexión ssh

Vemos que hay un puerto ssh habilitado, usaremos el comando hydra y la base de datos de contraseñas de rockyou.txt para romper la contraseña y poder conectarnos

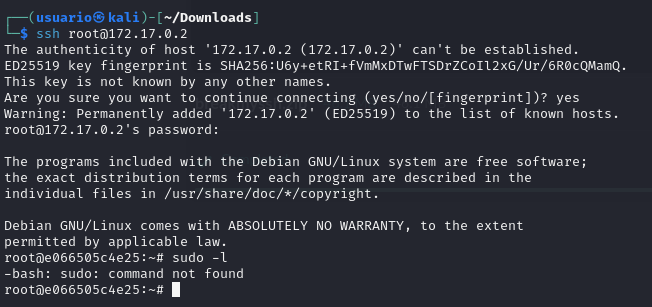


Vamos a usar wireshark mientras hacemos el ataque de fuerza bruta de ssh



# Conexión

Una vez que tenemos el usuario y contraseña, iniciaremos sesión con ssh



Aquí no hace falta escalada de privilegios, ya que hemos entrado mediante el usuario root