PRÁCTICA 5: ROGUE ONE.

David Tardío Montoya, 2 GM B, Servicios en Red.

Recordatorio: Mirar primero el vídeo adjuntado con este documento, a modo de extra sin importancia.

Índice

[1: Preparación. 1](#_Toc90404845)

[2: Pasos del plan. 1](#_Toc90404846)

[2.1: Lograr una conexión SSH en Bastión y obtener el intérprete. 1](#_Toc90404847)

[2.2: Investigar la red imperial en busca de servicios explotables. 2](#_Toc90404848)

[Parte 3: Exploración, recopilación de datos y obtención de los planos. 4](#_Toc90404849)

[Parte 4: Entrega de los planos a la Alianza Rebelde. 7](#_Toc90404850)

# 1: Preparación.

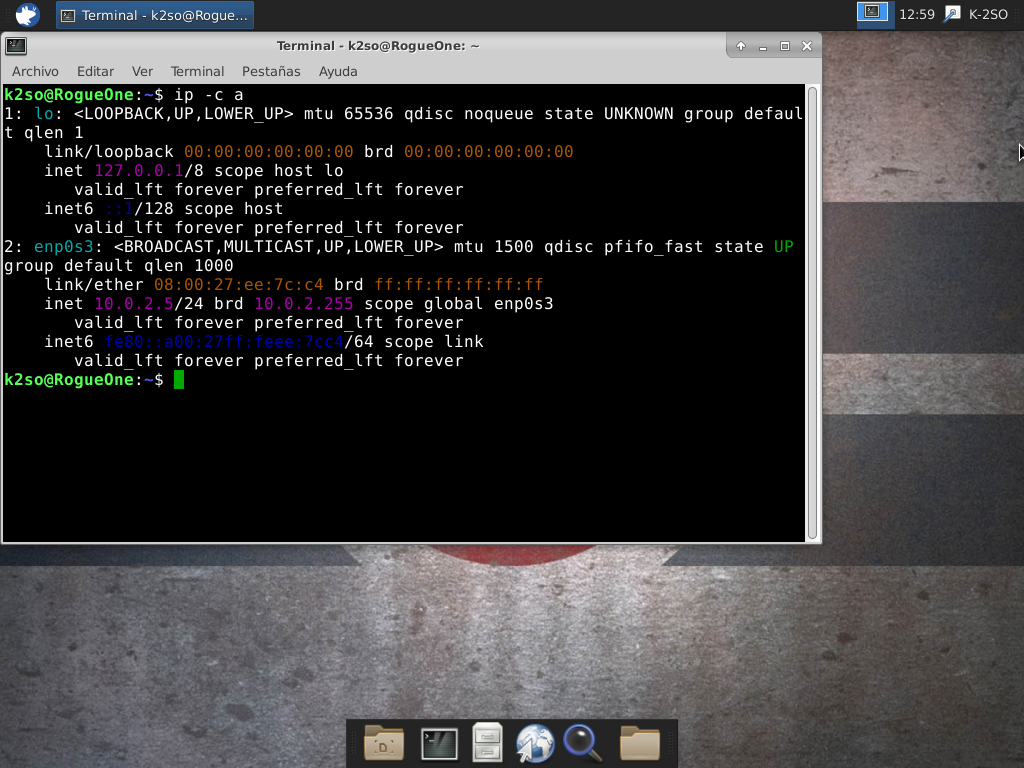
Es necesario descargar las máquinas virtuales en la máquina real, además de crear una red NAT, la cual unirá ROGUE ONE y BASTIÓN IMPERIAL. Su nombre será NAT\_A (aunque no hay más redes NAT). No hay mucha más preparación necesaria.

# 2: Pasos del plan.

## 2.1: Lograr una conexión SSH en Bastión y obtener el intérprete.

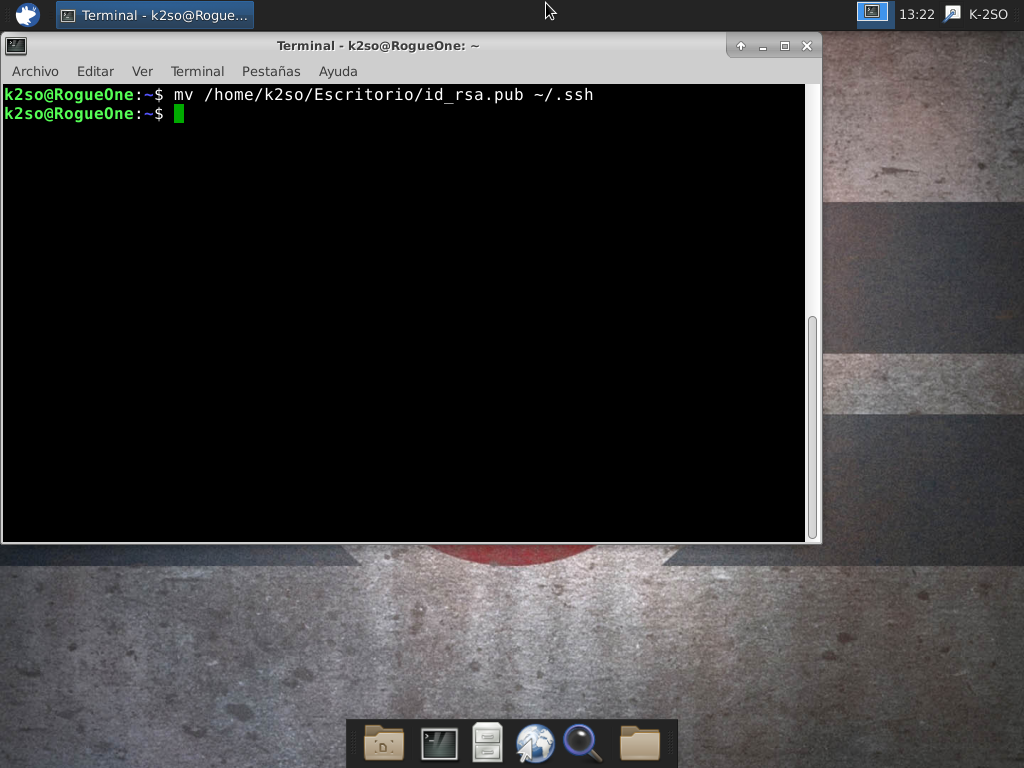
Para ello, tendremos que entrar en la máquina de ROGUE ONE, para la cual tenemos las claves de acceso de K2SO, por lo que entraremos usando de usuario y contraseña **k2so / k2so**.

Para conseguir realizar una conexión SSH con BASTIÓN, necesitaremos saber su IP, además de un usuario y una contraseña. Sabemos que su IP es estática, y que es la siguiente a la nuestra; por lo que podemos averiguarla mirando nuestra IP (la de ROGUE ONE) y sumando 1. Se puede hacer con sencillez entrando en una terminal y escribiendo el comando ***Ip –c a***.



IP averiguada.

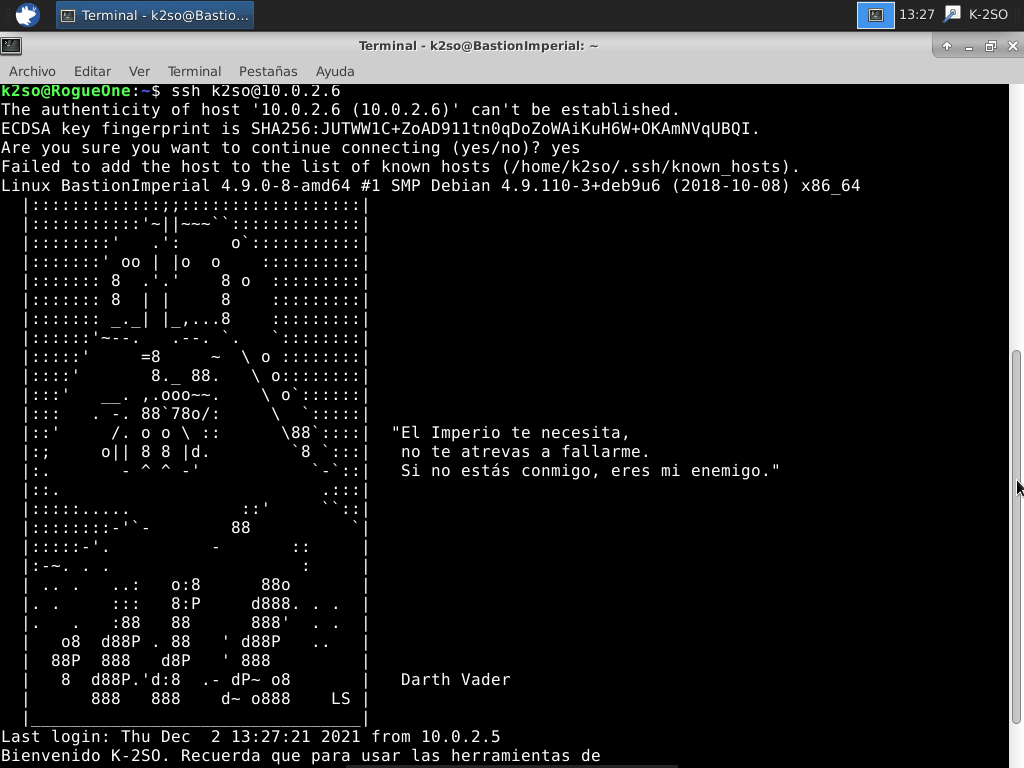
Por lo tanto, se puede deducir que su IP será **10.0.2.6**. Ahora, sólo necesitamos el usuario y la contraseña. Para ello, hay que usar las antiguas credenciales de K2SO. Sabemos que el usuario es k2so, pero necesitamos usar las claves ofrecidas para poder acceder a BASTIÓN. Pero las claves no están donde BASTIÓN espera que estén, por lo que deberemos mover manualmente las claves al directorio en el que deberían estar: **~/.ssh**. Para ello, primero vamos a descomprimir el paquete de forma gráfica. Tras ello, abriremos otro terminal. Lo primero, es averiguar dónde está la clave actualmente. El paquete estaba directamente en el escritorio, al igual que las claves, por lo que su ubicación es **/home/k2so/Escritorio**. Lo moveremos de ahí a la carpeta destino usando el comando ***mv /home/k2so/Escritorio/*id\_rsa.pub** **~/.ssh**.



Clave pública movida

Hay que realizar lo mismo con la clave privada.

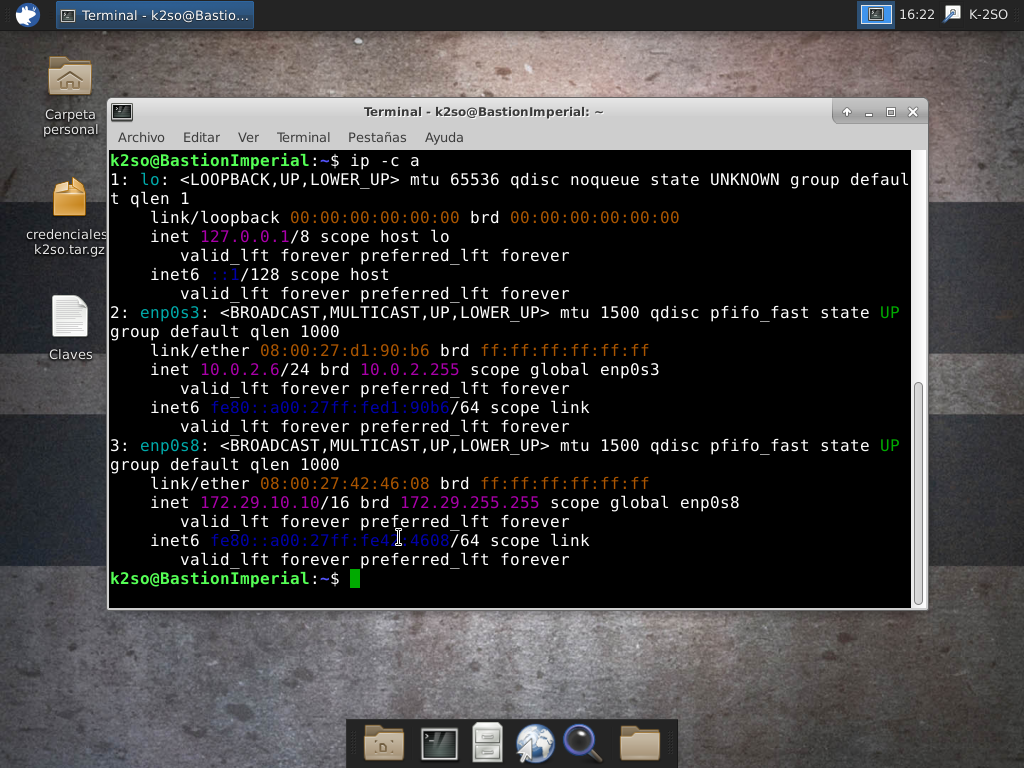
A continuación, nos conectaremos por SSH al BASTIÓN, usando como usuario a **k2so** y de IP la **10.0.2.6.** En el terminal, escribiremos el comando **ssh** [**k2so@10.0.2.6**](mailto:k2so@10.0.2.6).



Sesión en BASTIÓN iniciada

## 2.2: Investigar la red imperial en busca de servicios explotables.

A continuación, deberemos ver cuál es la IP de la tarjeta de red de BASTIÓN que está conectada a la red imperial, haciendo desde el túnel en BASTIÓN un ***ip -c a***. Miraremos la IP de enp0s8.



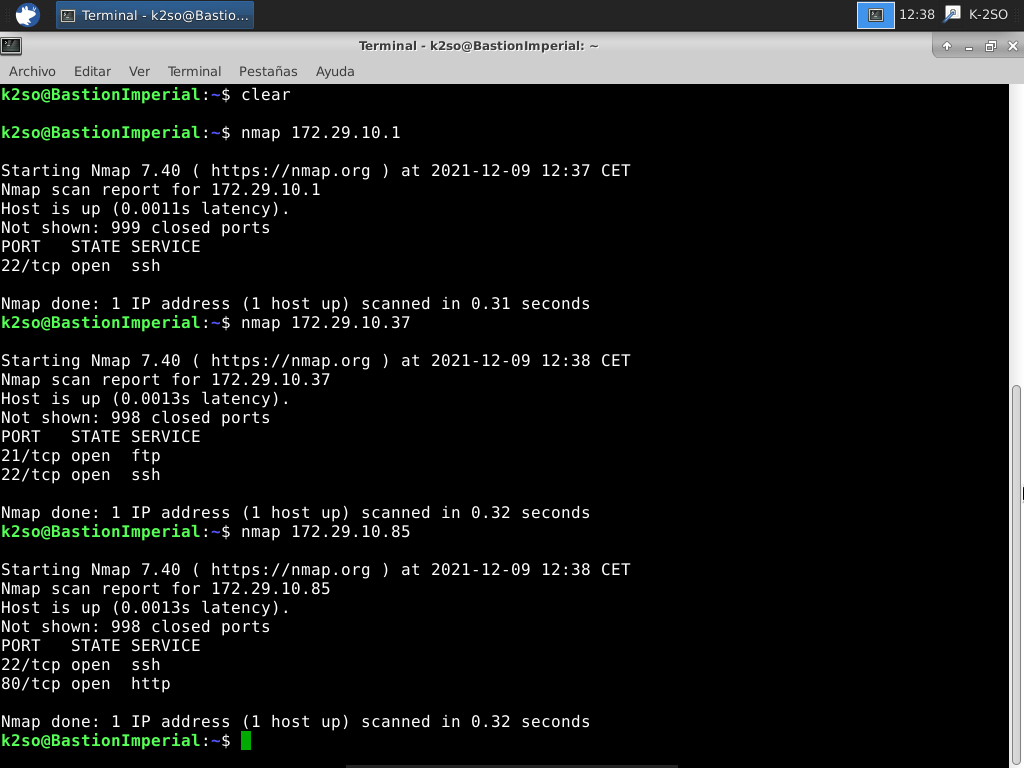
IPs de BASTIÓN

Ahora sabemos que la IP de esa segunda tarjeta de red es la 172.29.10.10 continuación, utilizaremos la herramienta ***netdiscover.*** Esta herramienta nos permitirá ver qué direcciones IPs hay conectadas a la red imperial. Para ello, hay que usar el comando ***sudo netdiscover -i enp0s8 172.29.10.0/24***. Una vez termine el proceso, aparecerán las IPs conectadas a la red.



IPs conectadas a la red

Ahora, tenemos que averiguar qué puertos podemos explotar (metafóricamente) para nuestro beneficio. Para ello, podemos usar la herramienta ***nmap***. Si ponemos el comando seguido de cada una de las IP que hemos descubierto anteriormente, podremos ver qué puertos están abiertos. Aquí el resultado.



Puertos posibles para consumir.

Con esto, sabemos que en la 172.29.10.37 hay un servicio activo de FTP, y que en el 172.29.10.85 hay una página web por http. Ahora, podremos escoger entre si ir directamente al servicio FTP o en si ir al http.

# Parte 3: Exploración, recopilación de datos y obtención de los planos.

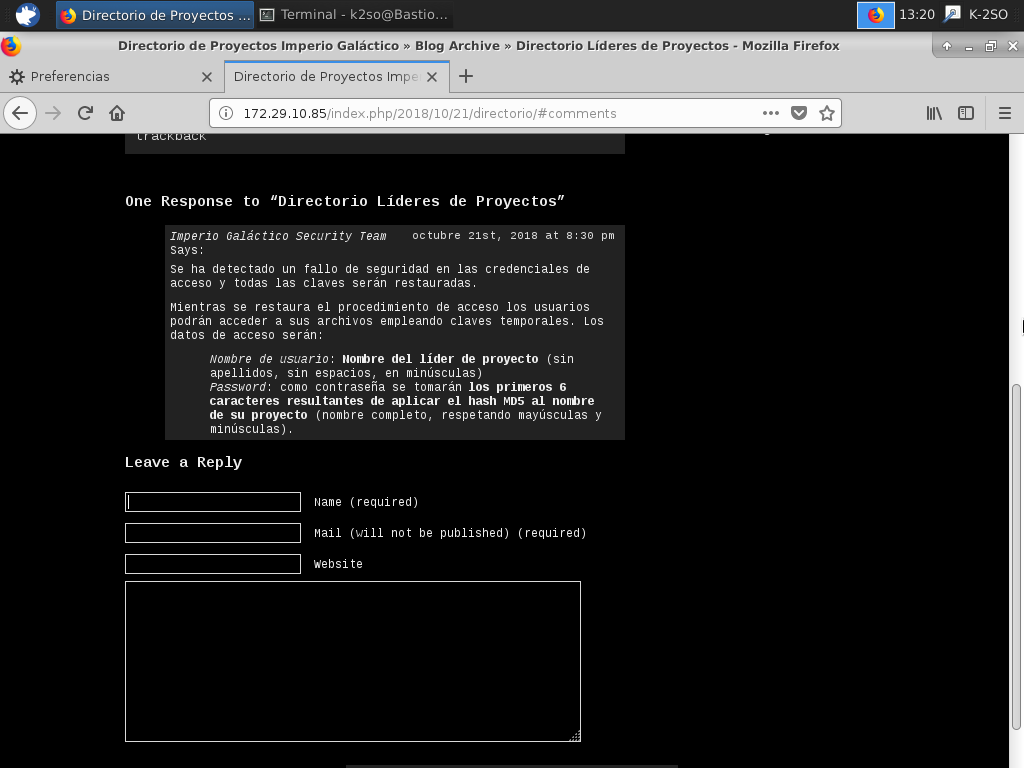
En este caso, iremos primero a utilizar el servicio http, ya que puede contener información relevante para nuestra misión.

Utilizaremos el servicio escribiendo en un navegador la IP del servidor (siempre y cuando sigamos con el túnel dinámico SSH activo). Es decir, hay que introducir en la barra de búsqueda la IP 172.29.10.85.



Bingo

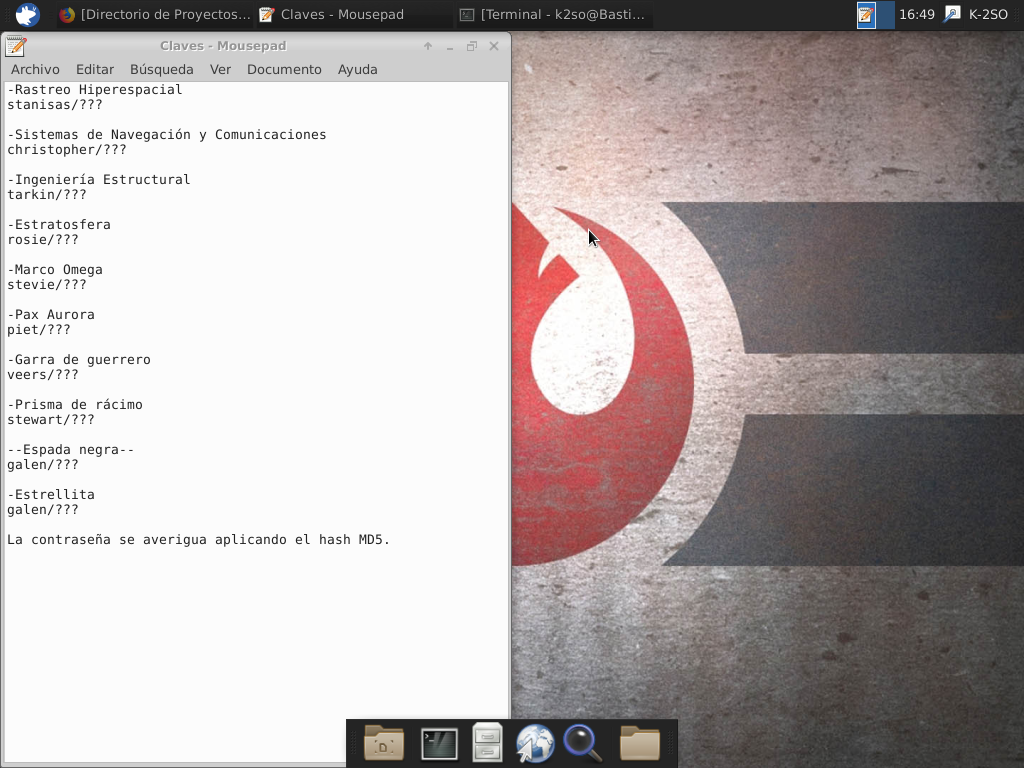
Hemos consumido el servicio HTTP. Ahora, en la página, aparecen una lista de nombres y de proyectos, además de un comentario al que podremos acceder seleccionando la parte de los comentarios con el ratón.



Comentario

Esto quiere decir que las claves de acceso de todos los usuarios son, como usuario, el nombre del líder del proyecto, y como contraseña los primeros caracteres al aplicar el hash al nombre de su proyecto. Las contraseñas se pueden calcular de forma sencilla usando el comando ***md5sum*** y el nombre del proyecto.

En mi caso, haré un .txt en el que apuntaré todos los usuarios en función de lo mencionado en ese comentario.



Usuarios

Nota: Espada negra es, en realidad, Galen Erso. Esto se averigua con información de la historia.

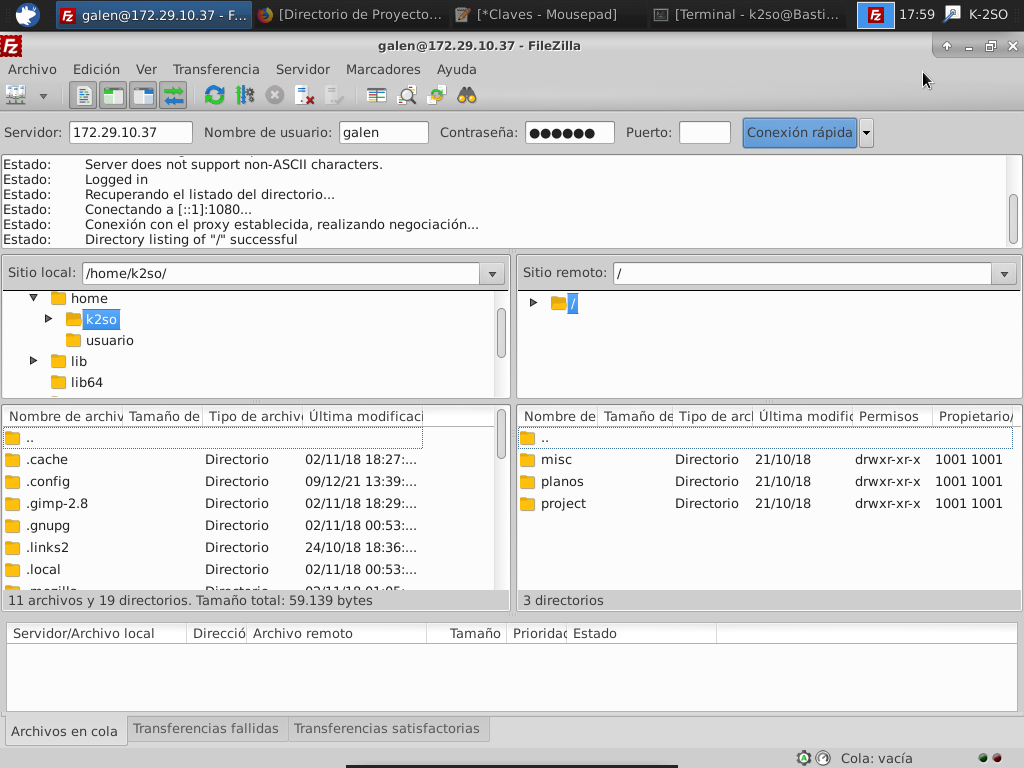
Ahora, lo que resta, sería crear un directorio con archivos en los que introduzca el nombre del proyecto, y averiguar su hash, usando el comando ***echo -n (proyecto) | md5sum.*** Actualizaré la lista con las claves correspondientes.



Listado realizado.

Una vez tengamos todas las claves, deberemos ir al servicio FTP del servidor 172.29.10.37. Para ello, instalaremos de forma gráfica la herramienta ***Filezilla*** mientras sigamos conectados a BASTIÓN por SSH. Una vez instalado y extraído, lo utilizaremos. Debemos ir a la pestaña edición, opciones, y proxy genérico. Ahí cambiaremos el puerto del proxy al mismo que hemos utilizado para abrir el túnel dinámico.

En el apartado de servidor, pondremos la IP. Ya que Galen tiene un vídeo preparado para nosotros, utilizaremos de usuario “galen” (que figura en el listado de la página web), y de contraseña su hash de “Estrellita” que hemos calculado con anterioridad.

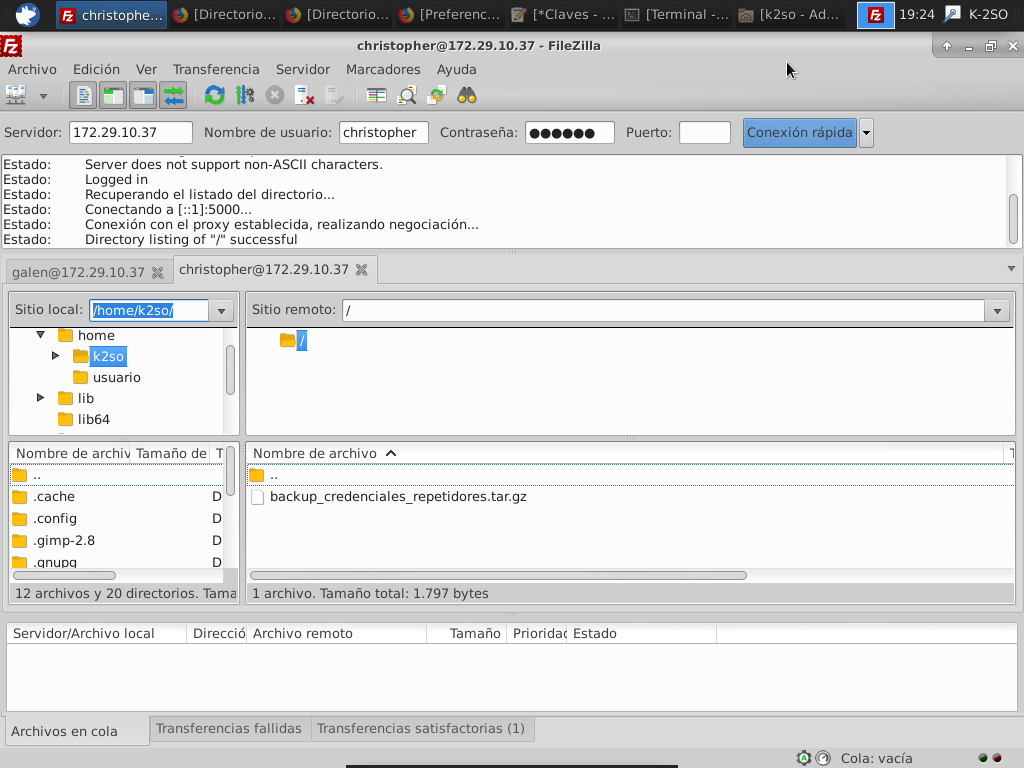


Conexión exitosa

Ahora, debemos descargar los planos a la máquina BASTIÓN. Eso se realizará de forma gráfica.

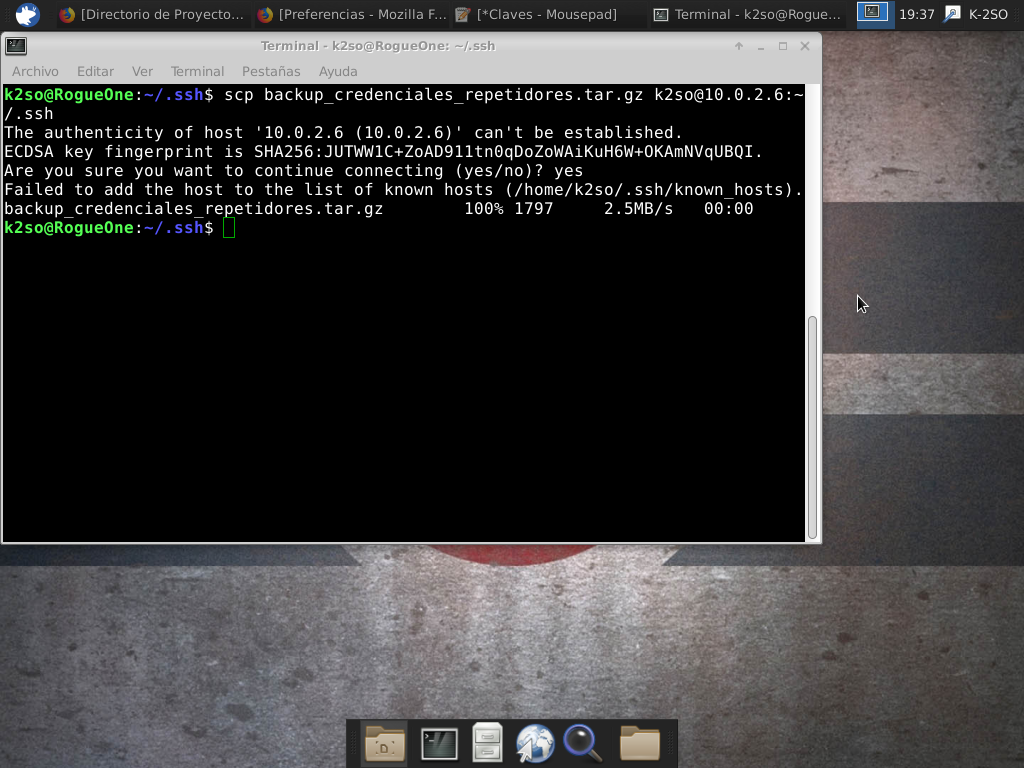
# Parte 4: Entrega de los planos a la Alianza Rebelde.

Para acceder a la antena, necesitaremos las claves necesarias de Christopher para poder conectarnos por SSH. Para ello, necesitaremos ir al FTP y probar las claves de otro usuario. Usaremos las claves de Christopher.



Claves disponibles

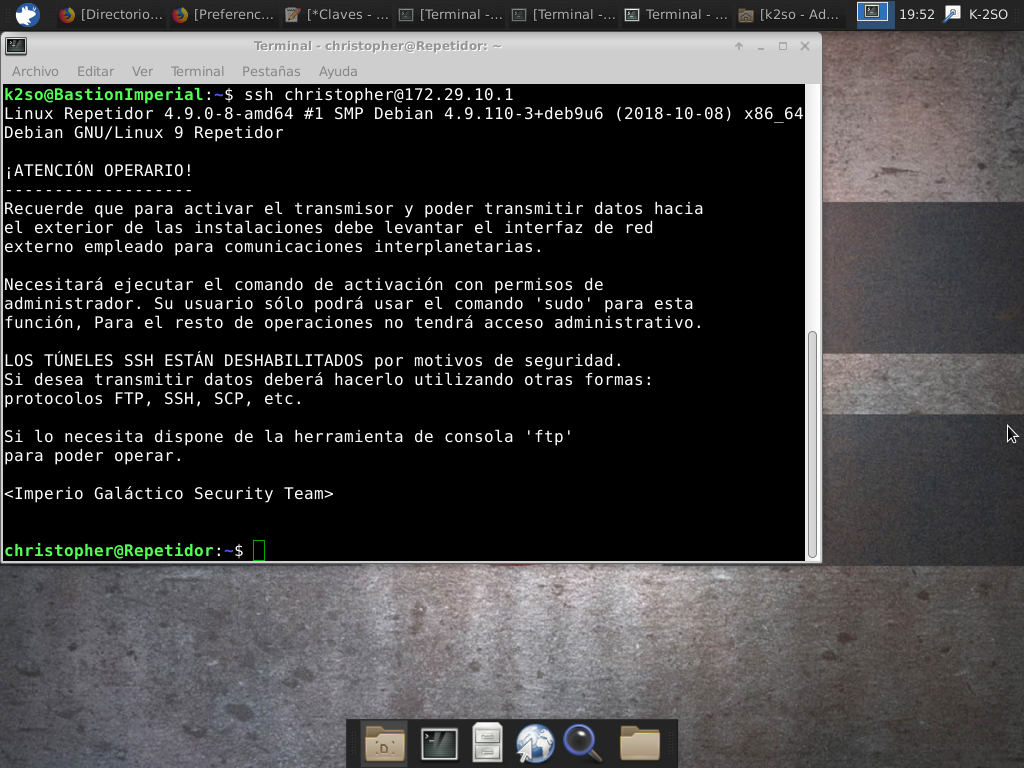
Tras ello, las claves deben estar dónde se esperan que estén. Es decir, en ***~/.ssh***. DEBEN ESTAR EN LA MÁQUINA BASTIÓN. Esto se realizará usando el comando ***scp backup\_credenciales\_repetidores.tar.gz*** [***k2so@10.0.2.6:~/.ssh***](mailto:k2so@10.0.2.6:~/.ssh), que además de transmitir el archivo a BASTIÓN, lo dejará en el directorio esperado.



Credenciales movidas con éxito

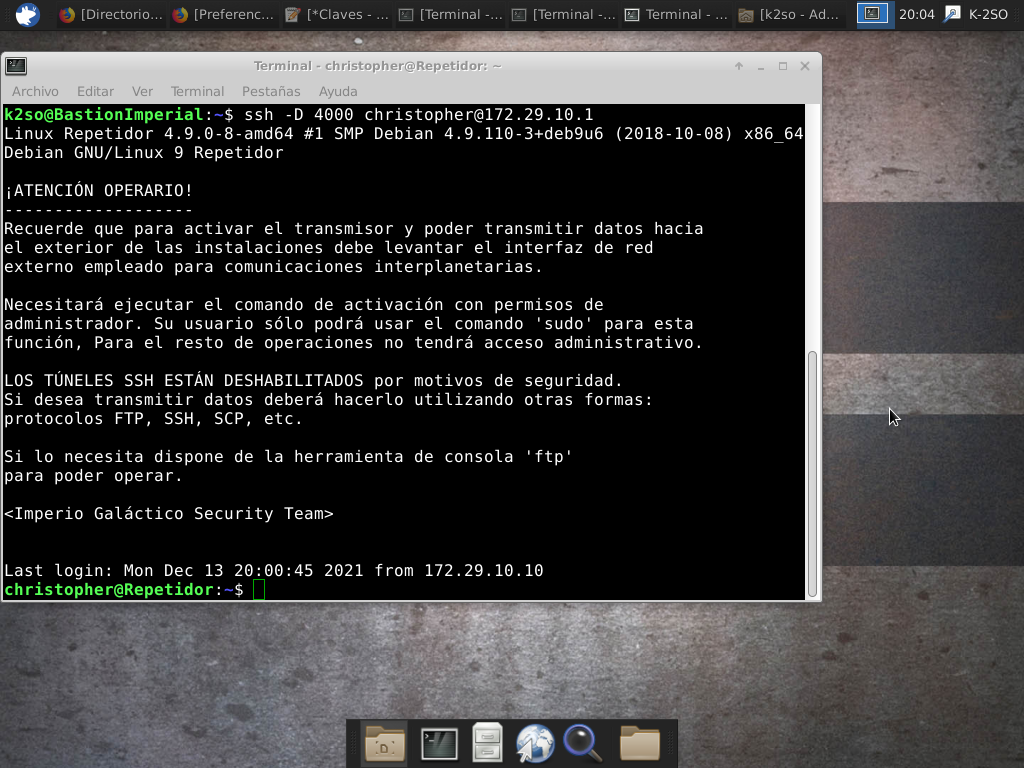
Una vez desde BASTIÓN, estemos en el directorio ~/.ssh, deberemos desempaquetar el par de claves usando el comando ***tar -xf (par de claves)***. Una vez hecho, se desempaquetarán en ***~/.ssh/.ssh***, por lo que moviendo el par de claves al directorio padre será suficiente.

Ahora, desde ROGUE ONE crearemos otro túnel SSH local hacia la IP del repetidor para poder ver qué servicios tiene Profundity. Por lo que habrá que usar el comando ***ssh*** [***christopher@172.29.10.1***](mailto:christopher@172.29.10.1)***.***

******

Conexión establecida

De esto, podemos averiguar que debemos activar algunos interfaces de red, y que los túneles no servirán si intentamos utilizar el repetidor a modo de “bastión”. Saldremos de esa sesión, y haremos un túnel dinámico, usando el comando ***ssh -D 4000 christopher@172.29.10.1***



Túnel realizado

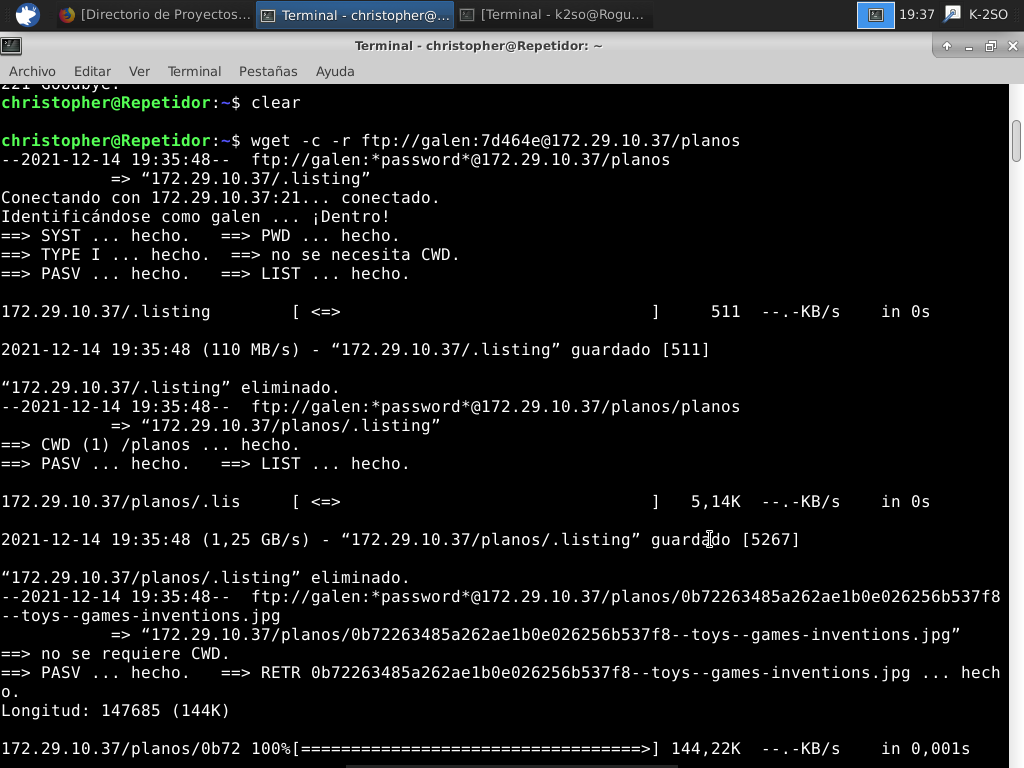
Estamos cerca de finalizar. Ahora, deberemos abrir las interfaces de red usando el comando ***sudo ifup (interfaz)***. Podemos ayudarnos de ***ip –c a*** para hacerlo. Tras ello, necesitaremos averiguar la IP de Profundity.

Por fortuna, podemos hacer una llamada espacial a Profundity para que nos comuniquen su IP a través de un holograma, y muestre un holograma de la pantalla de la terminal de Profundity.



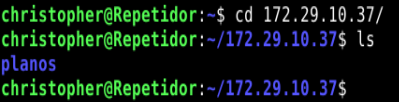
Holograma con la IP

Ahora, aunque tenemos los planos en Rogue One, compartirlos por SCP o similares podría ser demasiado arriesgado y complicado, por lo que desde un túnel dinámico en el que estemos conectados en REPETIDOR, usaremos el servicio FTP del servidor FTP con las claves de Galen para volver a descargar los planos. Esto se hará en una terminal, usando el comando ***wget -c -r*** [***ftp://galen:7d464e@172.29.10.37/planos***](ftp://galen:7d464e@172.29.10.37/planos). Esto permitirá la descarga de los planos.



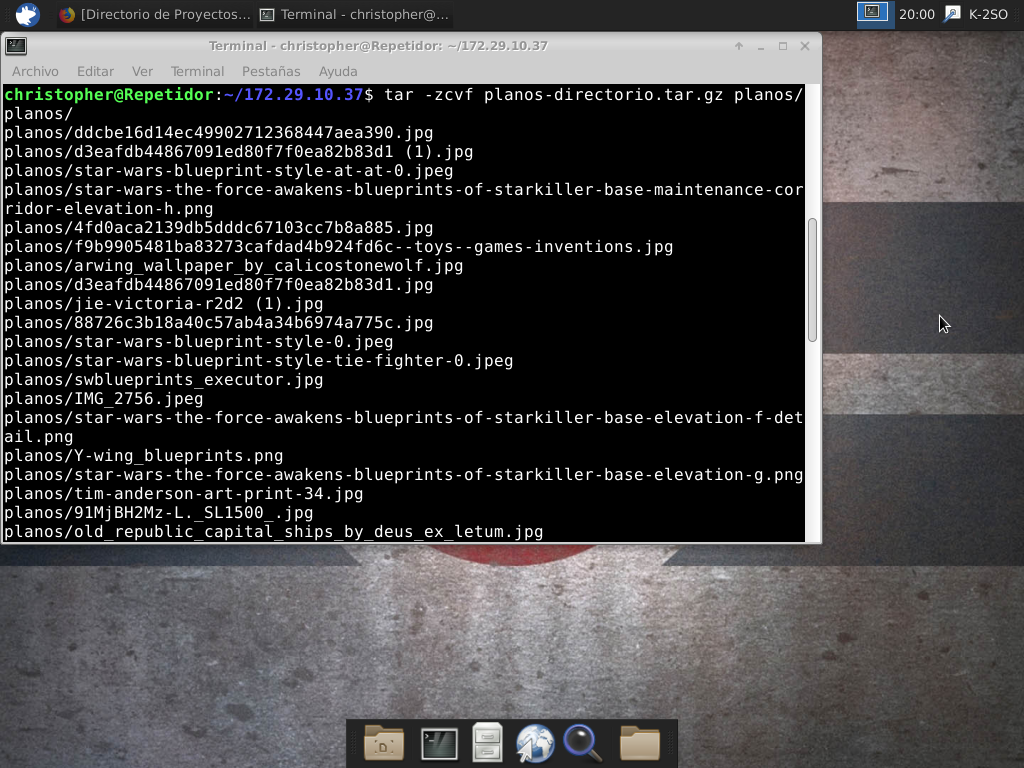
Planos descargados

Ahora, todavía en el REPETIDOR, deberemos ir a un directorio creado con la misma IP del servidor, y dentro estará la carpeta de planos.



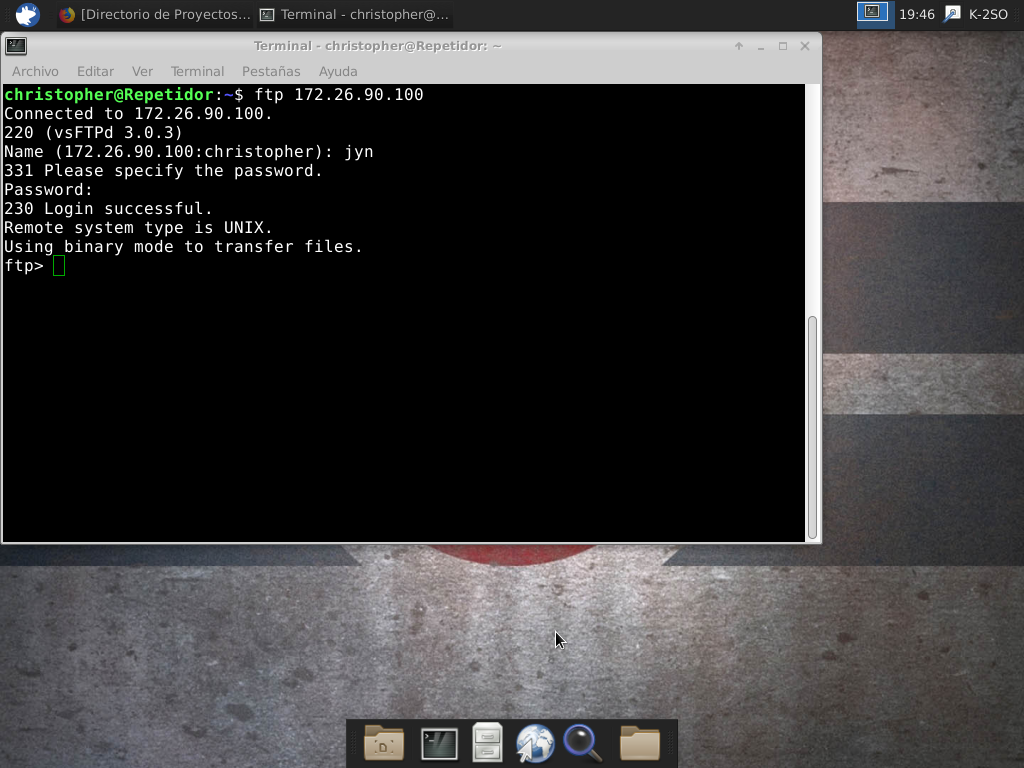
Demostración de que los planos están en Repetidor

El último paso es entregar los planos a Profundity, para lo cual usaremos el comando ***ftp 172.26.90.100***, cuya IP averiguamos gracias a la llamada espacial. Sin embargo, FTP no es capaz de transmitir directorios por defecto, por lo que se comprimirá desde REPETIDOR el directorio de los planos utilizando el comando ***tar -zcvf planos-directorio.tar.gz planos/*** (siempre y cuando estemos en el directorio 172.29.10.37).



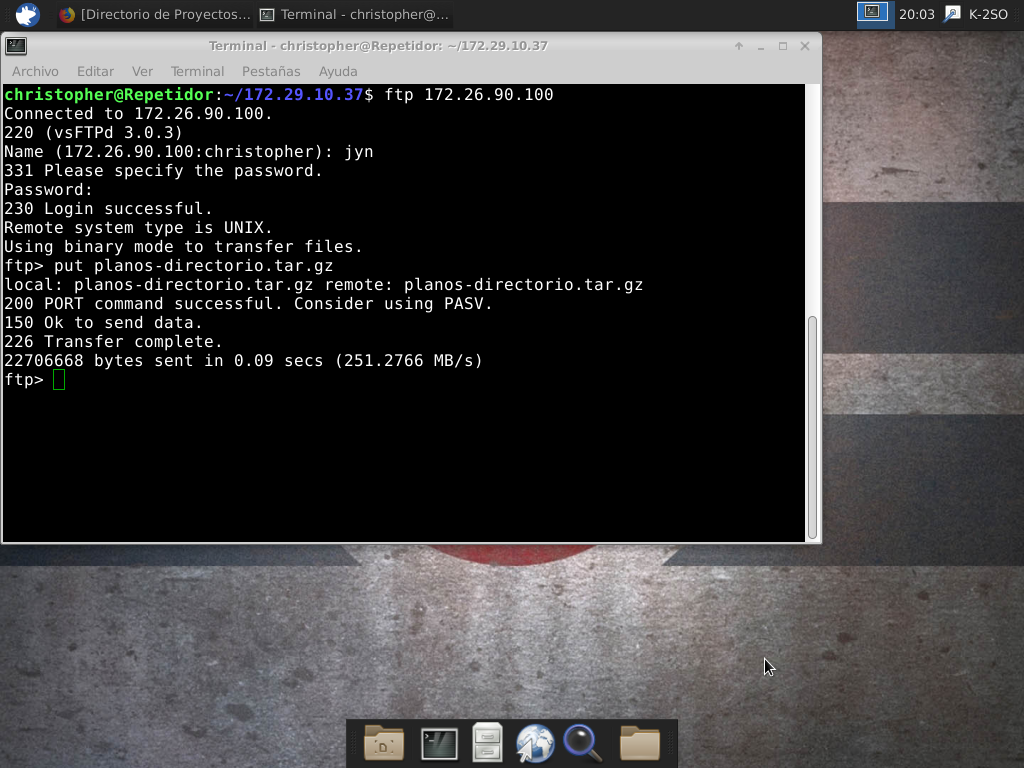
Planos comprimidos

Tras ello, habrá que iniciar una sesión FTP usando el comando ***ftp 172.26.90.100***, y habrá que poner de usuario **jyn** y de contraseña **jyn**, que fue proporcionada anteriormente.



Conexión FTP realizada

Para finalizar, usaremos el comando ***put planos-directorio.tar.gz***

******

PLANOS ENTREGADOS

Ahora, desde PROFUNDITY o desde donde la Alianza desee, sólo deben utilizar el comando ***tar -xf planos-directorio.tar.gz*** para acceder a los planos.

Misión cumplida.

<https://www.secnot.com/comprimir-directorio-linux.html>

<https://www.carlosegea.es/2009/08/12/descargar-un-directorio-entero-desde-ftp/>

<https://docs.oracle.com/cd/E24842_01/html/E22524/remotehowtoaccess-14.html>