Practica 5 Star Wars

Carlos González Martín

2ºB de Grado Medio de Sistemas Microinformáticos y Redes

Las Naves Salesianos

Curso 2021-2022

Contenido

[1. Que necesitamos 3](#_Toc90825737)

[2. Haremos una red nat en VirtualBox 3](#_Toc90825738)

[3. Iniciamos las maquinas 4](#_Toc90825739)

[4. Descomprimimos los archivos 4](#_Toc90825740)

[5. ssh 5](#_Toc90825741)

[6. Escaneo de direcciones 6](#_Toc90825742)

[7. Puertos dinamicos 6](#_Toc90825743)

[8. Firefox 7](#_Toc90825744)

[9. Hash MD5 8](#_Toc90825745)

[10. FileZilla 9](#_Toc90825746)

[11. Descomprimimos los archivos 11](#_Toc90825747)

[12. Puerto Local 12](#_Toc90825748)

[13. Conexión a repetidor 13](#_Toc90825749)

[14. FTP 13](#_Toc90825750)

[15. Levantamos interfaces 14](#_Toc90825751)

[16. Conexión a profundity 15](#_Toc90825752)

Ilustraciones

[Ilustración 1: Creando red nat 4](#_Toc90824787)

[Ilustración 2: Iniciando sesión en RogueOne 4](#_Toc90824788)

[Ilustración 3: inicio de sesión 5](#_Toc90824789)

[Ilustración 4: Descomprimimos los archivos 5](#_Toc90824790)

[Ilustración 5: Copiando las credenciales a .ssh 5](#_Toc90824791)

[Ilustración 6: ssh a bastión 6](#_Toc90824792)

[Ilustración 7: inundando la red en busca de máquinas encendidas 6](#_Toc90824793)

[Ilustración 8: comando nmap para descubrir los servicios de cada maquina 7](#_Toc90824794)

[Ilustración 9: Túnel dinámico 7](#_Toc90824795)

[Ilustración 10: SOCKS 8](#_Toc90824796)

[Ilustración 11: Pagina web 8](#_Toc90824797)

[Ilustración 12: Viendo la Pagina web 9](#_Toc90824798)

[Ilustración 13: Contraseña md5 de Estrellita 9](#_Toc90824799)

[Ilustración 14: Proxy genérico en FileZilla 9](#_Toc90824800)

[Ilustración 15: Conexión correcta de FileZilla 10](#_Toc90824801)

[Ilustración 16: Copia exitosa de los archivos 10](#_Toc90824802)

[Ilustración 17: Calculo de hash md5 10](#_Toc90824803)

[Ilustración 18: Conexión de FileZilla con el usuario Christopher 11](#_Toc90824804)

[Ilustración 19: Copia del archivo comprimido 11](#_Toc90824805)

[Ilustración 20: Descomprimimos los archivos 11](#_Toc90824806)

[Ilustración 21: Directorio .ssh en el escritorio 12](#_Toc90824807)

[Ilustración 22: Copiando clave privada 12](#_Toc90824808)

[Ilustración 23: Copiando la clave publica 12](#_Toc90824809)

[Ilustración 24: Túnel ssh 12](#_Toc90824810)

[Ilustración 25: Conexión ssh establecida 13](#_Toc90824811)

[Ilustración 26: Probando ftp 13](#_Toc90824812)

[Ilustración 27: Copiamos los archivos 14](#_Toc90824813)

[Ilustración 28: Comprimimos los archivos 14](#_Toc90824814)

[Ilustración 29: Levantando los interfaces de red 15](#_Toc90824815)

[Ilustración 30: IP maquina profundity 15](#_Toc90824816)

[Ilustración 31: Conexión a la maquina profundityç 15](#_Toc90824817)

[Ilustración 32: Copiamos los archivos a la antena 15](#_Toc90824818)

# Que necesitamos

Para esta practica necesitamos la ova facilitada ya que contendrá las máquinas que necesitamos

Todas las maquinas son Debían sin entorno grafico salvo la RogueOne que es un Debian Xfce

# Haremos una red nat en VirtualBox

Para que tengamos ip y también conexión usaremos la red nat de VirtualBox

Nos iremos a Archivo/Preferencias y luego a Red y le damos en añadir adaptador de red

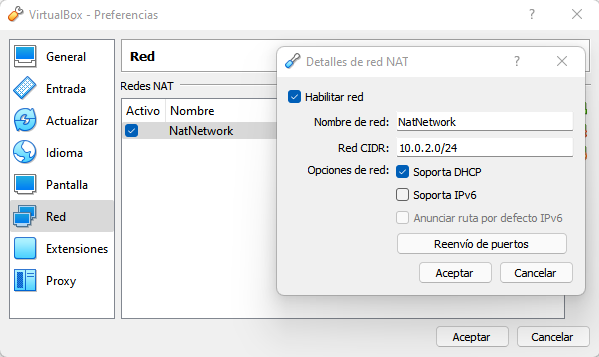


Ilustración : Creando red nat

# Iniciamos las maquinas

Una vez iniciadas las maquinas escribimos usuario y contraseña en RogueOne con el usuario k2so y la contraseña es igual al nombre de usuario

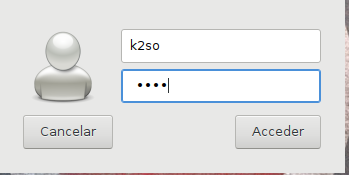


Ilustración : Iniciando sesión en RogueOne

Una vez iniciado sesión veremos un archivo comprimido con las credenciales de k2so en la cual la tendremos que descomprimir y copiar en el directorio .ssh



Ilustración : inicio de sesión

# Descomprimimos los archivos

Vemos que hay un archivo comprimido en el escritorio vamos a descomprimirlo con el siguiente comando

$ tar -xf credenciales-k2so.tar.gz

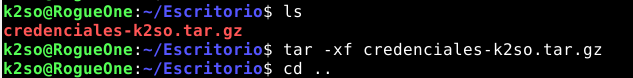


Ilustración : Descomprimimos los archivos

Una vez descomprimido los archivos copiaremos los archivos al directorio .ssh

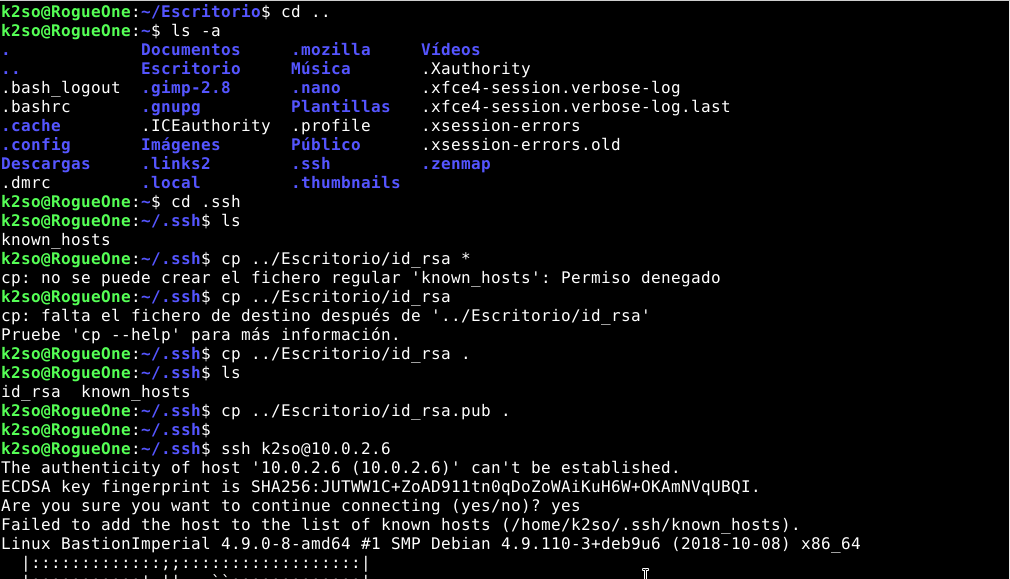


Ilustración : Copiando las credenciales a .ssh

# ssh

Una vez que hemos copiado los archivos veremos si nos podemos conectar a bastión

$ ssh k2so@10.0.2.6



Ilustración : ssh a bastión

# Escaneo de direcciones

Ya hecho el ssh tendremos que hacer o un nmap o un netdiscover para saber las IPs de las maquinas ya que vamos a ciegas y necesitamos conseguir los planos

$ sudo netdiscover -i enp0s8 172.29.0.0/16

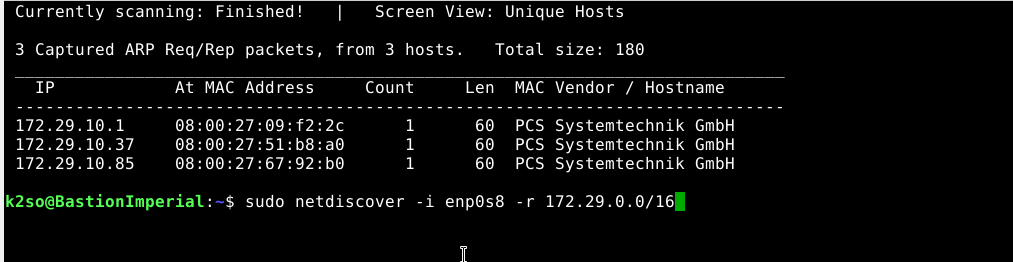


Ilustración : inundando la red en busca de máquinas encendidas

Una vez hecho esto no nos sirve de nada ya que no sabemos que servicios tenemos corriendo en las IPs que nos ha dicho netdiscover, con el comando nmap podemos ver los servicios que hay corriendo

$ nmap 172.29.10.X

Tendremos que poner las ip que nos a arrojado netdiscover

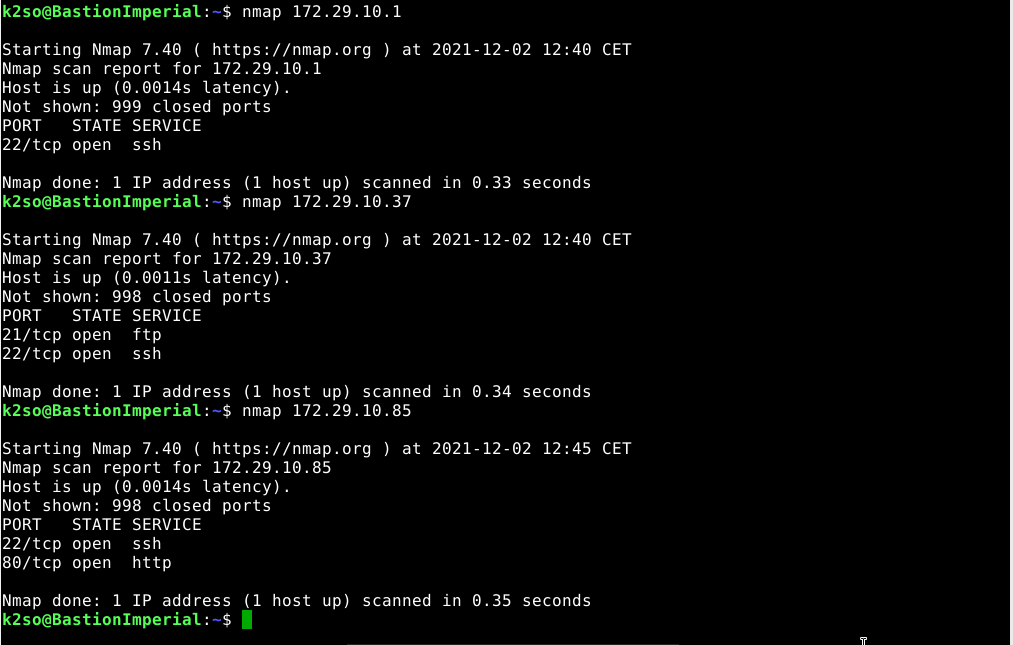


Ilustración : comando nmap para descubrir los servicios de cada maquina

# Puertos dinámicos

Vemos que en la ip 172.29.10.85 hay un servicio http abierto, abriremos un túnel dinámico en el puerto 1080 para que nos podamos conectar a la maquina

$ ssh -D 1080 k2so@10.0.2.6



Ilustración : Túnel dinámico

# Firefox

Una vez hecho esto abriremos Firefox y nos vamos a preferencias/proxy de red y activamos la opción de Configuración manual del proxy y luego en host SOCKS ponemos localhost y el puerto que hemos puesto en ssh que en mi caso es el 1080



Ilustración : SOCKS

Ahora le damos a aceptar y escribimos la ip del servidor http que es la 172.29.10.85

y veremos que se nos carga una pantalla de directorios de los lideres de proyectos



Ilustración : Pagina web

esto esta muy bien pero no nos sirve de nada lo que tendremos que hacer es darle donde pone “Directorio Lideres de Proyectos” que esta en amarillo para que nos salga mas cosas y saber como sigue la practica

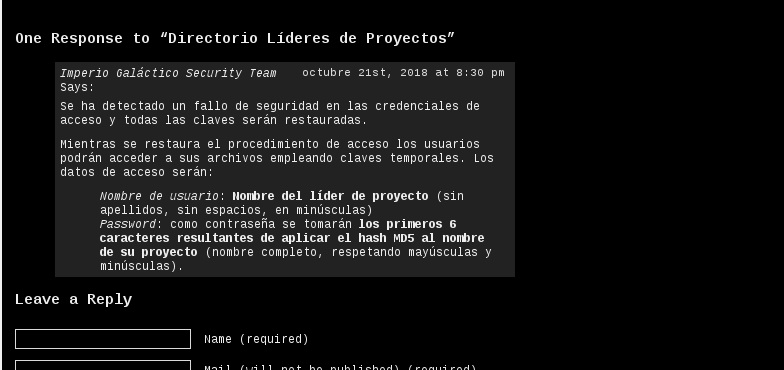


Ilustración : Viendo la Pagina web

# Hash MD5

Con esto ya sabemos un poco más de su usuario y contraseña, pero no sabemos quienes pueden acceder y viendo la practica vemos que Galen es uno de los que pueden acceder y para conseguir la contraseña vemos que necesitamos calcular el hash md5 al nombre de su proyecto que es Estrellita

$ echo -n Estrellita | md5sum



Ilustración : Contraseña md5 de Estrellita

Una vez hecho esto abriremos el cliente FileZilla para poder ver los archivos no sin antes configurar el proxy genérico de FileZilla, nos vamos a Edición/opciones y luego a proxy genérico y ponemos el puerto 1080 ya que el puerto dinámico ya lo tenemos abierto, pero podemos abrir el puerto 2021 por ejemplo

# FileZilla

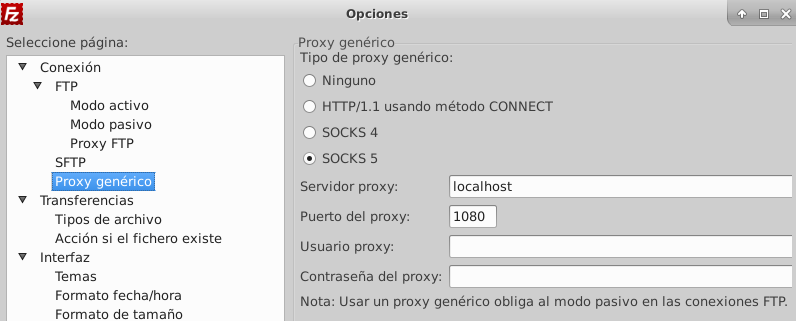


Ilustración : Proxy genérico en FileZilla

Una vez hecho esto le damos a aceptar y escribimos la ip de 172.29.10.37 ya que tiene un servicio ftp con el usuario Galen en minúsculas y con la contraseña que son los primeros 6 dígitos del hash md5 que hemos calculado antes.

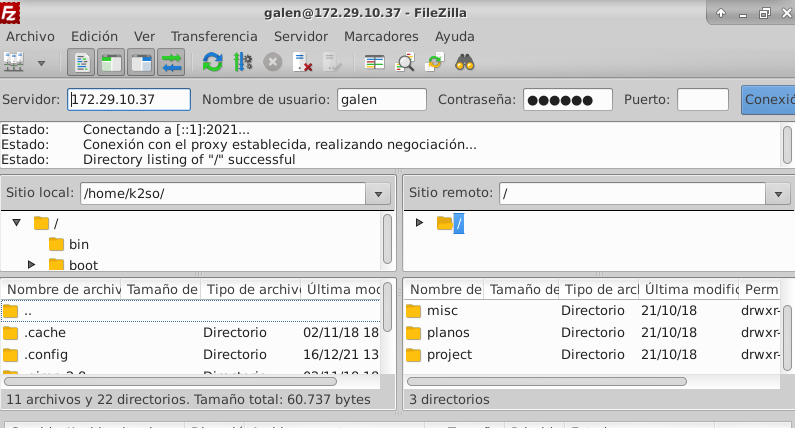


Ilustración : Conexión correcta de FileZilla

Una vez hecha la conexión nos podemos copiar los archivos a RogueOne

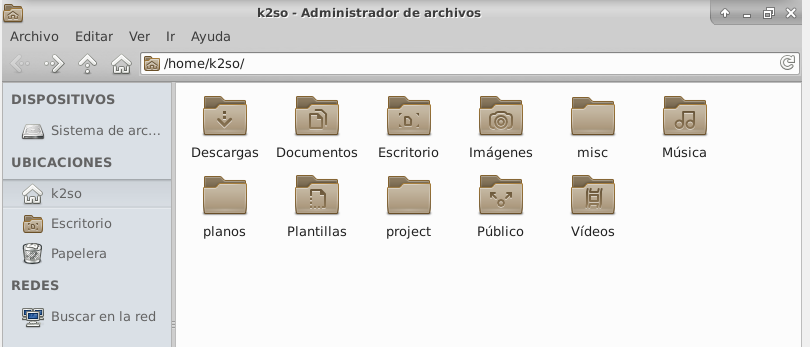


Ilustración : Copia exitosa de los archivos

Como dije antes hay varias personas que pueden acceder a la maquina con ftp y aparte de Galen pueden iniciar sesión Christopher que la contraseña es calculando el hash md5 de su proyecto

$ echo -n Sistemas de Navegación Y Comunicaciones | mds5sum

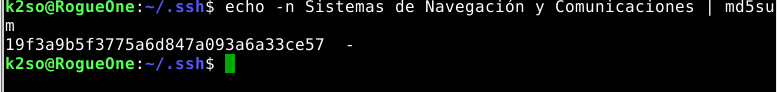


Ilustración : Calculo de hash md5

Ahora probamos con FileZilla si podemos conectarnos con el usuario Christopher

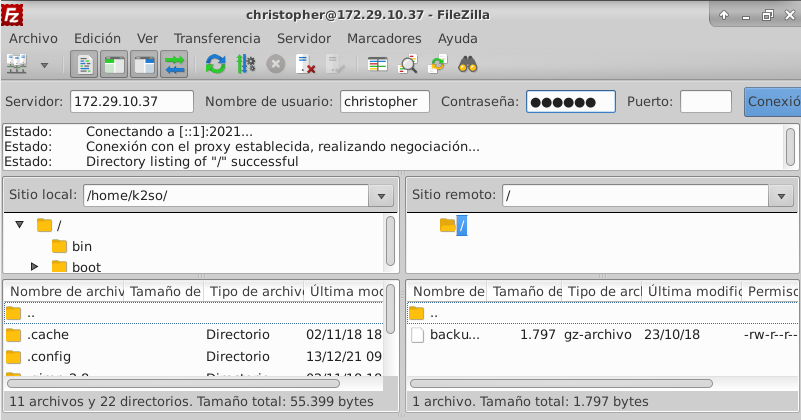


Ilustración : Conexión de FileZilla con el usuario Christopher

Vemos que hay un archivo lo copiamos a RogueOne y lo descomprimimos

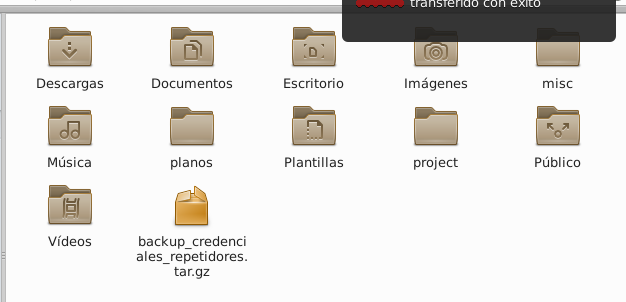


Ilustración : Copia del archivo comprimido

# Descomprimimos los archivos

lo descomprimimos con el siguiente comando

$ tar -xf backup\_credenciales\_repetidores.tar.gz



Ilustración : Descomprimimos los archivos

vemos que no ha hecho nada lo que recomiendo es hacerlo en otra carpeta distinta a /home porque si no nos deja entrar a bastión ya que las credenciales han cambiado por que hemos copiado las credenciales del repetidor, por eso lo hago en el escritorio

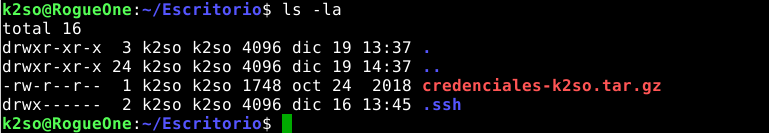


Ilustración : Directorio .ssh en el escritorio

Una vez descomprimido el archivo tendremos que copiar los archivos a .ssh en el directorio /home/k2so con el comando cp.

/.ssh$ cp /home/k2so/Escritorio/.ssh/id\_rsa /home/k2so/.ssh/id\_rsa\_antena



Ilustración : Copiando clave privada

Haremos lo mismo con la clave publica, pero poniendo .pub en el id\_rsa

/.ssh$ cp /home/k2so/Escritorio/.ssh/id\_rsa.pub /home/k2so/.ssh/id\_rsa\_antena.pub



Ilustración : Copiando la clave publica

# Puerto Local

Una vez hecho esto podemos ver si nos podemos conectar a repetidor no sin antes hacer un túnel

$ ssh -L 2222:172.29.10.1:22 k2so@10.0.2.6

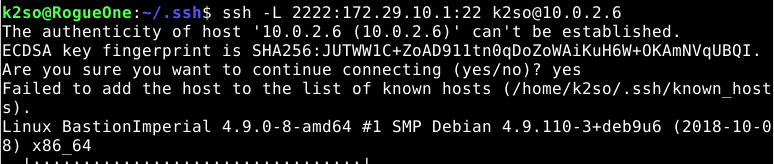


Ilustración : Túnel ssh

# Conexión a repetidor

Una vez hecho el túnel con el parámetro -i podemos elegir que clave podemos usar

$ ssh -i id\_rsa\_antena -p 2222 christopher@localhost

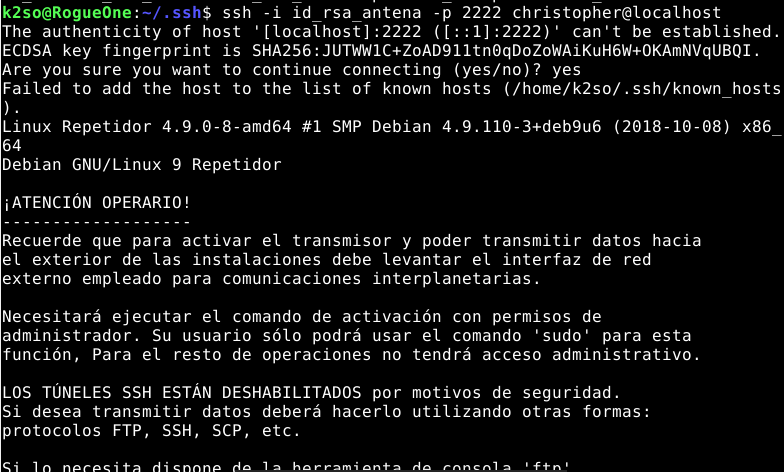


Ilustración : Conexión ssh establecida

# FTP

Una vez hecho vemos si funciona ftp con la ip de la antena que es la 172.29.10.37

$ ftp 172.29.10.37

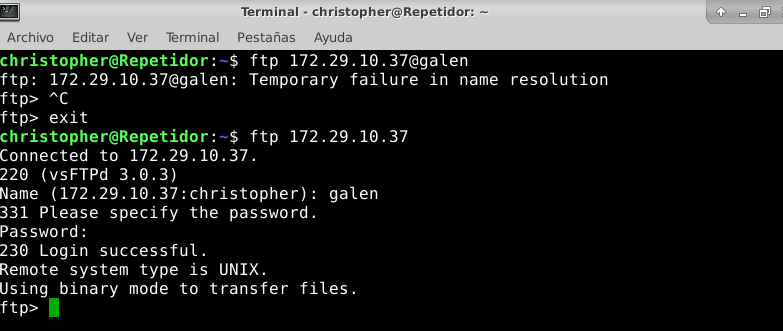


Ilustración : Probando ftp

Una vez que hemos comprobado que funciona ftp escribimos el comando para que nos copie los archivos

$ wget -c -r ftp://galen:7d464e@172.29.10.37/

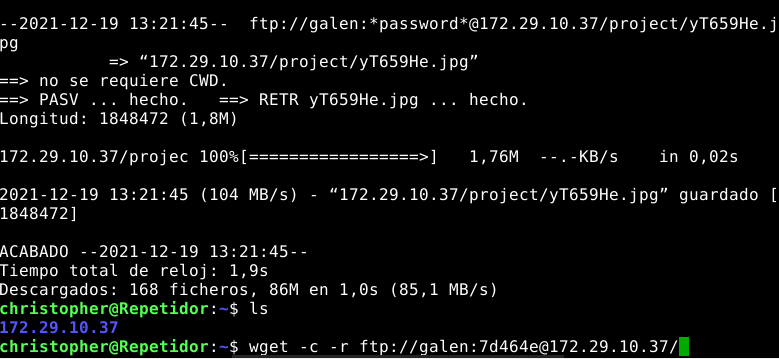


Ilustración : Copiamos los archivos

Vemos que nos a copiado todos los archivos ahora podemos comprimir los archivos con el siguiente comando dentro del directorio que nos a generado

$ tar -cvf planos.tar misc planos project

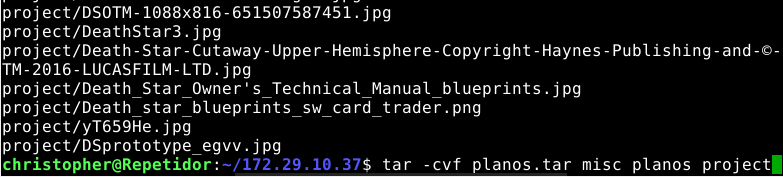


Ilustración : Comprimimos los archivos

# Levantamos interfaces

Una vez que hemos comprimido los archivos no podemos subir los archivos ya que están los interfaces apagados y con el comando sudo lo podemos hacer

$ sudo ifup enp0s3

Escribimos tantas veces como interfaces tenga cambiando el último número por el número que hay al hacer un ip -c a

$ ip -c a

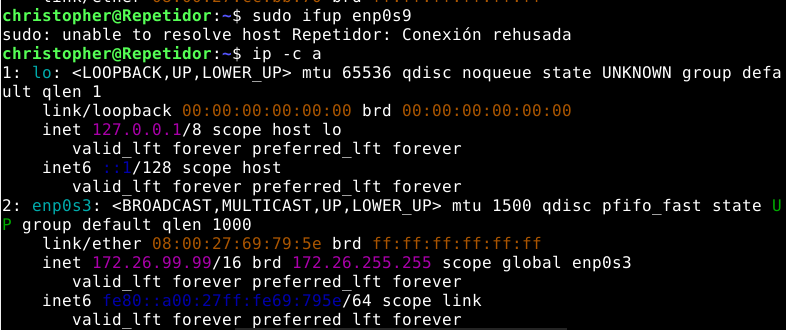


Ilustración : Levantando los interfaces de red

# Conexión a profundity

Una vez hecho esto en la maquina profundity vemos la ip que tiene la maquina por lo cual nos guardamos esa ip para usarla mas adelante

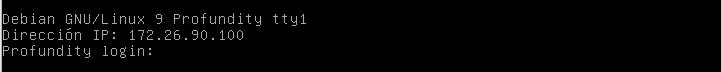


Ilustración : IP maquina profundity

Ya que hemos hecho esto podemos hacer un ftp a la maquina profundity y copiar los archivos

$ ftp 172.29.90.100

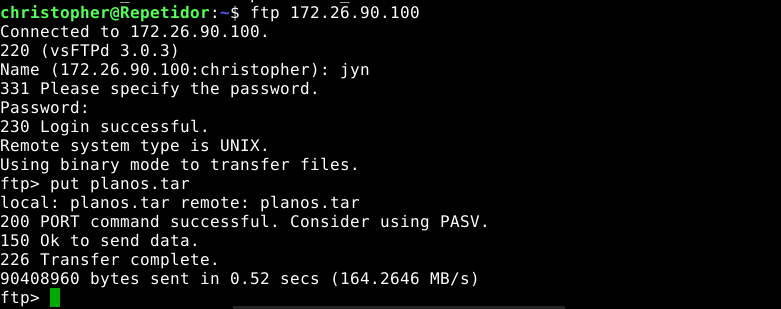


Ilustración : Conexión a la maquina profundity

Una vez hecho esto escribimos el siguiente comando para transferir los archivos

ftp> put planos.tar

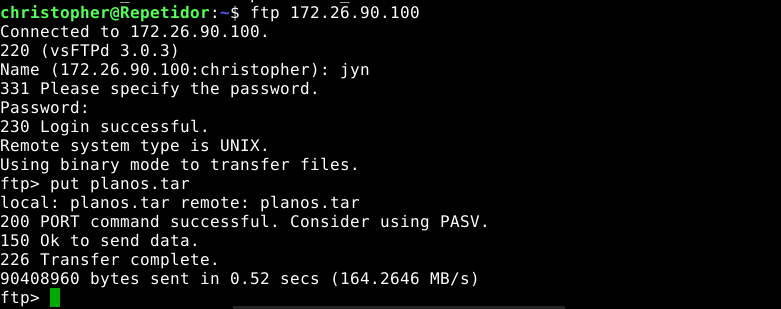


Ilustración : Copiamos los archivos a la antena