

RETO1 UD2

Protocolo FTP y SSH

Asignatura: DAW

Alumnos: Carolain Maccha,Luis Ayllon, Arancha Chicharro.

Reto1-UD2

Empezando con transferencias de ficheros y conexión a Shell remota

1.-FTP

- *Prueba varios clientes de ftp y muestra su funcionamiento conectándote a servidores FTP de tu elección.*

Como servidor FTP hemos elegido una máquina virtual linux.

Y como clientes máquinas linux y windows.

Para empezar, vamos a instalar y configurar el servicio FTP en linux.

Instalación

`sudo apt-get install vsftpd`

Configuración

configuramos parámetros generales del servidor:

-El servidor permite el acceso a todos los usuarios del sistema (locales y anónimos).
anonymous_enable=YES

El directorio por defecto de usuario anonymous es: /srv/ftp
local_enable=YES

-Permite descargas a todos los usuarios del sistema:
download_enable=YES

-Poner el siguiente mensaje de bienvenida: "Bienvenido a mi Servidor FTP"
ftpd_banner=Bienvenido a mi servidor FTP CAROL

-Permite la escritura en el sitio.

write_enable=YES

anon_upload_enable=YES

-Permite listar recursivamente sus carpetas:

ls_recurse_enable=YES

Configuramos párametros para USUARIOS LOCALES:

chroot_local_user=YES

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd.chroot_list

local_umask=037

Agregamos usuarios:

adduser usuario2

adduser usuario3

En /etc/vsftpd.conf modificamos los parámetros correspondientes:

Sudo nano /etc/vsftpd.conf

```
GNU nano 4.8                               /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# obviously need to create a directory writable by the
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with
# in your local time zone. The default is to display
# times returned by the MDTM FTP command are also affected
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port
connect_from_port_20=YES
#
```

```
GNU nano 4.8                               /etc/vsftpd.conf
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftp_banner=Bienvenido FTP carol service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Appar
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories. See the FAQ i
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their h
# directory. If chroot_local_user is YES, then this list becomes a list o
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sur
# the user does not have write access to the top level directory within
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled b
# default to avoid remote users being able to cause excessive I/O on la
# sites. However, some broken FTP clients such as "ncFTP" and "mirror" a
# the presence of the "-R" option, so there is a strong case for enabling
ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, t
# directory should not be writable by the ftp user. This directory is us
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
```

Creamos dos usuarios para hacer comprobaciones: usuario2 y usuario3:

```
usuario@usuario-VirtualBox:/$ sudo adduser usuario2
Añadiendo el usuario `usuario2' ...
Añadiendo el nuevo grupo `usuario2' (1001) ...
Añadiendo el nuevo usuario `usuario2' (1001) con grupo `usuario2' ..
Creando el directorio personal `/home/usuario2' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para usuario2
Introduzca el nuevo valor, o presione INTRO para el predeterminado
    Nombre completo []:
    Número de habitación []:
    Teléfono del trabajo []:
    Teléfono de casa []:
    Otro []:
¿Es correcta la información? [S/n] s
usuario@usuario-VirtualBox:/$ sudo adduser usuario3
Añadiendo el usuario `usuario3' ...
Añadiendo el nuevo grupo `usuario3' (1002) ...
Añadiendo el nuevo usuario `usuario3' (1002) con grupo `usuario3' ..
Creando el directorio personal `/home/usuario3' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para usuario3
Introduzca el nuevo valor, o presione INTRO para el predeterminado
    Nombre completo []:
    Número de habitación []:
    Teléfono del trabajo []:
    Teléfono de casa []:
    Otro []
¿Es correcta la información? [S/n] s
```

Agregamos los usuarios a vsftpd.chroot_list

```
GNU nano 4.8          /etc/vsftpd.chroot_list
usuario
usuario2
```

Reiniciamos el sistema

Sudo systemctl restart vsftpd.service

```
Navegador web Firefox
usuario@usuario-VirtualBox: ~
usuario@usuario-VirtualBox:/$ sudo nano /etc/vsftpd.chroot_list
usuario@usuario-VirtualBox:/$ sudo systemctl restart vsftpd.service
usuario@usuario-VirtualBox:/$
```

Comprobamos:

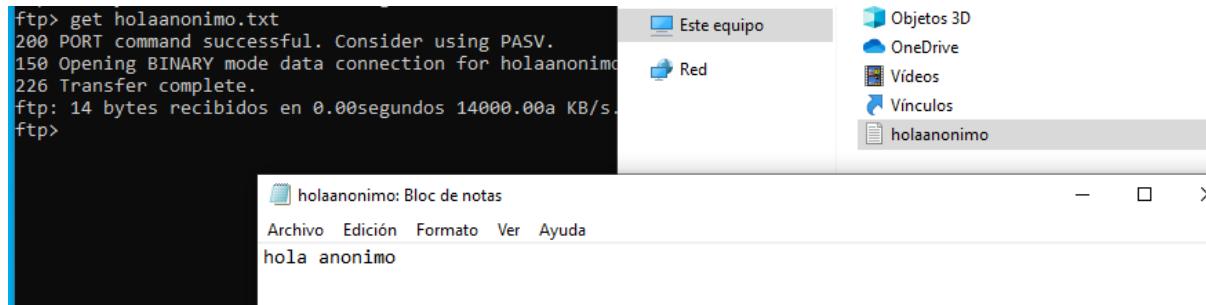
LINUX-WINDOWS

Inicio sesión usuario anonymous:

Ruta por defecto en el servidor de anonymous es /srv/ftp

```
ubuntu20.04-SW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 9 de nov 19:49
usuario@usuario-VirtualBox: ~
usuario@usuario-VirtualBox:~$ ls /srv/ftp
holaanonimo.txt
usuario@usuario-VirtualBox:~$ ip a
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:15:58:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.242/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
```

```
C:\Windows\system32\cmd.exe - ftp 192.168.1.242
C:\Users\carolain>ftp 192.168.1.242
Conectado a 192.168.1.242.
220 Bienvenido FTP carol service.
200 Always in UTF8 mode.
Usuario (192.168.1.242:(none)): anonymous
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
holaanonimo.txt
226 Directory send OK.
ftp: 20 bytes recibidos en 0.00segundos 20000.00a KB/s.
ftp> get holaanonimo.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for holaanonimo.txt (14 bytes).
226 Transfer complete.
ftp: 14 bytes recibidos en 0.00segundos 14000.00a KB/s.
ftp>
```



Inicio sesión de usuarios:

Si están incluidos en esta lista quiere decir que su raíz es el directorio home.

```
GNU nano 4.8          /etc/vsftpd.chroot_list
usuario
usuario2
```



```
C:\Users\carolain>ftp 192.168.1.242
Conectado a 192.168.1.242.
220 Bienvenido FTP carol service.
200 Always in UTF8 mode.
Usuario (192.168.1.242:(none)): usuario
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
Descargas
Documentos
Escritorio
Imágenes
Música
Plantillas
Público
Vídeos
public_html
snap
226 Directory send OK.
ftp: 108 bytes recibidos en 0.01segundos 7.20a KB/s.
ftp>
```

- Prueba una conexión FTP segura. Prueba la conexión desde el explorador de archivos en Windows y en alguna distribución GNU/Linux.**

Generamos certificado ssl :

```
sudo openssl req -x509 -nodes -keyout /etc/ssl/private/vsftpd.pem -out
/etc/ssl/private/vsftpd.pem -days 365 -newkey rsa:2048
```

```

usuario@usuario-VirtualBox: /etc/ssl
usuario@usuario-VirtualBox:/etc/ssl$ sudo openssl req -x509 -nodes -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem -days 365 -newkey rsa:2048
[sudo] contraseña para usuario:
Lo sentimos, vuelva a intentarlo.
[sudo] contraseña para usuario:
Generating a RSA private key
.....+++++
.....+
+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:servidorcarol
Email Address []:
```

Modificamos en vsftpd.conf las siguientes líneas:

```
sudo nano /etc/vsftpd/vsftpd.conf
```

Comentamos las siguientes líneas usando el carácter # de la siguiente manera:

```
#rsa_cert_file=/etc/ssl/private/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

Luego, agregamos las siguientes líneas para definir la ubicación del certificado SSL y el archivo de clave:

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
```

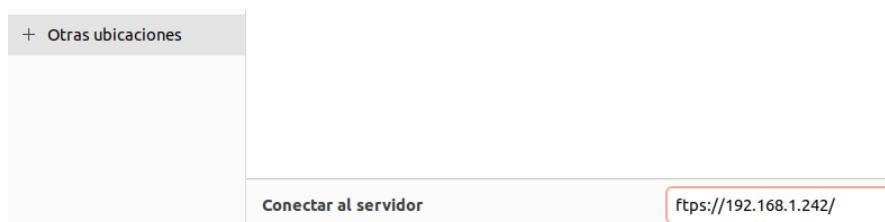
Reiniciamos el servicio ftp

```
Sudo systemctl restart vsftpd.service
```

PRUEBA EN CLIENTE LINUX:

En el gestor de archivos introducimos:

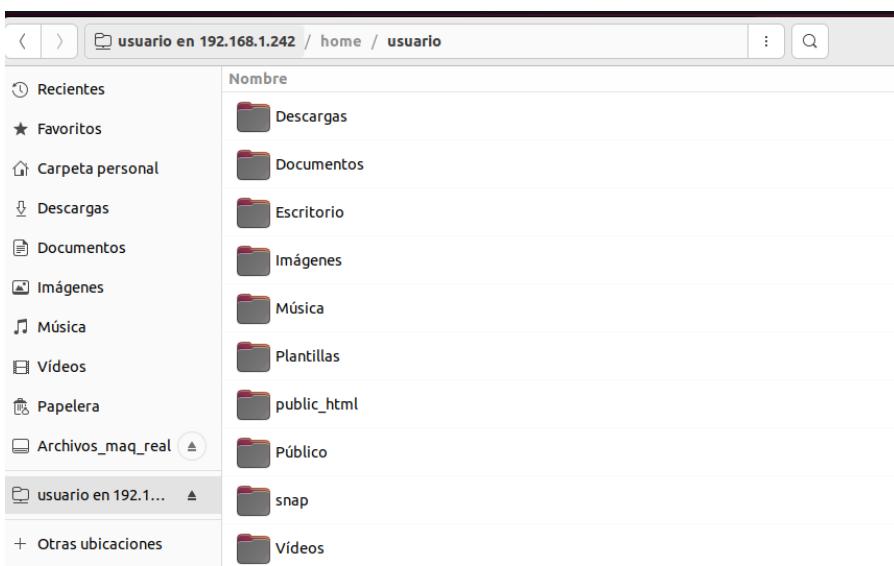
```
ftps://192.168.1.242(ip de mi servidor ftp)
```



Nos aparece un aviso de confirmar el certificado le damos que si:



Nos conectamos con usuario y contraseña al usuario “usuario” y automáticamente nos meterá dentro de home de usuario.

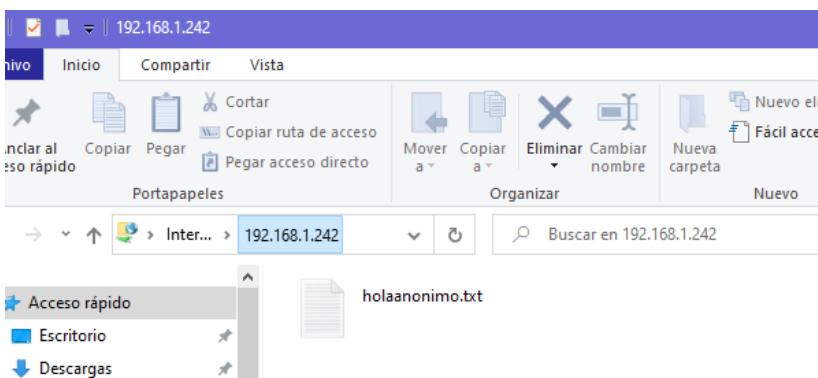


PRUEBA EN CLIENTE WINDOWS:

En el explorador de archivos de windows introducimos:

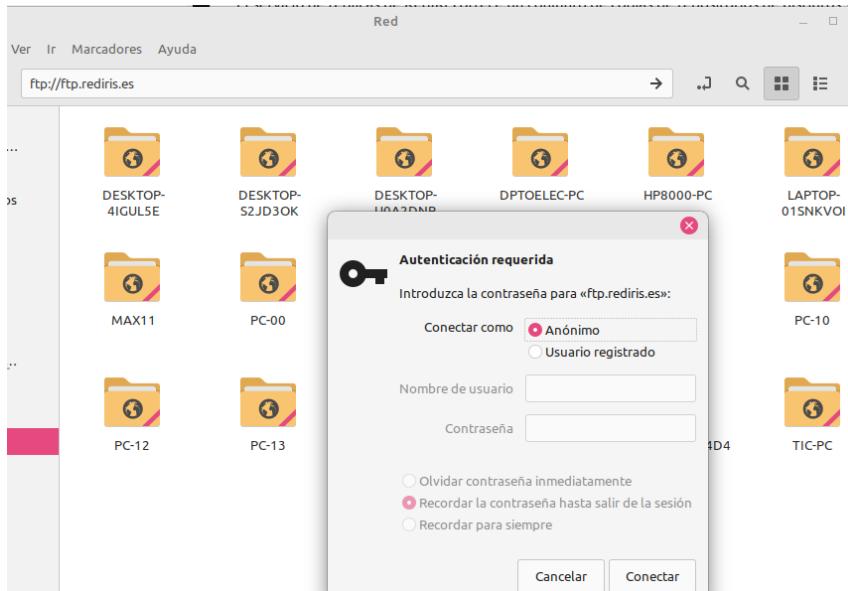
`ftp://192.168.1.242(ip de mi servidor ftp)`

Se conecta con el usuario anonimo.

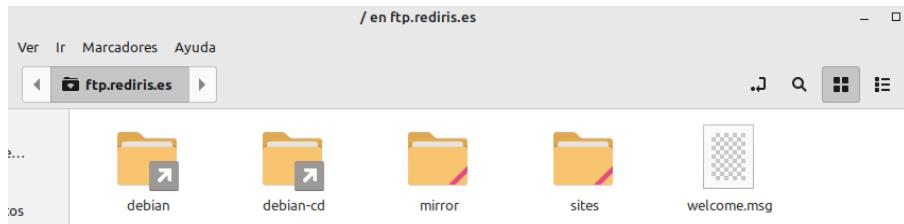


- **Opcional: muestra con Wireshark si puedes ver el usuario y la contraseña utilizados.**

Nos conectamos a rediris.es mediante ftp:



Nos mostrara las carpetas de ftp de rediris una vez accedamos:



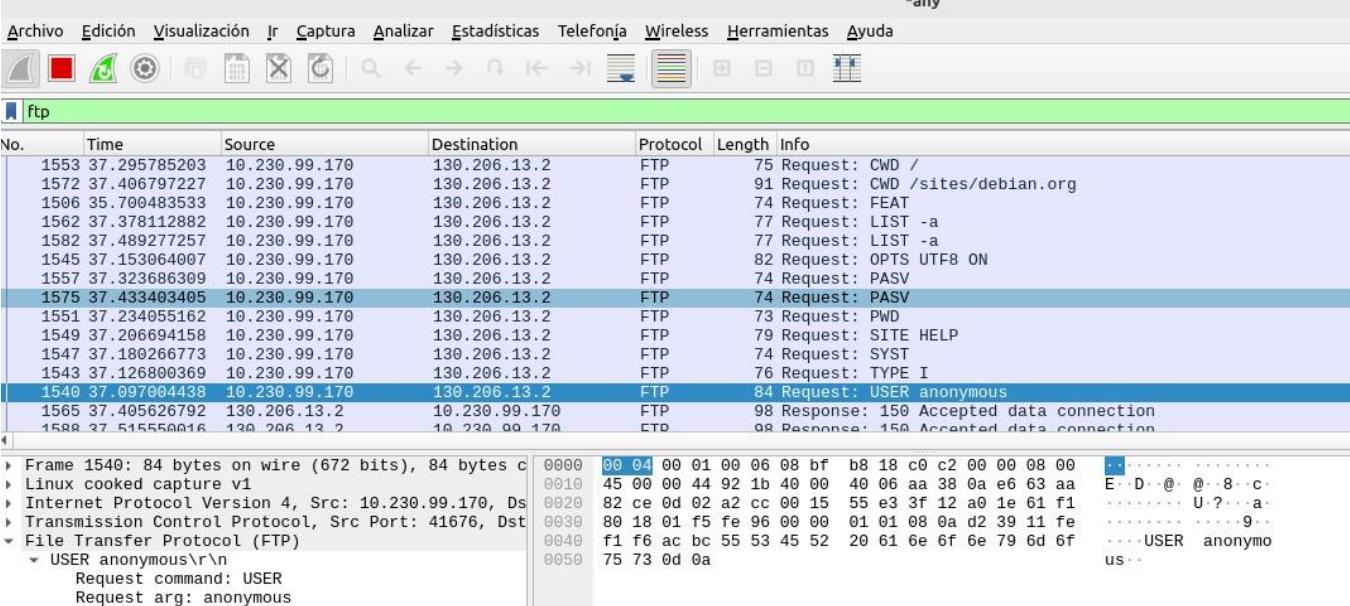
Filtrando ftp con wireshark nos aparece las siguientes líneas:

Archivo	Edición	Visualización	Jr	Captura	Analizar	Estadísticas	Teléfono	Wireless	Herramientas	Ayuda
ftp										
any										
No.	Time	Source		Destination	Protocol	Length	Info			
80729	224.675125138	130.206.13.2		10.230.99.170	FTP	211	Response: 220- Bienvenido al servicio de replicas de RedIRIS.			
80731	224.675327771	10.230.99.170		130.206.13.2	FTP	78	Request: AUTH TLS			
80734	224.702563226	130.206.13.2		10.230.99.170	FTP	88	Response: 234 AUTH TLS OK.			
84637	311.507976618	130.206.13.2		10.230.99.170	FTP	211	Response: 220- Bienvenido al servicio de replicas de RedIRIS.			
84639	311.508170471	10.230.99.170		130.206.13.2	FTP	74	Request: FEAT			
84641	311.534215988	130.206.13.2		10.230.99.170	FTP	301	Response: 211-Extensions supported:			
84900	318.945419561	10.230.99.170		130.206.13.2	FTP	84	Request: USER anonymous			
84901	318.973047803	130.206.13.2		10.230.99.170	FTP	306	Response: 230- RedIRIS - Red Académica y de Investigación Española			
84903	318.973167625	10.230.99.170		130.206.13.2	FTP	76	Request: TYPE I			
84904	318.998884868	130.206.13.2		10.230.99.170	FTP	98	Response: 200 TYPE is now 8-bit binary			
84905	318.999629978	10.230.99.170		130.206.13.2	FTP	82	Request: OPTS UTF8 ON			
84907	319.025187842	130.206.13.2		10.230.99.170	FTP	91	Response: 200 OK, UTF-8 enabled			
84908	319.025312430	10.230.99.170		130.206.13.2	FTP	74	Request: SYST			
84909	319.051372139	130.206.13.2		10.230.99.170	FTP	87	Response: 215 UNIX Type: L8			
84910	319.051507299	10.230.99.170		130.206.13.2	FTP	79	Request: SITE HELP			
84911	319.077773788	130.206.13.2		10.230.99.170	FTP	185	Response: 214-The following SITE commands are recognized			
84912	319.077917828	10.230.99.170		130.206.13.2	FTP	73	Request: PWD			
84913	319.104869186	130.206.13.2		10.230.99.170	FTP	102	Response: 257 "/" is your current location			
84914	319.139940455	10.230.99.170		130.206.13.2	FTP	75	Request: CWD /			
84915	319.166803942	130.206.13.2		10.230.99.170	FTP	108	Response: 250 OK. Current directory is /			
84916	319.167011146	10.230.99.170		130.206.13.2	FTP	74	Request: PASV			
84917	319.193293196	130.206.13.2		10.230.99.170	FTP	118	Response: 227 Entering Passive Mode (130,206,13,2,133,133)			
84921	319.219867617	10.230.99.170		130.206.13.2	FTP	77	Request: LIST -a			
84922	319.246326298	130.206.13.2		10.230.99.170	FTP	99	Response: 150 Accepted data connection			
84925	319.247927538	130.206.13.2		10.230.99.170	FTP	110	Response: 226-Options: -a -l			
84929	319.248069836	10.230.99.170		130.206.13.2	FTP	91	Request: CWD /sites/debian.org			
84931	319.274610485	130.206.13.2		10.230.99.170	FTP	111	Response: 250 OK. Current directory is /sites/debian.org			
84932	319.274779140	10.230.99.170		130.206.13.2	FTP	74	Request: PASV			
84933	319.301653687	130.206.13.2		10.230.99.170	FTP	118	Response: 227 Entering Passive Mode (130,206,13,2,121,245)			
84937	319.339063741	10.230.99.170		130.206.13.2	FTP	77	Request: LIST -a			
84938	319.365225042	130.206.13.2		10.230.99.170	FTP	98	Response: 150 Accepted data connection			
84939	319.365542182	130.206.13.2		10.230.99.170	FTP	110	Response: 226-Options: -a -l			

Nos muestra que hemos ingresado con Anonymous sin contraseña

*any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda



No.	Time	Source	Destination	Protocol	Length	Info
1553	37.295785203	10.230.99.170	130.206.13.2	FTP	75	Request: CWD /
1572	37.406797227	10.230.99.170	130.206.13.2	FTP	91	Request: CWD /sites/debian.org
1506	35.700483533	10.230.99.170	130.206.13.2	FTP	74	Request: FEAT
1562	37.378112882	10.230.99.170	130.206.13.2	FTP	77	Request: LIST -a
1582	37.489277257	10.230.99.170	130.206.13.2	FTP	77	Request: LIST -a
1545	37.153064007	10.230.99.170	130.206.13.2	FTP	82	Request: OPTS UTF8 ON
1557	37.323686309	10.230.99.170	130.206.13.2	FTP	74	Request: PASV
1575	37.433403405	10.230.99.170	130.206.13.2	FTP	74	Request: PASV
1551	37.234055162	10.230.99.170	130.206.13.2	FTP	73	Request: PWD
1549	37.206694158	10.230.99.170	130.206.13.2	FTP	79	Request: SITE HELP
1547	37.180266773	10.230.99.170	130.206.13.2	FTP	74	Request: SYST
1543	37.126800369	10.230.99.170	130.206.13.2	FTP	76	Request: TYPE I
1540	37.097004438	10.230.99.170	130.206.13.2	FTP	84	Request: USER anonymous
1565	37.405626792	130.206.13.2	10.230.99.170	FTP	98	Response: 150 Accepted data connection
1588	37.51550016	130.206.13.2	10.230.99.170	CTD	98	Response: 150 Accepted data connection

```

> Frame 1540: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.230.99.170, Dst: 130.206.13.2
> Transmission Control Protocol, Src Port: 41676, Dst Port: 21
> File Transfer Protocol (FTP)
  > USER anonymous\r\n
    Request command: USER
    Request arg: anonymous
  [Current working directory: ]

```

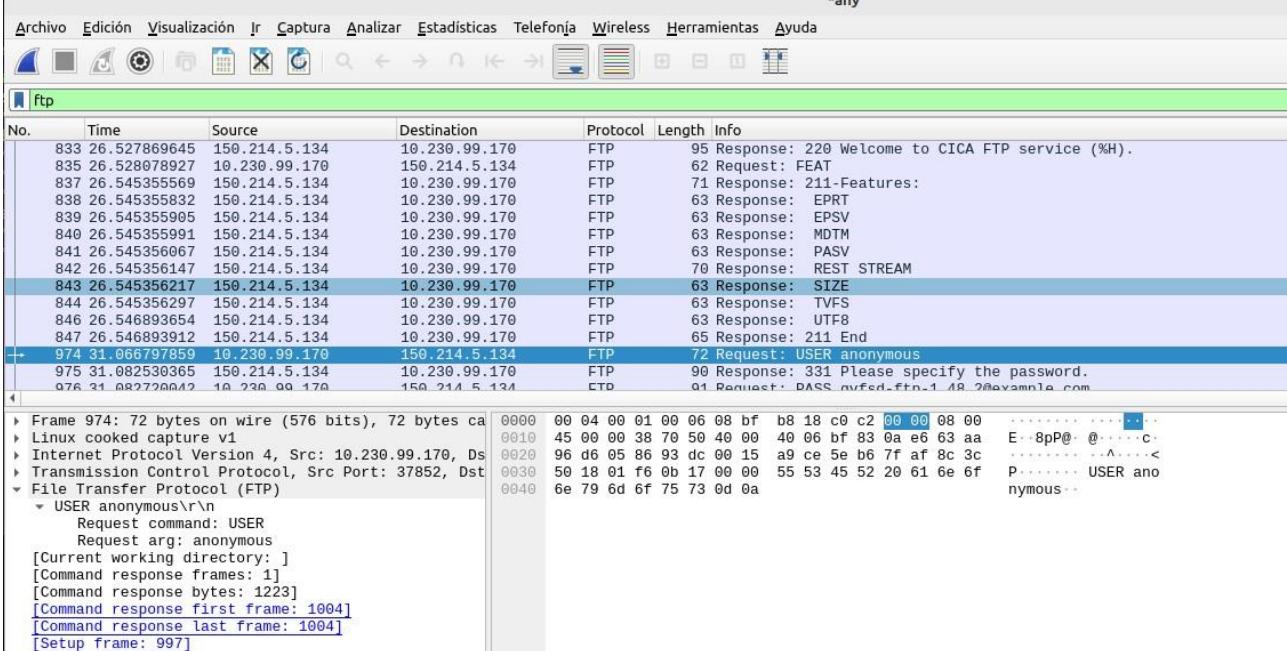
Frame details and bytes pane are visible on the right.

Con <ftp://ftp.cica.es>:

Nos muestra que hemos ingresado con Anonymous sin contraseña:

*any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda



No.	Time	Source	Destination	Protocol	Length	Info
833	26.527869645	150.214.5.134	10.230.99.170	FTP	95	Response: 220 Welcome to CICA FTP service (%H).
835	26.528078927	10.230.99.170	150.214.5.134	FTP	62	Request: FEAT
837	26.545355569	150.214.5.134	10.230.99.170	FTP	71	Response: 211-Features:
838	26.545355832	150.214.5.134	10.230.99.170	FTP	63	Response: EPRT
839	26.545355905	150.214.5.134	10.230.99.170	FTP	63	Response: EPSV
840	26.545355991	150.214.5.134	10.230.99.170	FTP	63	Response: MDTM
841	26.545356067	150.214.5.134	10.230.99.170	FTP	63	Response: PASV
842	26.545356147	150.214.5.134	10.230.99.170	FTP	70	Response: REST STREAM
843	26.545356217	150.214.5.134	10.230.99.170	FTP	63	Response: SIZE
844	26.545356297	150.214.5.134	10.230.99.170	FTP	63	Response: TVFS
846	26.546893654	150.214.5.134	10.230.99.170	FTP	63	Response: UTF8
847	26.546893912	150.214.5.134	10.230.99.170	FTP	65	Response: 211 End
974	31.066797859	10.230.99.170	150.214.5.134	FTP	72	Request: USER anonymous
975	31.082530365	150.214.5.134	10.230.99.170	FTP	90	Response: 331 Please specify the password.
976	31.09279002	10.230.99.170	150.214.5.134	CTD	91	Request: DASS_nufed-fhn.1 10.230.99.170@maxmilla.com

```

> Frame 974: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.230.99.170, Dst: 150.214.5.134
> Transmission Control Protocol, Src Port: 37852, Dst Port: 21
> File Transfer Protocol (FTP)
  > USER anonymous\r\n
    Request command: USER
    Request arg: anonymous
  [Current working directory: ]
  [Command response frames: 1]
  [Command response bytes: 1223]
  [Command response first frame: 1004]
  [Command response last frame: 1004]
  [Setup frame: 997]

```

Frame details and bytes pane are visible on the right.

2.- SSH

- Instala el servidor openssh en una máquina con GNU/Linux (openssh-server) y otra con Windows. A partir de ahí:*

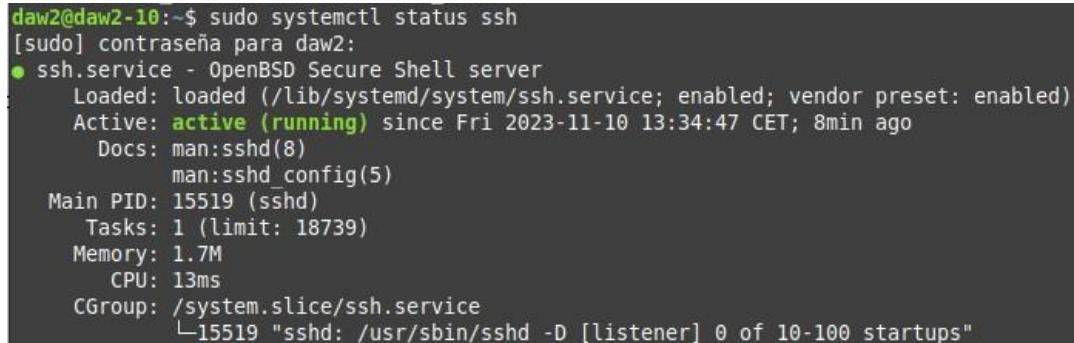
En Máquina ubuntu:

sudo apt install openssh-server



```
daw2@daw2-10:~$ sudo apt install openssh-server
[sudo] contraseña para daw2:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  openssh-client openssh-sftp-server
Paquetes sugeridos:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
Se actualizan los siguientes paquetes:
  openssh-client openssh-server openssh-sftp-server
3 actualizados, 0 nuevos se instalarán, 0 para eliminar y 121 no actualizados.
Se necesita descargar 1.378 kB de archivos.
Se utilizarán 0 B de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.4 [38,7 kB]
```

sudo systemctl status ssh



```
daw2@daw2-10:~$ sudo systemctl status ssh
[sudo] contraseña para daw2:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2023-11-10 13:34:47 CET; 8min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 15519 (sshd)
     Tasks: 1 (limit: 18739)
    Memory: 1.7M
      CPU: 13ms
     CGroup: /system.slice/ssh.service
             └─15519 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Si el servidor SSH sigue inactivo y al reiniciarlo no está activado el inicio automático, puedes cambiarlo introduciendo otros dos comandos:

sudo systemctl enable ssh

sudo systemctl start ssh

sudo ufw allow ssh

CONFIGURACIÓN

sudo nano /etc/ssh/sshd_config

sudo service ssh restart

Por defecto el archivo de configuración tiene pocos parámetros habilitados muchos de ellos están comentados.

```

GNU nano 6.2                               sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

# The strategy used for options in the default sshd config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

```

- *Demuestra el acceso CLI entre cliente y servidor demostrando que los comandos se están ejecutando efectivamente en el servidor.*

En cliente Linux:

Nos conectamos con ssh desde el pc Linux de “arancha” al pc Linux de “daw2” (pc’s de clase conectados en la misma red), y vemos que se hace la conexión:

```

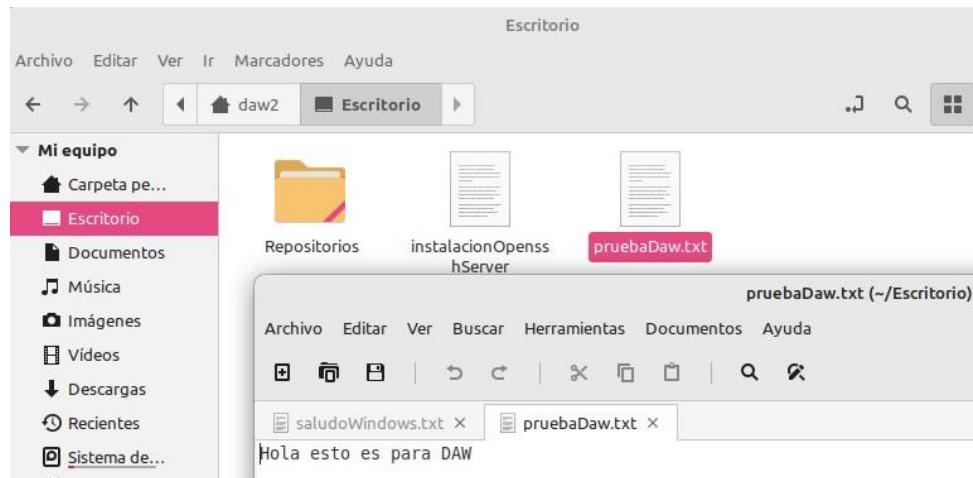
daw2@daw2-10: ~
Archivo Editar Ver Buscar Terminal Ayuda
arancha@daw2-01:~$ ssh -p 22 daw2@10.230.99.170
The authenticity of host '10.230.99.170 (10.230.99.170)' can't be established.
ED25519 key fingerprint is SHA256:2CT0l8o80LrbNISbI6secu9G/hk+PSmmJDP262KgBTY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.230.99.170' (ED25519) to the list of known hosts.
daw2@10.230.99.170's password:
daw2@daw2-10:~$ 

```

Hacemos una prueba accediendo a Escritorio y creando un archivo txt con contenido:

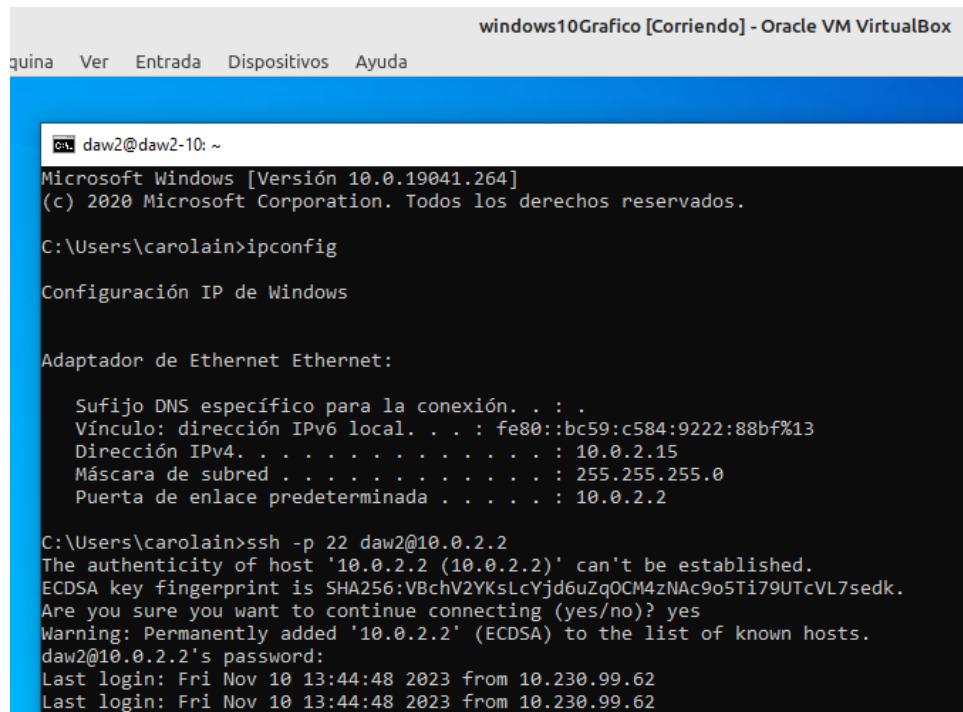
```
daw2@daw2-10:~$ cd Escritorio
daw2@daw2-10:~/Escritorio$ echo "Hola esto es para DAW" > pruebaDaw.txt
daw2@daw2-10:~/Escritorio$ ls
instalacionOpenSSHServer pruebaDaw.txt Repositorios
daw2@daw2-10:~/Escritorio$ cat pruebaDaw.txt
Hola esto es para DAW
daw2@daw2-10:~/Escritorio$
```

En el servidor Linux ssh del pc del usuario daw2, comprobamos que se ha creado y se puede visualizar dicho archivo:

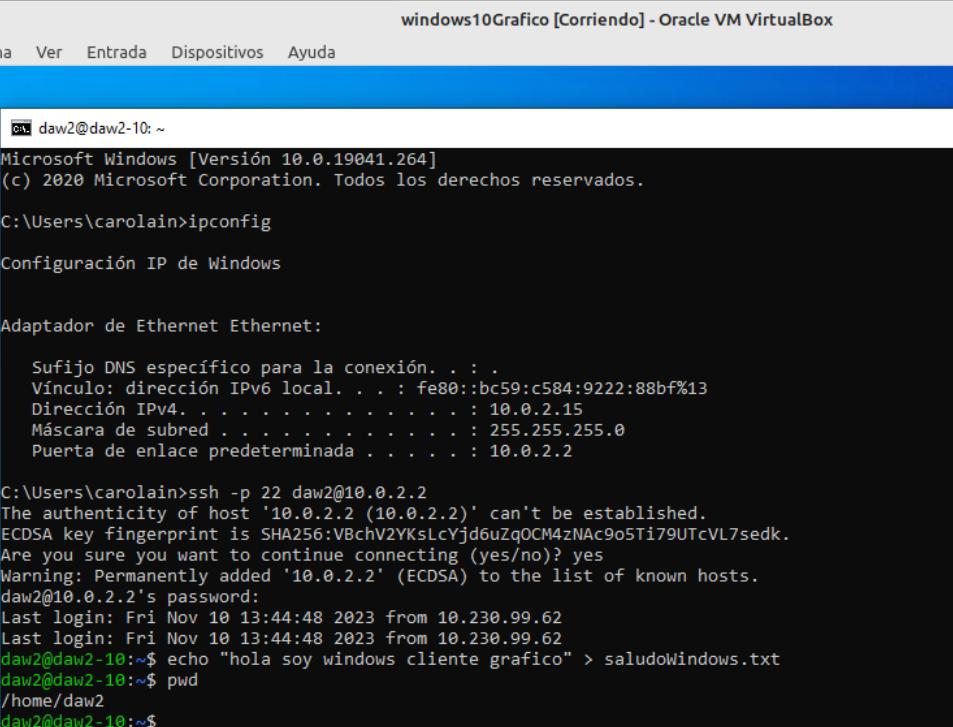


En cliente windows:

Me deja conectarme al servidor linux ssh:



Para comprobar creo un archivo de texto dando un saludo al ssh servidor:



```

windows10Grafico [Corriendo] - Oracle VM VirtualBox
File Ver Entrada Dispositivos Ayuda

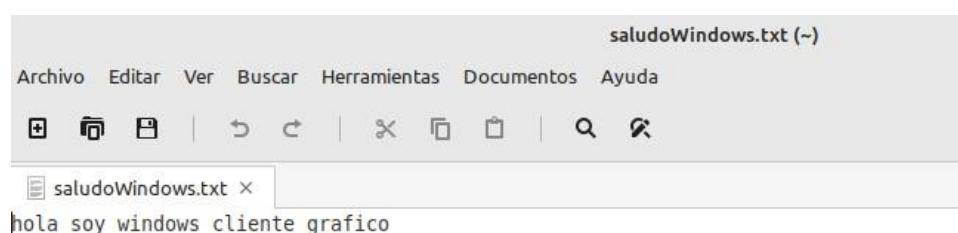
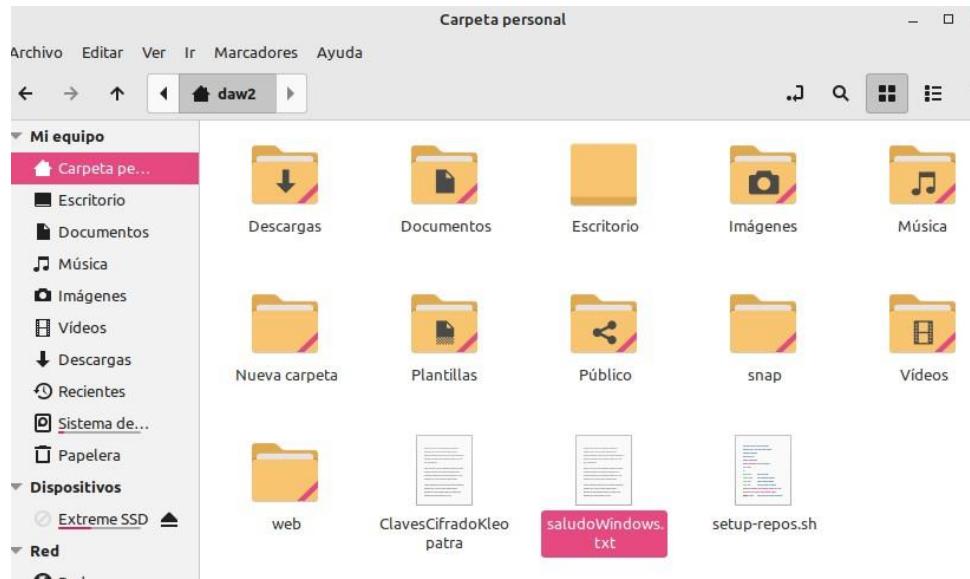
daw2@daw2-10: ~
Microsoft Windows [Versión 10.0.19041.264]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\carolain>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . .
  Vínculo: dirección IPv6 local. . . : fe80::bc59:c584:9222:88bf%13
  Dirección IPv4. . . . . : 10.0.2.15
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : 10.0.2.2

C:\Users\carolain>ssh -p 22 daw2@10.0.2.2
The authenticity of host '10.0.2.2 (10.0.2.2)' can't be established.
ECDSA key fingerprint is SHA256:VBchV2YKsLcYjd6uZq0CM4zNAc9o5Ti79UTcVL7sedk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.2' (ECDSA) to the list of known hosts.
daw2@10.0.2.2's password:
Last login: Fri Nov 10 13:44:48 2023 from 10.230.99.62
Last login: Fri Nov 10 13:44:48 2023 from 10.230.99.62
daw2@daw2-10:~$ echo "hola soy windows cliente grafico" > saludoWindows.txt
daw2@daw2-10:~$ pwd
/home/daw2
daw2@daw2-10:~$
```

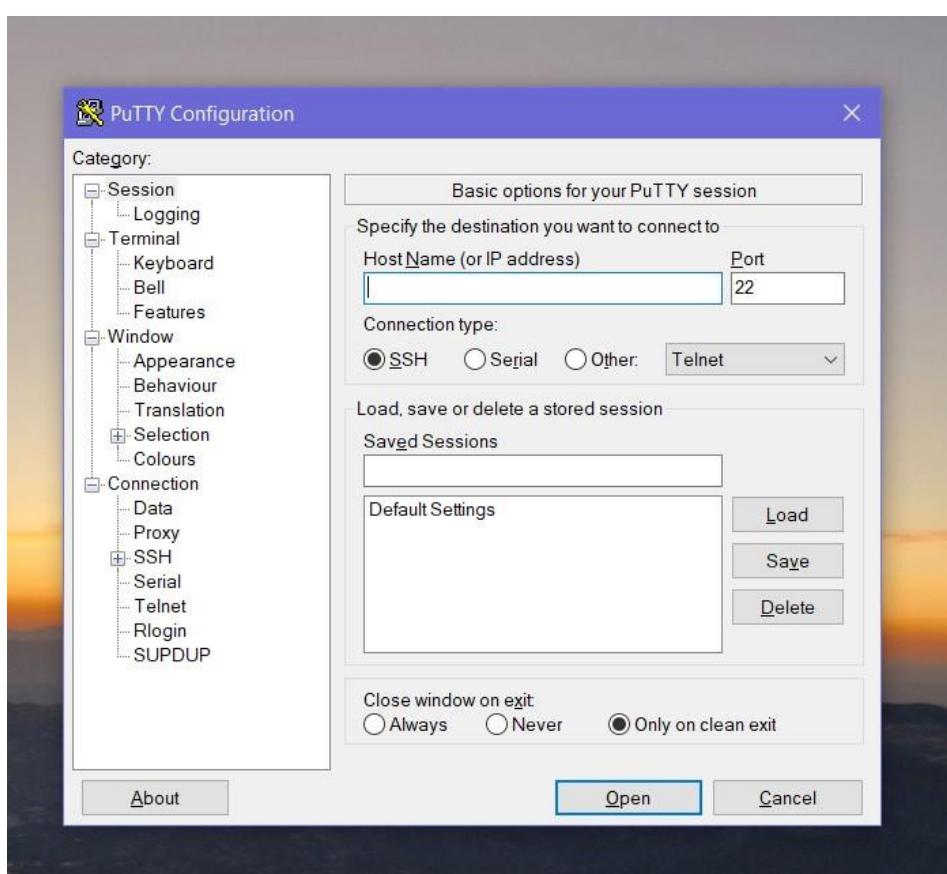
En mi servidor Linux ssh compruebo que se ha creado y se pude visualizar dicho archivo:

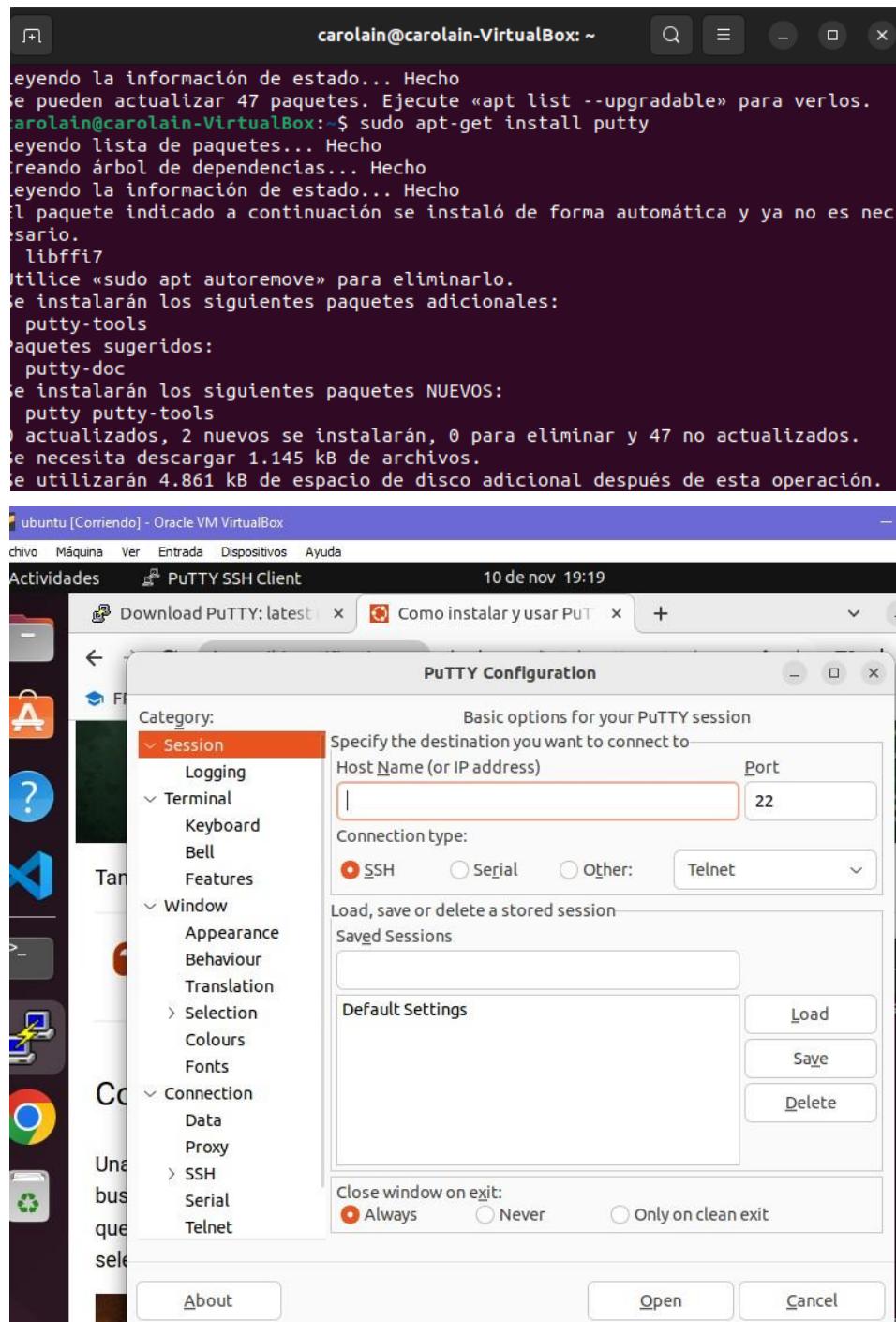


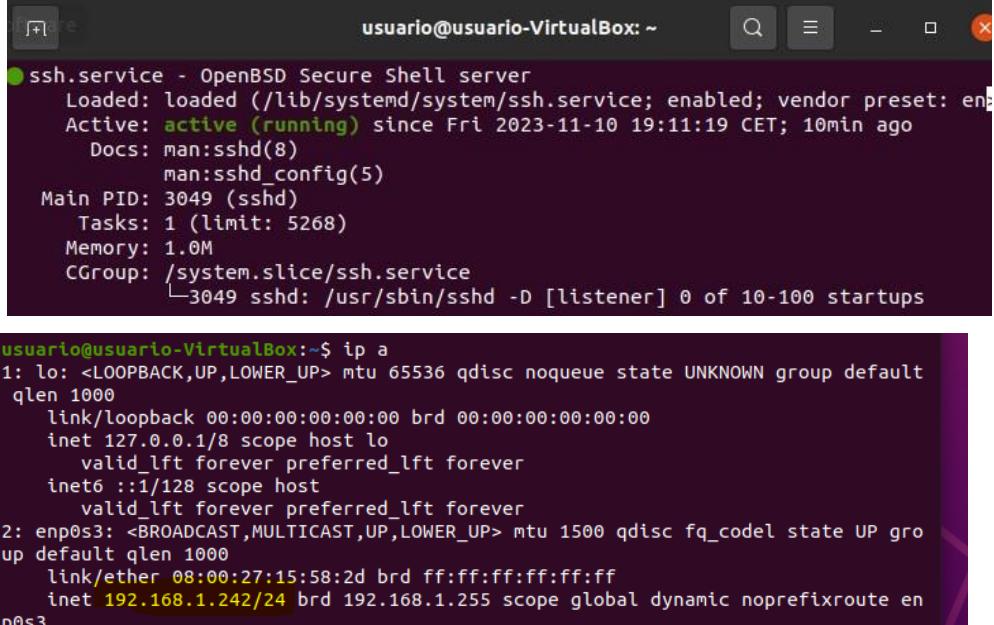
Otro cliente con CLI es putty:

Instalamos putty en windows y linux cliente.

Windows cliente:



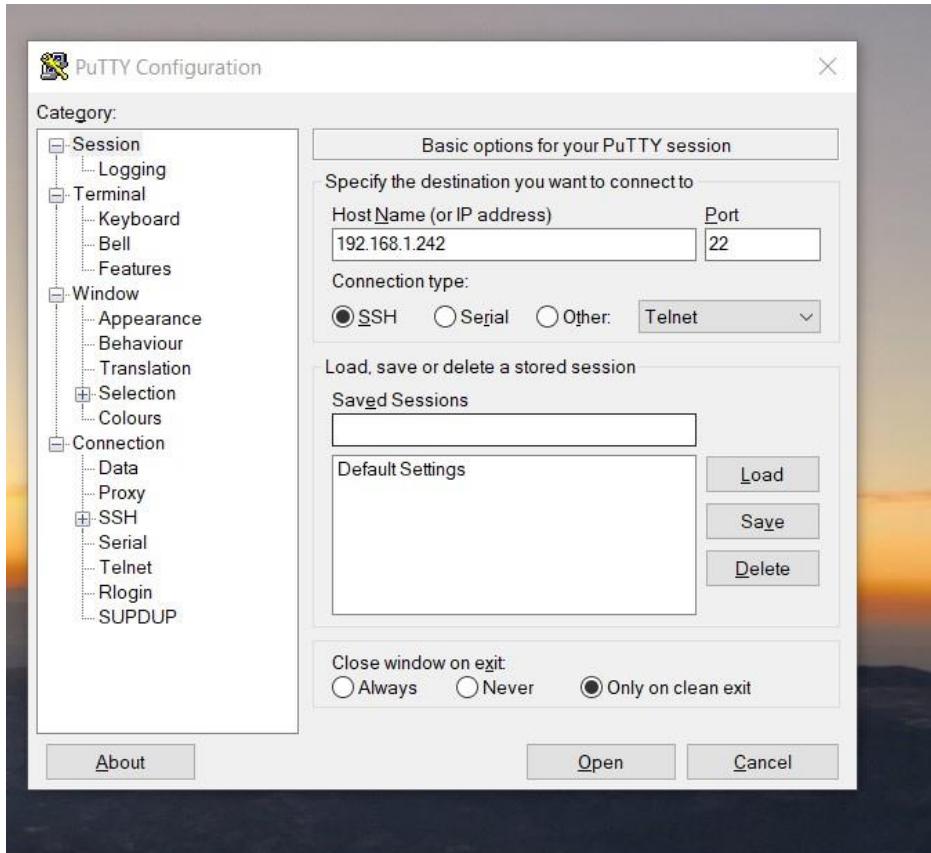
Linux cliente:

Servidor SSH Linux:


```
usuario@usuario-VirtualBox: ~
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2023-11-10 19:11:19 CET; 10min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Main PID: 3049 (sshd)
     Tasks: 1 (limit: 5268)
    Memory: 1.0M
      CGroup: /system.slice/ssh.service
              └─3049 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

usuario@usuario-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
  qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
  qlen 1000
    link/ether 08:00:27:15:58:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.242/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
```

Nos metemos con cliente Windows al servidor ssh Linux 192.168.1.242:



Aceptamos que reconocemos el servidor:

```
192.168.1.242 - PuTTY
PuTTY Security Alert

The host key is not cached for this server:
192.168.1.242 (port 22)

You have no guarantee that the server is the computer you think it is.

The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:sjO1ofZxT2l+PrY7274/01TVnBzCvO3MiY7zMIGLD0k

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

More info... Accept Connect Once Cancel

usuario@usuario-VirtualBox: ~
login as: usuario
usuario@192.168.1.242's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

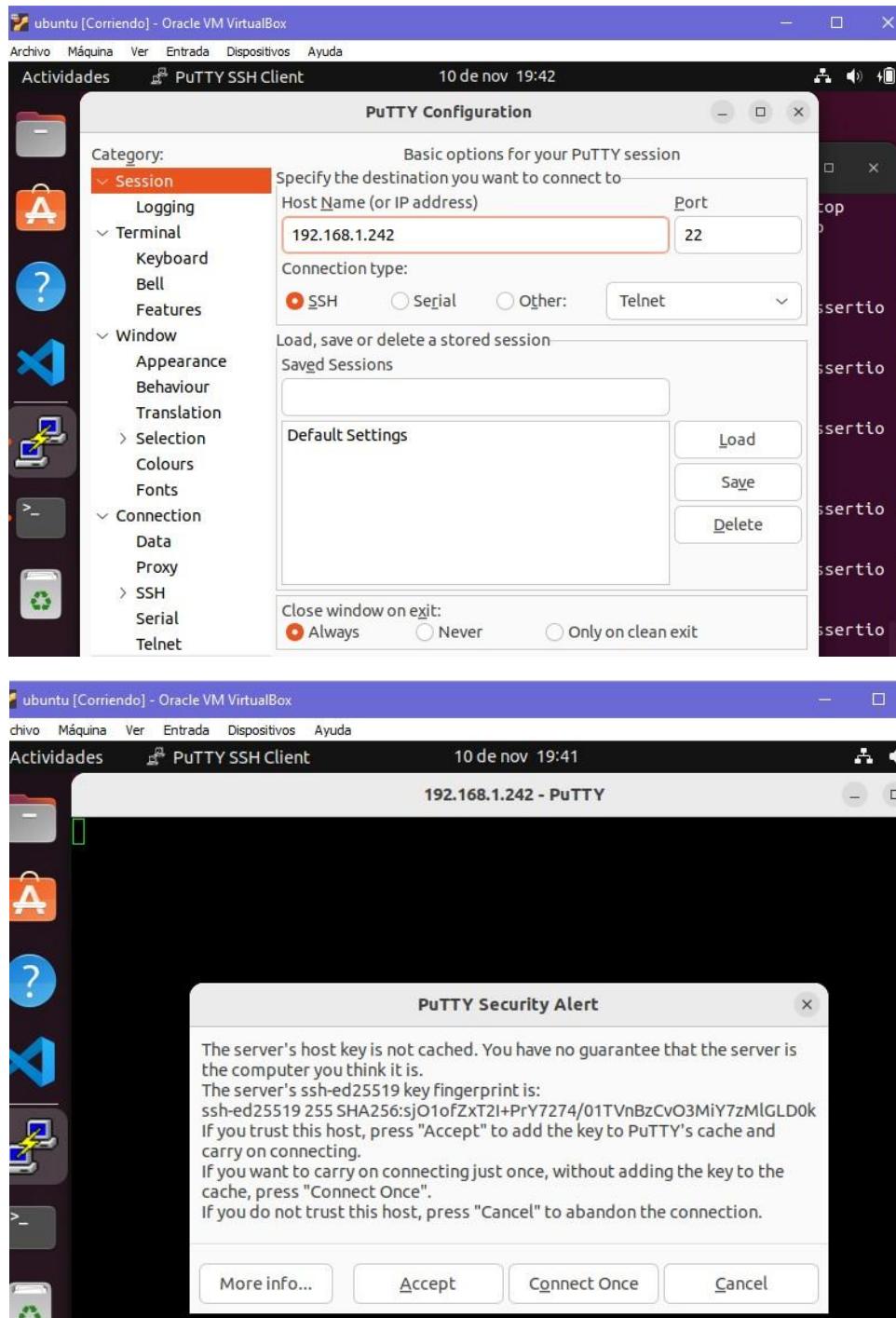
247 actualizaciones se pueden instalar inmediatamente.
26 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Nos metemos con cliente Linux al servidor ssh Linux 192.168.1.242 y aceptamos que reconocemos el servidor:



```

ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades PuTTY SSH Client 10 de nov 19:41
usuario@usuario-VirtualBox: ~
login as: usuario
usuario@192.168.1.242's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

247 actualizaciones se pueden instalar inmediatamente.
26 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Nov 10 19:28:19 2023 from 192.168.1.124
usuario@usuario-VirtualBox:~$ 
```

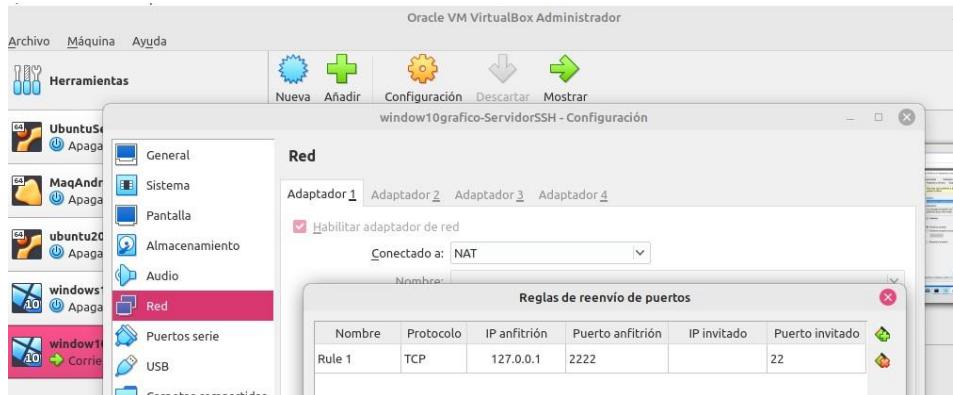
SSH SERVIDOR EN WINDOWS:

Me ha conectado correctamente el SSH server de windows.

Los pasos que he seguido:

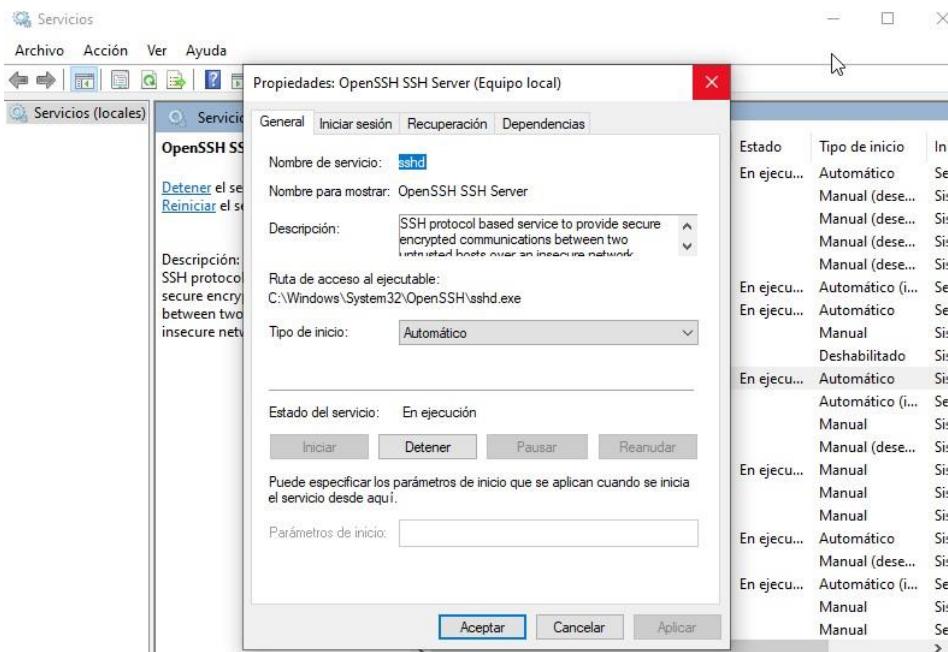
1)Poner en modo NAT mi adaptador de red.

2)hacer un reenvío de puertos:



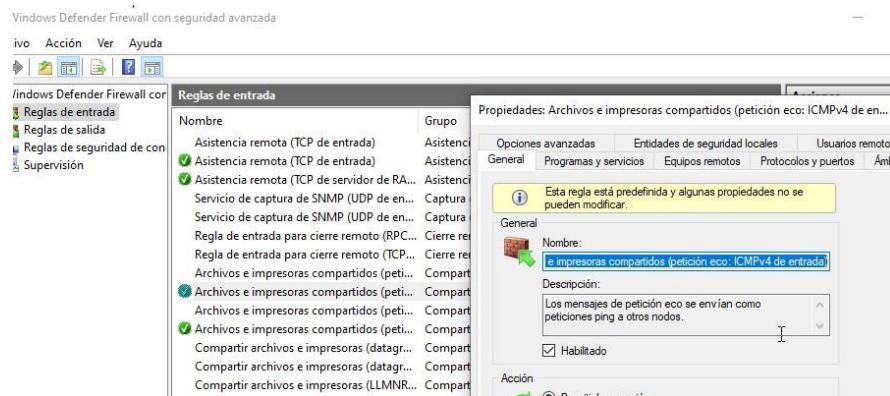
3)instalar el openSSH server en características opcionales de aplicaciones y características.

4)Windows+R he buscado services.msc que te abrirá la ventana de servicios y en propiedades de openSSh Server he iniciador el servicio , aplicar y aceptar.



5) no olvidar habilitar la regla de entrada de firewall de:

- Archivos e impresoras compartidos ICMPv4
- Archivos e impresoras compartidos ICMPv6
- Ambas en ámbito privado.*



Resultado:

```
Administrador: C:\Windows\system32\conhost.exe
Archivo Editar Ver Buscar Terminal Ayuda
daw2@daw2-10:~$ ssh -p 2222 servidor@localhost
servidor@localhost's password:

Microsoft Windows [Versión 10.0.19041.264]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

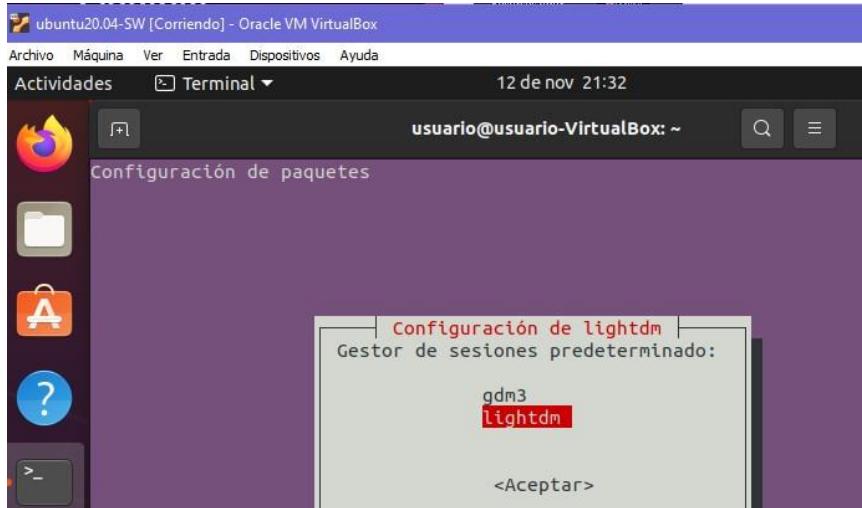
servidor@DESKTOP-V10ATG0 C:\Users\servidor>
```

- *Demuestra el acceso con algún cliente gráfico. Entre este apartado y el anterior asegúrate de haber hecho los 4 escenarios posibles (linux-linux, linux-windows, windows-linux, windows-windows)*

SERVIDOR LINUX:

En el servidor instalamos el gestor lightdm:

```
sudo apt install lightdm
```

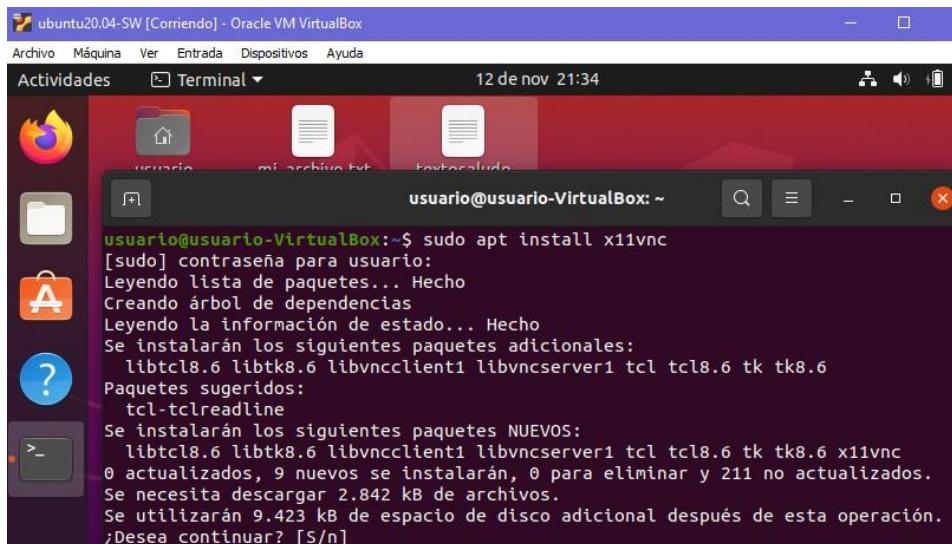


Reiniciamos el sistema:

```
sudo reboot
```

Instalamos x11vnc:

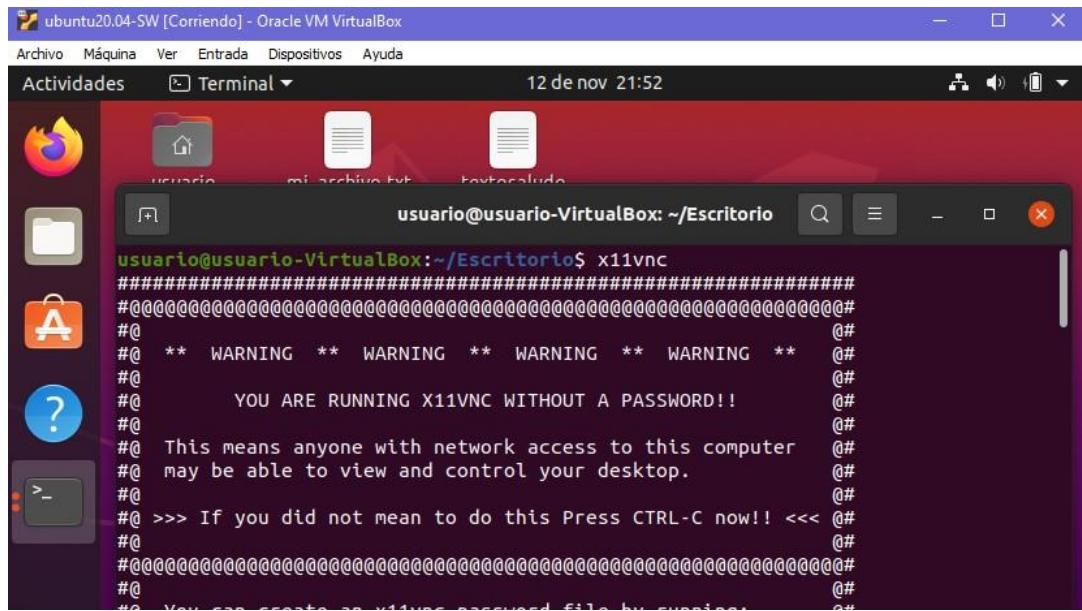
```
sudo apt install x11vnc
```



Algunas de las características de x11vnc son:

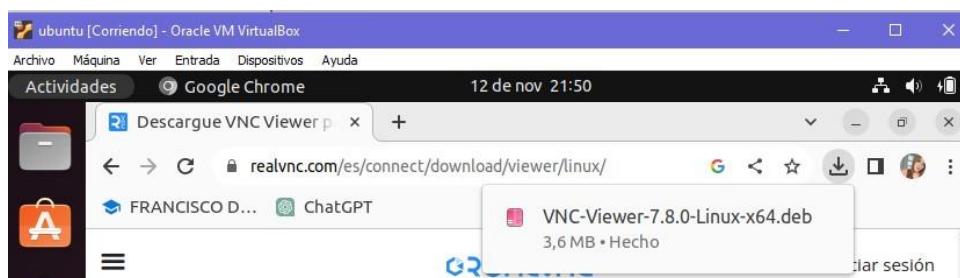
- Cuenta con cifrado SSL / TLS incorporado.
- Autenticación RSA de 2048 bits, incluida la compatibilidad con VeNCrypt.
- Soporte de inicio de sesión de cuenta y contraseña UNIX.
- Escalado del lado del servidor.
- HTTPS / HTTP + VNC de puerto único.
- Publicidad del servicio Zeroconf.
- Transferencia de archivos TightVNC y UltraVNC.
- Cuenta con un modo de Servicios de Terminal encriptado (opciones -create, -svc o -xdmsvc) basado en nombres de usuario.

E iniciamos x11vnc:

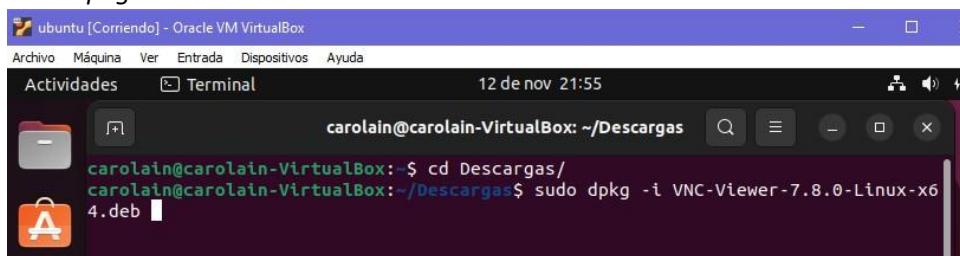


- Cliente Linux:

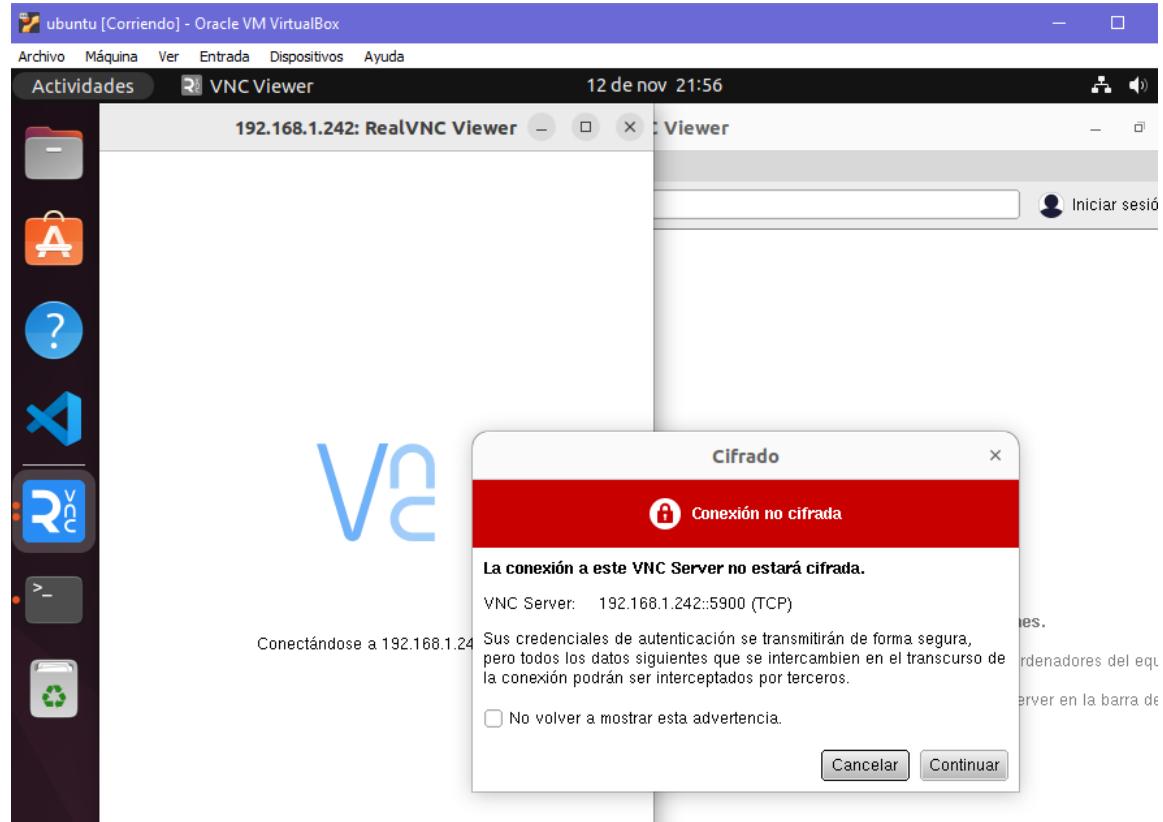
Nos descargamos vnc viewer:



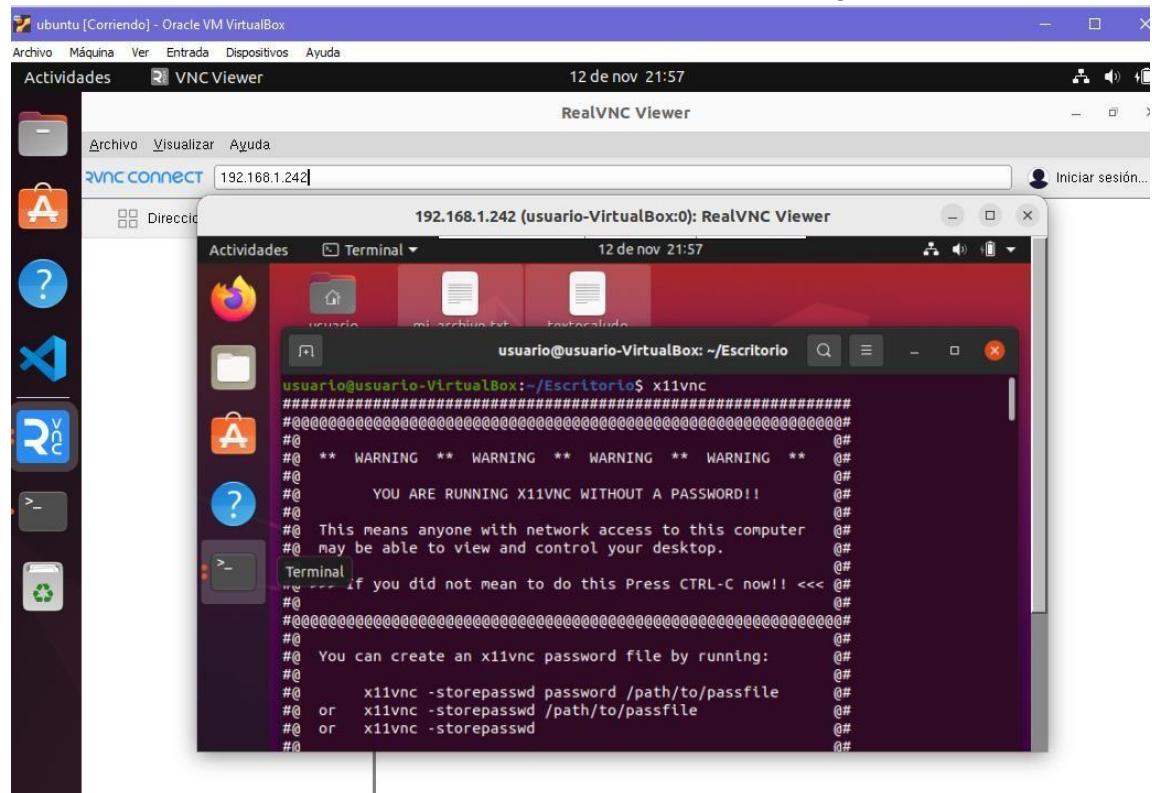
Sudo dpkg -i VNC-Viewer-7.8.0-Linux-x64.deb



Abrimos la aplicación y nos vamos al servidor 198.168.1.242, damos aceptar:



Como resultados nos aparecerá una ventana con la interfaz gráfica de servidor remoto:



- Cliente Windows:

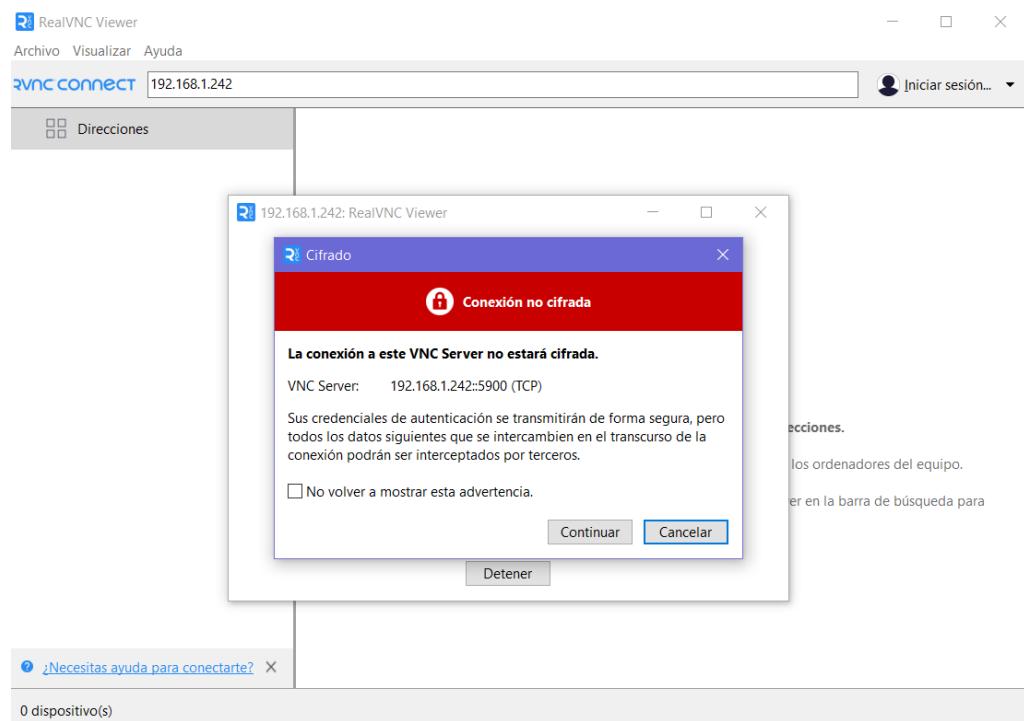
Instalamos



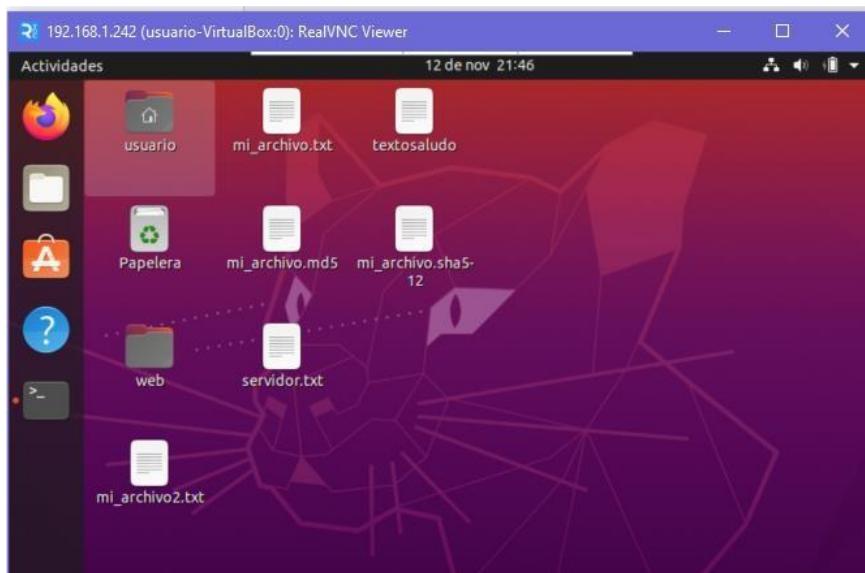
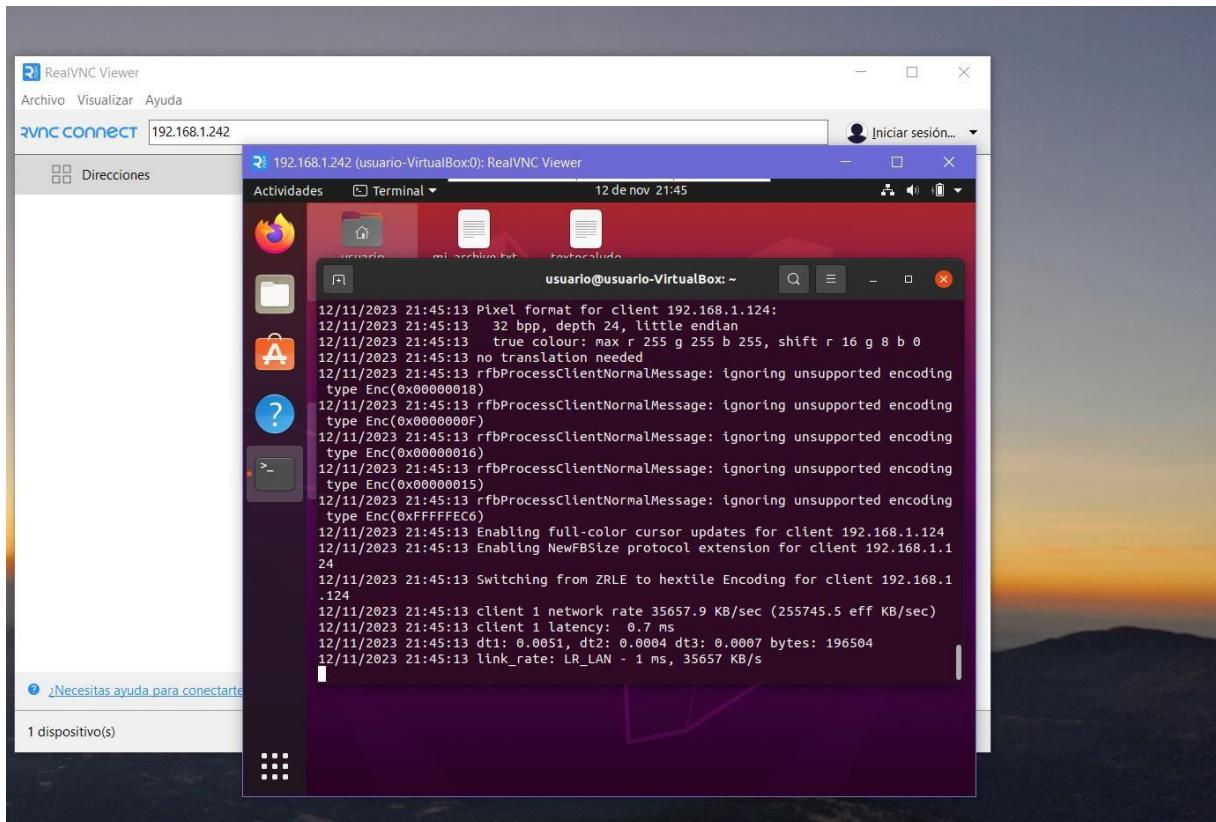
Nos metemos al servidor:



Le damos a aceptar:



Resultado: Nos abrirá una interfaz gráfica del servidor 192.168.1.242:



Bibliografía:

<https://www.solvetic.com/tutoriales/article/8924-instalar-vnc-en-ubuntu-2004-vnc-server/>

- **Demuestra el uso del comando scp para cargar o descargar archivos remotos o incluso pasarlos de una máquina remota a otra remota distinta.**

Copiar desde el sistema local a un sistema remoto:

`scp archivo_local.txt usuario@192.168.1.242:/home/usuario/`

Desde cliente:

- Creamos el archivo que se va a descargar en el servidor remoto.
- Copiamos el archivo al servidor remoto:

```
scp archivo_local.txt usuario@192.168.1.242:/home/usuario/
```

>cliente.txt' being run, followed by 'scp cliente.txt usuario@192.168.1.242:/home/usuario'. The password 'cliente.txt' is entered, and the transfer progress is shown as 100% at 40.1KB/s."/>

```
ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 21:03
carolain@carolain-VirtualBox:~/Escritorio$ echo "hola desde cliente">>cliente.txt
carolain@carolain-VirtualBox:~/Escritorio$ scp cliente.txt usuario@192.168.1.242:/home/usuario
usuario@192.168.1.242's password:
cliente.txt 100% 19 40.1KB/s 00:00
```

Verificamos en el servidor que se ha descargado el archivo cliente.txt

```
ubuntu20.04-SW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 21:05
usuario@usuario-VirtualBox:~/Escritorio$ cd /
usuario@usuario-VirtualBox:/$ cd ~
usuario@usuario-VirtualBox:~$ pwd
/home/usuario
usuario@usuario-VirtualBox:~$ cat cliente.txt
hola desde cliente
usuario@usuario-VirtualBox:~$
```

Copiar desde un sistema remoto al sistema local:

```
scp usuario@192.168.1.242:/home/usuario/Escritorio/servidor.txt
/home/carolain/Escritorio/
```

Desde el servidor:

- Creamos el archivo que va a ser descargado.

```
ubuntu20.04-SW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 21:07
usuario@usuario-VirtualBox:~$ cd Escritorio/
usuario@usuario-VirtualBox:~/Escritorio$ echo "hola desde servidor">> servidor.txt
```

Desde el cliente:

- Copiamos el archivo del servidor al cliente:

```
scp usuario@192.168.1.242:/home/usuario/Escritorio/servidor.txt /home/carolain/Escritorio/
```

```
ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 21:13
carolain@carolain-VirtualBox:~/Escritorio$ scp usuario@192.168.1.242:/home/usuario/Escritorio/servidor.txt /home/carolain/Escritorio/
usuario@192.168.1.242's password:
servidor.txt 100% 20 23.4KB/s 00:00
```

```
ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 21:14
carolain@carolain-VirtualBox: ~/Escritorio
carolain@carolain-VirtualBox:~/Escritorio$ cat servidor.txt
hola desde servidor
carolain@carolain-VirtualBox:~/Escritorio$
```

- Demuestra el uso similar a FTP mediante un cliente gráfico (Filezilla) y conexión sftp a tu servidor SSH.

En cliente linux:

Instalamos filezilla:

```
carolain@carolain-VirtualBox:~$ sudo apt install filezilla
[sudo] contraseña para carolain:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  libffi7
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
  filezilla-common libfilezilla-common libfilezilla24 libpugixml1v5
  libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
Se instalarán los siguientes paquetes NUEVOS:
  filezilla filezilla-common libfilezilla-common libfilezilla24 libpugixml1v5
  libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
0 actualizados, 7 nuevos se instalarán, 0 para eliminar y 14 no actualizados.
Se necesita descargar 10,1 MB de archivos.
Se utilizarán 36,9 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Y nos conectamos al servidor 192.168.1.242 en el puerto 22:

Servidor: sftp://usuario@192.168.1.242 Nombre de usuario: usuario Contraseña: Puerto: 22 Conexión rápida

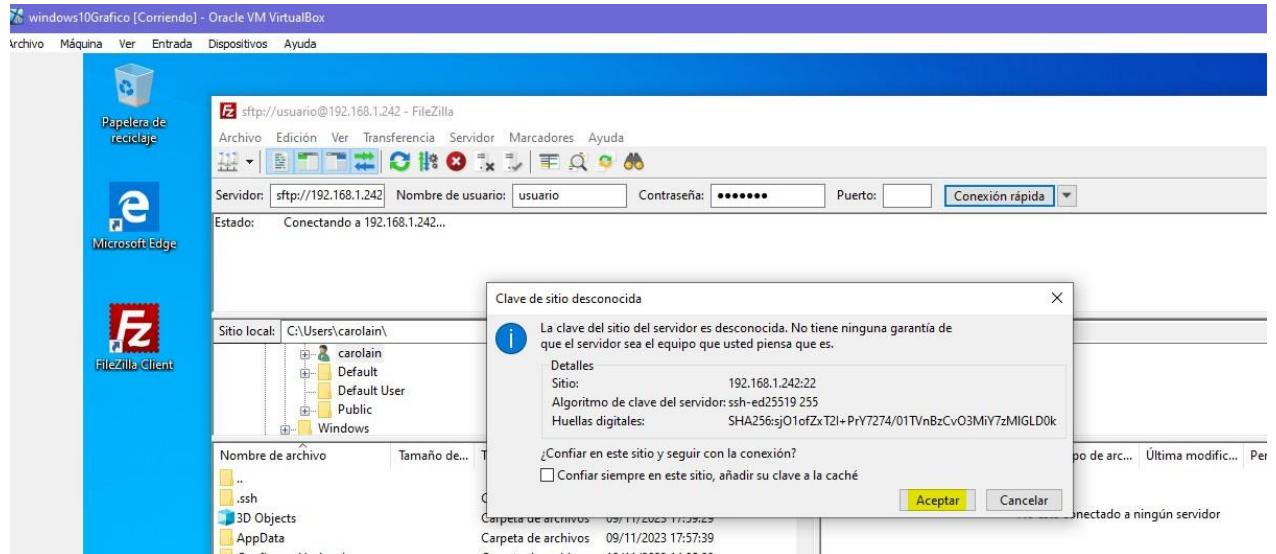
Estado: Conectando a 192.168.1.242...
Estado: Using username "usuario".
Estado: Connected to 192.168.1.242.
Estado: Recuperando el listado del directorio...
Estado: Listing directory /home/usuario
Estado: Directorio "/home/usuario" listado correctamente
Estado: Recuperando el listado del directorio "/home"...
Estado: Listino directorio /home

Nombre de archivo	Tamaño	Tipo de archivo	Última modificación	Permisos	Propietario
..					
.cache		Directorio	12/11/23 20:30...		
.config		Directorio	12/11/23 20:30...		
.dotnet		Directorio	09/10/23 23:32...		
web		Directorio	18/09/23 22...	drwxrwx...	usuario u.
textosaludo	28 B	Archivo	12/11/23 19...	-rw-rw-r-	usuario u.

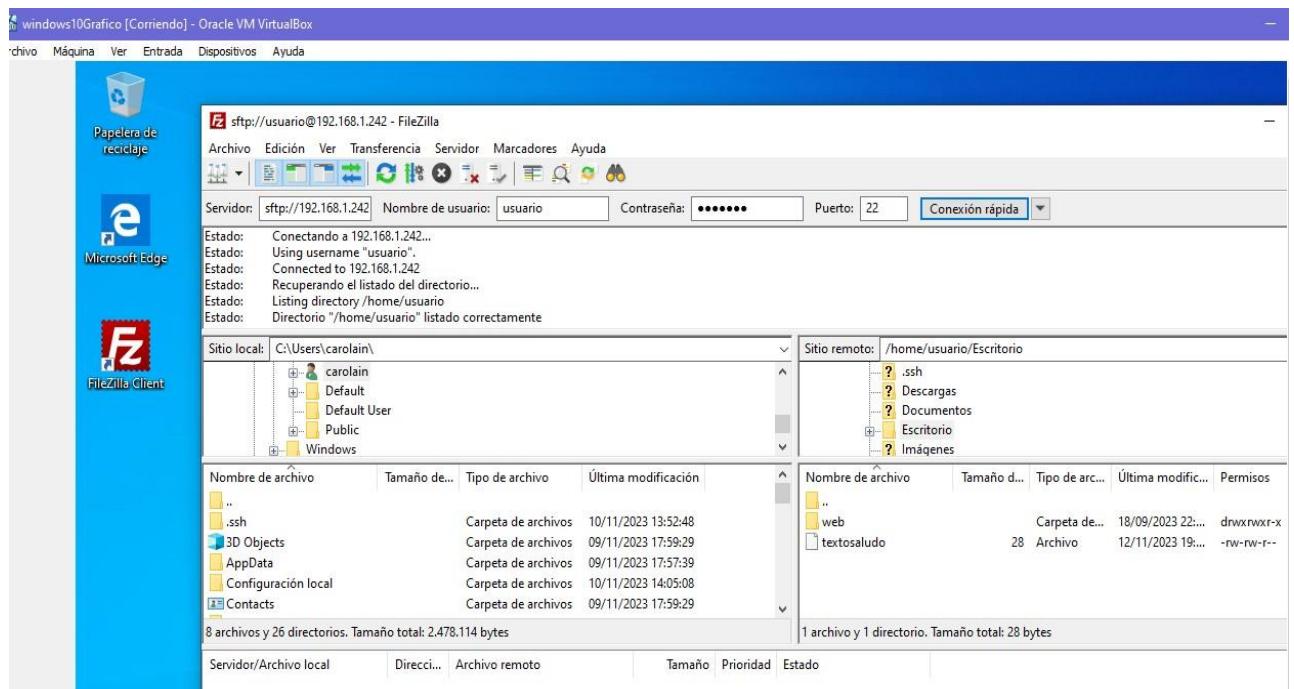
En cliente Windows:

Hacemos el mismo procedimiento en FileZilla servidor 192.168.1.242 y puerto 22.

Damos a aceptar que confiamos en el servidor.



Resultado:



- Opcional: crea en el servidor un fichero y genera un resumen con md5sum o sha512sum, verifica tras la descarga del fichero que el re-cálculo del resumen coincide con el resumen bajado del servidor.**

Con sha512sum:

- un archivo llamado mi_archivo.txt con el contenido especificado

```
echo "Contenido del archivo" > mi_archivo.txt
```

- un archivo llamado **mi_archivo.sha512** que contiene el hash SHA-512 del archivo:

```
sha512sum mi_archivo.txt > mi_archivo.sha512
```

- Verificación del resumen después de la descarga:

```
sha512sum -c mi_archivo.sha512
```

Con md5sum:

- un archivo llamado **mi_archivo2.txt** con el contenido especificado

```
echo "Contenido del archivo" > mi_archivo2.txt
```

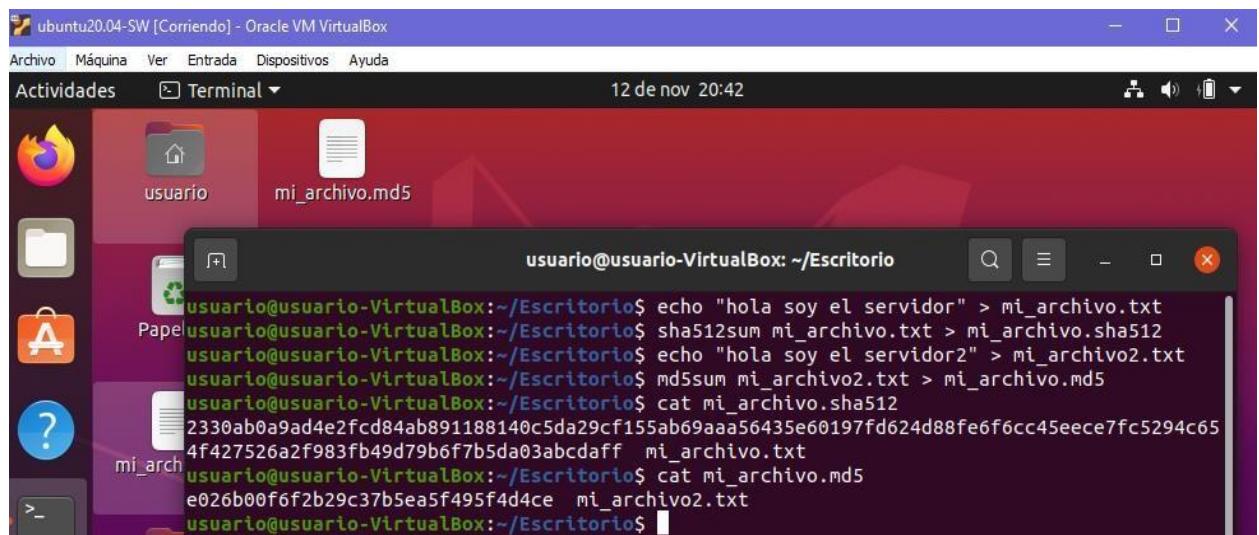
- un archivo llamado **mi_archivo.md5** que contiene el hash MD5 del archivo:

```
md5sum mi_archivo.txt > mi_archivo.md5
```

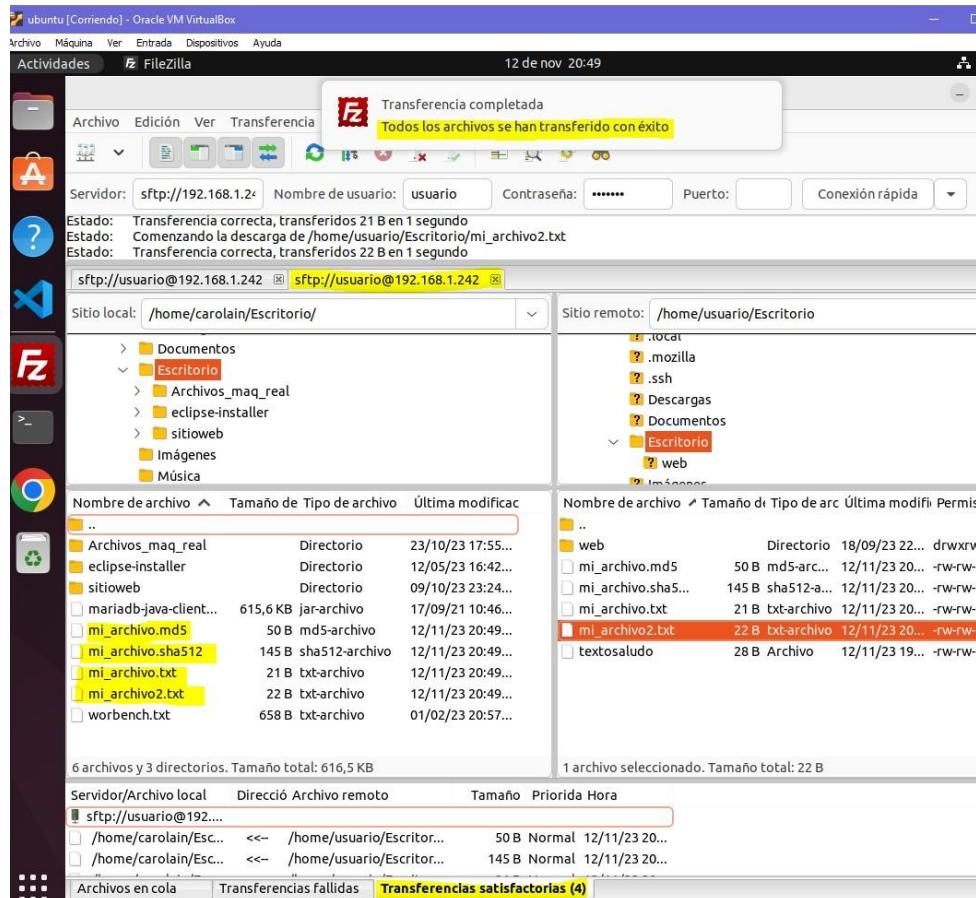
- Verificación del resumen después de la descarga:

```
md5sum -c mi_archivo.md5
```

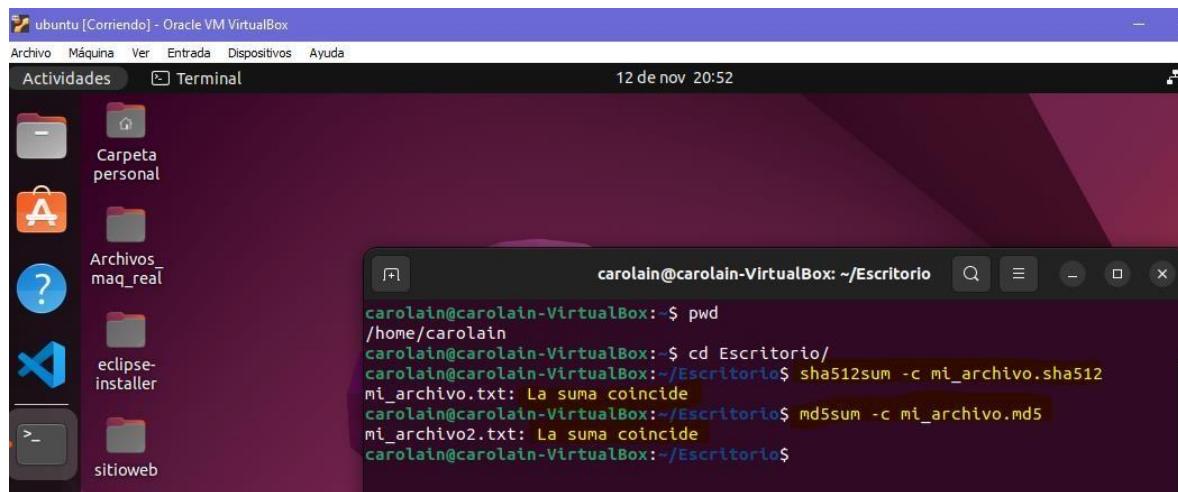
Creo en el servidor los archivos:



En el cliente me descargo los ficheros correspondientes:

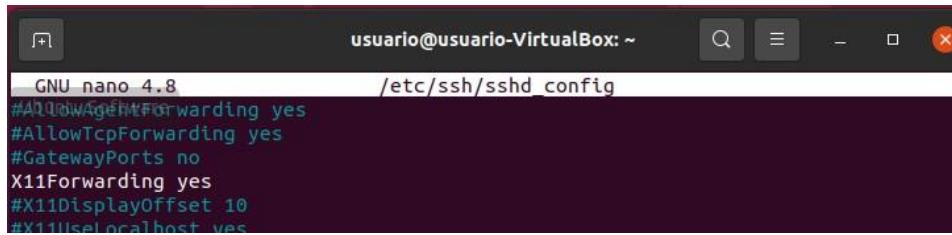


Hago las verificaciones correspondientes:



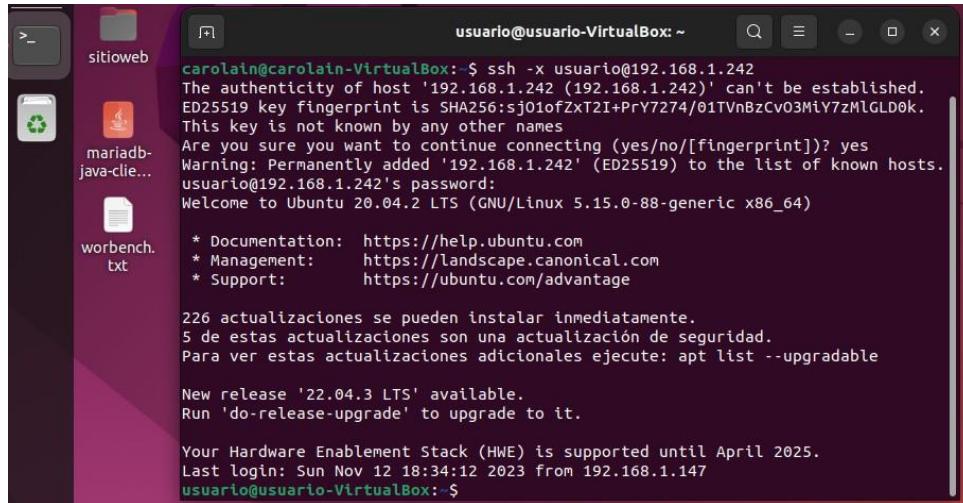
- Opcional: ilustra entre máquinas GNU/Linux la transmisión del GUI mediante ssh -X avanzado, opcional ¿funciona bajo WSL?

Verificamos que el servidor ssh tiene en yes el parametro x11Forwarding:



```
GNU nano 4.8
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
```

Nos conectamos mediante ssh -x usuario@192.168.1.242



```
carolain@carolain-VirtualBox:~$ ssh -x usuario@192.168.1.242
The authenticity of host '192.168.1.242 (192.168.1.242)' can't be established.
ED25519 key fingerprint is SHA256:sj01ofZxT2I+PrY7274/01TVnBzCv03M1Y7zMlGLD0k.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.242' (ED25519) to the list of known hosts.
usuario@192.168.1.242's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

226 actualizaciones se pueden instalar inmediatamente.
5 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

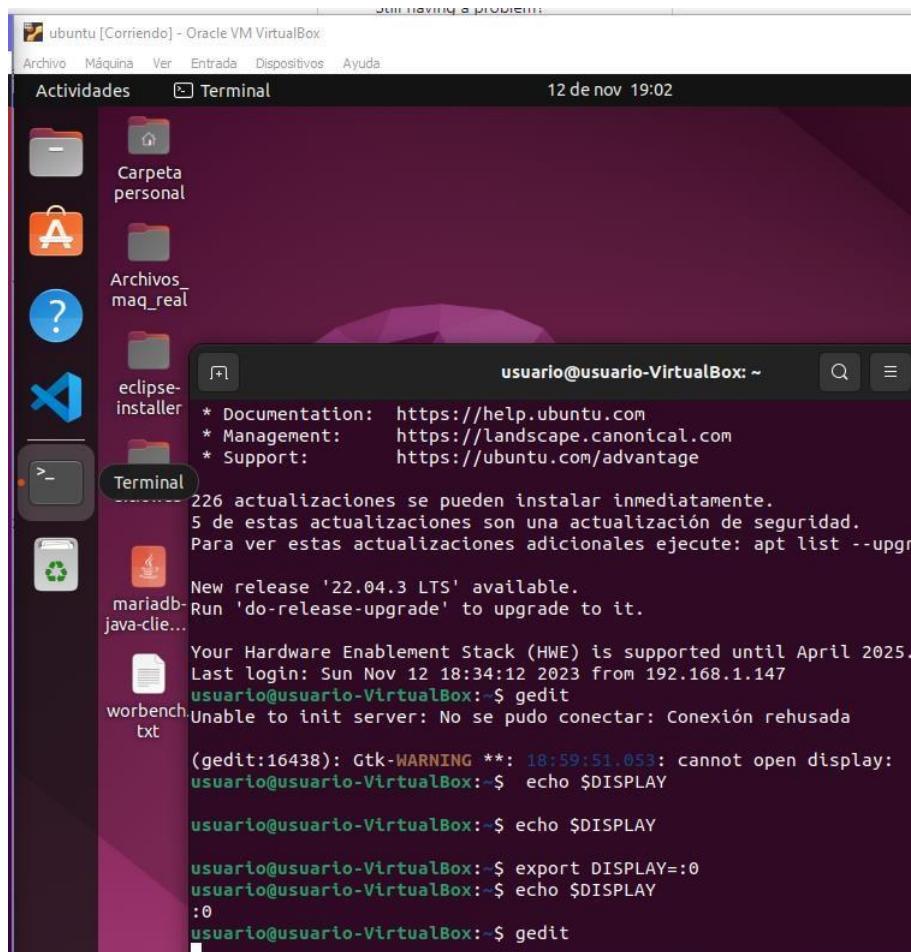
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Nov 12 18:34:12 2023 from 192.168.1.147
usuario@usuario-VirtualBox: $
```

Intenté abrir gedit pero me dió un problema sobre DISPLAY. La primera solución fue aplicar el siguiente comando:

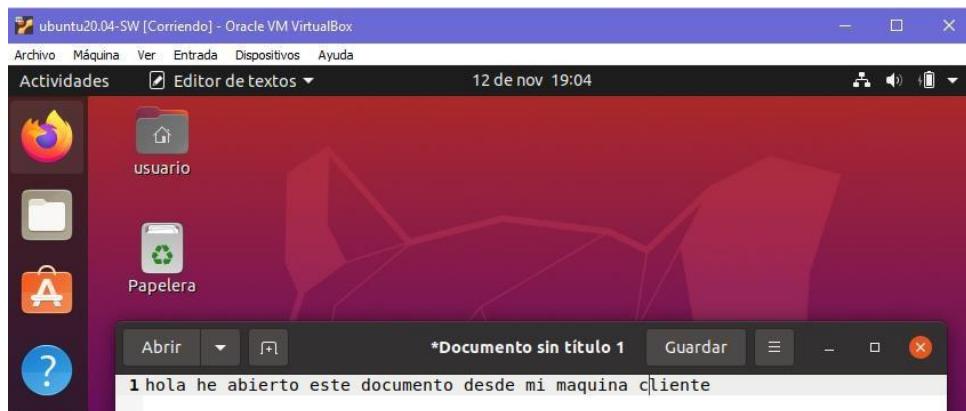
Export DISPLAY=:0

Y con ello conseguí abrir gedit en el servidor.

Máquina del cliente:



Máquina del servidor:

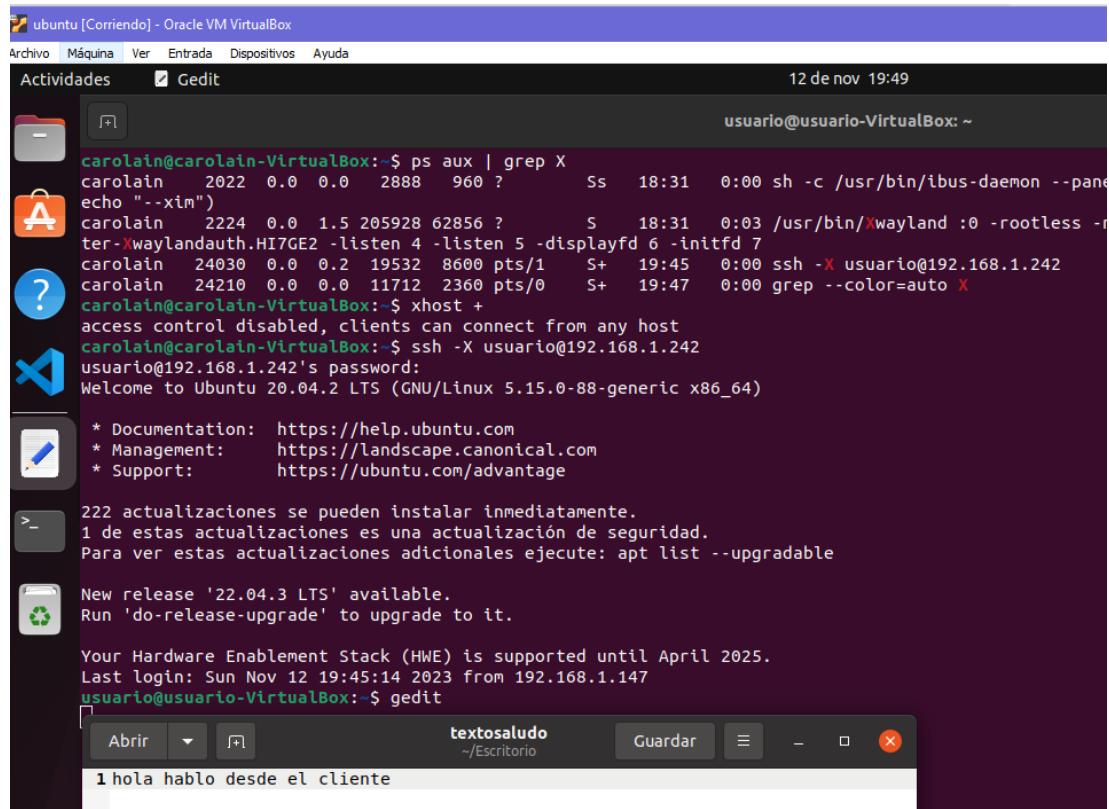


Como segunda solución para poder abrir la aplicación desde la maquina local tuve que utilizar el comando siguiente:

xhost + (desactiva la seguridad del servidor X temporalmente).

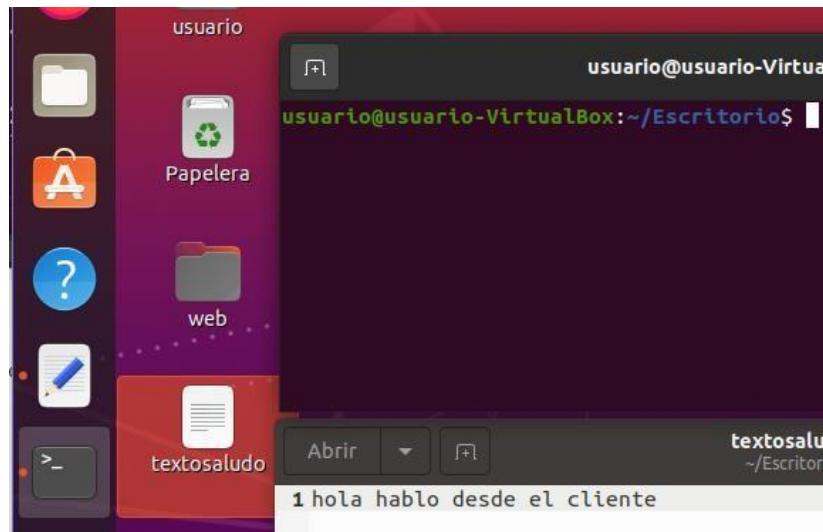
Con ello conseguí abrir gedit en el cliente conectado desde ssh a la maquina remota.

Maquina cliente:



Máquina de servidor:

Aquí podemos comprobar el archivo creado con el mensaje desde la maquina local y la aplicación gráfica gedit.



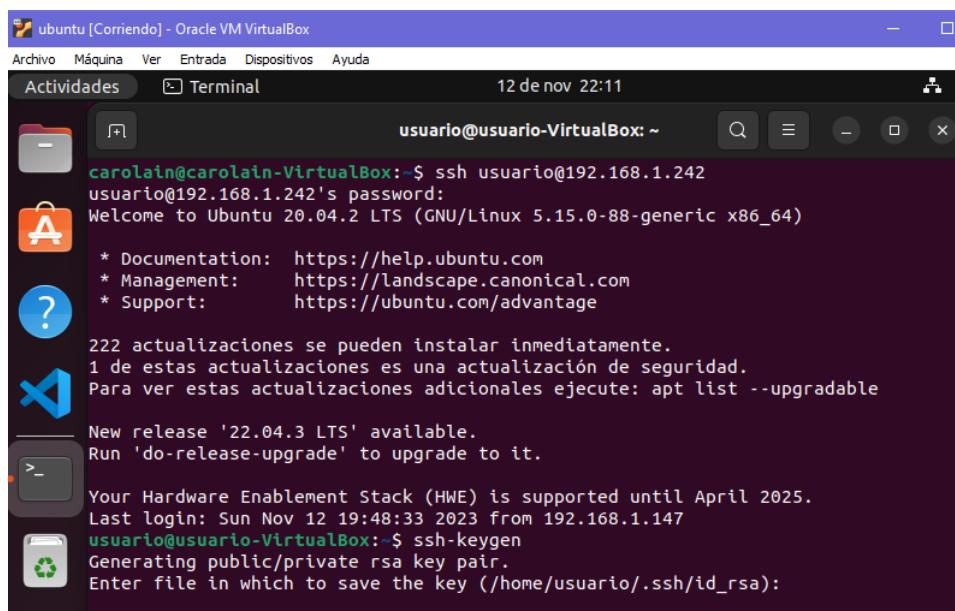
- Crea el par de clave pública/privada para un usuario y demuestra el acceso al servidor remoto basándose en dicha clave sin necesidad de proporcionar usuario/contraseña.**

En cliente linux:

Nos metemos al usuario:usuario en el servidor remoto 192.168.1.242

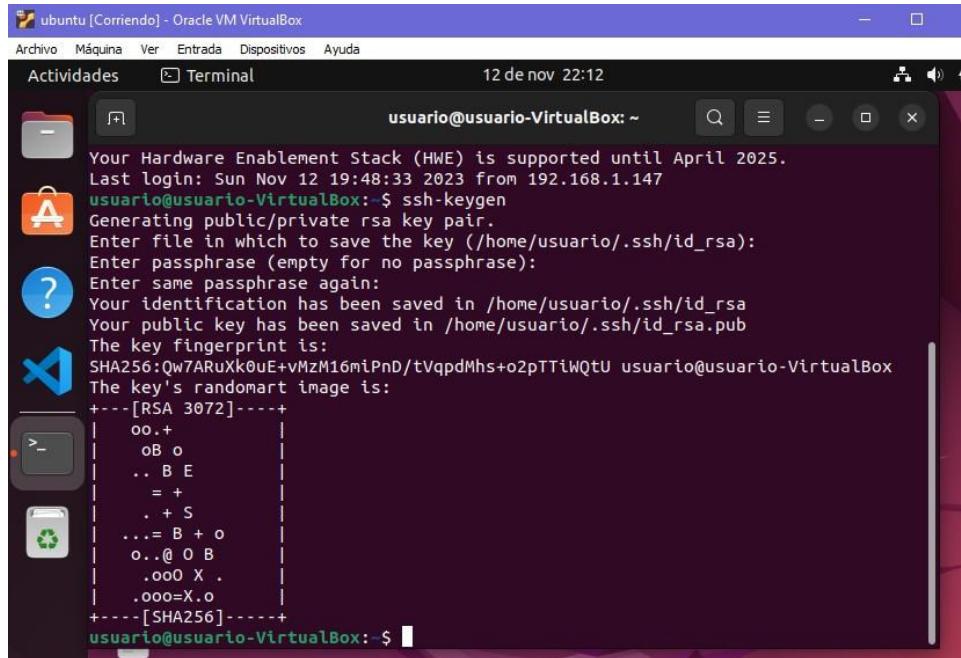
Generamos las claves pública y privada:

```
ssh-keygen -t rsa
```



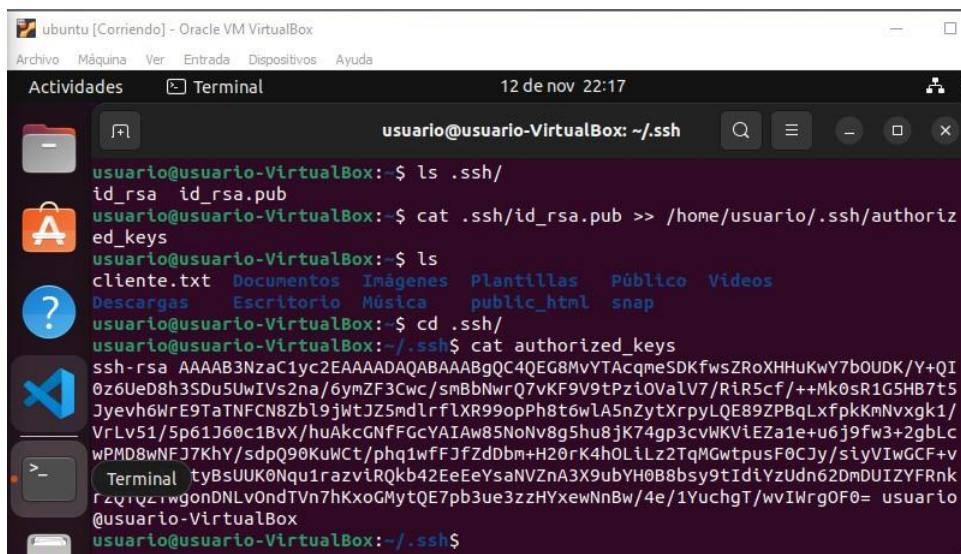
Introducimos una frase de paso para nuestra llave, en este caso es:

Passphrase: "contraseña"



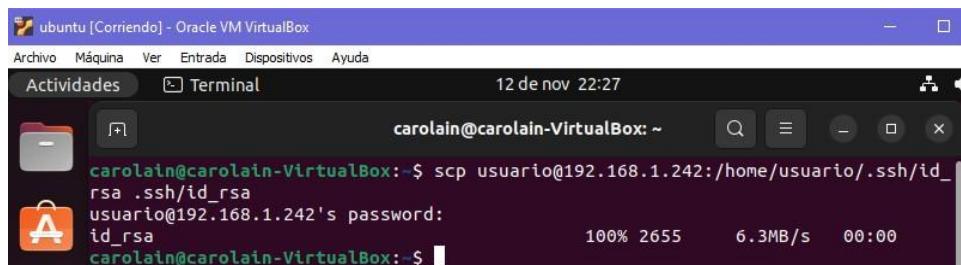
```
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Nov 12 19:48:33 2023 from 192.168.1.147
usuario@usuario-VirtualBox:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_rsa
Your public key has been saved in /home/usuario/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Qw7ARuXk0E+vMzM16mtPnD/tVqpdMhs+o2pTTtWQtU usuario@usuario-VirtualBox
The key's randomart image is:
+---[RSA 3072]---+
| oo.+ |
| oB o |
| .. B E |
| = + |
| . + S |
| ...= B + o |
| o...@ O B |
| .ooO X . |
| .ooo=X.o |
+---[SHA256]---+
usuario@usuario-VirtualBox:~$
```

Guardamos el contenido de la llave privada en authorized_keys:



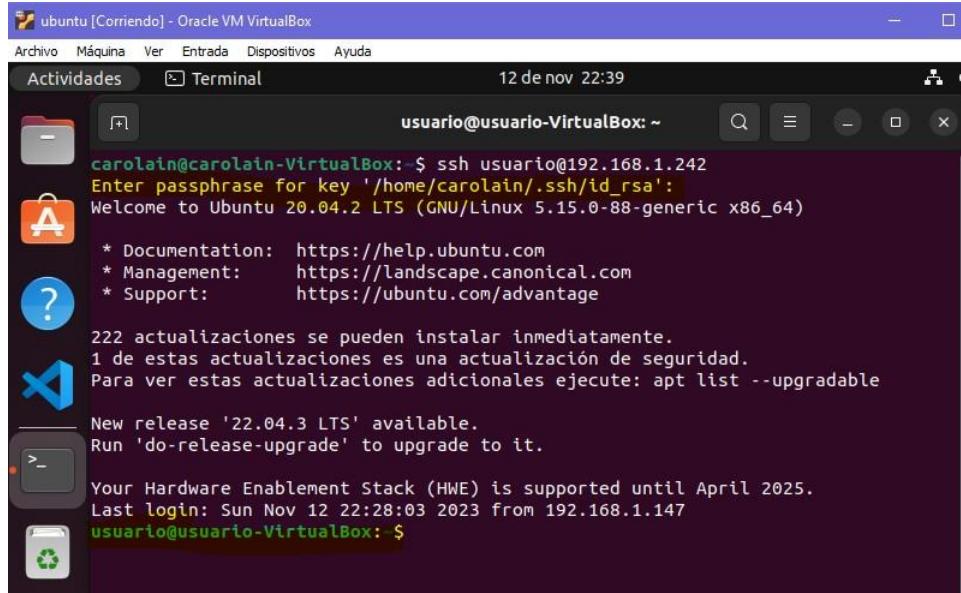
```
ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 22:17
usuario@usuario-VirtualBox:~/ssh
id_rsa id_rsa.pub
usuario@usuario-VirtualBox:~$ cat .ssh/id_rsa.pub >> /home/usuario/.ssh/authorized_keys
usuario@usuario-VirtualBox:~$ ls
cliente.txt Documentos Imágenes Plantillas Público Videos
Descargas Escritorio Música public_html snap
usuario@usuario-VirtualBox:~$ cd .ssh/
usuario@usuario-VirtualBox:~/ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQBgQC40EG8MvYTAcqmeSDKfwzRoXHuKwY7b0UDK/Y+QI
0z6UeD8h3SDu5UwIVs2na/6ymZF3Cwc/smBbNwrQ7vKF9V9tPzi0ValV7/RiR5cf/++Mk0sR1G5Hb7t5
Jyevh6WrE9TaNFCN8Zb19jWtJ25mdlrfIxr99opPh8t6wlA5nZytXrpyLQE89ZPBqlLxfpkKmNvxgk1/
VrLv51/5p61J60c1BvX/huAkGNGcYAIAw85NoNv8gShu8jK74gp3cvWKViEza1+u6j9fw3+2gbLc
wPMD8wNFJ7KhY/sdpQ90KuWct/phq1wfFJfZdDbm+H20rK4h0LiLz2TqMGwtppusF0CJy/siyVIwGCF+v
Terminal tyBsUUK0Nqu1azviRQkb42EeEeYsaNVZnA3X9ubYH0B8bsy9Id1yzUdn62DmDUIZYFRnk
rzq1qrwgonDNLw0ndTVn7hKxoGMytQE7pb3ue3zzHYxewNnBw/4e/1YuchgT/wvIWrg0F0= usuario
@usuario-VirtualBox
usuario@usuario-VirtualBox:~/ssh$
```

Copiamos la llave privada en nuestra maquina local en .ssh/id_rsa



```
ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 22:27
carolain@carolain-VirtualBox:~$ scp usuario@192.168.1.242:/home/usuario/.ssh/id_
rsa .ssh/id_rsa
usuario@192.168.1.242's password:
id_rsa
100% 2655      6.3MB/s   00:00
carolain@carolain-VirtualBox:~$
```

Iniciamos el servicio ssh y nos pedirá la frase de paso “contraseña” :



```
ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 22:39
usuario@usuario-VirtualBox: ~
carolain@carolain-VirtualBox: $ ssh usuario@192.168.1.242
Enter passphrase for key '/home/carolain/.ssh/id_rsa':
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

222 actualizaciones se pueden instalar inmediatamente.
1 de estas actualizaciones es una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

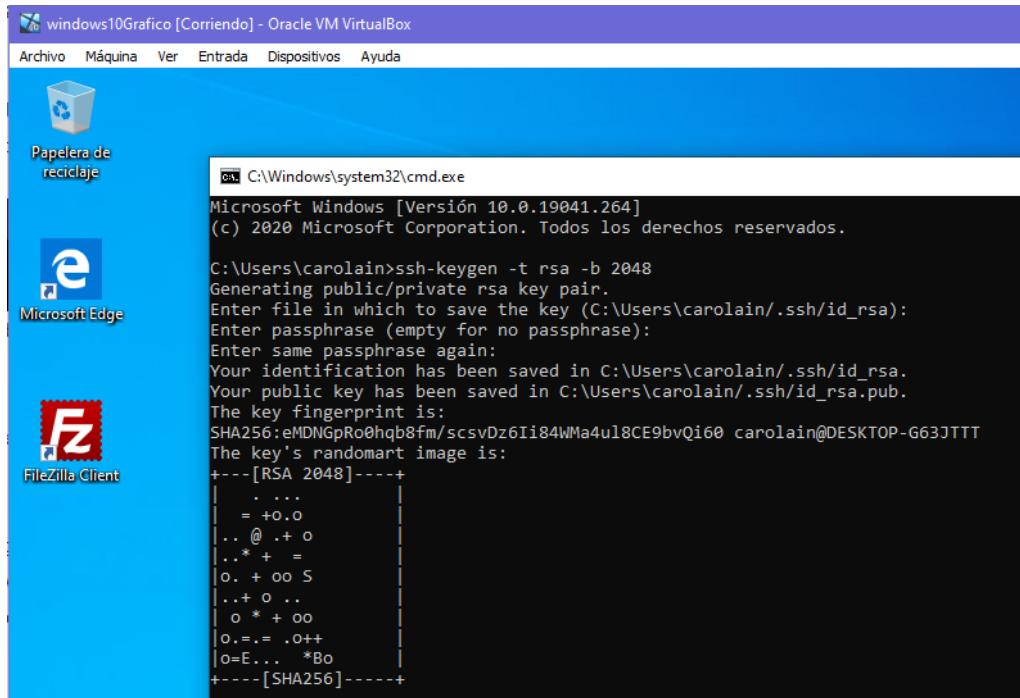
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Nov 12 22:28:03 2023 from 192.168.1.147
usuario@usuario-VirtualBox:~$
```

En cliente Windows:

Generamos las llaves pública y privada:

```
ssh-keygen -t rsa -b 2048
```

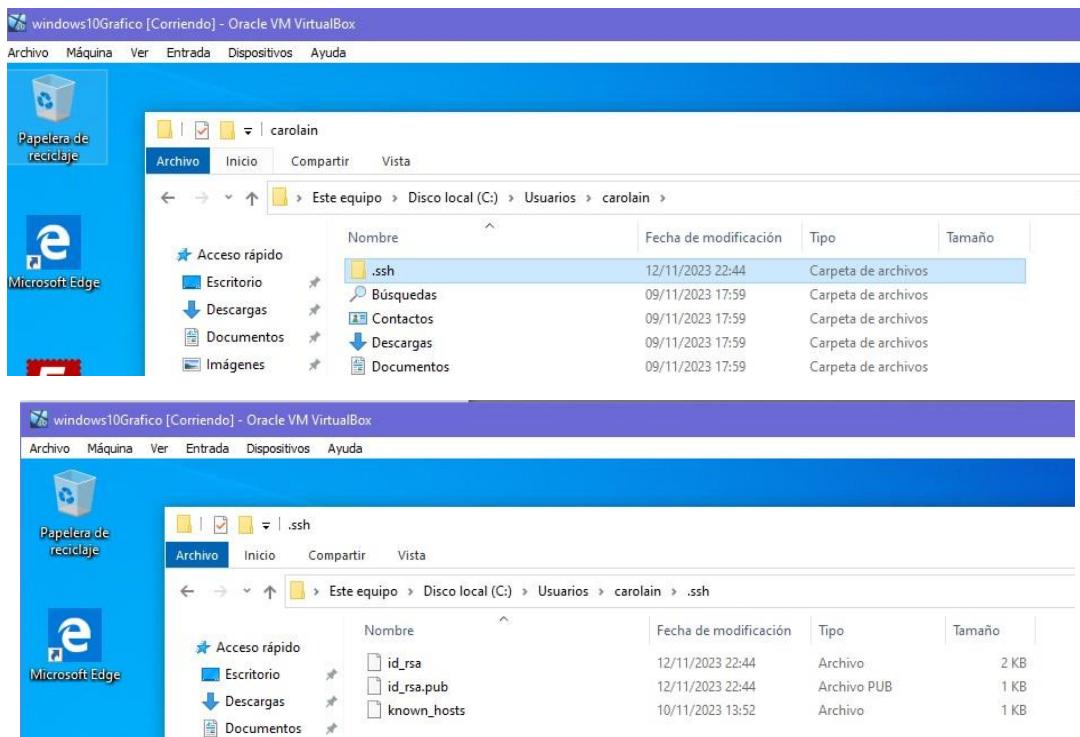
Con frase de paso “contraseña”



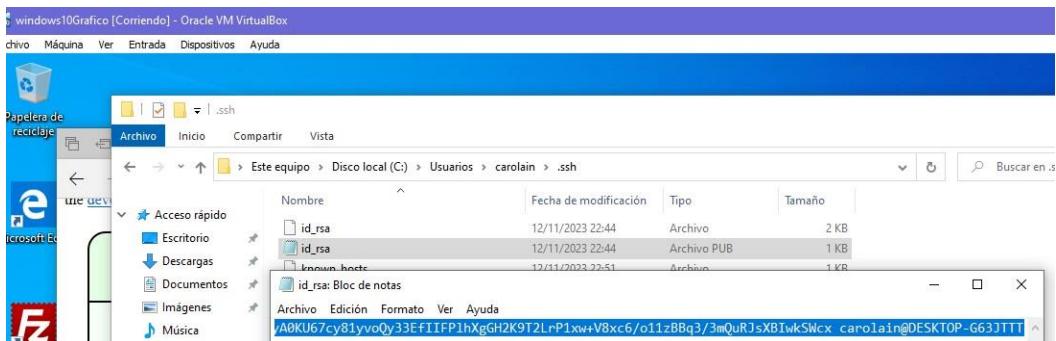
```
windows10Grafico [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje Microsoft Edge FileZilla Client
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19041.264]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\carolain>ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\carolain/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\carolain/.ssh/id_rsa.
Your public key has been saved in C:\Users\carolain/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:emDNGpRo0hqb8fm/scsvDz6Ii84WMa4u18CE9bvQ160 carolain@DESKTOP-G63JTTT
The key's randomart image is:
+---[RSA 2048]---+
|   . ...
|   = + o o
|... @ . + o
|... * + =
|o. + oo S
|... + o ...
| o * + oo
|o.= .o+o
|o=E... *Bo
+---[SHA256]---+
```

Podemos ver que se ha creado la carpeta .ssh en el usuario carolain y dentro las llaves:

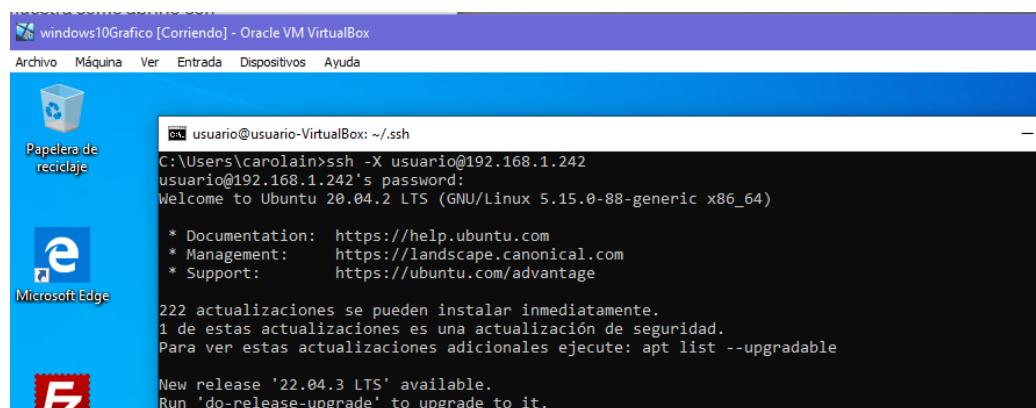


Copiamos la llave pública:



Para guardar la clave publica en el servidor remoto nos conectamos a él mediante ssh:

`ssh -X usuario@192.168.1.242`

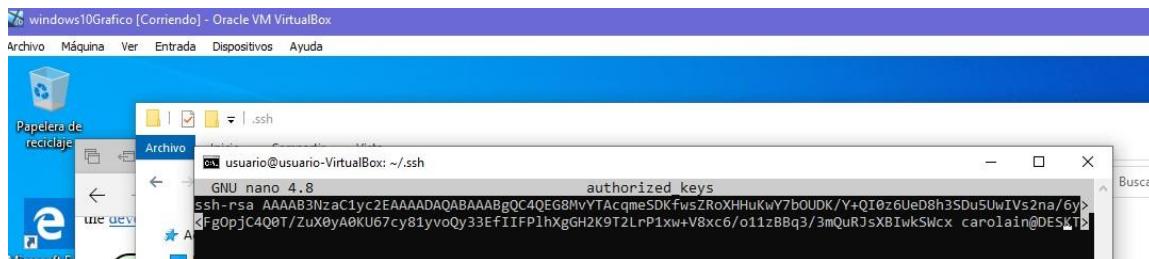


Lo guardamos en el fichero authorized_keys:

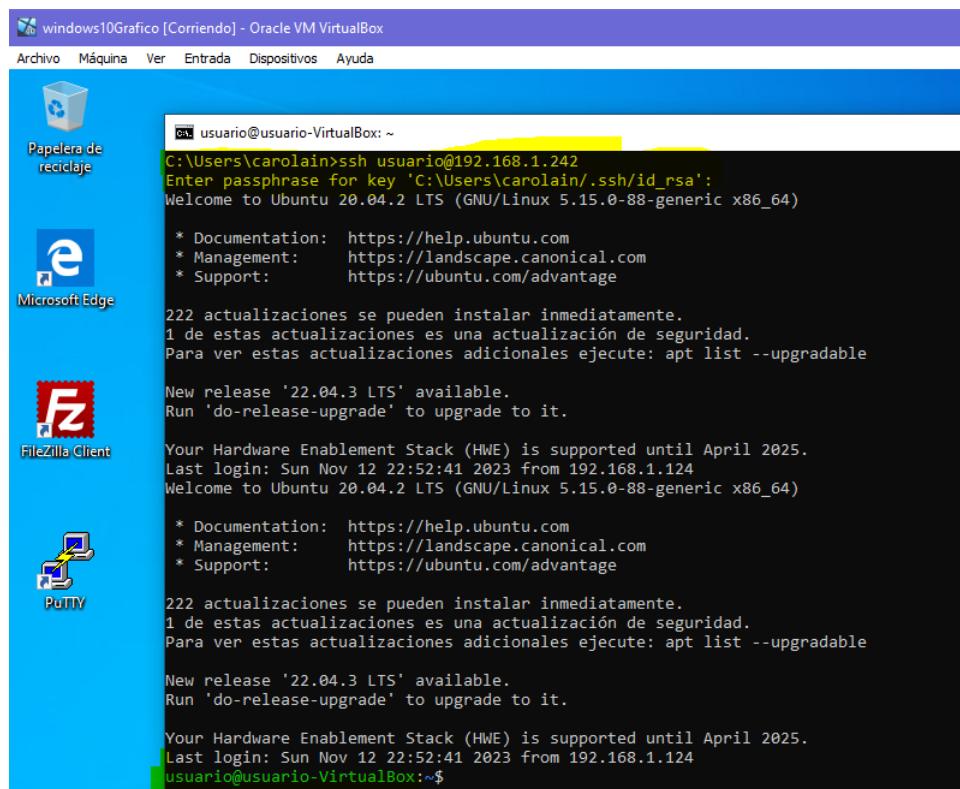
```
sudo nano authorized_key
```

```
usuario@usuario-VirtualBox:~/.ssh$ sudo nano authorized_keys
[sudo] contraseña para usuario:

usuario@usuario-VirtualBox:~/.ssh$ usuario@usuario-VirtualBox:~/.ssh$ sudo chmod 700 *
usuario@usuario-VirtualBox:~/.ssh$ sudo chmod 600 authorized_keys
usuario@usuario-VirtualBox:~/.ssh$
```



Como resultado nos volveremos a conectar con ssh a usuario@192.168.1.242 y nos pedirá la frase de paso. Ya no la contraseña de usuario.



- Localiza en Windows y en GNU/Linux si queda algún registro de las conexiones realizadas por SSH.

En Servidor Linux:

- En sistemas como Ubuntu, podemos encontrar información en /var/log/auth.log:

```
grep sshd /var/log/auth.log
```

```

ubuntu20.04-SW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 20:08
usuario@usuario-VirtualBox:~$ grep sshd /var/log/auth.log
Nov 12 18:34:12 usuario-VirtualBox sshd[3173]: Accepted password for usuario from
192.168.1.147 port 41827 ssh2
Nov 12 18:34:12 usuario-VirtualBox sshd[3173]: pam_unix(sshd:session): session ope
ned for user usuario by (uid=0)
Nov 12 18:49:57 usuario-VirtualBox sudo:  usuario : TTY=pts/0 ; PWD=/home/usuario
; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
Nov 12 18:57:39 usuario-VirtualBox sshd[3173]: pam_unix(sshd:session): session clo
sed for user usuario
Nov 12 18:58:50 usuario-VirtualBox sshd[14014]: Accepted password for usuario from
192.168.1.147 port 37446 ssh2
Nov 12 18:58:50 usuario-VirtualBox sshd[14014]: pam_unix(sshd:session): session op
ened for user usuario by (uid=0)
Nov 12 19:12:15 usuario-VirtualBox sshd[14297]: Received disconnect from 192.168.1
.147 port 37446:11: disconnected by user
Nov 12 19:12:15 usuario-VirtualBox sshd[14297]: Disconnected from user usuario 192
.168.1.147 port 37446
Nov 12 19:12:15 usuario-VirtualBox sshd[14014]: pam_unix(sshd:session): session cl
osed for user usuario
Nov 12 19:13:16 usuario-VirtualBox sshd[16525]: pam_unix(sshd:auth): authenticatio
n failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.147 user=usuario
Nov 12 19:13:17 usuario-VirtualBox sshd[16525]: Failed password for usuario from 1

```

- Podemos revisar los últimos inicios de sesión utilizando el comando last:

```

ubuntu20.04-SW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 20:02
usuario@usuario-VirtualBox:~/Escritorio
usuario@usuario-VirtualBox:~/Escritorio$ last
usuario pts/2      192.168.1.147  Sun Nov 12 19:48 - 19:56  (00:08)
usuario pts/0      192.168.1.147  Sun Nov 12 19:45 - 19:56  (00:11)
usuario pts/0      192.168.1.147  Sun Nov 12 19:43 - 19:45  (00:02)
usuario pts/0      192.168.1.147  Sun Nov 12 19:27 - 19:43  (00:16)
usuario pts/0      192.168.1.147  Sun Nov 12 19:13 - 19:26  (00:13)
usuario pts/1      192.168.1.147  Sun Nov 12 18:58 - 19:12  (00:14)
usuario pts/1      192.168.1.147  Sun Nov 12 18:34 - 18:57  (00:23)

```

- Explora brevemente el fichero de configuración del servidor y comenta las directivas que te llamen la atención.

Los que más nos ha llamado la atención son:

Port (22): Especifica el puerto en el que el servidor SSH escucha las conexiones.

PermitRootLogin: Determina si se permite o no que el usuario root inicie sesión a través de SSH.

PasswordAuthentication: Controla si se permite la autenticación por contraseña.

LogLevel: Establece el nivel de detalle de los mensajes de registro.

UsePAM: Controla si el servidor SSH utiliza el módulo Pluggable Authentication Modules (PAM).

X11Forwarding: Permite o deshabilita el reenvío de X11 (gráficos) a través de la conexión SSH.

```

ubuntu20.04-SW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 12 de nov 20:20
Navegador web Firefox usuario@usuario-VirtualBox: ~
GNU nano 4.8 /etc/ssh/sshd_config
Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

```

```

usuario@usuario-VirtualBox: ~
GNU nano 4.8 /etc/ssh/sshd_config
# PAM authentication via ChallengeResponseAuthentication
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

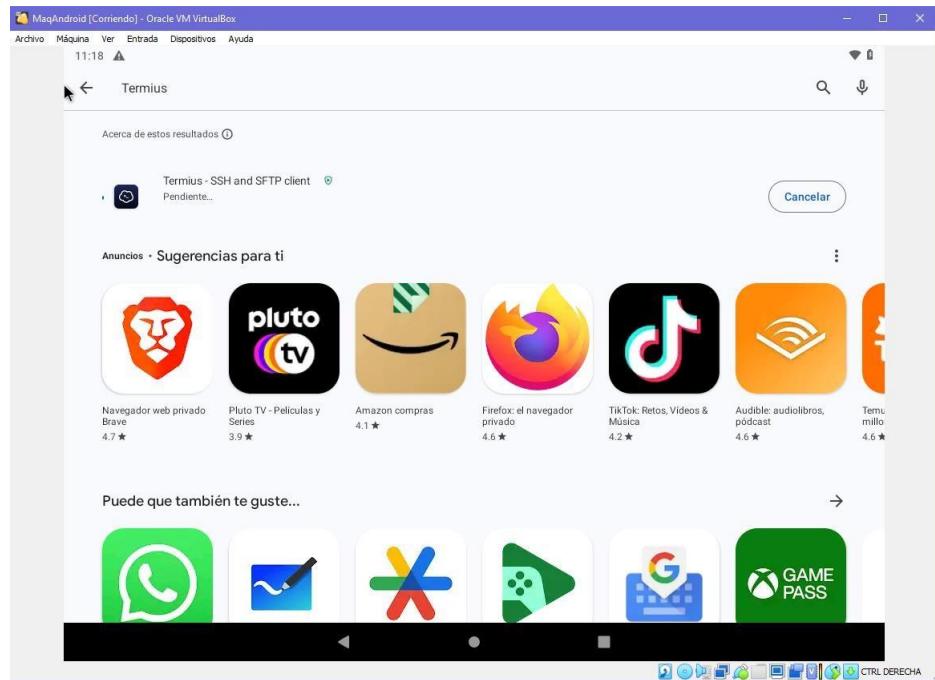
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes

```

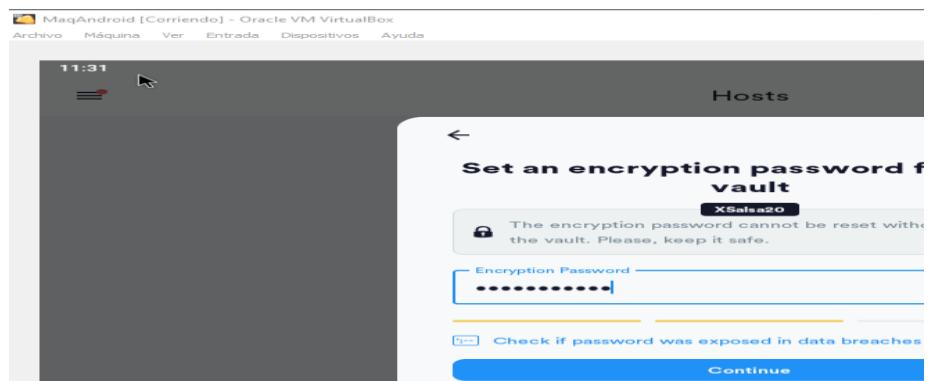
3.- Opcional: explora clientes y servidores de SSH en Android y demuestra su uso.

Cliente SSH (Termius):

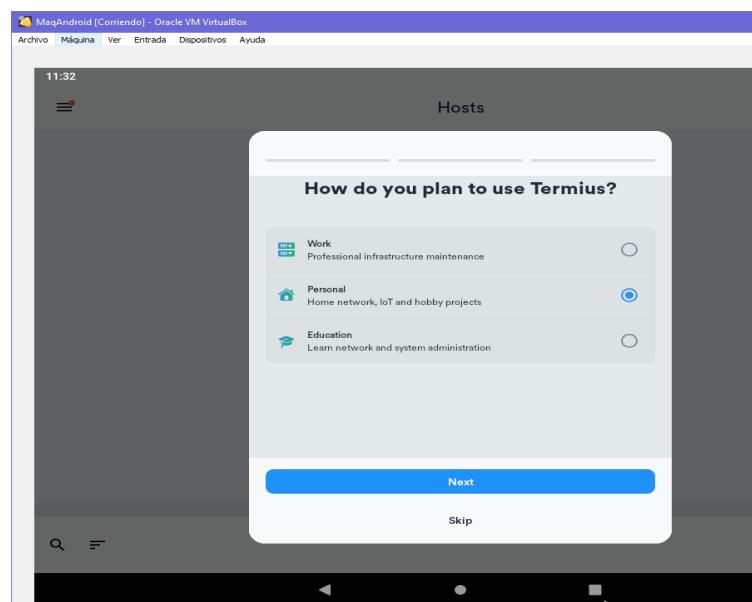
En mi máquina virtual android instalo un cliente SSH como Termius:



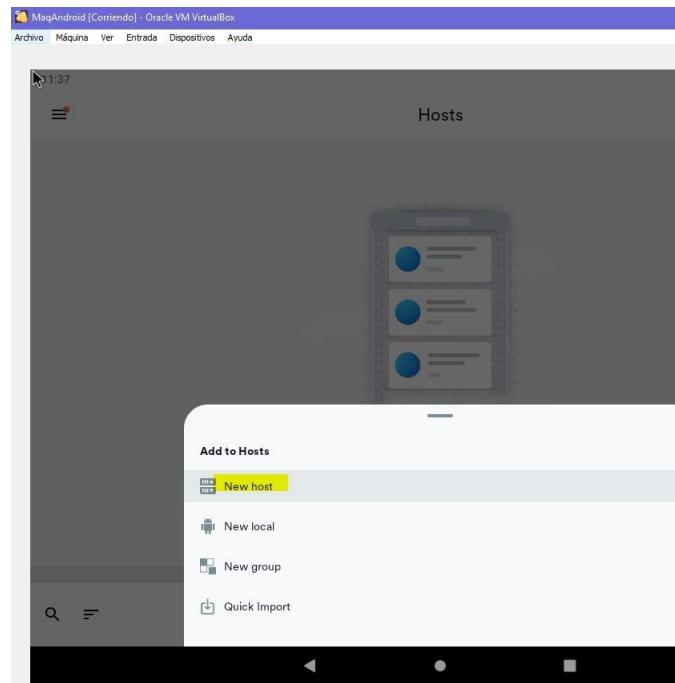
Creo una contraseña para mi nueva cuenta de Termius:



Selecciono uso personal y sigo los pasos:



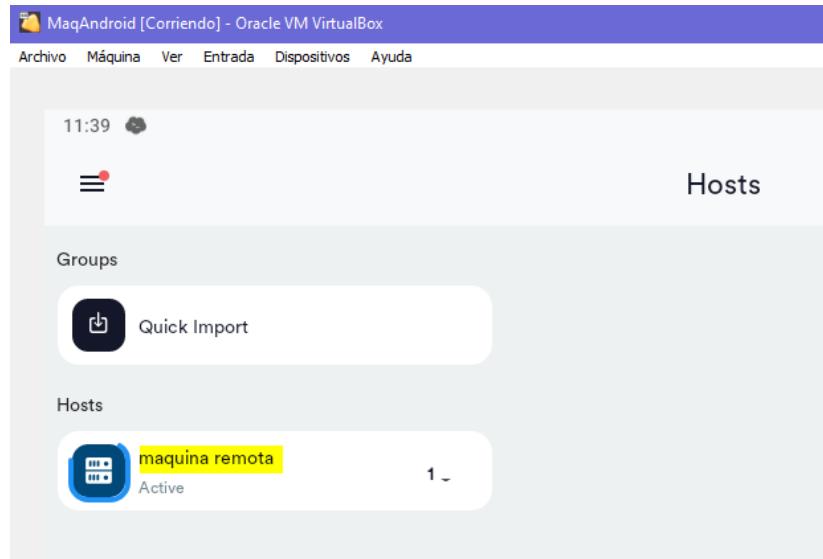
Creo un nuevo Host:



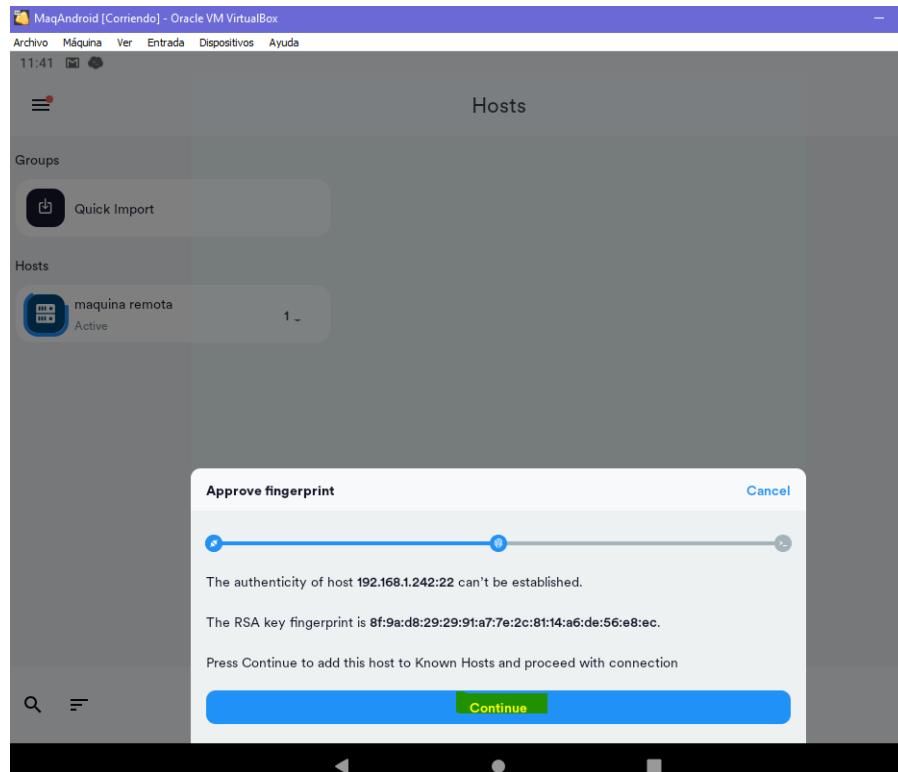
Realizo las configuraciones pertinentes para conectarme al servidor:

Two screenshots of the 'New host' configuration dialog in Oracle VM VirtualBox Manager. The top screenshot shows the 'New host' configuration page with fields for 'Alias' (set to 'maquina remota') and 'Hostname or IP Address' (set to '192.168.1.242'). The bottom screenshot shows the 'SSH' configuration page, where 'SSH' is checked (indicated by a blue checkmark), 'Port' is set to '22', 'Username' is set to 'usuario', and 'Password' is masked with dots. There are also 'Mosh' and 'Learn more...' options, and icons for 'Group' and 'Tags'.

Nos conectamos al servidor haciendo clic en maquina remota:

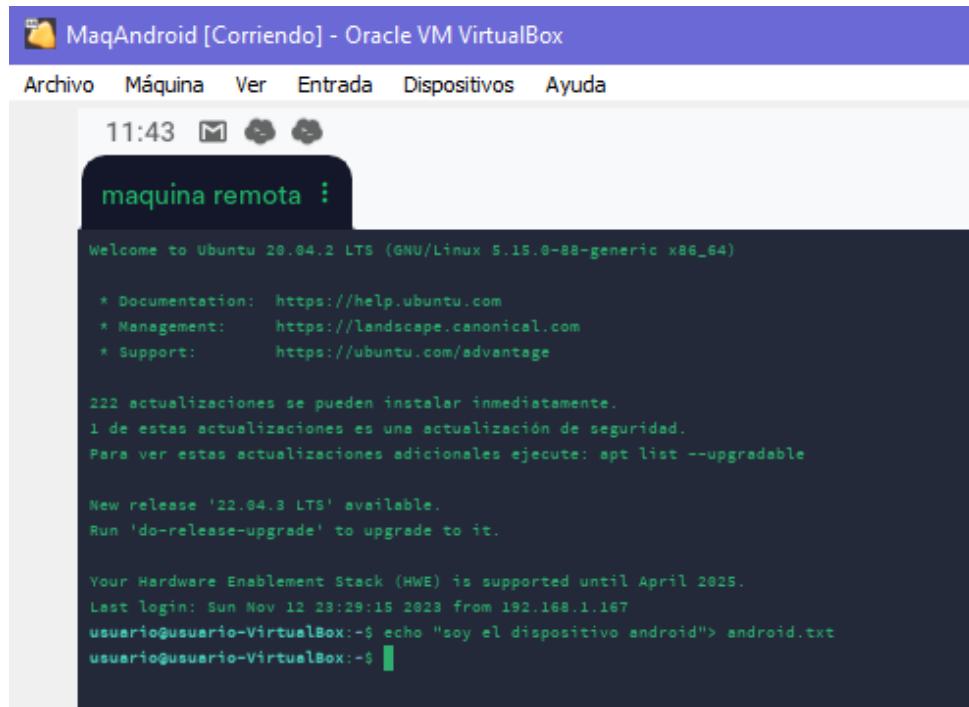


Damos clic a aceptar la autenticidad del host:

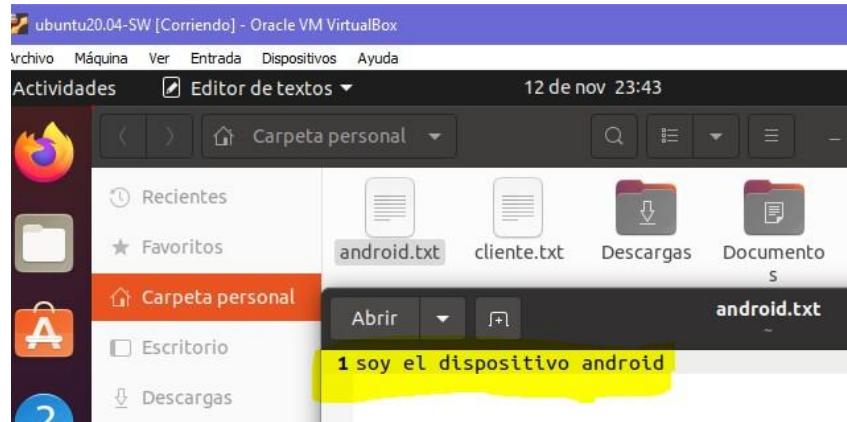


Como resultado ya estaremos en una terminal accediendo al servidor remoto.

Para hacer una prueba he creado un archivo android.txt para verificar la conexión:

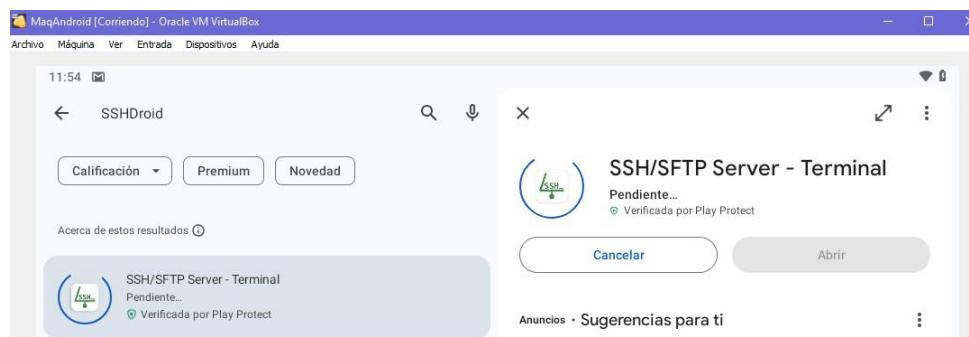


Comprobamos en el servidor, y nos aparece el archivo de texto creado desde el dispositivo Android.

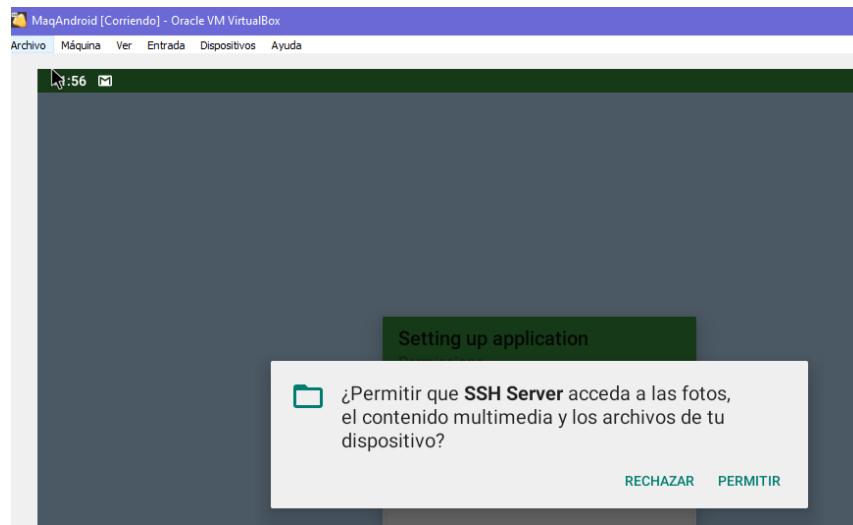


Servidor SSH (SSH/SFTP Server):

Instalamos la aplicación:

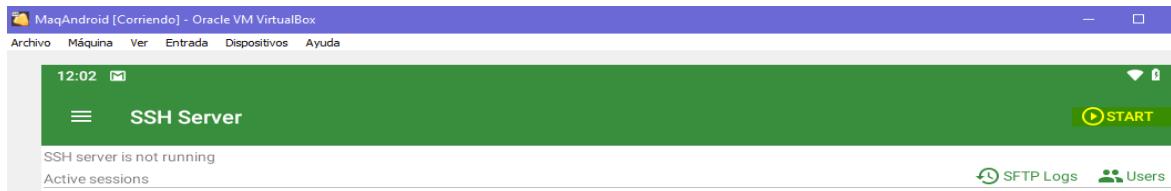


Permitimos acceso al dispositivo android:



En users creamos un usuario llamado carolina con contraseña: carolina.

Luego damos a START en el servidor:

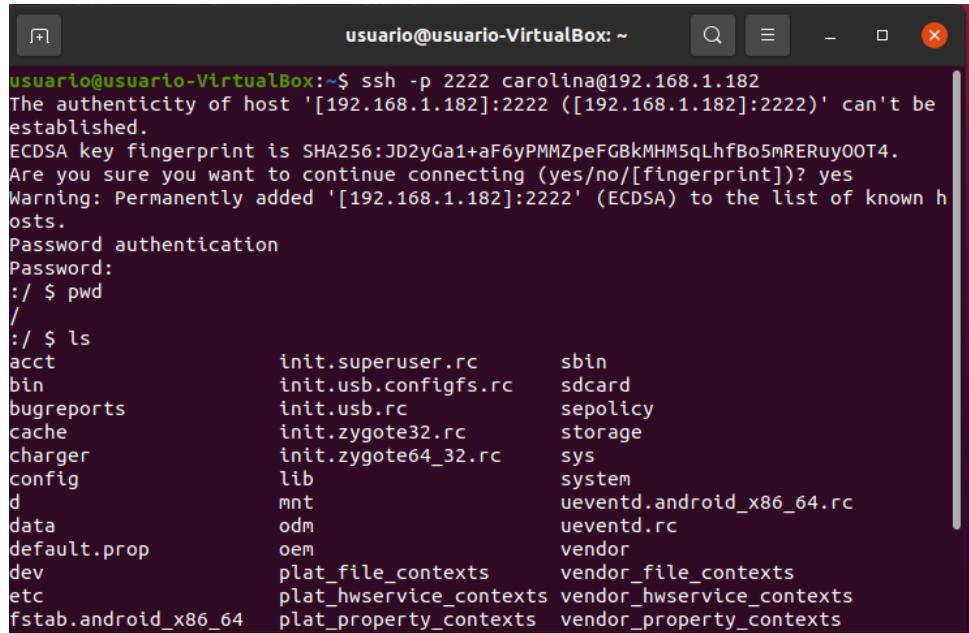


Nos aparecerá la ip y el puerto de ssh



En un cliente cualquiera: en este caso he utilizado una máquina Ubuntu, nos conectamos mediante ssh:

```
Ssh -p 2222 carolina@192.168.1.182
```

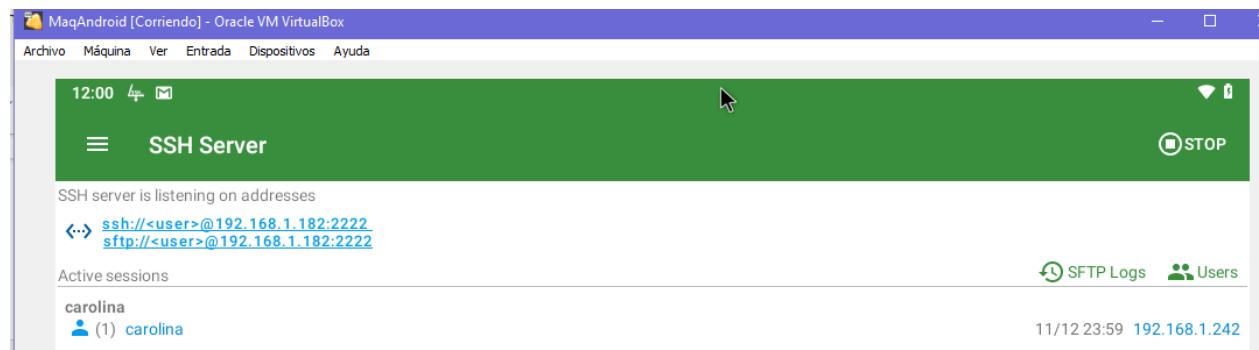


```

usuario@usuario-VirtualBox:~$ ssh -p 2222 carolina@192.168.1.182
The authenticity of host '[192.168.1.182]:2222 ([192.168.1.182]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:JD2yGa1+aF6yPMMZpeFGBkMHM5qLhfBo5mRERuy00T4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.182]:2222' (ECDSA) to the list of known h
osts.
Password authentication
Password:
:/ $ pwd
/
:/ $ ls
acct          init.superuser.rc      sbin
bin           init.usb.configfs.rc  sdcard
bugreports    init.usb.rc          sepolicy
cache          init.zygote32.rc     storage
charger        init.zygote64_32.rc   sys
config         lib                  system
d              mnt                  ueventd.android_x86_64.rc
data           odm                  ueventd.rc
default.prop   oem                  vendor
dev            plat_file_contexts  vendor_file_contexts
etc            plat_hwservice_contexts  vendor_hwservice_contexts
fstab.android_x86_64  plat_property_contexts  vendor_property_contexts

```

Nos aparecerá el servidor una máquina conectada al usuario carolina en este caso la máquina Ubuntu con IP 192.168.1.242



4.- WebDav:

¿ Que es WebDAV ? es un protocolo que nos permite guardar archivos, editarlos, moverlos y compartirlos en un servidor web, no necesitaremos utilizar otros protocolos de intercambio de archivos en red local o Internet, como Samba, FTP o NFS.



Ventajas de WebDAV

Este sistema está basado en HTTP, por lo cual para la transferencia utilizar el puerto 80, estándar de HTTP, que, al ser un puerto habitual, no se ve bloqueado por el firewall que tengamos instalado, salvo que se especifique previamente y es compatible con:

Microsoft IIS: -> módulo WebDAV propio.

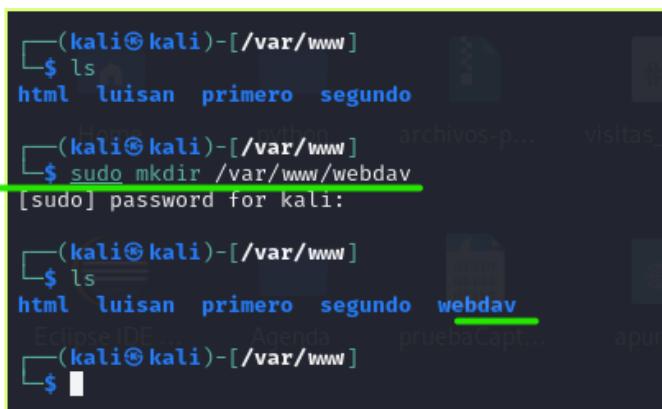
Apache HTTP: módulos -> Linux dav,davfs

Nestcloud y ownCloud cuenta con servicios en la nube que cuenta con soporte para WebDAV.

Actualmente el protocolo WebDAV es un estándar, y lo tenemos disponible de manera predeterminada en todos los sistemas operativos de escritorio como Windows, Linux y también macOS

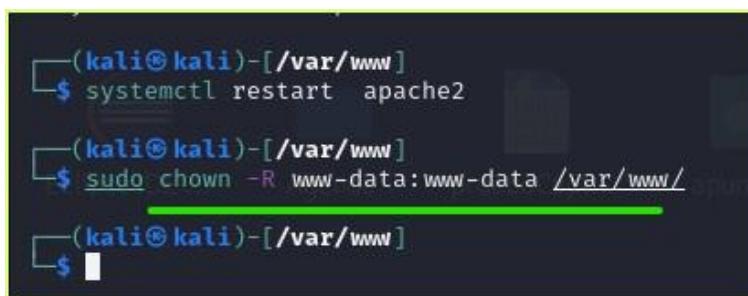
Activa el módulo dav y dav_fs en tu servidor Apache y configura una carpeta para su acceso WebDav siguiendo el tutorial en el aula virtual.

Creamos carpeta webdav:



```
(kali㉿kali)-[~/www]
$ ls
html luisan primero segundo
(kali㉿kali)-[~/www]
$ sudo mkdir /var/www/webdav
[sudo] password for kali:
(kali㉿kali)-[~/www]
$ ls
html luisan primero segundo webdav
(kali㉿kali)-[~/www]
$
```

Le daremos permisos al usuario y grupo www-data de forma recursiva a todas las carpetas y ficheros del servidor:



```
(kali㉿kali)-[~/www]
$ systemctl restart apache2
(kali㉿kali)-[~/www]
$ sudo chown -R www-data:www-data /var/www/*
(kali㉿kali)-[~/www]
$
```

Habilitar los módulos dav y dav_fs en Apache:

```
sudo a2enmod dav
sudo a2enmod dav_fs
```

```
(kali㉿kali)-[~/var/www]
$ sudo a2enmod dav
Enabling module dav.
To activate the new configuration, you need to run:
    systemctl restart apache2

(kali㉿kali)-[~/var/www]
$ sudo a2enmod dav-fs
ERROR: Module dav-fs does not exist!

(kali㉿kali)-[~/var/www]
$ sudo a2enmod dav_fs
Considering dependency dav for dav_fs:
Module dav already enabled
Enabling module dav_fs.
To activate the new configuration, you need to run:
    systemctl restart apache2

(kali㉿kali)-[~/var/www]
$
```

Reiniciaremos el servidor Apache :

`sudo systemctl restart apache2`

```
(kali㉿kali)-[~/var/www]
$ sudo systemctl restart apache2

(kali㉿kali)-[~/var/www]
```

kali@kali: /var/www

File Actions Edit View Help

GNU nano 6.3 /etc/apache2/sites-available/000-default.conf

```
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

Alias /webdav  /var/www/webdav
<Directory  /var/www/webdav>
    DAV On
</Directory>

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example,
# following line enables the CGI configuration for this host
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execut

Comprobamos el acceso:

Name	Last modified	Size	Description
Parent Directory	-	-	-

Apache/2.4.57 (Debian) Server at 192.168.174.134 Port 80

- Demuestra el acceso desde Windows y GNU/Linux, explora la integración con el explorador de archivos y clientes adicionales. Muestra que puedes subir archivos, borrar y descargar.

Comprobamos acceso desde linux la dirección debe de ser la ip del servidor y la carpeta webdav.

Name	Last modified	Size	Description
Parent Directory	-	-	-

Apache/2.4.57 (Debian) Server at 192.168.174.134 Port 80

Comprobamos el acceso desde windows:

Name	Last modified	Size	Description
Parent Directory	-	-	-

Apache/2.4.57 (Debian) Server at 192.168.174.134 Port 80

Instalamos el cliente cadaver en linux:

```
(kali㉿kali)-[~/etc]
$ sudo apt-get install cadaver
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libneon27-gnutls
The following NEW packages will be installed:
cadaver libneon27-gnutls
0 upgraded, 2 newly installed, 0 to remove and 16 not upgraded.
Need to get 155 kB of archives.
After this operation, 432 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libneon27-gnutls amd64 0.32
.5-2 [70.4 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 cadaver amd64 0.24+dfsg-2 [
```

Nos conectamos a través de cadaver:

```
(kali㉿kali)-[~/etc]
$ cadaver http://192.168.174.134/webdav/
dav:/webdav/> 
```

Subiendo ficheros con cadaver con el comando:

put /home/kali/Desktop/pruebaDavWeb.txt

Name	Last modified	Size	Description
Parent Directory	-	0	
pruebaDavWeb.txt	2023-11-11 12:02	0	

```
Apache/2.4.57 (Debian) Server at 192.168.174.134 Port 80
File Actions Edit View Help
$ 
(kali㉿kali)-[~/etc]
$ cadaver http://192.168.174.134/webdav/
dav:/webdav/> put /home/kali/Desktop/pruebaDavWeb.txt
Uploading /home/kali/Desktop/pruebaDavWeb.txt to `'/webdav/pruebaDavWeb.txt': success
dav:/webdav/> 
```

Borrando archivo desde linux con el comando delete:

The screenshot shows a browser window displaying the contents of a WebDAV directory at `192.168.174.134/webdav/`. The page title is "Index of /webdav". The table lists one file:

Name	Last modified	Size	Description
Parent Directory		-	
pruebawindowWebdav.txt	2023-11-11 12:21	0	

Below the table, a message reads: "Apache/2.4.57 (Debian) Server at 192.168.174.134 Port 80".

Below the browser, a terminal window titled "kali@kali: /etc" shows the following session:

```

kali@kali: /etc
File Actions Edit View Help
(kali㉿kali)-[~/etc]
$ cadaver http://192.168.174.134/webdav/
dav:/webdav/> put /home/kali/Desktop/pruebaDavWeb.txt
Uploading /home/kali/Desktop/pruebaDavWeb.txt to `/webdav/pruebaDavWeb.txt'.
dav:/webdav/> delete pruebaDavWeb.txt
Deleting `pruebaDavWeb.txt': succeeded.
dav:/webdav/>

```

Descargando archivos con cadaver desde linux con el comando get

The screenshot shows a terminal window on the left and a Windows File Explorer window on the right. The terminal window is titled "root@kali: /var/www/webdav" and shows the command:

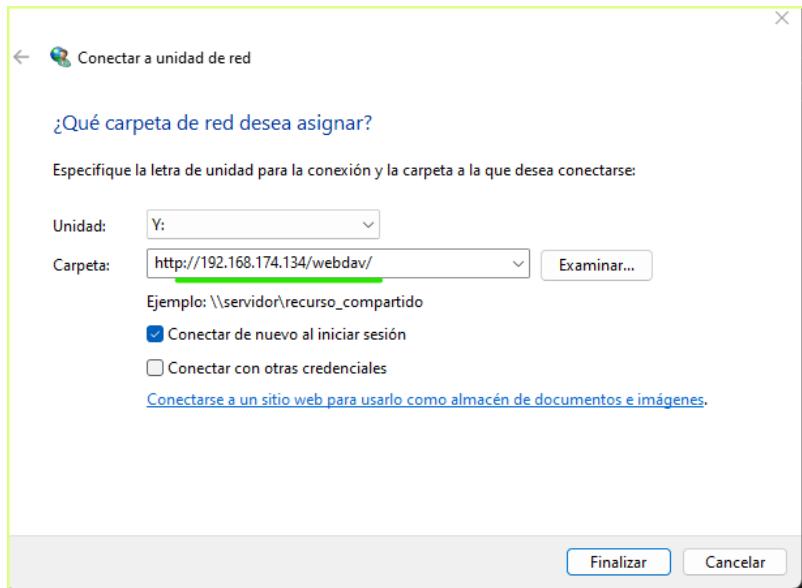
```

root@kali: /var/www/webdav
File Actions View Help
1157 ip_servidor/webdav
1158 ipconfig
1159 ifconfig
(kali㉿kali)-[~/var/www/webdav]
$ sudo su
[sudo] password for kali:
[root@kali]-[~/var/www/webdav]
# cadaver http://192.168.174.134/webdav/
dav:/webdav/> get pruebawindowWebdav.txt
Enter local filename for '/webdav/pruebawindowWebdav.txt': get pruebawindowWebdav.txt
Downloading '/webdav/pruebawindowWebdav.txt'
to get pruebawindowWebdav.txt:
Progress: [=====] 100.0% of 41 bytes succeeded.
dav:/webdav/>

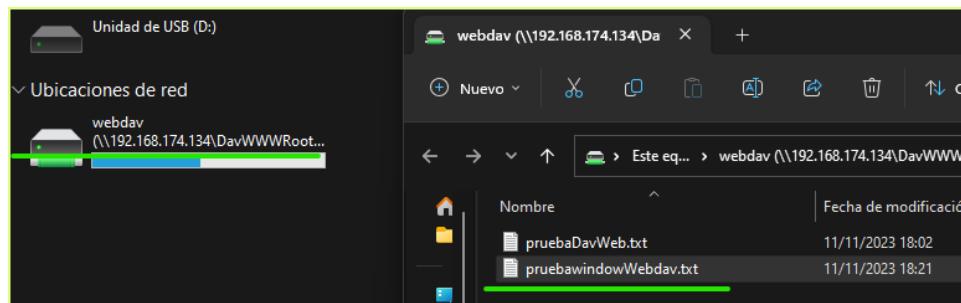
```

The Windows File Explorer window shows the downloaded file "pruebawindowWebdav.txt" in the "Documents" folder. The file is 41 bytes large.

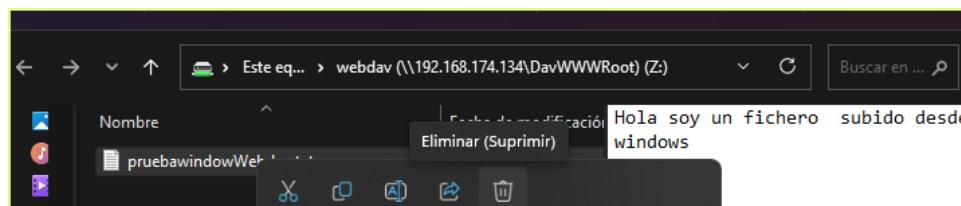
Windows tiene acceso a webdav agregando una unidad de red, agregamos la url.



Subida de fichero desde windows:



Borrando archivos desde windows :



Para descargar bastaría con copiar o pegar en algún sitio de tu pc que quieras guardarla.

- **Compara con la funcionalidad sftp de SSH y busca para ésta ejemplos de integración con los exploradores de archivos.**

SEGURIDAD	
SFTP:	WebDAV:
Utiliza SSH (Secure Shell) para proporcionar un canal seguro de transferencia de archivos. Proporciona cifrado de extremo a extremo, autenticación segura y protección contra amenazas comunes como ataques de intermediarios.	
PORTABILIDAD	
SFTP:	WebDAV:
Estándar de facto en sistemas basados en Unix y Linux. También es compatible con sistemas operativos Windows y macOS.	Estándar HTTP que puede utilizarse en una variedad de sistemas operativos. Mayormente utilizado en entornos web y puede integrarse con servicios en la nube y aplicaciones web.
Manipulación de Archivos	
SFTP:	WebDAV:
Ofrece comandos para navegar y manipular archivos en un sistema de archivos remoto de manera similar a las operaciones locales. Mayor control y flexibilidad para operaciones de archivos.	Diseñado para ser más extensible y es compatible con operaciones a través de HTTP, como propiedades y colecciones de recursos. Adecuado para escenarios de colaboración y gestión de documentos en entornos web.
Acceso a Recursos	
SFTP	WebDAV
Principalmente utilizado para la transferencia de archivos. No es intrínsecamente adecuado para acceder a recursos de manera colaborativa.	Diseñado para facilitar la colaboración y el acceso a recursos compartidos, con soporte para bloqueo de archivos, propiedades y control de versiones.

SFTP

Ideal para entornos donde la seguridad y la simplicidad son prioridades.

WebDAV

Ideal para entornos donde la colaboración y la interoperabilidad con aplicaciones web son esenciales.

Ejemplos de integración WebDAV en Exploradores de Archivos:

- Explorador de windows
- Nautilus -> (linux)
- Finder -> (Mac)

5.-Investiga protocolos para la distribución de archivos que usen el modelo P2P en vez de cliente servidor y explica las diferencias, ventajas e inconvenientes frente al modelo clásico cliente/servidor.

Modelo Cliente/Servidor: Depende de un servidor central para servicios y recursos.

Ejemplo: ssh.

Protocolos P2P: BitTorrent, eDonkey2000, Gnutella, Ares etc., permiten a los usuarios compartir archivos directamente.

1. BitTorrent:

- **Descarga simultánea:** Los usuarios pueden descargar y cargar (compartir) simultáneamente.
- **Ventajas:**
 - **Eficiencia:** Distribución de la carga entre pares, reduciendo la dependencia de un servidor central.
 - **Velocidad:** Descargas más rápidas al recibir datos de múltiples fuentes.

2. eDonkey/eMule:

- **Kad Network:** Integra una red Kademlia para buscar archivos sin un servidor central.
- **Ventajas:**
 - **Red descentralizada:** Mayor resistencia a fallos y dificultad para cerrar la red.
 - **Busqueda eficiente:** La red Kademlia mejora la eficiencia en la búsqueda de archivos.

3. Gnutella:

- **Búsqueda por consulta:** Los nodos envían consultas de búsqueda a la red y reciben respuestas.
- **Ventajas:**
- **Red descentralizada:** Menos vulnerable a ataques y cierres.
- **Amplia variedad de archivos:** No limitada a un conjunto específico de archivos.

Diferencias:

- **Centralización:** El modelo P2P carece de un servidor central, distribuyendo las funciones entre los nodos.
- **Eficiencia:** Los usuarios pueden descargar y cargar simultáneamente en P2P, mejorando la eficiencia.

Ventajas:

- **Descentralización:** Mayor resistencia a fallos y dificultad para cerrar la red.
- **Velocidad:** Descargas más rápidas al aprovechar múltiples fuentes.

Inconvenientes:

- **Dependencia de semillas:** Algunos protocolos P2P pueden experimentar ralentizaciones si hay pocos usuarios compartiendo.
- **Complejidad:** Algunos protocolos P2P pueden ser más complejos de configurar que los sistemas cliente/servidores simples.

Comparación: P2P ofrece descentralización y eficiencia, pero puede ser complejo y enfrentar desafíos legales. La elección depende de las necesidades específicas.