

Informe sobre TP N°5

Juan Ignacio Massacesi, Gabriel Lopez Romero

Mayo 2025

1 Actividad 1

En esta actividad instalamos SSH para conectarnos remotamente entre dos computadoras. Uno hacía de servidor (con Linux) y el otro de cliente, y después intercambiamos los roles para probar ambos lados.

Durante el proceso pudimos ver la IP y archivos del equipo servidor, crear archivos con el comando 'touch', pagar la computadora con el comando 'sudo shutdown' y también probamos el comando 'ssh -X' para abrir programas del otro equipo como Firefox.

```
user@ubuntu:/home/estudiante$ sudo ssh kali@10.65.4.119
The authenticity of host '10.65.4.119 (10.65.4.119)' can't be established.
ED25519 key fingerprint is SHA256:lNaAkav2B5RzGg7BeGTVZoXMZTciwypOtEfuFOdrPk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.65.4.119' (ED25519) to the list of known hosts.
kali@10.65.4.119's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 21 14:00:51 2025 from 10.65.4.120
kali@kali:~$ touch juaniArchivo.txt
```

No.	Time	Source	Destination	Protocol	Length	Info
282	50.33842258	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
283	50.339160205	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
284	50.332184007	10.65.4.119	10.65.4.117	TCP	60	43744 -> 22 [ACK] Seq=27 Ack=37 Win=23416 Len=0 TSeq=2094205740 TSrc=324114673
285	50.350538546	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
286	50.351042403	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
287	50.372719172	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
288	50.37271984	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
289	50.393535051	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
290	50.393762057	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
291	50.414840205	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
292	50.415160000	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
293	50.436517435	10.65.4.119	10.65.4.117	SSH	130	Client: Encrypted packet (len=72)
294	50.436640041	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
295	50.437615133	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
296	50.438717051	10.65.4.119	10.65.4.117	TCP	60	43744 -> 22 [ACK] Seq=28 Ack=35 Win=23416 Len=0 TSeq=2094205805 TSrc=324114779
297	50.458552229	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
298	50.458764017	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
299	50.488158208	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
300	50.488362124	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
301	50.508736802	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
302	50.508133017	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
303	50.521154939	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
304	50.521154939	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
305	50.543891154	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
306	50.543172504	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
307	50.564889809	10.65.4.119	10.65.4.117	SSH	130	Client: Encrypted packet (len=72)
308	50.565237725	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
309	50.565154051	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
310	50.56724793	10.65.4.119	10.65.4.117	TCP	60	43744 -> 22 [ACK] Seq=30 Ack=305 Win=23416 Len=0 TSeq=2094205984 TSrc=324114908
311	50.585513800	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
312	50.585760744	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
313	50.606617438	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
314	50.607674209	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
315	50.627648477	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
316	50.627673871	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)
317	50.648888809	10.65.4.119	10.65.4.117	SSH	102	Client: Encrypted packet (len=96)
318	50.648834807	10.65.4.117	10.65.4.119	SSH	102	Server: Encrypted packet (len=96)

Frame 384: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface em106, id 0

Ethernet II, Src: VMware_08:00:11:00:56:16:04:13 (08:00:16:04:13), Dst: VMware_08:00:11:00:56:16:04:13

Internet Protocol Version 4, Src: 10.65.4.117, Dst: 10.65.4.119

Transmission Control Protocol, Src Port: 22, Dst Port: 43744, Seq: 361, Ack: 397, Len: 36

SSH Protocol

0000 00 50 56 00 04 13 00 56 56 04 11 00 00 45 10 PV P V ... E

0010 00 50 16 02 00 00 00 04 01 0a 01 04 75 0a 01 X 0 0 a A u A

0020 04 77 09 18 aa e0 00 72 21 c0 05 00 c0 00 09 18 w ! Q |

0030 13 2e 1d 18 00 00 01 01 00 00 13 51 99 00 7c 04 Q |

0040 44 72 72 05 13 18 e0 40 22 44 07 30 f4 97 4a 09 Drr ... A * 0 0

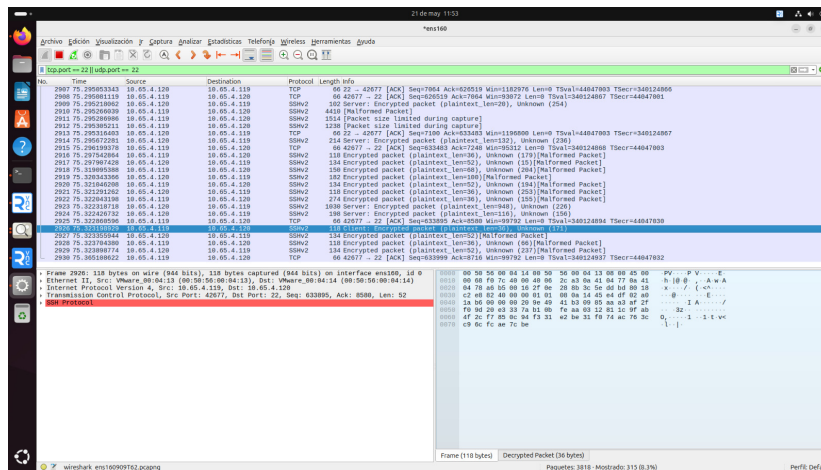
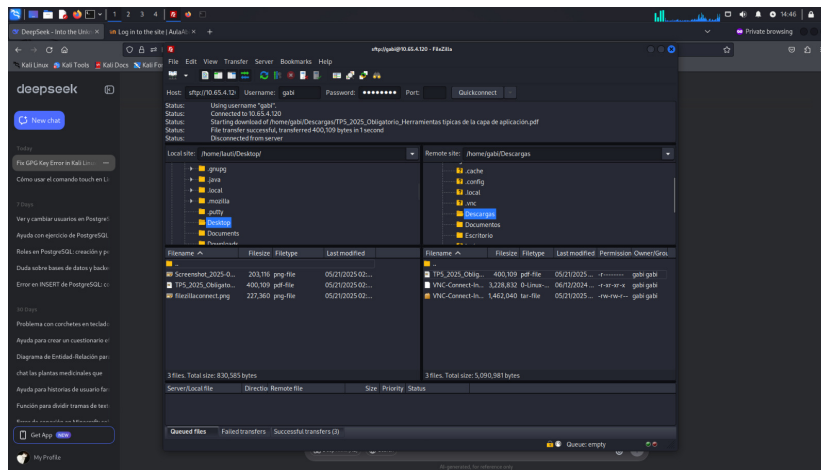
0050 07 44 07 3a 00 e1 70 01 90 73 50 31 00 7c 4a 02 y A i j 0

0060 13 59 91 07 00 ea

2 Actividad 2

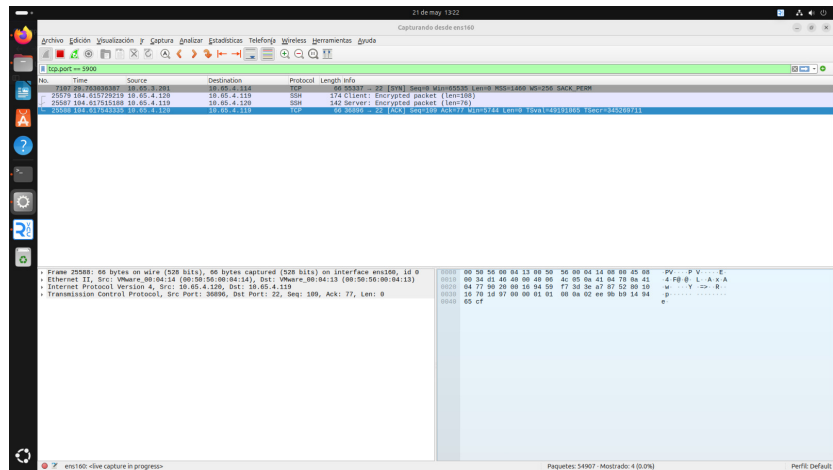
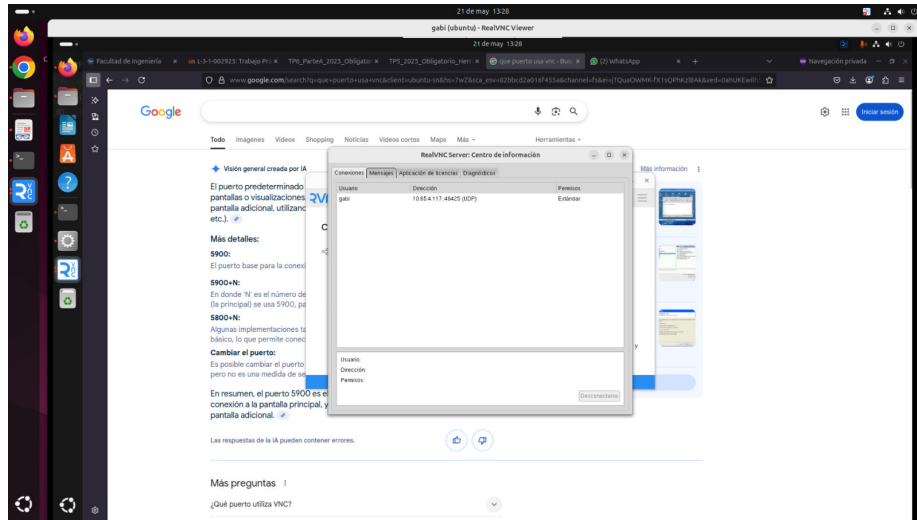
En esta actividad usamos FTP para enviar archivos entre dos computadoras conectadas en red. Primero, instalamos vsftpd como servidor FTP en una computadora con Linux y en la otra instalamos FileZilla que tiene interfaz gráfica como cliente.

Después configuramos el servidor (habilitando la opción de escritura en el archivo `/etc/vsftpd.conf`) para conectarnos desde FileZilla usando la IP del servidor, el usuario y la contraseña. En la primera captura podemos observar que transferimos el archivo `'TP5_2025.Obligatorio.Herramientas típicas de la capa de aplicación.pdf'` de la computadora cliente a la computadora servidor.



3 Actividad 3

En esta actividad probamos el uso de VNC para controlar una computadora de forma remota con entorno gráfico. Instalamos un servidor VNC (x11vnc) en una computadora con Linux y un cliente VNC (RealVNC) en otra. Nos conectamos desde el cliente usando la IP del servidor, un nombre de usuario y una contraseña.



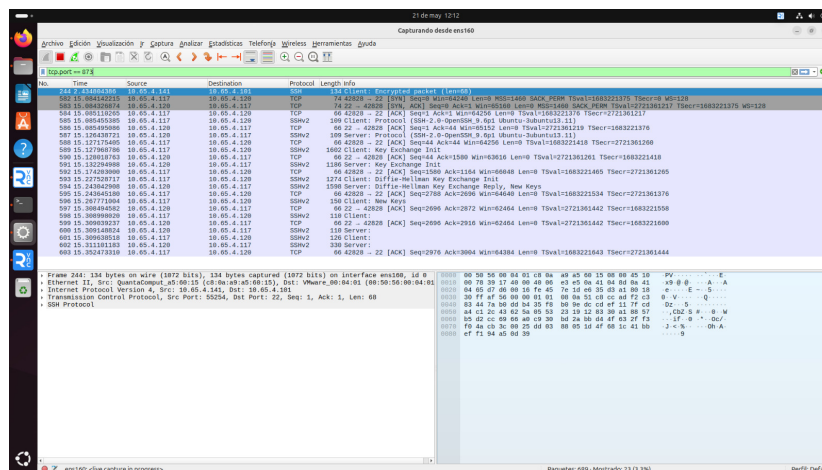
4 Actividad 4

En esta actividad usamos rsync para sincronizar archivos entre dos computadoras. Primero, instalamos rsync y configuramos el archivo '/etc/default/rsync' cambiando 'RSYNC_ENABLE=false' por true.

Después, usamos el comando 'sudo rsync -r -v /home/user/Descargas/server.py gabi@10.65.4.120:/home/usuario2/Descargas/' desde la terminal para copiar el archivo 'server.py' en la otra computadora. La sincronización fue rápida, transfirió el archivo nuevo.

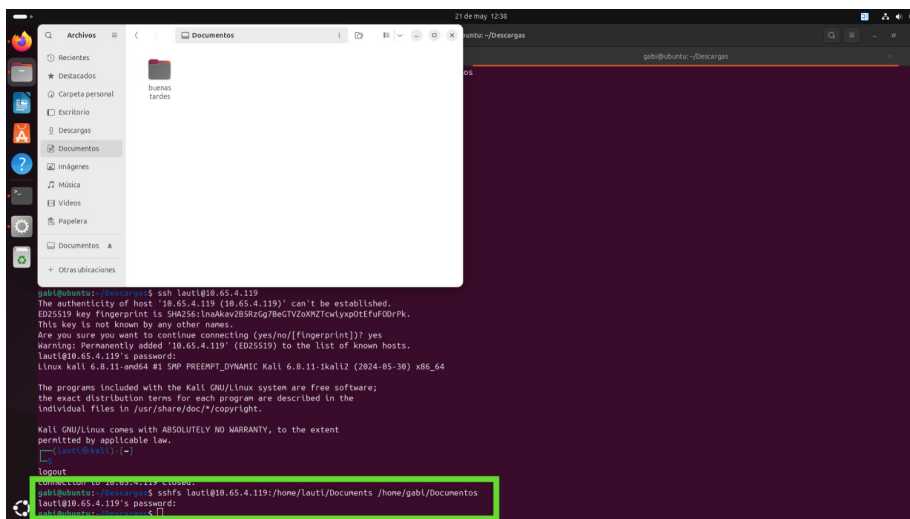
```
user@ubuntu:/home/estudiante$ sudo rsync -r -v /home/user/Descargas/server.py gabi@10.65.4.120:/home/gabi/Descargas/
gabi@10.65.4.120's password:
sending incremental file list
server.py

sent 2.893 bytes  received 35 bytes  448,92 bytes/sec
total size is 2.789  speedup is 0,96
user@ubuntu:/home/estudiante$
```



5 Actividad 5

Finalmente, en esta actividad utilizamos sshfs para montar una carpeta de una computadora remota en una carpeta de nuestro equipo. Primero, instalamos sshfs en ambas computadoras con 'sudo apt install sshfs' (debemos tener ssh cliente y servidor instalados y corriendo). Luego, utilizando el comando 'sshfs laut@10.65.4.119:/home/lauti/Documents /home/gabi/Documents', siendo la primera ruta la de la carpeta remota y la segunda la de nuestra computadora. Finalmente, podemos observar los resultados, ya que el contenido de la carpeta 'Documents' de la otra PC se encuentra en la nuestra y cualquier cambio se verá reflejado en ambos equipos. Por ultimo, podemos desmontar la carpeta con 'umount /home/user2/carpeta_montaje'



The screenshot shows a Kali Linux desktop environment. On the left, a file manager window is open to the 'Documents' directory, showing a folder named 'buenas tardes'. On the right, a terminal window displays the following commands and output:

```
gabi@kali:~$ ssh laut@10.65.4.119
The authenticity of host '10.65.4.119 (10.65.4.119)' can't be established.
ED25519 key fingerprint is SHA256:lnaKav2B5RzGg78eGTVZ0XMTcWlyxQTEfUf0DrPk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.65.4.119' (ED25519) to the list of known hosts.
laut@10.65.4.119's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-kali2 (2024-05-30) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

└─(laut@kali)─┐
logout
connection to 10.65.4.119 closed.
gabi@kali:~/Descargas$ sshfs laut@10.65.4.119:/home/lauti/Documents /home/gabi/Documents
laut@10.65.4.119's password:
gabi@kali:~/Descargas$
```

