

SSH

Ejercicio 1

Busca un article que expliqui com fer SSH entre 2 màquines sense necessitat de introduir contrasenya.

El client (imitant un PC de casa contra un servidor remot) es connectarà al servidor sense contrasenya.

Pista: es recomana la documentació oficial de Debian o d'Ubuntu, son molt clares i és un tema típic.

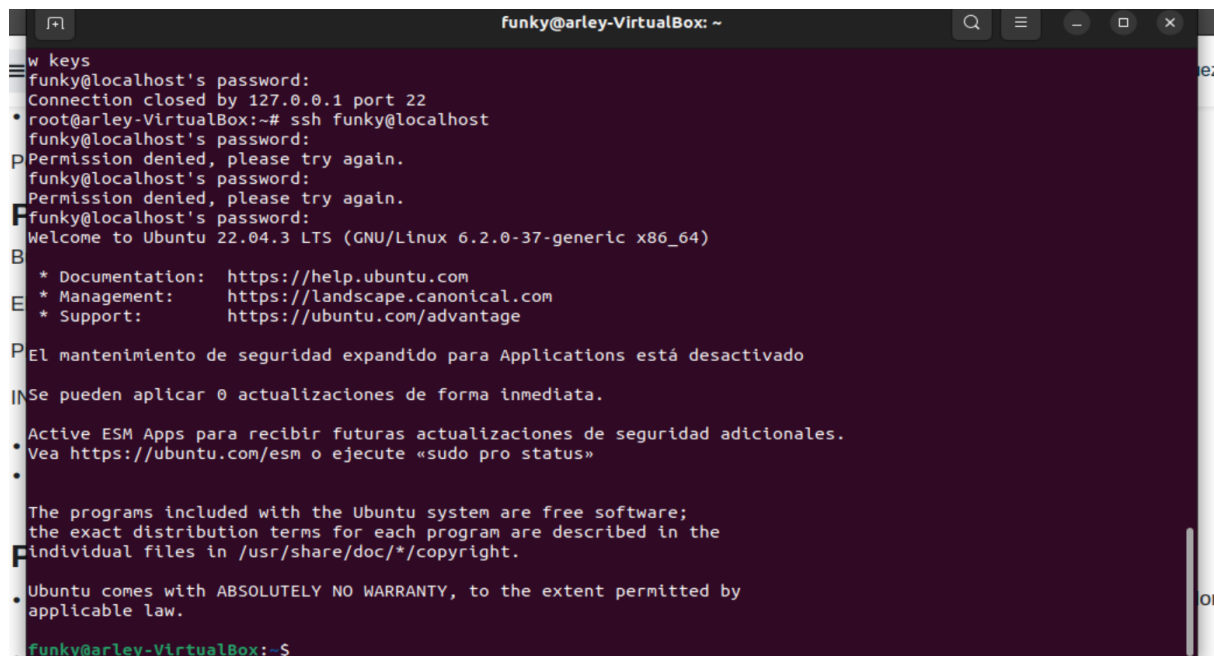
INFORME: llista tots els arxius i comandes implicats i explica per a què serveix cadascun. En particular:

comandos:

ssh-keygen -t rsa

ssh-copy-id funky@localhost

ssh funky@localhost



```
funky@arley-VirtualBox: ~  
w keys  
funky@localhost's password:  
Connection closed by 127.0.0.1 port 22  
root@arley-VirtualBox:~# ssh funky@localhost  
funky@localhost's password:  
Permission denied, please try again.  
funky@localhost's password:  
Permission denied, please try again.  
funky@localhost's password:  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-37-generic x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/advantage  
  
El mantenimiento de seguridad expandido para Applications está desactivado  
  
Se pueden aplicar 0 actualizaciones de forma inmediata.  
  
Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.  
Vea https://ubuntu.com/esm o ejecute «sudo pro status»  
  
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.  
funky@arley-VirtualBox:~$
```

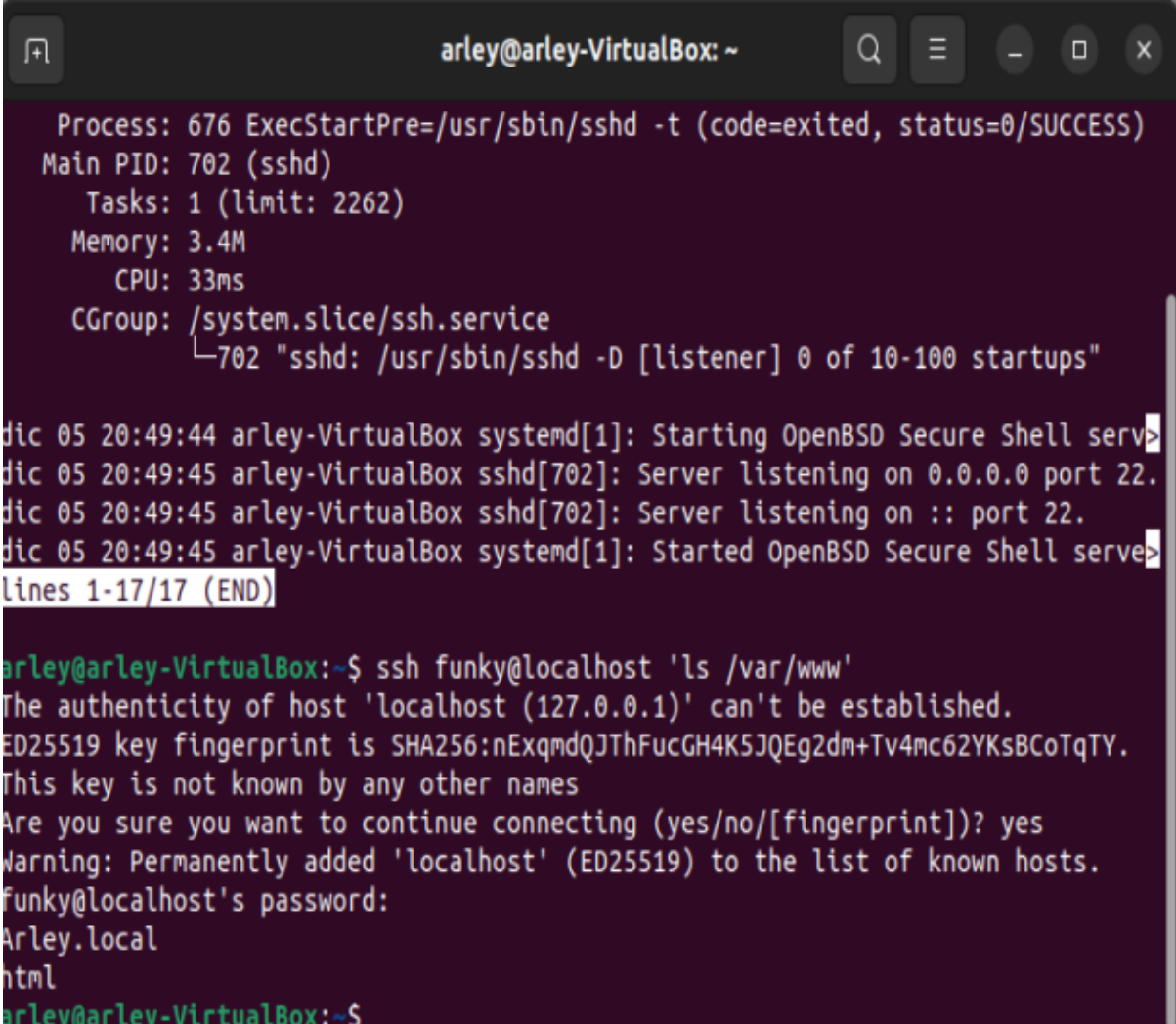
Ejercicio 2

Part 2 - execució remota

- Busca la manera d'executar comandes remotament sense entrar en mode interactiu. És a dir, has de poder entrar en el servidor, executar la comanda i sortir, escrivint una sola comanda des del client.
- Busca la manera d'executar comandes de superusuari (root) remotament sense entrar contrasenya.
Per exemple: engegar o parar un servidor web.

comando:

`ssh funky@localhost 'ls /var/www'`



```
arley@arley-VirtualBox: ~
Process: 676 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 702 (sshd)
Tasks: 1 (limit: 2262)
Memory: 3.4M
CPU: 33ms
CGroup: /system.slice/ssh.service
└─702 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

dic 05 20:49:44 arley-VirtualBox systemd[1]: Starting OpenBSD Secure Shell server: sshd.
dic 05 20:49:45 arley-VirtualBox sshd[702]: Server listening on 0.0.0.0 port 22.
dic 05 20:49:45 arley-VirtualBox sshd[702]: Server listening on :: port 22.
dic 05 20:49:45 arley-VirtualBox systemd[1]: Started OpenBSD Secure Shell server: sshd.
lines 1-17/17 (END)

arley@arley-VirtualBox:~$ ssh funky@localhost 'ls /var/www'
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:nExqmdQJThFucGH4K5JQEg2dm+Tv4mc62YKsBCoTqTY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
funky@localhost's password:
Arley.local
html
arley@arley-VirtualBox:~$
```

Ejercicio 3

Part 3 - SCP

El SSH també serveix per fer transferència segura de fitxers. Realitza:

1. Utilitza la comanda "scp" per transferir arxius del host al servidor i viceversa.
2. Cerca la manera de pujar de cop una carpeta amb subcarpetes i arxius.

host a servidor:

```
scp archivo.txt usuario@servidor:/ruta/en/el/servidor
```

servidor a host:

```
scp usuario@servidor:/ruta/en/el/servidor/archivo.txt /ruta/en/el/local
```

Copiar una carpeta completa de manera recursiva desde el host local al servidor:

```
scp -r carpeta usuario@servidor:/ruta/en/el/servidor
```

Copiar una carpeta completa de manera recursiva desde el servidor al host local:

```
scp -r usuario@servidor:/ruta/en/el/servidor/carpeta /ruta/en/el/local
```

Ejercicio 4

Part 4 - Configuració del servidor

4.1 Canvi de port

Els servidors reben molts atacs i el port 22 és el primer de la llista. Canvia el port del servidor al nº 1022.

- Quina comanda has de fer servir ara per connectar-te?
- Com faràs ara un SCP?

Si no tenies xarxa interna, crea la interfície i configura el client correctament i comprova que fa pings però no connecta per SSH i sí ho deixa fer des de la màquina amfitriona.



```
root@arley-VirtualBox: /home/arley
GNU nano 6.2 /etc/hosts.deny *
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:  ALL: some.host.name, .some.domain
#          ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
sshd: 10.0.2.15
```

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^J Ejecutar	^G Ubicación	M-U Deshacer	M-A Poner marca
^X Salir	^R Leer fich.	^_ Reemplazar	^U Pegar	^J Justificar	^/ Ir a línea	M-E Rehacer	M-6 Copiar

```
root@arley-VirtualBox: /home/arley
root@arley-VirtualBox:/home/arley# apt-get install denyhost
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
E: No se ha podido localizar el paquete denyhost
root@arley-VirtualBox:/home/arley# nano /etc/denyhost.conf
root@arley-VirtualBox:/home/arley# nano /etc/hosts.deny
root@arley-VirtualBox:/home/arley# nano /etc/hosts.deny
root@arley-VirtualBox:/home/arley# service ssh restart
root@arley-VirtualBox:/home/arley#
```

Informe:

INFORME

Part 1 - Claves SSH

Arxius utilitzats:

- En el servidor:
 - Clau pública: `~/.ssh/id_rsa.pub`
 - Clau privada: `~/.ssh/id_rsa`
 - Fitxer `authorized_keys`: `~/.ssh/authorized_keys`
- En el client:
 - Clau pública: `~/.ssh/id_rsa.pub`
 - Clau privada: `~/.ssh/id_rsa`

Configuració:

1. Generar claus SSH en el servidor i el client.
2. Afegir la clau pública del client al fitxer `authorized_keys` del servidor.
3. Assegurar els permisos de fitxers i carpetes.

Joc de proves:

- Establecer una conexión SSH desde el cliente al servidor sin ingresar una contraseña.
- Verificar que se puede conectar sin problemas y realizar operaciones.

Prevenió de l'atac "Man in the middle":

- Utilització de `ssh-keyscan` per emmagatzemar el "fingerprint" de la clau del servidor al fitxer `known_hosts`. Això ajuda a prevenir l'atac "Man in the middle" alertant sobre canvis en la clau del servidor.

bash

```
ssh-keyscan -H servidor >> ~/.ssh/known_hosts
```

Part 2 - Execució remota

Arxius utilitzats:

- Configuració de claus SSH ja establerta.

Configuració:

1. Configurar ejecución remota de comandos desde el cliente al servidor.
2. Configurar ejecución remota de comandos de superusuario sin contraseña.

Joc de proves:

- Ejecutar comandos desde el cliente al servidor de forma remota.
 - Ejecutar comandos de superusuario desde el cliente al servidor sin contraseña.
-

Part 3 - Transferencia segura de archivos con SCP

Arxius utilitzats:

- Configuració de claus SSH ja establerta.

Configuració:

1. Utilitzar `scp` para transferir archivos entre el host y el servidor.

Joc de proves:

- Transferir archivos desde el host al servidor y viceversa utilizando `scp`.
 - Transferir una carpeta completa de manera recursiva.
-

Part 4.1 - Canvi de port

Arxius utilitzats:

- Configuració de claus SSH ja establerta.

Configuració:

1. Canviar el port predeterminat de SSH al número 1022.

Joc de proves:

- Realizar una conexión SSH al servidor utilizando el nuevo puerto.
-

Part 4.2 - Restriccions per IP

Arxius utilitzats:

- Configuració de claus SSH ja establerta.
- Configuració de DenyHosts.

Configuració:

1. Restringir el acceso al servidor SSH por IP utilizando DenyHosts y configuración de SSH.

Joc de proves:

- Intentar acceder al servidor desde direcciones IP permitidas y denegadas.
- Comprobar que DenyHosts bloquea direcciones IP después de intentos fallidos.