

Exámenes ISE P2

Javier Gómez López

Exámen Aarón

Primero comenzamos creando un directorio en la máquina virtual de Ubuntu llamado `examenIseP2`. Dentro de él crearemos `backup` y `alumnosdb`.

```
[jgomez@ubuntui:~] 2023-04-21 14:12:35 $ pwd
/home/jgomez
[jgomez@ubuntui:~] 2023-04-21 14:12:38 $ mkdir examenIseP2
[jgomez@ubuntui:~] 2023-04-21 14:12:44 $ cd examenIseP2/
[jgomez@ubuntui:~/examenIseP2] 2023-04-21 14:12:45 $ mkdir backup
[jgomez@ubuntui:~/examenIseP2] 2023-04-21 14:12:50 $ mkdir alumnosdb
[jgomez@ubuntui:~/examenIseP2] 2023-04-21 14:13:00 $ ls
alumnosdb backup
[jgomez@ubuntui:~/examenIseP2] 2023-04-21 14:13:02 $
```

Ahora, dentro de `alumnosdb` creamos un archivo `.csv`.

```
56 21/04/23 14:12:44 mkdir examenIseP2
57 21/04/23 14:12:45 cd examenIseP2/
58 21/04/23 14:12:50 mkdir backup
59 21/04/23 14:13:00 mkdir alumnosdb
60 21/04/23 14:13:02 ls
61 21/04/23 14:14:21 cd alumnosdb/
62 21/04/23 14:14:23 pwd
63 21/04/23 14:14:32 touch alumnos.csv
64 21/04/23 14:14:35 nano alumnos.csv
65 21/04/23 14:15:06 cat alumnos.csv
```

```
[jgomez@ubuntui:~/examenIseP2/alumnosdb] 2023-04-21 14:15:17 $ cat alumnos.csv
Nombre, Apellido, DNI, Correo
Javier, Gómez, 123456782, javi5454@correo.ugr.es
```

Ahora tenemos que hacer `rsync` entre los archivos de `examenIseP2` y nuestra máquina Rocky.

Puesto que no es objeto de este ejercicio, usaremos la configuración por defecto de `sshd` que tiene Rocky instalada. Para `rsync`, instalaremos nuestra llave pública de Ubuntu (previamente generada) en nuestra máquina Rocky.

```
[jgomez@ubuntui:~/examenIseP2/alumnosdb] 2023-04-21 14:23:02 $ ssh-copy-id jgomez@192.168.56.20
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/jgomez/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.20 (192.168.56.20)' can't be established.
ECDSA key fingerprint is SHA256:u+cDdgN+12AcXhubN/TwowDMMW2doka33/+E6SgfuG8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install all the new keys
jgomez@192.168.56.20's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'jgomez@192.168.56.20'"
and check to make sure that only the key(s) you wanted were added.

[jgomez@ubuntui:~/examenIseP2/alumnosdb] 2023-04-21 14:23:38 $
```

Crearemos un directorio en nuestra máquina Rocky, llamado `copiaUbuntu`, donde haremos el `rsync` (`rsync` tiene que estar instalado en Rocky también).

```
[jgomez@localhost:~] 2023-04-21 16:21:30 $ pwd
/home/jgomez
[jgomez@localhost:~] 2023-04-21 16:24:48 $ mkdir copiaUbuntu
[jgomez@localhost:~] 2023-04-21 16:24:52 $ ls
copiaUbuntu
[jgomez@localhost:~] 2023-04-21 16:24:53 $
```

Y ejecutamos el programa:

```
[jgomez@ubuntuise:~] 2023-04-21 14:30:32 $ rsync -aviz -e "ssh" /home/jgomez/examenIseP2/. jgomez@92.168.56.20:/home/jgomez/copiaUbuntu
sending incremental file list
./
.d..tp..... ./
cd+++++++ alumnosdb/
<f+++++++ alumnosdb/alumnos.csv
cd+++++++ backup/

sent 281 bytes received 50 bytes 220.67 bytes/sec
total size is 80 speedup is 0.24
[jgomez@ubuntuise:~] 2023-04-21 14:30:54 $ _
```

```
[jgomez@localhost:~/copiaUbuntu] 2023-04-21 16:29:08 $ ls -laZ
total 0
drwxrwxr-x. 4 jgomez jgomez unconfined_u:object_r:user_home_t:s0 37 Apr 21 16:13 .
drwx----- 4 jgomez jgomez unconfined_u:object_r:user_home_dir_t:s0 132 Apr 21 16:24 ..
drwxrwxr-x. 2 jgomez jgomez unconfined_u:object_r:user_home_t:s0 25 Apr 21 16:27 alumnosdb
drwxrwxr-x. 2 jgomez jgomez unconfined_u:object_r:user_home_t:s0 6 Apr 21 16:12 backup
[jgomez@localhost:~/copiaUbuntu] 2023-04-21 16:30:59 $ _
```

Ahora pasaremos a crear un archivo de sólo 16kib en `examenIseP2/backup` en nuestra máquina Ubuntu.

```
[jgomez@ubuntuise:~/examenIseP2/backup] 2023-04-21 14:35:17 $ pwd
/home/jgomez/examenIseP2/backup
[jgomez@ubuntuise:~/examenIseP2/backup] 2023-04-21 14:35:22 $ dd if=/dev/zero of=./archivo bs=1 count=51k
51000+0 records in
51000+0 records out
51000 bytes (51 kB, 50 KiB) copied, 0.188814 s, 270 kB/s
[jgomez@ubuntuise:~/examenIseP2/backup] 2023-04-21 14:35:26 $ ls -laZ
total 60
drwxrwxr-x 2 jgomez jgomez ? 4096 Apr 21 14:35 .
drwxrwxr-x 4 jgomez jgomez ? 4096 Apr 21 14:13 ..
-rw-rw-r-- 1 jgomez jgomez ? 51000 Apr 21 14:35 archivo
[jgomez@ubuntuise:~/examenIseP2/backup] 2023-04-21 14:35:29 $ _
```

Por último, modificaremos el archivo `.csv` en nuestra máquina de Ubuntu y volveremos a sincronizar.

```
102 21/04/23 14:36:20 cd ../alumnosdb/
103 21/04/23 14:36:25 pwd
104 21/04/23 14:36:27 nano alumnos.csv
105 21/04/23 14:37:02 history
106 21/04/23 14:37:04 cat
107 21/04/23 14:37:07 history
jgomez@ubuntuise:~/examenIseP2/alumnosdb] 2023-04-21 14:37:07 $ cat alumnos.csv
Nombre, Apellido, DNI, Correo
Javier, Gómez, 123456782, javi5454@correo.ugr.es
Lara, Bolivar, 234567898, clarab@correo.ugr.es
Celedad, Ruiz, 34567891R, sunage@correo.ugr.es
jgomez@ubuntuise:~/examenIseP2/alumnosdb] 2023-04-21 14:37:09 $
```

```
[jgomez@ubuntuise:~/examenIseP2] 2023-04-21 14:37:30 $ rsync -aviz -e "ssh" /home/jgomez/examenIseP2/ jgomez@192.168.56.20:/home/jgomez/copiaUbuntu
sending incremental file list
.d..t..... alumnosdb/
<f.st..... alumnosdb/alumnos.csv
.d..t..... backup/
<f+++++++ backup/archivo

sent 462 bytes  received 68 bytes  1,060.00 bytes/sec
total size is 51,175  speedup is 96.56
[jgomez@ubuntuise:~/examenIseP2] 2023-04-21 14:38:01 $ _
```

```
jgomez@localhost:~/copiaUbuntu/alumnosdb] 2023-04-21 16:31:48 $ cat alumnos.csv
Nombre, Apellido, DNI, Correo
Javier, Gómez, 12345678Z, javi5454@correo.ugr.es
Clara, Bolívar, 23456789B, clarab@correo.ugr.es
Soledad, Ruiz, 34567891R, sunage@correo.ugr.es
[jgomez@localhost:~/copiaUbuntu/alumnosdb] 2023-04-21 16:38:09 $ cd ..
[jgomez@localhost:~/copiaUbuntu] 2023-04-21 16:38:13 $ ls -laZ backup/
total 52
lrwxrwxr-x. 2 jgomez jgomez unconfined_u:object_r:user_home_t:s0 21 Apr 21 16:35 .
lrwxrwxr-x. 4 jgomez jgomez unconfined_u:object_r:user_home_t:s0 37 Apr 21 16:13 ..
-rw-rw-r--. 1 jgomez jgomez unconfined_u:object_r:user_home_t:s0 51000 Apr 21 16:35 archivo
[jgomez@localhost:~/copiaUbuntu] 2023-04-21 16:38:19 $ _
```

Pregunta teórica: ¿Cómo utiliza ssh la clave pública y privada para garantizar la seguridad?

SSH, al inicio de la conexión, comparte las claves públicas de cada una de las partes que deseen conectarse. En caso de ser un cliente que se conecta por primera vez a un servidor, este le mostrará un resumen (fingerprint) de su clave pública para que, de manera **out-of-bound**, el cliente esté seguro de donde se conecta y evitar ataques man-in-the-middle. Tras esto, el cliente y servidor inician un algoritmo de negociación de una clave compartida, pero encriptando la comunicación con el cifrado asimétrico de las claves públicas-privadas de cada uno. En el momento en el que se llega a un acuerdo, se comparten la clave común de manera cifrada con las claves públicas de cada uno, y se inicia una comunicación con cifrado simétrico, mucho más eficiente.