

¿Cómo conectarse remotamente desde casa a un laboratorio?

- Uy! Me olvidé un archivo del tp en el labo.
- A mi compu no de la para correr **nasm**.
- Quiero esa linda instrucción de **SSE 4** que me soluciona la vida.

son situaciones que pueden presentarse a lo largo de la cursada de esta materia y de la carrera. Este apunte está orientado a solucionar dichos inconvenientes.

¿Qué necesito?

- **ssh**

*SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.*¹

Lo instalamos abriendo una consola y ejecutando: `sudo apt-get install ssh`.

- Una cuenta en **milagro**
- Una cuenta de **Linux**

Ambas las obtenemos pidiéndolas al conservador.

¿Y ahora?

Ahora vamos a crear un túnel ssh; para ello abrimos una consola y escribimos:

```
ssh usuario@milagro.dc.uba.ar -LpuertoAlto:10.2.laboratorio.maquina:22
```

Donde **usuario** es su usuario en **milagro**, **puertoAlto** es un número de puerto entre 2^{10} y $2^{32} - 1$, **laboratorio** es un número de laboratorio y **maquina** es un número de computadora.

Veamos un ejemplo: si Penélope Glamour² se quiere conectar a la computadora 3 del laboratorio 5 debería escribir:

```
ssh pglamour@milagro.dc.uba.ar -L2200:10.2.5.3:22
```

Listo! Ahora tenemos un túnel entre nuestra casa y una computadora del laboratorio, pasando por **milagro**.

Si queremos compilar el tp en una computadora de la Facultad desde casa, abrimos una nueva consola y **sin cerrar la anterior** escribimos:

```
ssh -p puertoAlto usuario@localhost
```

Para Penélope sería:

```
ssh -p 2200 pglamour@localhost
```

Esta consola nos va a permitir ver nuestro **home** de la Facultad y desde aquí mismo vamos a poder hacer **make** para compilar nuestro tp.

Finalmente para copiar archivos entre las computadoras conectadas mediante **ssh** utilizaremos un programa llamado **scp**:

¹Wikipedia, the free encyclopedia.

²http://es.wikipedia.org/wiki/Penelope_Glamour

*Secure Copy o SCP es un medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo Secure Shell (SSH).*³

Si queremos copiar un archivo desde la computadora de casa a la del laboratorio, abrimos una tercer consola y, nuevamente **sin cerrar las dos anteriores**, escribimos:

```
scp -r -P puertoAlto usuario@localhost:fuelle destino
```

y del laboratorio a casa:

```
scp -r -P puertoAlto destino usuario@localhost:fuelle
```

Donde **fuelle** es la ruta y el archivo a copiar y **destino** es la ruta donde queremos que éste aparezca.

Si Penélope quisiera copiar el archivo *main.c* de la Facultad a su casa, debería escribir:

```
scp -r -P 2200 pglamour@localhost:/home/pglamour/main.c /home/pglamour/Documentos/maincopia.c
```

Y una vez modificado, si quisiera copiarlo a su **home** en la Facultad:

```
scp -r -P 2200 /home/pglamour/Documentos/maincopia.c pglamour@localhost:/home/pglamour/main.c
```

Bonus track

En caso de que necesitéramos trabajar con el entorno gráfico de la máquina a la cual nos conectamos de manera remota (i.e. redirigir el tráfico de X), realizamos los mismos pasos descritos anteriormente a excepción del segundo en el cual escribimos:

```
ssh -p puertoAlto -X -C usuario@localhost
```

Advertencia: Conectarse de esta manera produce un aumento considerable en la latencia de los datos provocando que la conexión sea lenta.

Mas bonus track

Si queremos simplificar el procedimiento de autenticación de nuestro usuario podemos generar un par de claves: una pública y una privada. Estas claves se almacenarán en nuestra computadora y nos permitirán acceder a nuestra sesión sin la necesidad de ingresar la contraseña.

Veamos mas formalmente de que se trata:

*La criptografía asimétrica (en inglés symmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.*⁴

*En criptografía, RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.*⁵

³Wikipedia, the free encyclopedia.

⁴http://es.wikipedia.org/wiki/Criptografia_asimetrica

⁵<http://es.wikipedia.org/wiki/RSA>

Lo que vamos a hacer es generar una clave **RSA** para lo cual abrimos una consola y escribimos:

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

Muy importante: responder **yes** a las preguntas que siguen y, cuando termine y nos devuelva la línea de comandos, escribimos:

```
ssh-copy-id usuario@milagro.dc.uba.ar
```

Ingresamos nuestra contraseña de **milagro** y **yes**, cuando corresponda y terminamos.

Si queremos conectarnos de la misma forma a alguna computadora del laboratorio, basta copiar los archivos `id_rsa` e `id_rsa.pub` situados en la carpeta `.ssh` de nuestra computadora a la carpeta con el mismo nombre, en **milagro**. Finalmente desde la línea de comandos de **milagro**, ejecutamos:

```
ssh-copy-id usuario@10.2.laboratorio.maquina
```

y listo! Ahora podremos conectarnos desde casa a una computadora de los laboratorios mediante un túnel, sin la necesidad de ingresar contraseñas.

Aclaración: Vale destacar que aunque invoquemos `ssh-copy-id` para una computadora en particular, los archivos necesarios para manipular las claves **RSA** están guardados en el **home** asociado a nuestro usuario, el cual es el mismo en cualquier computadora de los laboratorios. Esto quiere decir que no hace falta repetir este procedimiento para cada computadora; una vez realizado, sirve para todas.

Problemas frecuentes

- La cuenta de Milagro dice que no tiene un **home** asociado a mi usuario.

Esto se arregla mandando un mail a **soporte-tecnico@dc.uba.ar** desde su cuenta de mail registrada en el sistema de inscripciones, comentando dicha situación y listo!

- No me puedo conectar. La consola dice: `ssh_exchange_identification: Connection closed by remote host`

A veces sucede que la computadora a la cual estamos intentando acceder está apagada o logueada en Windows. En este caso debemos elegir otra computadora para conectarnos.

Para comprobar que computadoras están en condiciones de aceptar una conexión **ssh**, podemos probar conectarnos mediante **telnet** desde **milagro**:

```
telnet 10.2.laboratorio.maquina 22
```