**LABORATORIO No 8: Secure Shell - SSH**

**Objetivos**

Al finalizar el taller, se espera que el estudiante esté en capacidad de:

* Instalar el servidor SSH en Linux.
* Configurar el servicio teniendo en cuenta los requerimientos y seguridad.
* Iniciar el servicio SSH.
* Probar que el servidor SSH funcione en un ambiente de red.

# SSH (Secure Shell)

# SSH (Secure SHell ó intérprete de órdenes segura) 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. En resumen, permite ejecutar comandos del shell de un equipo remoto desde otro como si estuviésemos administrando el equipo remoto. Correctamente configurado el equipo remoto también permite abrir ventanas de GNU Linux en el modo gráfico de Windows.

# Además de la conexión a otras máquinas, SSH permite copiar datos de forma segura, gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

# SSH funciona de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

# En resumen, SSH es un protocolo utilizado para control remoto de otros equipos de la red y para transferencia cifrada de ficheros.

## OpenSSH

OpenSSH es una versión gratuita (freeware) del paquete de herramientas de comunicación segura del protocolo SSH/SecSH para redes. OpenSSH, al contrario que otros programas para el protocolo SSH (telnet, rlogin, ftp), cifra todo el tráfico (incluidas las contraseñas). Además, OpenSSH ofrece amplias posibilidades para la creación de túneles seguros, aparte de una variedad de métodos de autenticación.

OpenSSH es un proyecto desarrollado principalmente por el Proyecto OpenBSD, y su primera integración en un sistema operativo fue en OpenBSD 2.6. Estos programas se desarrollan usando código de unos 10 países distintos. Este código es de libre utilización bajo la licencia BSD.

OpenSSH (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo [SSH](http://www.ajpdsoft.com/modules.php?name=News&file=article&sid=444#definicionssh). Fue creado como una alternativa libre y abierta al programa Secure Shell, que es software propietario. El proyecto está liderado por Theo de Raadt

OpenSSH incluye las siguientes herramientas:

* **ssh**: reemplaza a rlogin y telnet para permitir el acceso remoto a otra máquina.
* **scp**: reemplaza a rcp para copiar ficheros.
* **sftp**: reemplaza a ftp para transferir archivos entre dos equipos.
* **sshd**: servidor demonio SSH sshd.
* **ssh-keygen**: herramienta para inspeccionar y generar claves RSA y DSA que son usadas para la autenticación del cliente o usuario.
* **ssh-agent** y **ssh-add**: herramientas para autenticarse de manera más fácil, manteniendo las claves listas para no tener que volver a introducir la frase de acceso cada vez que utilice la clave.
* **ssh-keyscan**: escanea una lista de clientes y recolecta sus claves públicas.

**Instalación de OpenSSH**

Para instalar SSH, se escribe el siguiente comando:

$ sudo apt-get install openssh-server openssh-client

**Configuración de OpenSSH**

Para dar acceso a los usuarios que requiere mediante SSH, se edita el fichero sshd\_config, ubicado en /etc/ssh/. Para ello editaremos el archivo con nano, ejecutaremos el comando:

sudo nano /etc/ssh/sshd\_config

Se adiciona el siguiente línea para permitir el acceso mediante SSH al usuario "estudiante":

AllowUsers estudiante

Si se quiere permitir el acceso mediante SSH al super usuario root, se adiciona la siguiente línea a este archivo:

PermitRootLogin yes

Aunque esto no es muy recomendable por cuestiones de seguridad. Para indicar con qué interfaz de red se establecerá la conexión (en el caso de que se tenga varias interfaces de red con varias IPs en el servidor) se adiciona la línea:

ListenAddress 192.168.1.254

También se puede cambiar el puerto por defecto para SSH (es recomendable por seguridad), que es el 22, añadiendo (o modificando si existe) la línea:

Port 2222

Donde "2222" será el número del nuevo puerto que utilizará SSH.

Para que se apliquen los cambios se requiere reiniciar el servicio de SSH con el comando:

$ sudo service ssh restart

### Ejecución de comandos por consola desde otro equipo mediante PuTTY

PuTTY es un cliente SSH gratuito, que permite acceder remotamente al equipo con OpenSSH y GNU Linux, para ello mediante un cliente que admita SSH como [PuTTY](http://www.ajpdsoft.com/modules.php?name=Encyclopedia&op=content&tid=674), descargando PuTTY (es gratuito) desde su propia web:

*http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html*

Ejecutando el fichero descargado *putty.exe*, en "Host Name (or IP address)" introduciremos la IP del equipo con GNU Linux y OpenSSH, en "Port" introducimos "22" y pulsamos en "Open", como se muestra en la Figura 1.

Figura 1. Interfaz del cliente SSH PuTTY

