Grupo de Investigación Linux-IDES

Taller De Configuración de ssh

Autor: Gonzalo Alvarez Flores

1. Introducción

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 el ordenador mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.

Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), 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 trabaja 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; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

El protocolo SSH cuenta con dos versiones. La primera de ellas se mantiene por motivos de compatibilidad, pero se recomienda generalmente el uso de la segunda, por su mayor seguridad. OpenSSH es una implementación, usable en sistemas Linux, de cliente y servidor para estos protocolos, la versión disponible para Debian permite usar tanto SSH1 como SSH2.

Tal como se describe en uno de los borradores de la especificación temporal "SSH Protocol Architecture", ssh es un protocolo para iniciar sesiones en máquinas remotas que ofrece autenticación, confidencialidad e integridad. Consta de tres componentes:

1) Protocolos de transporte y red: Que normalmente opera sobre TCP/IP dando autenticidad, confidencialidad e integridad.
2) Protocolo de autenticación de usuario: Que autentica al usuario ante el servidor.

3) Protocolo de conexión: Que multiplexa un canal cifrado en diversos canales lógicos.

Este protocolo requiere que los servidores tengan "llaves", las cuales son usadas por los clientes cada vez que se conectan a un servidor para verificar que no fue suplantado. Una llave es un número codificado y cifrado en un archivo. Para el cifrado de llaves, OpenSSH ofrece los algoritmos RSA y DSA (de los cuales para la versión 2 recomendamos DSA).

Cuando se instale el servidor OpenSSH se generarán un par de "llaves" para su computador, una pública y una privada.

www.wikipedia.org

2. Instalación

- Instalación de los paquetes:
  - Debian y derivados:
    ```
    #apt-get install ssh
    ```
  - Red Hat y derivados:
    ```
    #yum install openssh-client openssh-server
    ```
- Iniciar el demonio (servidor ssh):
  ```
  #/etc/init.d/ssh start
  ó
  #service sshd start
  ```

3. Configuración del servidor SSH

El demonio sshd lee información del archivo de configuración /etc/ssh/sshd_config, éste archivo contiene pares de valores opción-valor por cada línea, las líneas que comienzan con “#” son comentarios.

Apenas se instala el servidor viene con algunas opciones seteadas por defecto, sin embargo, todas las posibles opciones están descritas en el archivo manual de sshd_config, para poder verlo bastará ejecutar: `$man sshd_config`

4. Configuración del cliente SSH

El cliente SSH nos permite loguearnos en una computadora remota y así poder ejecutar comandos en ella. Provee de comunicación segura encriptada entre 2 hosts en una red insegura.

El comando SSH puede recibir varias opciones en la línea de comandos, todas las posibles opciones están descritas en el archivo manual de ssh, para poder verlo bastará ejecutar: `$man ssh`

SSH obtiene información de configuración de las siguientes fuentes y en el siguiente orden:

1) Opciones por linea de comandos.
2) Archivo de configuración del usuario (~/.ssh/config)
3) Archivo de configuración global (/etc/ssh/ssh_config)

Descripción del archivo /etc/ssh/ssh_config:

Para cada parámetro, el primer valor obtenido es el usado. Los archivos de configuración contienen secciones separadas por especificación de cada “Host”, y cada sección es aplicada sólo para los hosts que coincidan con uno de los patrones dados en la especificación. El nombre del host encontrado es el dado en la línea de comandos.

El archivo tiene el siguiente formato:

Las líneas que comienzan con el carácter “#” son comentarios.
Para setear el valor de una opción se escribe en el formato “opción valor”, ambos valores separados por un espacio o un carácter “=”.

Las posibles opciones están descritas en el archivo manual de ssh_config, para poder verlo bastará ejecutar: `$man ssh_config`

Tener en cuenta que los valores son sensitivos a mayúsculas y minúsculas.

Ejemplo:

```
$ssh userx@192.168.1.10
```

Con esta sentencia se lograría la conexión remota a la computadora con direccinón ip 192.168.1.10 como usuario userx.

5. El cliente SCP

SCP permite copiar archivos entre host en una red. Éste usa a ssh para la transferencia de datos, usa la misma autenticación y provee de la misma seguridad que ssh.

Las opciones de scp están descritas en el archivo manual de scp, para poder verlo bastará ejecutar: `$man scp`

Ejemplo:
Para copiar el archivo /home/userx/documentos/archivo.odt del usuario userx en el host 192.168.2.10 al directorio home del usuario actual logueado:

```
$scp userx@192.168.2.10:documentos/archivo.odt .
```

6. Bibliografía

- Wikipedia: http://en.wikipedia.org/wiki/Secure_Shell
- Documentación de OpenSSH en paquetes openssh-client, openssh-server.