Secure Shell, mas comúnmente conocido como SSH, es el nombre de un protocolo y del programa que lo administra. La utilidad que tiene es la de permitir el acceso remoto a un servidor a través de una puerta trasera, lo cual nos permite operar el servidor por medio de un interprete de comandos (también permite en algunos casos la ejecución de programas gráficos). Además de proveer la conexión a otros dispositivos, también ofrece la funcionalidad de copiar datos.

Decidimos usar el protocolo SSH porque, según se especifica en los requerimientos de la materia Taller de Mantenimiento, el gerente viaja seguido por lo que se encuentra poco tiempo en la oficina, debido a lo cual solicito la posibilidad de acceso remoto a sistema. Para cumplir este requerimiento decidimos la instalación de OpenSSH en el servidor, un conjunto de aplicaciones que permite realizar configuraciones cifradas a través de una red usando el protocolo SSH.

Configuración de SSH

Para cambiar la configuración de OpenSSH, se debe acceder y modificar el archivo ubicado en /etc/ssh/opensshd\_config .

En pos de aumentar la seguridad del servidor, decidimos modificar algunas configuraciones de OpenSSH, en base a los siguientes puntos:

* Como el único usuario al que se le permite el acceso de forma remota es el cliente, decidimos limitar los usuarios que pueden ingresar en base al grupo primario al que pertenecen. Como mencionamos en el estudio de roles del sistema, todos los gerentes tendrán como grupo 'gerentes'. Teniendo esto cuenta, solo los usuarios que tienen como grupo primario 'gerentes' podrán acceder remotamente al sistema por medio de SSH. Para ello hay que agregar la siguiente línea al archivo de configruraión antes mencionado:

AllowGroups gerentes

Esto limitara la cantidad de usuarios que pueden acceder remotamente al sistema, lo cual lo hará que sea menos vulnerable.

* Considerando que el único usuario que se conectará remotamente es un gerente, y que los usuarios que tienen como grupo primario 'gerentes' ya tendrán los permisos que sean necesarios para administrar el sistema, decidimos no permitir que el superusuario 'root' se conecte remotamente a través de SSH, pues ninguna de las funcionalidades extra que ofrece será necesaria por el gerente a través del acceso remoto, y si de dejarlo habilitado alguien logrará acceder a él tendría control total sobre el sistema. Para ello modificaremos la línea que dice PermitRootLogin a:

PermitRootLogin no

Con esto no se podrá acceder remotamente al usuario 'root', lo cual le daría privilegios innecesarios a cualquier usuario que logrará acceder a él.

* Decidimos que, pasado un tiempo en el cuál el servidor no reciba datos del cliente, el servidor enviara un mensaje para confirmar si se sigue usando la sesión; luego de enviar una determinada cantidad de mensajes y recibir como respuesta que no se está usando la sesión, la conexión remota se cortará. Para ello se deberán agregar las líneas ClientAliveInterval y ClientAliveCount, que indidarán cada cuanto tiempo se enviará un mensaje para verificar si se sigue usando la sesión y luego de cuantos mensajes se cortará la conexión, respectivamente. Nótese que el tiempo en ClientAliveInterval deberá ser especificado en segundos.

Para nuestro sistema, decidimos que el mensaje de verificación se enviará cada 5 minutos, y se enviarán 4 de estos mensajes antes de terminar la conexión remota. Por lo tanto, tenemos que agregar las siguientes líneas al archivo de configuración:

ClientAliveInterval 300

ClientAliveCount 4

Esto hará que luego de 20 minutos sin recibir datos por parte del cliente se termine la conexión.