



Sistemas Operativos

TRABAJO PRÁCTICO LABORATORIO N° 5: Configuración de servicios. Caso SSH.

Observaciones: Para resolver este trabajo debes contar con usuario administrador (root) en la máquina en la que trabajes. Esto se debe a que necesitarás instalar software y acceder a archivos de configuración de acceso restringido.

En los casos que considere necesario, indicar los comandos usados para resolver lo solicitado.

1. Explicar brevemente qué es y para qué sirve SSH. ¿Qué es OpenSSH?
2. En alguna instalación de GNU/Linux, derivada de Debian, instalar cliente y servidor de OpenSSH (ver apt-get install, o aptitude).
3. Iniciar el servidor SSH en la máquina y comprobar que escucha conexiones remotas (ver systemctl).
4. Configurar el servicio SSH para que no admita conexiones con el usuario root.
5. Configurar el servicio para que solo permita conexiones remotas a ciertos usuarios.
6. El servicio SSH por defecto escucha en el puerto 22. Modificarlo para que atienda en el puerto 10022 (u otro) y averiguar cuál es el comando utilizado para poder acceder al servidor en el nuevo puerto. (consultar man ssh).
7. Por defecto, al autenticarnos correctamente en el servidor SSH, éste nos muestra la fecha y hora de la última vez que nos conectamos. Buscar la forma de modificar este aspecto.
8. Configurar el servidor SSH de forma adecuada para que acepte la redirección X11, de tal forma que se puedan ejecutar aplicaciones gráficas de forma remota. Comprobar su funcionamiento.
9. Configurar el servidor para realizar desde el cliente, autenticación por clave pública.
10. Probar conectarse desde un cliente SSH de Windows (ejemplo: Putty) a un servidor de SSH de GNU/Linux y comprobar si es posible hacerlo correctamente.

Recursos

<http://www.openssh.com/manual.html>

<https://www.hostinger.com.ar/tutoriales/que-es-ssh>