UT 6 – Despliegue Aplicaciones WAMP/LAMP

P6.2 – Instalación Servidor OpenSSH

Objetivo

Tras la instalación de un servidor LAMP y un servidor FTP en la máquina Linux de la Red Virtual vamos a instalar en la misma máquina un servidor OpenSSH (http://www.openssh.com/) que nos permita su administración remota.

Desarrollo de la Práctica

1. Instalar el servidor ***OpenSSH*** desde los repositorios oficiales de Ubuntu

   Al instalar el servidor:

   - Se crean los ficheros de configuración.
   - Se generan las parejas de claves RSA, DSA y ECDSA que se almacenan en el directorio **/etc/ssh**. Además, en este directorio encontramos entre otros archivos:

     ✓ sshd_config: archivo de configuración del servidor SSH
     ✓ ssh_config: archivo de configuración del cliente SSH
     ✓ ssh_host_*_key: clave privada de la máquina (* puede ser rsa o dsa o ecdsa)
     ✓ ssh_host_*_key.pub: clave pública de la máquina (* puede ser rsa o dsa o ecdsa)

2. Consulta las claves públicas (*.pub) y privadas (sin extensión) dentro del directorio **/etc/ssh**

3. Comprobar que el servidor está iniciado y escuchando peticiones en el puerto 22/TCP

4. Iniciar/parar el servidor desde la línea de comandos y probaremos que funciona correctamente.

5. **Configuración de SSH**

   a) Consultar en el fichero de configuración del servidor **/etc/ssh/sshd_config** las directivas habilitadas

   b) Podemos realizar cualquier cambio en el fichero de configuración. Configurar como puerto de escucha del siguiente modo (equipo 01 puerto 2201, equipo 02 puerto 2202, …)

6. **Conexión al servidor**

   a) Para comprobar que podemos conectarnos lo haremos con el siguiente comando desde cualquier de las otras máquinas Linux de la red virtual

   ```
   sudo ssh [usuario]@[IP maquina] –p [puerto]
   ```

   b) Vamos a comprobar que podemos conectarnos desde la máquina Windows7 de la red virtual. Para ello utilizaremos el cliente **Putty** para establecer una conexión SSH al servidor.

   Al conectarnos, el servidor envía un resumen ***fingerprint*** de su clave pública RSA. En este punto debemos comprobar que es realmente el resumen de la clave del servidor para evitar una suplantación de identidad. Para ello, desde el mismo servidor podemos ejecutar el comando

   ```
   ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key
   ```

   y así obtener el ***fingerprint*** de la clave. El cliente SSH almacena el ***fingerprint*** de la clave del servidor. En las próximas conexiones, ya no pide la aceptación por parte del usuario. Si en una conexión el ***finngerprint*** enviado por el servidor no coincide con el almacenado por el cliente se avisará al usuario.

7. **Configuración avanzada de SSH**

   a) Crear en la MV donde se ha instalado el servidor SSH un nuevo usuario **profesor**. Configurar el servidor SSH para que sólo pueda conectarse el usuario **profesor**

   b) Restringir aún más el acceso, permitiendo que el usuario ***profesor*** pueda conectarse únicamente desde la IP del equipo del profesor 192.168.206.100

   c) Limitar el número de reintentos de conexión a 3 mediante la directiva correspondiente

Documentación a Entregar

Se entregará un documento PDF **P62-ServidorOpenSSH.pdf**, en el que se explicará los pasos realizados en la instalación y configuración del servidor.

Además, se comprobará por parte del profesor el correcto funcionamiento de la misma.