Práctica Seguridad 2020-2021

Siguiendo los materiales de los apuntes de SSH, utiliza 2 máquinas con sistemas operativos Debian o Ubuntu para montar un cliente y un servidor SSH (si tu sistema principal es Linux, entonces necesitarás una máquina virtual con Debian/Ubuntu para montar SSH y otra con Windows 10 para el cliente). Las máquinas virtuales deben tener la red en modo puente (bridge).

Debes realizar los siguientes pasos (hasta el paso 6, se utilizará como cliente una máquina Linux):

1. Instala el servidor de OpenSSH en una de las máquinas (está será el servidor). Crea un usuario llamado **daw** con el directorio home → /home/daw.
2. Desde la otra máquina prueba a conectarte a dicho usuario (daw) en el servidor.
3. Crea un par de claves privada/pública en el cliente y copia (usando un comando) la clave pública en el servidor. Registra la clave pública para el usuario **daw** en el archivo correspondiente (apuntes).
4. En el servidor, desactiva el acceso por contraseña y reinicia el servicio SSH. Prueba a conectarte por SSH usando la clave privada.
5. Finalmente, copia un archivo desde la máquina cliente al servidor (en la carpeta home de daw), y ejecuta de forma remota el comando "ls -l" para comprobar que se ha copiado correctamente. Ten en cuenta que debes indicar la clave privada (opción -i).
6. Conéctate ahora desde una máquina Windows (puede ser el sistema anfitrión) al servidor SSH usando Putty y Puttygen.
    - Con PuttyGen debes convertir la clave privada a formato Putty y usarla como se indica en los apuntes https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Ficheros a entregar:

Debes crear un documento (pdf) indicando los pasos que has seguido y los comandos utilizados, acompañado de capturas de pantalla donde se verá en todo momento el usuario y la fecha del sistema. Puedes ejecutar en el terminal el comando **date** para visualizar la fecha si no quieres hacer una captura a pantalla completa.