Que:

Con los datos que vemos en clase y la información que podáis encontrar en Internet tenéis que:

1. Seleccionar un Servidor SSH, justificar su elección y finalmente instalarlo
2. Configurarlo para permitir su acceso por clave publica/privada
3. Si no existe o es incorrecta que permita el acceso por contraseña con un único intento
4. Si se borra la clave en el cliente NO ha de poder entrar sin contraseña

Per a Que:

Haciendo esta actividad aprenderé a instalar y configurar un servidor SSH en mi caso el servidor OpenSSH que es uno de los mas problemáticos en Ubuntu sobre todo entender los términos de clave privada y publica también en como configurar tu servidor y cliente para que puedan conectarse entre si ademas aprenderé a como prevenir fallos que seria haciendo copias de seguridad de todo lo que vaya a utilizar como claves, fichero de configuración, etc..

Sobre todo adquiriré conocimientos básicos en el manejo de comandos especializados con el manejo de SSH para así poder preparar tanto mi servidor OpenSSH como mi cliente incluso aumentare mi orientación navegando entre directorios del terminal y así facilitarme actividades futuras.

Com:

He elegido el servidor OpenSSH por varios motivos uno de ellos seria la facilidad de recolectar información de ester servidor SSH ya que lo hemos visto en clase y nuestro profesor nos ha otorgado apuntes y el openssh es bastante popular eso ayuda a recolectar información, también viene instalado en el Sistema Operativo Ubuntu sino fuera el caso con utilizar **sudo apt install openssh-server bastaría.**

Una vez descargado el servidor tendríamos que gestionar las claves, por posibles fallas futuras hare copia de las claves actuales en el directorio **/etc/ssh** antes de hacer el comando de copiar y pegar creare una carpeta con **mkdir** en Escriptori llamada claves una vez instaurada procedemos a abrir el terminal nos dirijamos al directorio que contiene las claves **/etc/ssh escr**ibimos el comando **sudo cp ssh_host* ~/Escriptori/claves** ahora generamos las claves con **ssh-keygen -t rsa** si hubiéramos puesto en mayúsculas RSA indicaríamos la versión y nosotros queremos la versión 2 que es la mas actual. Una vez creadas nos vamos a la ruta **/home/ricardo_mascarell_1daw/.ssh** con **cd** para ver que se hayan creado las claves del cliente.

Continuamos con la configuración para permitir acceso por clave publica/privada antes que nada iniciaremos el servidor con **sudo /etc/init.d/ssh start** nos situaremos en el directorio donde se encuentra el fichero de configuración del servidor ssh **/etc/ssh/** y abrimos el fichero **sshd_config** con el comando **sudo nano sshd_config** y una vez dentro buscamos **PubkeyAuthentication** esta por predeterminado en **yes** pero para evitar errores lo comprobamos y guardamos e salimos, para que los guardamos se establezcan habrá que reiniciar el servidos **sudo /etc/init.d/ssh restart** ahora nos vamos al siguiente directorio **/home/ricardo_mascarell_1daw/.ssh** con **cd** y procedemos a copiar las claves publicas del cliente al servidor para ello mi **compañero Vicent** hará de cliente y tendrá que iniciar el ssh ademas gastaremos el **usuarios lliurex** que esta en ambas maquinas, en la maquina cliente hacemos el siguiente comando que copiara las copiara las claves del cliente al

archivor del servidor **ssh-copy-id -i id_rsa.pub lliurex@10.0.109.13** como vemos **“id_rsa.pub”** es la clave que pasamos y **“10.0.109.13”** es mi IP.

Para que no haya problemas reiniciaremos ambos tanto cliente como servidor **sudo /etc/init.d/ssh restart,** ahora en el servidor volvemos al directorio **/home/ricardo_mascarell_1daw/.ssh** utilizaremos el comando **ls** para ver el contenido de la carpeta y veremos un archivo que antes no estaba llamado **“authorized_keys”** con esto el servidor podrá comprobar si el cliente tiene la clave privada y podremos acceder de cliente a servidor sin que nos pida la contraseña de usuario.

En este momento entraremos accederemos desde el **cliente al servidor** poniendo el siguiente comando en el terminal **ssh lliurex@10.0.109.13,** lliurex es el usuario en común que tienen ambos host ademas la ip es la del servidor y si todo funciona sin ningún problema nos pedirá la autenticación de la clave privada ahora ponemos exit para seguir con el siguiente paso.

Ahora para cuando no exista la clave o sea incorrecta que permita el acceso por contraseña con un único intento tendremos que empezar accediendo al fichero de configuración de ssh **/etc/ssh/sshd_config** con **cd** seguimos entrando al fichero **sshd_config** con **sudo nano sshd_config** una vez dentro buscamos **“MaxAuthTries”** la des comentamos y la dejamos en **2 ya que tiene dos intentos 1 para la clave publica y el otro para la contraseña,** reiniciamos para que se apliquen los cambios **sudo /etc/init.d/ssh restart.**

Para acabar comprobaremos que solo permita un intento conectando de cliente al servidor de normal tienes hasta seis intento pero he lo he configurado para que solo tenga un intento el cliente, precedemos desde la maquina de mi compañero a poner este comando para conectar **ssh lliurex@10.0.109.13 y** me funciona correctamente.

Cuando borremos la clave del cliente no ha de poder entrar sin contraseña una vez eliminada la clave del cliente en el directorio **/home/ricardo_mascarell_1daw/.ssh** con el comando **rm .ssh//id_rsa.pub,** esto no nos causara ningún problema al servido ya que las claves se puede generar nuevamente con el comando **ssh-keygen -t rsa**. Ahora **reiniciamos la maquina** así **borramos los datos de cache de ubuntu** y iniciamos otra vez el servidor **sudo /etc/init.d/ssh start** y probamos a entrar desde el cliente pero no nos deja ya que hemos eliminado los datos cache reiniciando el host.

Conclusion:

Personalmente esta practica me ha parecido útil ya que me ha echo mas precavido a la hora de hacer mis elecciones porque con que cometa un error grave podría hacer que mi servidor ssh no funciones y también me ha parecido conveniente hasta el punto 4 de las actividad ya que nadie de la clase la ha podido hacer y no hemos podido aprender como hacerla y es algo a mi parecer que deberíamos habernos introducido mas a fondo por el resto de apartado que aun con la falta de información nos ha ido bastante bien, ademas cambiar lo que he comentado antes de la actividad 4 dedicar una practica solo para ella o explicarla paso a paso como hacerlo y así conseguir mas experiencia con el manejo de del servidor SSH OpenSHH incluso añadiría otro ejercicio parecido al 4 habiendo sido explicado con antelación.

Si soy sincero no me a gustado por que hemos empezado la practicas sin tener algunos términos entendidos como por ejemplo el funcionamiento de cada clave tanto la publica y privada también a la hora de conectarse al servidor no sabia si era copiando la publica o privada, me ha ido apareciendo dudas parecidas mientras recolectaba información para hacerlo y el enunciado no nos explicaba exactamente como realizar dicha practica esto se hubiera simplificado si se hubiera bajado de nivel ya que es la primera actividad y todavía estamos un poco verdes respecto a este tema.