**SERVICIOS BÁSICOS EN LINUX. SSH**

### ¿Qué es SSH?

**1**

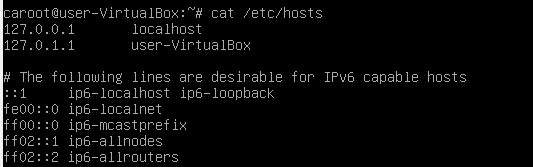
**Pasos Previos a la actividad**

1.- Máquina Ubuntu: **Nombre : servertunombre**

2.- Máquina Ubuntu: **Nombre: clientetunombre**

3.-Para cambiar el nombre a los equipos en /etc/hostname y en /etc/hosts

3.1.- En /etc/host (es posible definir una pequeña tabla que asocie direcciones IP y nombres de equipos)



Sustituimos User-VirtualBox por el nombre

3.2.- En /etc/hostname (nombre de la máquina propiamente dicha. Ahí quitamos el nombre y ponemos el nuevo.



4.- Red : adaptador puente.

**2**

**Servicios básicos en Linux. SSH**

* **Objetivo general:**

Que los alumnos dominen los pasos necesarios para instalar y probar de forma básica un servidor SSH en Linux (en este caso vamos a utilizar openssh-server).

SSH es un servicio que permite acceder a una consola remota. Encripta la información.

* **Pasos de la actividad:**

***Pasos en el servidor para instalar el servicio SSH:***

* **Paso 1**: Comprobar que está instalado el paquete ssh

Indica el comando usado.

* **Paso 2**: Instalación del paquete ssh

Indica el comando usado.

* **Paso 3**: Comprobación de la red. El servicio SSH funciona en la capa de aplicación y para que funcione es necesario que las capas inferiores funcionen. Para ello:

Ifconfig , dándome información de IP asignada

Inserta una captura de pantalla con el resultado de la ejecución.

|  |
| --- |
|  |

* **Paso 4**: Comprobación de puerto y reinicio del servicio (Nos vale para ver si el servicio realmente está OK)

**4.1.-** Comprobar si el puerto está abierto (Cuando el servicio se lanza se abre el puerto 22)

Para ello debemos usar el comando netstat, que primeramente instalaremos.(este es el nombre completo de netstat-nat)

Indica el comando usado.

Luego ejecutamos : **sudo netstat -putan | grep 22 ,**si el puerto está a la escucha es que está abierto

**4.2.-** Reiniciar el servicio

En el diretorio /etc/init.d ejecutar: **./ssh restart**

* **Paso 5**: Ver la IP asignada al servidor

Ejecutar:**Ifconfig e indica la IP**

***Pasos en el cliente para utilizar el servicio SSH:***

* **Paso 6**: En el pc cliente el sofware cliente ssh, está activado por defecto.

Creamos un usuario manolo,en el servidor

Y en el cliente ejecutamos**: ssh**[**manolo@IP\_ del\_ servidor**](mailto:usuario@172.16.2.x) **-p 22**

Tener en cuenta que:

1. [**IP\_ del\_ servidor**](mailto:usuario@172.16.2.x)es la dirección IP del equipo remoto (del equipo servidor) al que te conectas.
2. **usuario** es el nombre del usuario del equipo remoto ( de equipo servidor) con cuyas credenciales te vas a conectar.
3. **-p 22** indica que nos vamos a conectar al **puerto 22** del equipo remoto ya que por este puerto escucha SSH (a no ser que lo modifiquemos). Al ser el 22 el puerto por defecto no es necesario especificar esta opción.
4. La primera vez que conectas al servidor nos pide que validemos la clave pública del servidor (tecleamos yes). Cuando hayamos terminado la sesión para salir ejecutamos **exit**.

Inserta una captura de pantalla en la que se vea como conectas al servidor, ejecutas algún comando por ejemplo pwd y terminas la sesión.

(Por ejemplo, para ver que estamos en el servidor desde el cliente. Crear en el / un directorio llamado prueba y desde el cliente una vez iniciada la conexión ver el raíz del servidor)

|  |
| --- |
|  |

**exit** para cerrar la conexión

***Pasos a realizar para la configuración avanzada del servidor SSH.***

* **Paso 7**: Ten en cuenta que en la configuración del servicio SSH entran en juego los siguientes ficheros:
* **/etc/init.d/ssh**: fichero que permite iniciar/parar el servidor ssh.
* **/usr/bin/sshd**: archivo ejecutable del servidor.
* **/etc/ssh/sshd\_config**: fichero de configuración del servidor ssh.
* **/etc/ssh/ssh\_config**: fichero de configuración del cliente ssh.
* **Paso 8**: Antes de realizar cambios en el fichero de configuración del servidor siempre es conveniente hacer una copia de seguridad del original. Realizar una copia de sshd\_configcoon el nombre de sshd\_config.original

Indica como haz realizado la copia

* **Paso 9**: Edita el fichero de configuración del servidor

Indica el comando usado

* **Paso 10**: De forma predeterminada el servidor ssh escucha por el puerto 22. Podemos cambiar dicha opción haciendo:

port 20022

Deberíamos reiniciar el servicio en /etc/init.d con el comando **./sshrestart** pero si no lo coje reiniciamos el sistema.

Indicar conexión con usuario manolo y puerto 20022

**Paso 11**: De forma predeterminada el usuario root no puede acceder a través de ssh.

Tener en cuenta que:

1. El usuario **root** es el administrador del sistema, por defecto viene **desactivado** en Ubuntu, por eso se utiliza **sudo** para ejecutar tareas administrativas con el usuario que definimos en la instalación. Para **activar** el usuario root sólo hemos de **asignarle una contraseña** ejecutando:

sudopasswdroot

1. Para **cambiar de usuario** utilizamos el comando **su <usuario>**. Si queremos cambiar al usuario root ejecutamos:

suroot

1. Para volver al usuario user ejecutaríamos

suuser

1.- Asignar al equipo servidor una password a root

2.- Ver que desde cliente no podemos acceder mediante ssh, al usuario root

3.- Editar el fichero de configuración /etc/ssh/sshd\_config

4.- Modificar la línea PermitRootLogin e indicar parámetro yes

5.-Reiniciar

6.- Comprobar que ahora puedo acceder con root

Mostrar pantallazo del acceso

Tener en cuenta que:

Es por cuestiones de seguridad, no es bueno que desde una máquina podamos acceder de forma remota a otra máquina con root. Si alguien malintencionado lo lograse, podría hacer un destrozo

* **Paso 12**: Para permitir que el contenido del fichero **/etc/issue.net** se utilice como banner de bienvenida debemos descomentar (borrar la #) la siguiente línea:

Banner /etc/issue.net

* **Paso 13**: **editamos** el fichero /etc/issue.net y le introducimos un mensaje personalizado de bienvenida y reiniciamos servidor y la conexión desde el cliente.

BIENVENIDO AL SISTEMA DE CONEXIÓN REMOTA SSH

Acceder con manolo y ver que nos aparace el mensaje del fichero issue.net. Mostrar pantallazo

**En la conexión ejecutamos :ssh -X** [**manolo@172.16.1.14**](mailto:manolo@172.16.1.14)**-p 20022 y ejecutando xterm nos sale un terminal gráfico**

* **Paso 14:**En el fichero **/etc/ssh/sshd\_config**: fichero de configuración del servidor ssh se indica que está permitido ejecutar X en la llamada a la conexión:

entrada X11Forwarding yes en /etc/ssh/sshd\_config, y probar

**En la conexión ejecutamos :ssh -X** [**manolo@172.16.1.14**](mailto:manolo@172.16.1.14)**-p 20022 y ejecutando xterm nos sale un terminal gráfico**

* **Paso 15:** Si quiero copiar un fichero desde el servidor o hacia el servidor.

Vamos a realizar un ejercicio.

1.- En el Pc servidor, el usuario manolo que cree un directorio llamado transfer y un documento dentro del mismo llamado f1

2.- Para copiar ese fichero en un directorio del equipo cliente:

scp manolo@IP\_servidor:/home/manolo/transfer/f1 /home/user

(home/user, es del equipo cliente)

3.- Hacer un fichero de texto llamado f2 en cliente y copiarlo a /home/manolo/transfer

scp /home/user/f2 manolo@IP\_servidor:/home/manolo/transfer/

* **Paso 16:** Otra forma de conexión en lugar de hacerla por terminal usar el nautilus y en la barra (<ctrl><l>)

ssh:[//usuario@172.16.2.x](mailto://usuario@172.16.2.x)[:222 (:nº de puerto si lo he cambiado)](mailto:usuario@172.16.2.x)

otra forma de hacer esto es seleccionando del menú <lugares><conectar con el servidor>

**tipo de servicio**: SSH

**servidor**: ip del mismo

**puerto**: 22

**carpeta**: /home/manolo

**nombre de usuario**: manolo

* **Paso 17 :**Acceder desde Windows utilizando el putty al servidor ssh.

17.1.-Mostrar pantalla inicial donde indicas ip del servidor y el puerto a usar

17.2.- Pantalla de acceso con usuario autorizado

17.3.- Crear un directorio y dentro del mismo un fichero en el servidor y comprobar que se ha creado

### ¿Qué es SSH?

Inicialmente la administración remota se hacía con la orden telnet. Este servicio permite abrir una consola desde un terminal al servidor para trabajar en él.

Telnet no se creó pensando en la seguridad, sino en que fuera fácil de usar. En aquel momento la seguridad en las redes no era un aspecto crítico.

* Telnet enviá toda la información a través de la red en forma de texto plano, incluidas las contraseñas, por lo que cualquier herramienta capaz de monitorizar el tráfico de red que capture las tramas de datos puede obtener de ellas el login y contraseña de usuario fácilmente.
* Otro punto débil que tiene es que no permite restringir el acceso al usuario root y que no guarda la información acerca de los intentos fallidos de conexión.

En la actualidad la herramienta de administración remota más utilizada es Secure Shell (SSH). SSH permite realizar conexiones seguras entre equipos unidos mediante una red insegura como puede ser, por ejemplo, Internet. Utiliza el puerto 22 y sigue el modelo cliente/servidor.

Su objetivo es establecer conexiones remotas que permitan la transmisión segura de cualquier tipo de datos: archivos, contraseñas, órdenes de administración, sesiones gráficas remotas, etc.

### Algunas ventajas de utilizar SSH

Las principales ventajas que ofrece la utilización de SSH, como herramienta de administración remota, son:

* Después de la primera conexión, el cliente puede saber que se está conectando al **mismo servidor en futuras sesiones**.
* El cliente **transmite** la información de **autenticación** de forma **cifrada**.
* Todos los **datos** que se envián durante la conexión son **cifrados**.

Además de estas ventajas, con la utilización de SSH se evitan:

1. **La interceptación de la comunicación entre dos sistemas** por parte de una tercera máquina que copie la información que circula entre ellas, y puede introducir modificaciones y reenviarlas a la máquina destino.
2. **La suplantación de un host o enmascaramiento**, es decir, que una máquina pueda fingir que es la máquina destino de un mensaje. El cliente no se da cuenta de que está siendo engañado y continua la transmisión. (Ataque **man in themiddle**)

Ambos problemas se evitan con el **cifrado de paquetes** mediante claves que sólo son conocidas por el sistema local y remoto.