

Unidad de Trabajo n°1 – Actividad de desarrollo – Servicios en Linux - SSH

Servicios de red e Internet - I.E.S. Siete Palmas

- **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. Hasta aquí se trata de lo mismo que Telnet. La diferencia está en que Telnet no encripta la información mientras que SSH sí lo hace, por lo que se recomienda que se use *ssh* en vez de *telnet* siempre que sea posible.

- **Duración prevista:** 1 hora aproximadamente.
- **Software:** Distribución Ubuntu 11.04.
- **Mínimos que se persiguen en la actividad:**
 - Dominio de los pasos necesarios para instalar y utilizar los servicios básicos de Linux.
- **Documentación:**
 - Guías en español de las principales distribuciones de Linux (<http://linux-cd.com.ar>)
 - www.protocols.com
- **Pasos de la Actividad:**

Pasos en el Servidor para instalar el servicio SSH:

- **Paso 1:** Comprobar lo que hay instalado que tenga que ver con ssh.
`dpkg -l *ssh*`

```
root@rincon-desktop:~# dpkg -l *ssh*
Desired=Unknown/Install/Remove/Purge/Hold
| Estado=No/Instalado/Config-files/Desempaquetado/Fallo-config/Medio-inst/espera-disparo/pendien
e-disparo
|/ Err?=(ninguno)/Retenido/Requiere-reinst/X=ambos problemas (Estado,Err: mayúsc.=malo)
||/ Nombre Versión Descripción
+++-----+-----+-----+
un libpam-ssh <ninguna> (no hay ninguna descripción disponible)
un openssh-blacklist <ninguna> (no hay ninguna descripción disponible)
un openssh-blacklist <ninguna> (no hay ninguna descripción disponible)
ii openssh-client 1:5.1p1-5ubuntu1 secure shell client, an rlogin/rsh/rcp replacement
un openssh-server <ninguna> (no hay ninguna descripción disponible)
un ssh <ninguna> (no hay ninguna descripción disponible)
un ssh-askpass <ninguna> (no hay ninguna descripción disponible)
ii ssh-askpass-gnome 1:5.1p1-5ubuntu1 interactive X program to prompt users for a passphra
un ssh-client <ninguna> (no hay ninguna descripción disponible)
un ssh-krb5 <ninguna> (no hay ninguna descripción disponible)
root@rincon-desktop:~#
```

En la ventana anterior se ve que el paquete openssh-server no está instalado (u de Unknown en la primera columna) y estado no instalado (n de No en la segunda columna).

- **Paso 2:** Si no recordamos el nombre del paquete *openssh-server* podemos buscar en el repositorio todos los paquetes que tengan algo que ver con ssh.
`apt-cache search ssh`

- Paso 3: Instalación del paquete servidor de openssh-server.
apt-get install openssh-server

Nota: Como resumen de lo más importante que tiene que ver con la gestión de paquetes:

Comando	Significado
<i>dpkg -l <patron></i>	Busca el estado de todos los paquetes que cumplen con el patrón <patrón>
<i>apt-get install <paquete></i>	Instala el paquete <paquete>
<i>apt-cache search <patrón></i>	Busca en el repositorio todo lo que tiene que ver con el patrón <patrón>
<i>apt-get remove <paquete></i>	Desinstala el paquete <paquete>
<i>apt-get update</i>	Actualiza la lista de paquetes del repositorio a la que tiene acceso el equipo.
<i>apt-get upgrade</i>	Actualiza la versión de todos los paquetes instalados en el sistema.

- Paso 4: Comprobación de la red. El servicio *SSH* funciona en capa de aplicación y para que funcione es necesario que las capas inferiores funcionen. Para ello comprobamos:
ifconfig
ping www.terra.es
- Paso 5: Ejecución del servicio:
/etc/init.d/ssh start

Pasos en el Cliente para utilizar el servicio ssh:

- Paso 6: Realizamos la llamada al servidor desde el equipo cliente.
ssh administrador@172.30.22.1 -p 22

Ten en cuenta lo siguiente:

1. En la línea anterior se supone que *172.30.22.1* es la dirección IP del servidor SSH al que te conectas.
2. *administrador* es el usuario del sistema remoto al que te conectas.
3. La opción *-p 22* indica que te estás conectando al puerto 22 del equipo remoto, que es el valor por defecto por lo que no hace falta ponerlo. Si se cambiase, por razones de seguridad, el puerto de escucha del servidor SSH, deberíamos especificar ese puerto con la opción *-p*.

Pasos a realizar en la configuración avanzada de un servidor SSH:

- Paso 7: Ten en cuenta que en la configuración de un servidor SSH entran en juego los siguientes ficheros:

- */etc/init.d/ssh*: fichero que inicia el servidor ssh.
- */usr/sbin/sshd*: archivo ejecutable.
- */etc/ssh/sshd_config*: es el fichero de configuración del servidor ssh.
- */etc/ssh/ssh_config*: es el fichero de configuración del cliente ssh.

- Paso 8: Antes de realizar cambios en un fichero de Configuración siempre es interesante hacer una copia de seguridad del original.
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
- Paso 9: Edita el fichero de configuración del servidor openssh-server.
vi /etc/ssh/sshd_config
- Paso 10: De forma predeterminada el servidor ssh escucha por el puerto 22. Puedes cambiar dicha opción, aumentando la seguridad, haciendo:

port 20022

- Paso 11: De forma predeterminada el usuario root puede acceder a través de ssh. Puedes cambiar dicha opción, aumentando la seguridad, haciendo:
PermitRootLogin no
- Paso 12: Para permitir que el contenido del fichero /etc/issue.net se utilice como banner de bienvenida debes descomentar la siguiente línea:
Banner /etc/issue.net
- Paso 13: Para que todos estos cambios tengan efecto debes reiniciar el servidor openssh-server:
/etc/init.d/ssh restart
- Paso 14: Para que openssh-server arranque cuando lo haga el sistema:
update-rc.d ssh defaults
- Paso 15: Para que openssh-server no arranque cuando lo haga el sistema:
update-rc.d -f ssh remove