SSH o también conocido como Secure Shell, es un protocolo y el nombre del programa que lo implementa.

SSH es ampliamente conocido por ser el protocolo seguro para la administración remota de servidores, routers, switches y un largo etcétera de equipos.

El protocolo SSH permite manejar por completo el servidor o dispositivo de red mediante un intérprete de órdenes, además, también podemos redirigir el tráfico de X para ejecutar programas gráficos a través de la propia sesión SSH.

Otras características fundamentales de SSH son que nos va a permitir copiar datos de manera segura, tanto archivos como carpetas, a través del protocolo SFTP (SSH FTP), un protocolo hecho desde cero y que no tiene nada que ver con FTPS o FTPES (FTP sobre SSL/TLS).

El protocolo SSH es fundamental en el ámbito de las redes y sistemas, además, podremos configurarlo en detalle para dotar a nuestro sistema de la máxima seguridad posible.

Existen dos versiones de SSH, la versión 1 no se recomienda hoy en día usarla, de hecho, por defecto siempre se utiliza ya la versión SSHv2.

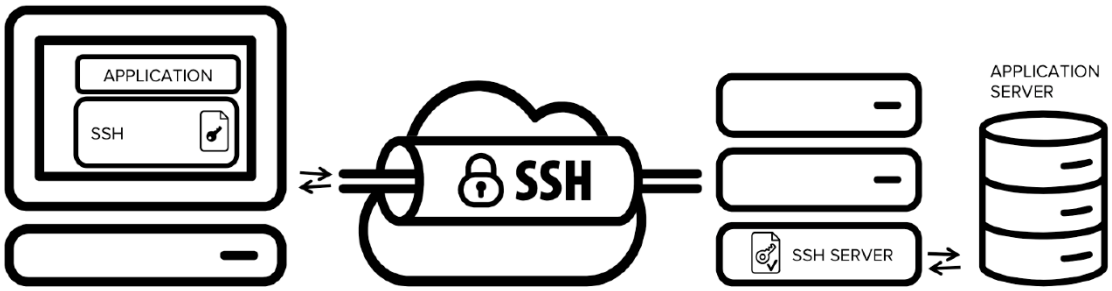
Por defecto SSH utiliza el protocolo TCP de la capa de transporte, y el número de puerto es el 22, no obstante, podremos cambiar el número de puerto para mitigar posibles escaneos de bots al servicio SSH.

Más información :

https://en.wikipedia.org/wiki/Secure_Shell

CONFIDENCIALIDAD

El protocolo SSH proporciona confidencialidad (los datos van cifrados punto a punto)



INTEGRIDAD

Si los datos se modifican o los modifica un usuario malintencionado se podrá detectar,

ya que usa HMAC para comprobar la integridad de todos y cada uno de los datos.

Más información :

https://es.wikipedia.org/wiki/HMAC

https://support.huawei.com/enterprise/es/doc/EDOC1100064353/a56bf8d3/ssh-client-secure-algorithms-hmac

COMPROBAR ESTADO DEL SERVIDOR SSH EN UBUNTU :

1. Obtener un listado de la totalidad de servicios, independientemente de si están activos o inactivos

root@nombrepc:~# systemctl list-units --type service --all

2. Obtener el estado del servicio ssh

root@nombrepc:~# systemctl list-units --type service ssh.service

Verificas que el servidor se encuentre activo con este comando:

root@nombrepc:~# sudo service ssh status

Instalar SSH : https://www.adaweb.es/servidor-ssh-en-ubuntu/

Para instalar SSH en el equipo podemos ejecutar el siguiente comando:

root@nombrepc:~# apt-get install ssh

Si ya tenemos instalado la última versión de ssh, el programa no instalará nada.

El directorio donde se encuentra instalado es /etc/ssh. 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)
- ssh_host_*_key.pub: clave pública de la máquina (* puede ser rsa o dsa).

INSTALACIÓN DEL SERVIDOR SSH EN UBUNTU :

https://help.ubuntu.com/community/SSH/OpenSSH/Configuring?_ga=2.74147152.312157118.1647942508-1909757974.1644235693

Instalación de OpenSSH y puesta en marcha

OpenSSH es el programa servidor/cliente SSH más utilizado por los routers, switches, servidores y un largo etcétera de dispositivos.

Este programa es completamente gratuito y de código abierto.

La instalación de este servidor SSH (si es que no lo tienes ya instalado por defecto) es muy sencilla, simplemente debemos poner en un terminal la siguiente orden:

```
root@nombrepc:~# sudo apt-get install openssh-server
```

- Deberá configurarlo editando el archivo sshd_config en el directorio /etc/ssh

- Primero, haga una copia de seguridad de su archivo sshd_config copiándolo en su directorio de inicio, o haciendo una copia de solo lectura en /etc/ssh haciendo lo siguiente:

```
root@nombrepc:~#  sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.factory-defaults
root@nombrepc:~#  sudo chmod aw /etc/ssh/sshd_config.factory-defaults
```

- Una vez que haya realizado una copia de seguridad de su archivo sshd_config , puede realizar cambios con cualquier editor de texto, por ejemplo;

```
root@nombrepc:~#  sudo gedit /etc/ssh/sshd_config
```

Iniciar el demonio SSH

Si queremos que nuestra máquina disponga de un servidor SSH debemos arrancar el servicio correspondiente.

El servicio SSH se puede encontrar en el directorio /etc/init.d junto a otros muchos servicios de Linux.

También es posible encontrarlo usualmente en /usr/sbin/sshd. Para arrancarlo basta con ejecutar el comando:

```
root@nombrepc:~# /etc/init.d/ssh start [stop | reload | force-reload | restart]
```

```
root@eso2prof:/etc/init.d# ./ssh start
```

```
Starting OpenBSD Secure Shell server... [ ok ]
OpenBSD Secure Shell server not in use (/etc/ssh/sshd_not_to_be_run)
```

Si nos aparece el mensaje anterior, significa que no hemos podido arrancar el servicio ya que se encuentra el archivo sshd_not_to_be_run en el directorio /etc/ssh/

que indica al proceso init que no inicie el servicio, por lo que nosotros tendremos que borrarlo.

Una vez borrado podremos arrancar el servicio SSH sin problemas.

Si posteriormente queremos volver a impedir que el proceso init ejecute el servicio SSH, por ejemplo para que no se inicie al arrancar, volveremos a crear el archivo

sshd_not_to_be_run. Ésto lo podemos hacer ejecutando la siguiente orden, dentro del directorio de ssh (por defecto: /etc/ssh):

```
root@nombrepc:~# touch sshd_not_to_be_run
```

Y finalmente si quieres cambiar el puerto interno de tu PC (que a su vez deberás indicar en el router) ejecutas el siguiente comando:

sudo gedit /etc/ssh/sshd_config

- Una vez que haya realizado los cambios (vea las sugerencias en el resto de esta página), puede aplicarlos guardando el archivo y luego haciendo:

root@nombrepc:~# sudo restart ssh

Si recibe el error "No se puede conectar a Upstart", reinicie ssh con lo siguiente:

root@nombrepc:~# sudo systemctl restart ssh

AUTENTICACIÓN

Podremos autenticarnos frente al servidor SSH de múltiples maneras,

con usuario/clave, criptografía de clave pública e incluso podremos configurar un segundo factor de autenticación

Otro directorio que tenemos que tener muy en cuenta es la de host conocidos,

ya que aquí también es donde configuraremos las claves criptográficas RSA/DSA.

El directorio donde se encuentran los hosts conocidos y las claves públicas es el siguiente:

/home/usuario/.ssh/

Este directorio por defecto está oculto (.ssh) y hay un directorio por cada usuario que haya en el sistema operativo y que se conecte a un servidor remoto.

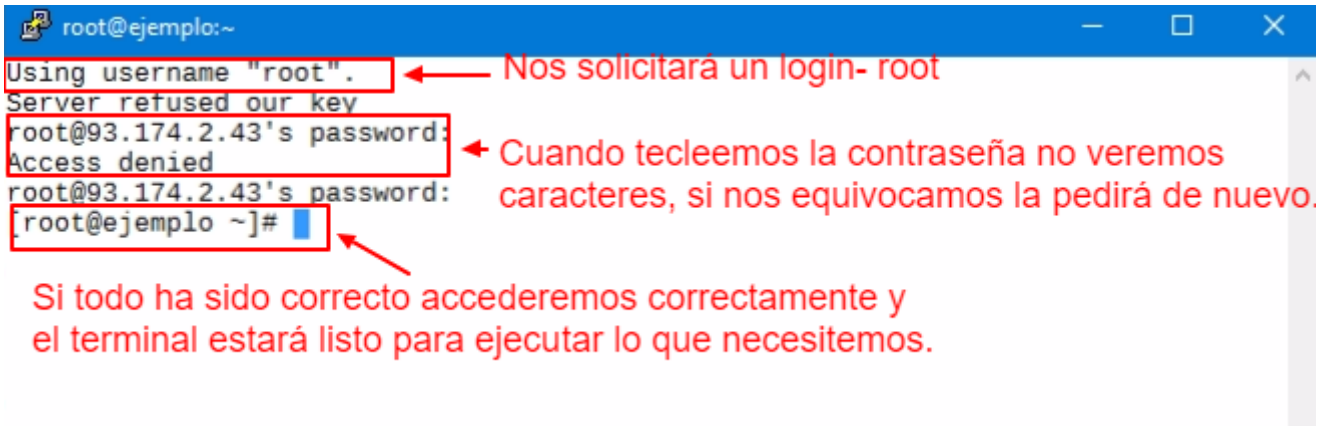
CONECTARNOS AL SERVIDOR SSH DESDE OTRO LINUX

- La aplicación cliente de SSH la encontramos normalmente en /usr/bin/ssh.

Podemos conectarnos a un servidor ssh ejecutando este comando con los siguientes parámetros:

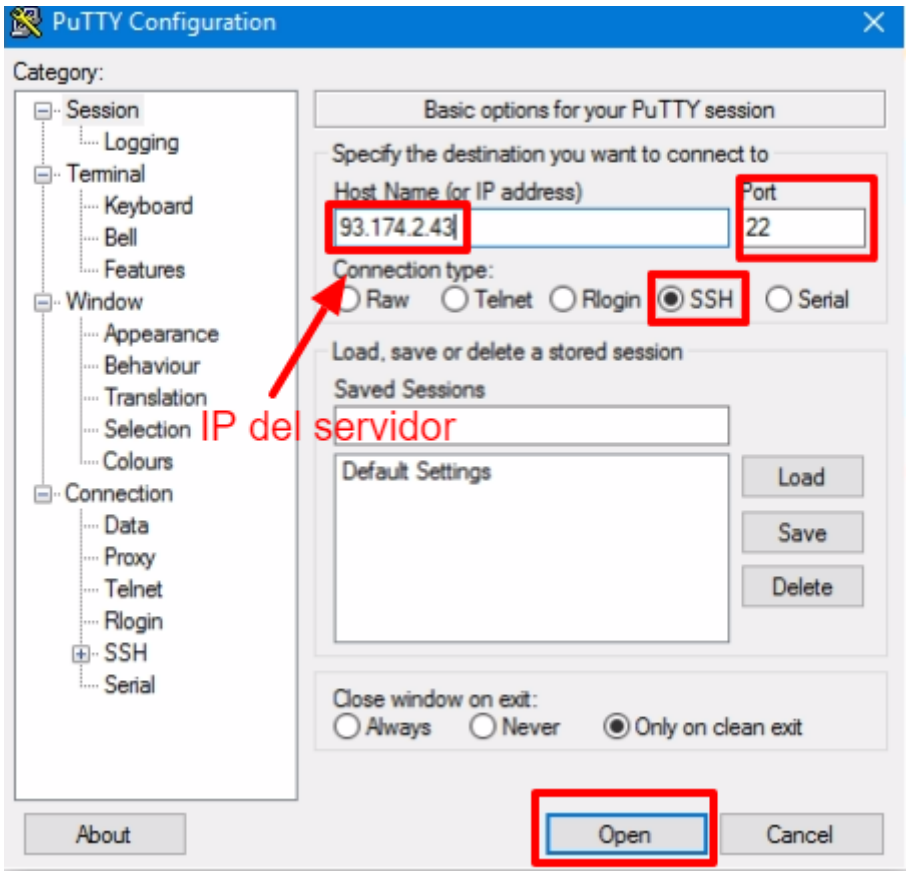
usuario@nombrepc:~$ ssh [nombre_usuario@]nombre_máquina

Una vez conectados se nos solicitará la el usuario que será **root** y la contraseña que se nos habrá facilitado al contratar el servicio.



CONECTARNOS AL SERVIDOR SSH DESDE WINDOWS

PuTTY es un cliente SSH, Telnet, rlogin, y TCP raw con licencia libre.



https://www.putty.org/

Securizando Nuestro SSH

https://help.ubuntu.com/community/SSH/OpenSSH/Configuring?_ga=2.74147152.312157118.1647942508-1909757974.1644235693

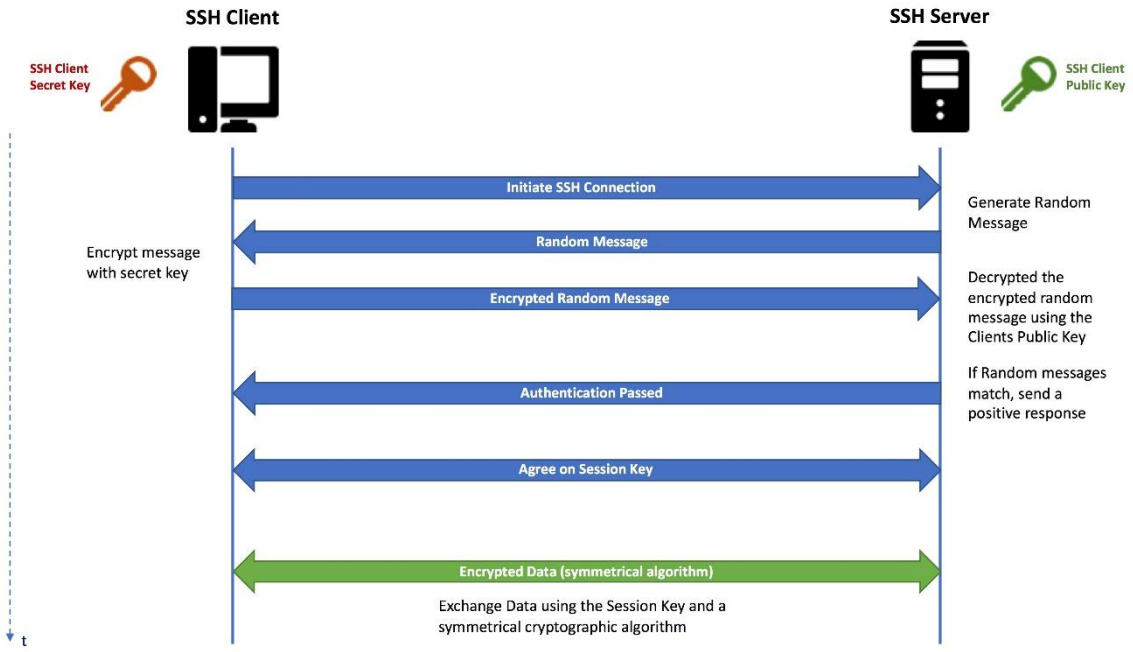
https://codigofacilito.com/articulos/tips-ssh

https://rm-rf.es/como-securizar-un-servidor-ssh/

https://manuelfrancoblog.wordpress.com/2017/06/07/securizar-nuestra-sesion-ssh/

https://www.redeszone.net/tutoriales/seguridad/servidor-ssh-comprobar-seguridad-proteger/

https://www.tiendalinux.com/docs/manuales/redhat/rhl-rg-es-7.1/s1-ssh-protocol.html



SOLUCIÓN A LA PRÁCTICA E1 :

http://sorenlinuxmiguel.blogspot.com/2016/01/practica-5-ssh.html

OTROS USOS DE SSH