SSH

Fecha: 30/11/2021

SSH

- **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.
- El **protocolo SSH** proporciona **confidencialidad** (los datos van cifrados punto a punto), **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**), 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).
- 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.
- https://github.com/KeshiKiD03/pam21/tree/master/pam21:python
- Links de interés:
    a. https://www.redeszone.net/tutoriales/servidores/servidor-openssh-linux-configuracion-maxima-seguridad/

Instalación

- **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:

```
sudo apt install openssh-server
```

- Una vez instalado, debemos tener en cuenta ciertos directorios y órdenes para iniciar, parar y reiniciar el servicio SSH.

```
sudo nano /etc/ssh/sshd_config
```

- 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
```

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

Cambiar el puerto por defecto del servidor SSH

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

```
sudo /etc/init.d/ssh restart
```

Bloquear el acceso root en las conexiones remotas

- Por defecto, cualquier usuario en el sistema operativo que tenga permisos de Shell, podrá iniciar sesión en el servidor. Además, debemos tener en cuenta que si tenemos activado el usuario root, también podrá conectarse al servidor de forma local o remota, evitando al atacante tener que «adivinar» el nombre

de usuario. Por defecto, los bots siempre intentan atacar el puerto 22 y al usuario «root».

- Desactivando al propio usuario root, y usando «sudo» para elevar a permisos de superusuario, evitaremos esto. Además, OpenSSH también nos permitirá deshabilitar el login del usuario root para dotar al sistema de mayor seguridad:

```
PermitRootLogin no
```

- De esta manera las conexiones root quedarán bloqueadas evitando que usuarios no autorizados puedan realizar ataques de fuerza bruta contra nuestro servidor SSH para adivinar las credenciales del usuario Root. También tenemos otras opciones en este apartado, como por ejemplo «PermitRootLogin without-password» donde se permite autenticación pero no con usuario y contraseña, sino con claves criptográficas RSA.

Configuraciones de seguridad adicionales

- Existen otras configuraciones recomendadas para evitar las conexiones no deseadas a nuestro servidor SSH. Estas conexiones son:
    - **LoginGraceTime**: Estableceremos el tiempo necesario para introducir la contraseña, evitando que el atacante tenga que «pensar mucho».
    - **MaxAuthTries**: Número de intentos permitidos al introducir la contraseña antes de desconectarnos.
    - **MaxStartups**: Número de logins simultáneos desde una IP, para evitar que se pueda utilizar la fuerza bruta con varias sesiones a la vez.

- **AllowUsers**: Es crear una lista blanca de usuario. Este parámetro nos permite configurar los usuarios que podrán conectarse. Una medida muy restrictiva pero a la vez muy segura ya que bloqueará todas las conexiones de los usuarios que no estén en el listado. Los usuarios que tengamos aquí podrán conectarse, y el resto no.
- **DenyUsers**: Parecido al anterior, pero ahora creamos una lista negra. Los usuarios que tengamos aquí no podrán conectarse, y el resto sí.
- **AllowGroups/DenyUsers**: Exactamente igual a lo anterior, pero en lugar de crear una lista blanca/negra de usuarios, es de grupos de usuarios.

- Por ejemplo, un archivo de configuración de sshd_config sería el siguiente:

```
Port 22445
PermitRootLogin no
LoginGraceTime 30
MaxAuthTries 3
MaxStartups 3
AllowUsers sergio sergio2
DenyUsers adrian adrian2
```

- Si hemos creado nuevas claves de RSA o DSA por unas con mayor longitud de bits, deberemos ponerlo en el fichero de configuración (o sustituir las anteriores, y así no tendremos que tocar el fichero de configuración), de esta forma obtendremos una seguridad adicional si por ejemplo usamos claves RSA de 4096 bits o superior.

```
HostKey /etc/ssh/ssh_host_ed25519_key
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
```

- Si hemos creado nuevas claves de RSA o DSA por unas con mayor longitud de bits, deberemos ponerlo en el fichero de configuración (o sustituir las anteriores, y así no tendremos que tocar el fichero de configuración), de esta forma obtendremos una seguridad adicional si por ejemplo usamos claves RSA de 4096 bits o superior.

```
Port 22445
PermitRootLogin no
LoginGraceTime 30
MaxAuthTries 3
MaxStartups 3
AllowUsers sergio sergio2
DenyUsers adrian adrian2
```

- Si hemos creado nuevas claves de RSA o DSA por unas con mayor longitud de bits, deberemos ponerlo en el fichero de configuración (o sustituir las anteriores, y así no tendremos que tocar el fichero de configuración), de esta forma obtendremos una seguridad adicional si por ejemplo usamos claves RSA de 4096 bits o superior.

```
Port 22445
PermitRootLogin no
LoginGraceTime 30
MaxAuthTries 3
MaxStartups 3
AllowUsers sergio sergio2
DenyUsers adrian adrian2
```

- Para generar unas claves RSA de 4096 bits nuevas, simplemente deberemos ejecutar el siguiente comando:

```
ssh-keygen -f /etc/ssh/ssh_host_rsa_key -t rsa -b 4096
```

- Si queremos generar nuevas claves ECDSA (con máxima longitud de 512 bits) o ED25519 tendremos que introducir los siguientes comandos:

```
ssh-keygen -f /etc/ssh/ssh_host_ecdsa_key -t ecdsa -b 521
ssh-keygen -f /etc/ssh/ssh_host_ed25519_key -t ed25519
```

Autenticación en SSH: Todos los modos explicados en detalle

- **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.

Usuario y clave

- Si queremos habilitar el login en el servicio a través del usuario y contraseña del sistema, el archivo de configuración deberá tener esta sentencia:

```
PasswordAuthentication yes
```

- De lo contrario, si queremos impedir la autenticación a través de usuario/clave, y permitir únicamente las conexiones a través de claves criptográficas, deberemos indicar no:

```
PasswordAuthentication no
```

- Esta sentencia afecta a todos los usuarios del sistema. Para no quedarnos sin acceso al servidor, deberíamos asegurarnos de que la sentencia **PubkeyAuthentication** esté configurada a «yes», para permitir el inicio de sesión con claves criptográficas.
- Hay otra sentencia relacionada con esto llamada **ChallengeResponseAuthentication**, si ponemos la configuración a «no», no permitirá las conexiones donde se interactúe con el teclado, por lo que si por ejemplo tenemos configurado un One Time Password, no podremos iniciar sesión en el sistema. Si únicamente vamos a usar claves criptográficas, podréis ponerlo a «no» sin problemas.

Clave pública SSH

- Para configurar el acceso con clave pública al servidor, deberemos poner la sentencia siguiente a «yes»:

```
PubkeyAuthentication yes
```

- Así es como activamos la configuración con clave pública SSH en el sistema, no obstante, aún hay algunos pasos que deberemos hacer para que nos podamos conectar a dicho servidor, y es pasar la clave pública al propio equipo. Para hacerlo, deberemos permitir (de momento) la autenticación con usuario/clave, una vez que terminemos todos los pasos podremos denegar la autenticación con usuario y contraseña sin ningún problema.
- Desde el ordenador donde nos queramos conectar al servidor con claves criptográficas, debemos crear dichas claves y pasarlas al servidor. Para crear unas claves RSA de 4096 bits tenemos que poner en el cliente SSH la siguiente orden:

```
ssh-keygen -t rsa -b 4096
```

- En el asistente de generación de estas claves, nos pondrá si queremos guardarlas en /home/usuario/.ssh/id_rsa, le decimos que sí. Posteriormente nos permitirá poner a la clave privada una contraseña de paso, de esta forma, si perdemos la llave privada no pasará nada porque no podrán conectarse, debido a que es necesario siempre introducir una contraseña de paso para poder realizar la conexión correctamente.
- Una vez que hayamos creado la clave pública y privada en nuestro equipo, debemos **enviar la clave pública al servidor SSH** donde nos queramos conectar, ojo: la clave pública.

```
ssh-copy-id usuario@IP_servidor
```

- Automáticamente la clave pública se copiará a dicho servidor, y ya podremos habilitar la autenticación con solo clave pública y automáticamente nos habremos dado de alta. La salida ofrecida por este comando debería ser similar a esto:

```
The authenticity of host '12.34.56.78 (12.34.56.78)' can't be established.
RSA key fingerprint is b1:2d:33:67:ce:35:4d:5f:f3:a8:cd:c0:c4:48:86:12.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '12.34.56.78' (RSA) to the list of known hosts.
user@12.34.56.78's password:
Now try logging into the machine, with "ssh 'user@12.34.56.78'", and check in:
~/.ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

- En esta salida, el usuario deberá confirmar que quiere añadir la identidad e introducir las credenciales de login para la cuenta que se quiere utilizar en ese servicio. Por este motivo es importante que en el servidor aún mantengamos la posibilidad de autenticarse con usuario/clave. Una vez completado este proceso, tendríamos que ser capaces de hacer inicie de sesión en este equipo sin introducir la contraseña:

```
ssh usuario@IP
```

- Recordad poner la directiva «PasswordAuthentication no» para no permitir accesos vía usuario y clave.

https://blog.infranetworking.com/servidor-ssh/

¿Cómo funciona?

- Establecer una **conexión SSH** es sencillo, la única herramienta que vamos a necesitar para hacerlo es una del tipo terminal o consola, como por ejemplo la clásica consola de Linux y Mac, o un programa como PuTTY en el caso de Windows.
- La conexión SSH usa tres ítems: un **usuario**, un **puerto** y un **servidor**. Con solo esos tres **elementos** podemos establecer una **conexión segura** entre dos servidores.
- Esta seguridad se logra mediante el uso de **llaves** y **técnicas** de cifrado. Cada **server** tiene su propia llave de cifrado, y al establecer una conexión por primera vez con un **server** tendremos que añadir el servidor en cuestión a una lista de servidores a los cuales es seguro conectarnos.

¿Cómo se usa?

- La sintaxis básica de conexión por medio de SSH es la siguiente:

```
ssh -p PUERTO USUARIO@SERVIDOR
```

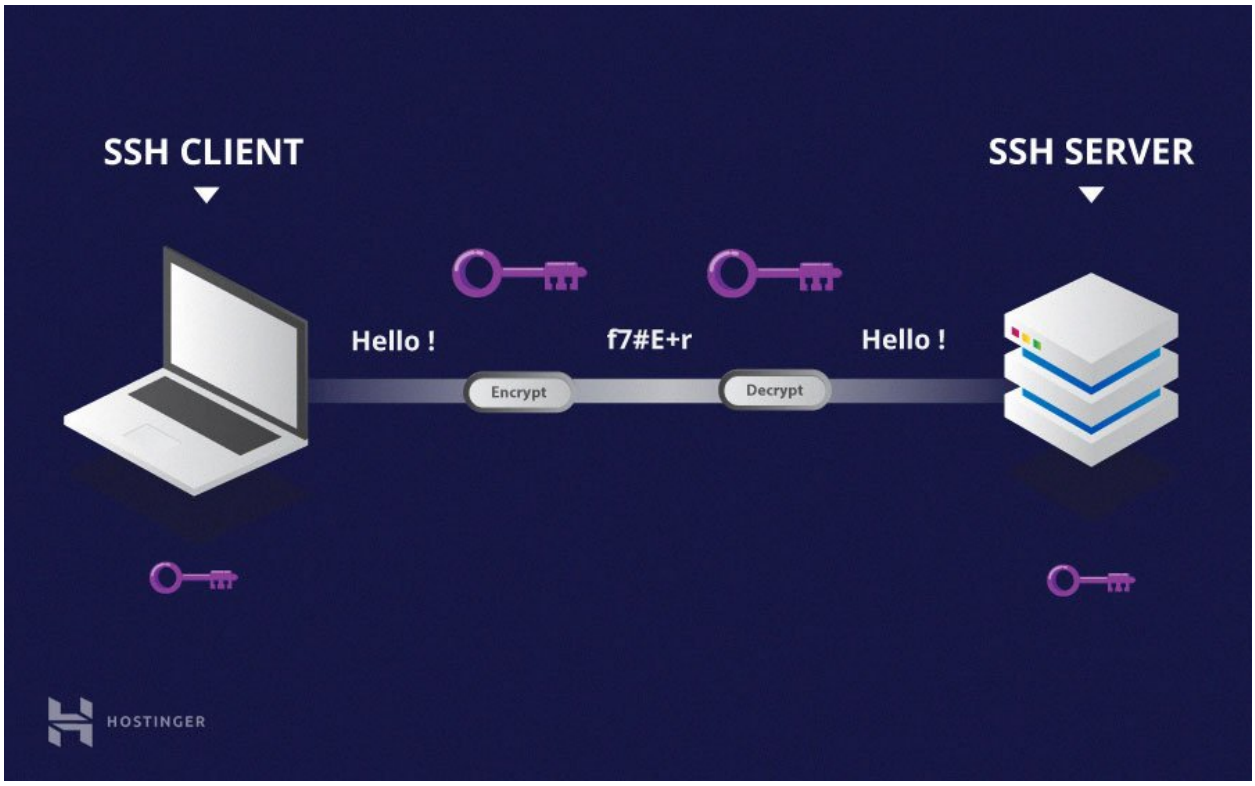
- Como decíamos antes, solo tres datos se requieren, y como podemos ver basándonos en el ejemplo se trata del puerto, del usuario y de la IP o hostame del server en cuestión, en algunos casos incluso no es necesario especificar un puerto si el servidor al cual vamos a conectar está usando el puerto de SSH estándar, que es el 22.

- Algunos ejemplos:
    - **-4 y -6:** la primera opción nos permite forzar la conexión a realizarse mediante una IPv4, mientras que la segunda por su lado hace lo mismo pero una IPv6.
    - **-C:** se utiliza para comprimir la conexión, ayudando a obtener mejores resultados, aunque solo es útil en redes lentas. Si se está trabajando sobre redes rápidas es mejor no utilizar esta opción, pues el efecto será lo opuesto a lo que buscamos.
    - **-p:** nos permite indicar cuál es el puerto de SSH al cual nos queremos conectar, se suele usar cuando dicho puerto es distinto al estándar (22).
    - **-q:** el llamado «modo silencioso», suprime la mayor parte de los mensajes y avisos que puedan aparecer durante la conexión.
    - **-v:** modo verboso, extremadamente útil para ver en detalle todo el proceso de conexión, lo cual nos puede ser de gran utilidad en el caso de que la conexión esté fallando y no logremos darnos cuenta de dónde puede estar el problema.

NOTAS VARIAS:

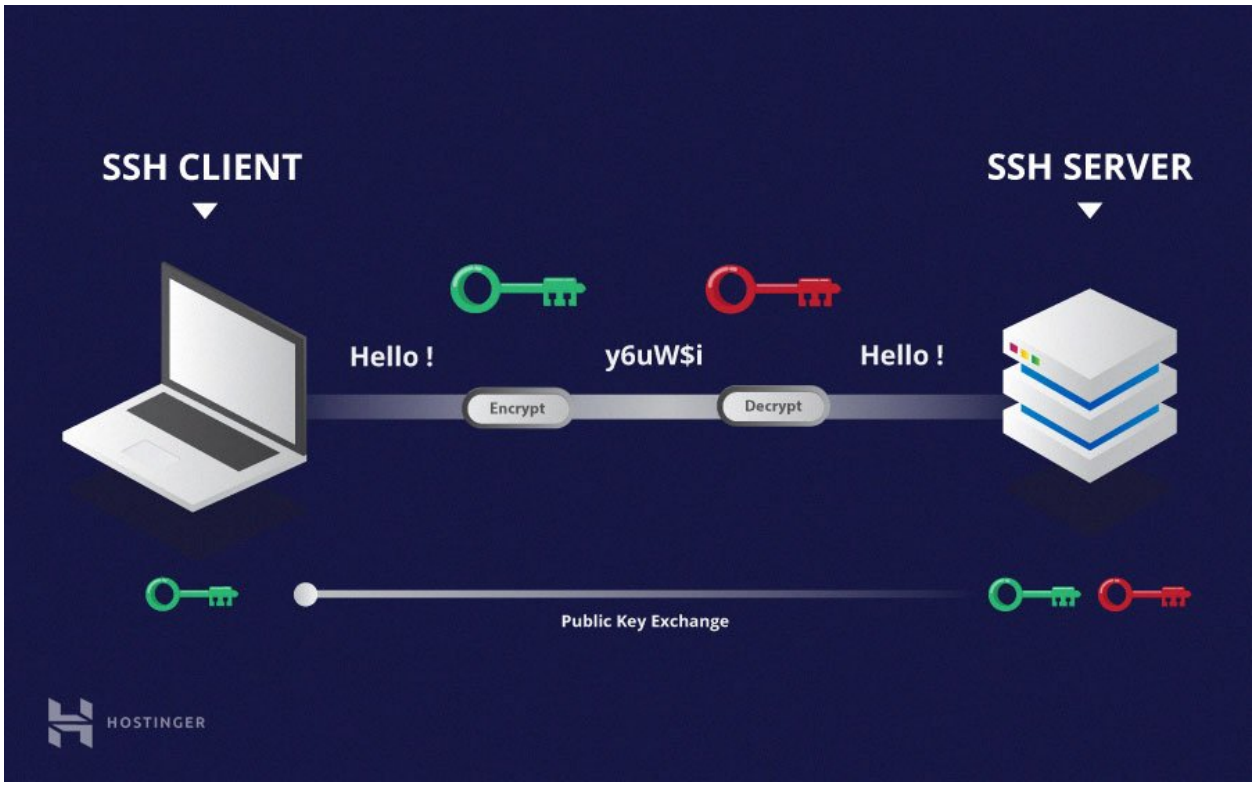
- Instalar el paquete de servidor: apt-get install openssh-server.
- Iniciar el servicio de SSH: service ssh start / restart.
- Iniciar el daemon de SSH: service sshd start.
- A

Cifrado simétrico:

- 

- Es una forma de cifrado en la que se utiliza la clave secreta para tanto el cifrado como el descifrado de un mensaje. Tanto por el cliente como para el host.
- El cifrado simétrico a menudo se llama clave compartida o shared key.
- La llave nunca se revela a terceros.
- El proceso de creación de una clave simétrica, se lleva a cabo mediante un algoritmo de intercambio de llaves.
- **En resumen, dos ordenadores entre sí comparten una clave secreta.**

Cifrado asimétrico:



- Estas dos claves se conocen como la clave pública (public key) y la clave privada (private key).
- Juntas, estas claves forman el par de claves pública-privada (public-private key pair).
- La clave pública, se atribuye abiertamente y se comparte con todas las partes.
- La clave privada no se puede calcular matemáticamente desde la clave pública.
- La relación entre las dos claves es altamente compleja: Un mensaje cifrado por la clave pública de una máquina, sólo puede ser descifrado por la misma clave privada de la máquina.
- Esta relación unidireccional, significa que la clave pública no puede descifrar sus propios mensajes ni descifrar nada cifrado por la clave privada.
- **En resumen, SSH solamente utiliza cifrado asimétrico para la autenticación de usuarios.**

- **Este sistema de cifrado se basa en que cada uno de los equipos involucrados en la comunicación, disponen de un par de claves, una clave pública (puede ser mostrada a cualquiera) y una privada.**
- **Mediante el comando ssh-keygen, puedes generar una pareja de claves pública y privada.**
- **Ejemplo:**

```
ssh-keygen -t rsa -b 4096 -f clave_secreta -N ''
```

Como puedes ver, el método usado para generar la clave es mediante el cifrado RSA. Sin embargo, existen otros muchos como EDCSA o ed25519, por ejemplo.

Te explico el resto de argumentos del comando anterior:

- **-b 4096**: Esto hace que el número de bits de la clave privada sean de 4096.
- **-f clave_secreta**: La clave se guarda en un archivo llamado clave_secreta.
- **-N''**: Evita que no solicite contraseña a la hora de usarla (sí, se puede añadir seguridad extra a las claves para que nadie pueda usarlas sin contraseña).

Estas claves funcionan de modo que **la clave privada**, que es la parte realmente importante, no sea accesible para otros. **Es la llave con la que se descifran los mensajes**.

La clave pública puede ser compartida ya que, en realidad, **a partir de una misma clave privada pueden generarse infinidad de claves públicas distintas**. De hecho, una clave pública se envía en la comunicación inicial entre el cliente y el servidor SSH.

Una vez dispones de una clave pública y otra privada, cuando inicias una conexión SSH puedes tratar de hacerlo con una conexión con cifrado asimétrico de forma que, **si la clave privada figura como 'autorizada' en el servidor, el proceso de autenticación será más rápido y seguro**.

Algunas configuraciones del SSHD.conf:

- **Este sistema de cifrado se basa en que cada uno de los equipos involucrados en la comunicación, disponen de un par de claves, una clave pública (puede ser mostrada a cualquiera) y una privada.**

- Cambiar el puerto por defecto:

Port 2022

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 11022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- Impedir que el usuario root pueda conectarse con contraseña, hay que modificar el valor de PermitRootLogin de YES a NO / Prohibit-Password

PermitRootLogin no

```
#LoginGraceTime 2m
PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

- Impedir que nadie pueda conectarse sin contraseña.

PermitEmptyPasswords no

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PermitEmptyPasswords no
PasswordAuthentication yes
```

- Establecer un timeout en la conexión de 5 minutos:

ClientAliveInterval 300

```
#Compression delayed
ClientAliveInterval 300
#ClientAliveCountMax 3
```

- Reiniciar

systemctl restart sshd

```
[ root@raiolanetworks.servidordepruebas.com ] # systemctl restart sshd
[ root@raiolanetworks.servidordepruebas.com ] # systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-21 11:51:31 EST; 5s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 5999 (sshd)
   CGroup: /system.slice/sshd.service
           └─5999 /usr/sbin/sshd -D

Feb 21 11:51:31 nuevo.cuentamemilongas.com systemd[1]: Starting OpenSSH server daemon...
Feb 21 11:51:31 nuevo.cuentamemilongas.com sshd[5999]: Server listening on 0.0.0.0 port 11022.
Feb 21 11:51:31 nuevo.cuentamemilongas.com sshd[5999]: Server listening on :: port 11022.
Feb 21 11:51:31 nuevo.cuentamemilongas.com systemd[1]: Started OpenSSH server daemon.
```

- Generar la clave pública y ponerlo en authorized_keys.
- Conectarse con la clave privada a través del puerto 11022:

```
fran@soporte $ ssh -p 11022 -i $HOME/.ssh/clave_secreta root@91.134.16.
Last login: Fri Feb 21 12:07:47 2020 from 144.178.129.35
Bienvenido a tu nuevo servidor en Raiola Networks!
[ root@raiolanetworks.servidordepruebas.com ] #
```

- Cambiar el banner en /etc/motd

```
echo 'Bienvenido a tu nuevo servidor en Raiola Networks!' >> /etc/motd
```

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:
- Port 22445

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- **Pluggable Authentication Modules for Linux**, son un conjunto de bibliotecas con las cuales será posible que el administrador del sistema, seleccione la forma en que las aplicaciones autentican a los usuarios de la red local.
- El mecanismo de cómo se autentican los usuarios es sencillo, primero la identidad del usuario se verifica cuando se ingresa la contraseña asignada al usuario, las contraseñas se almacenan en **/etc/passwd.**
- **PAM** se creó como nueva forma de autenticación entre usuarios, lectores de

imprenta digital, reconocimiento óptico de caras… etc.

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos

masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o

cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos

masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o

cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```

Configuración de sshd_config para la máxima seguridad

- Por defecto los servidores SSH utilizan el puerto 22 para las conexiones. Es recomendable cambiar este número de puerto, para evitar que bots o cibercriminales puedan intentar iniciar sesión, aunque por sí solo esto no proporciona seguridad, sí podremos pasar desapercibidos a los escaneos masivos desde Internet. Si por ejemplo queremos usar el puerto 22445 debemos poner en el fichero de configuración lo siguiente:

Cambiar el puerto por defecto del servidor SSH

- Para arrancar el servidor:

```
sudo /etc/init.d/ssh start
```

- Para parar el servidor:

```
sudo /etc/init.d/ssh stop
```

- Para reiniciar el servidor:

```
sudo /etc/init.d/ssh restart
```