TEMA 4 – SSH

INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS DE ACCESO REMOTO

ÍNDICE

1. SSH. ¿Qué es? ¿Para qué sirve?

SSH es el acrónimo de **Secure Shell**, y es un protocolo que se utiliza en el manejo de servidores de forma remota, permitiendo a un usuario realizar toda clase de tareas sobre el mismo.

En las conexiones realizadas por medio de SSH, **toda la información viaja de forma encriptada**, lo cual lo convierte en uno de los medios más seguros a la hora de trabajar en un servidor.

2. Ejemplos de uso de SSH

Copiado de datos: con el protocolo SSH podemos copiar datos, esto se puede lograr por ejemplo mediante herramientas como rsync o scp, que tienen sintaxis sencillas y que usan una conexión vía SSH para copiar datos entre servidores, lo cual hace que toda esta información viaje entre los servidores seguros.

Un ejemplo de esto pueden ser las migraciones de sitios entre servidores, o por supuesto también equipos locales y servidores, sin importar que estén en distintas localizaciones.

Ejecución de comandos remotos. gracias a SSH también tenemos la posibilidad de correr comandos en forma remota. Esto podemos lograr ejecutando una sintaxis en nuestro terminal o, si el comando es complejo, mediante un script en bash.

3. Funcionamiento

La conexión SSH usa tres ítems:

1. Un usuario
2. Un puerto (Por defecto, el 22)
3. Un servidor

Con solo esos tres elementos podemos establecer una conexión segura.

Dicha seguridad se logra mediante el uso de llaves y técnicas de cifrado. Cada servidor tiene su propia llave de cifrado, y al establecer una conexión por primera vez con un servidor tendremos que añadir el servidor en cuestión a una lista de servidores a los cuales es seguro conectarnos.

4. Tipos de Encriptación SSH

Como decíamos, parte de la seguridad que brinda SSH se logra gracias a las técnicas de cifrado, y hay tres de ellas:

- **Encriptación simétrica**: es quizá la más común, y se basa en el uso de una secret key, también llamada **clave secreta** en español. Esta clave se usa tanto en el cifrado como en el descifrado de la conexión.
  Por supuesto si alguien lograra interceptar la conexión y de alguna forma obtuvo la clave secreta (prácticamente imposible pues no es algo preestablecido, es decir que es única para cada conexión) entonces podrá ver claramente la información que se está transfiriendo entre los servidores.

- **Encriptación asimétrica**: en este tipo de conexión utilizamos un total de dos claves, es decir una más que en la simétrica. Se trata de una clave pública y de una clave privada. Cada clave pública está ligada a su propia clave privada, y la información encriptada solo se puede desencriptar conociendo la clave privada, así que incluso si tenemos la clave pública no vamos a poder ver los datos, para eso sí o sí se necesita la privada, la cual por supuesto no es compartida con terceros y no puede ser calculada a partir de la pública.
- ˇ

- **Hashing**: una conexión cifrada con un hash no puede ser revertida, es prácticamente única y casi imposible de predecir, de hecho, solo el servidor que recibirá los datos será capaz de leerlos correctamente. Las conexiones cifradas mediante hash se logran convirtiendo la información en una nueva cadena de datos que poseen una cierta longitud que jamás cambia. El hash que se originó en un

servidor tiene que ser idéntico al que es recibido por el otro servidor, si hubo alteraciones en el hash recibido quiere decir que la información de alguna forma fue interceptada y modificada. El hash que se originó en un servidor tiene que ser idéntico al que es recibido por el otro servidor, si hubo alteraciones en el **Hash** recibido quiere decir que la información de alguna forma fue interceptada y modificada.

5. ¿Cómo se usa?

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

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

Como ya se ha dicho anteriormente, solo tres datos se requieren, y como podemos ver basándonos en el ejemplo se trata del puerto, del usuario y de la IP o hostname del servidor 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.

Existen además otros parámetros adicionales que podemos utilizar en la conexión, todo dependiendo de lo que necesitemos. Algunos de estos parámetros adicionales son los siguientes:

- **-4 y -6**: la primera opción nos permite forzar la conexión a realizarse mediante una IPv4, mientras que la segunda fuerza a realizarse por 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.

6. Instalación

Para la instalación ejecutamos la siguiente instrucción, con privilegios de root:

apt install ssh

Una vez instalado podemos reiniciar el servicio, pararlo,etc... con la orden **systemctl.** Por ejemplo, para reinciar el servicio sería: systemctl restart ssh

Consta de dos componentes básicos:

- El **cliente SSH** que nos permite conectar con un servidor remoto.
- El **demonio del servidor SSH** (más conocido como **sshd**) que está configurado para aceptar conexiones SSH desde sistemas remotos.

Los archivos de configuración de cliente y servidor son diferentes, los podemos localizar en:

- Conf. del cliente: **/etc/ssh/ssh_config**
- Conf. del servidor: **/etc/ssh/sshd_config**

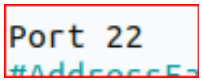
7. Configuración del puerto del servidor.

Por defecto, el servicio ssh corre en el *puerto 22* del servidor. Puesto que se trata de una configuración estándar y conocida, es necesario, por seguridad, cambiarlo. Para ello, debemos editar el fichero de configuración **sshd_config** que está en el directorio /etc/ssh:

nano /etc/ssh/sshd_config

Dentro de ese fichero modificaremos la línea:

También puede aparecer como:



La almohadilla no es necesaria, por tanto, la quitaremos y modificaremos el número del puerto.

Cambiaremos el 22 por otro número. Podemos asignar miles de números distintos, aunque lo recomendable es uno **mayor a 1024**, debido a que hay muchos servicios que corren en puertos menores y así no generamos problemas.

Una vez hemos asignado un nuevo número, simplemente guardamos los cambios y reiniciamos el servicio de SSH. A partir de entonces, estará corriendo nuestro SSH en el nuevo puerto que hemos especificado.