PROTOCOLO SSH

SSH (Secure Shell) es u*n protocolo de red* que permite el acceso remoto a través de una conexión cifrada. Proporciona una autenticación robusta y es compatible con el inicio de sesión remoto seguro, la ejecución de comandos, la transferencia de archivos, el control de acceso, el reenvío de TCP/IP, etc.

Puedes gestionar tus archivos y carpetas a través de una conexión SSH, modificar sus permisos, editar archivos directamente en el servidor, etc.

Es una herramienta para abordar vulnerabilidades que permiten ataques de rastreo de contraseñas. El protocolo ganó popularidad y ha evolucionado.

Posteriormente, se estableció como un estándar para la comunicación segura entre dispositivos.

Características de Secure Shell

- **Privacidad de tus datos** – Secure Shell protege tus datos de la divulgación cifrándolos.
- **Integridad de las comunicaciones** – el protocolo Secure Shell garantiza que la información intercambiada permanece inalterada.
- **Autenticación** – este protocolo requiere una prueba de identidad de los remitentes y receptores para establecer una conexión.
- **Autorización** – Secure Shell también te permite configurar el control de acceso a las cuentas, proporcionando a los usuarios diferentes privilegios.
- **Reenvío/tunelización para cifrar sesiones basadas en TCP/IP** – los usuarios pueden configurar túneles para transferir tráfico no cifrado a través de un canal de red cifrado.

USOS DEL PROTOCOLO SSH

La mayoría de las veces lo usan los administradores del sistema. Está implementado por defecto en servidores Unix, Linux, Windows y MAC. Este protocolo crea un canal seguro entre una computadora local y un servidor remoto, permitiendo la ejecución de comandos, acceso a recursos, transferencia de archivos, actualizaciones de rendimiento, etc.También se usa en varios protocolos de transferencia de archivos, enrutadores, administración y funcionamiento del hardware del servidor administración del sistema.

Además, el protocolo Secure Shell ayuda con la administración de identidad, el control de acceso y la automatización de procesos.

MÉTODOS DE AUTENTICACIÓN

- **Autenticación basada en contraseña**

Cuando un cliente intenta conectarse a un servidor remoto, identifica al usuario con un usuario y contraseña. Cuando un usuario escribe sus credenciales

de acceso, el servidor comprueba si están presentes en su base de datos. Los inicios de sesión se comparten a través de un canal cifrado; si coinciden, el servidor permite que el cliente se conecte. Aunque las contraseñas están cifradas mientras están en transición entre las computadoras remotas, desafortunadamente un **ataque de fuerza bruta** aún podría descifrarlas. Naturalmente, este hecho hace que las contraseñas sean un método de identificación menos seguro. La divulgación de tus credenciales SSH puede permitir el acceso raíz a un hacker, lo que conlleva terribles consecuencias.

❖ Autenticación PKI

La autenticación basada en claves es el método preferido y se recomienda sobre la autenticación basada en contraseña, que puede ser forzada.

La autenticación PKI utiliza claves criptográficas para establecer una relación de confianza entre el servidor y el cliente. La identificación basada en clave puede requerir una frase de contraseña (contraseña) o puede funcionar sin una frase de contraseña en la clave.

Para usar este tipo de autenticación, debes generar un par de claves SSH. El par de claves consta de una clave pública y una privada. La clave pública se mantiene en el servidor, mientras que la clave privada se mantiene en tu ordenador.

Cuando te conectas a través de Secure Shell, se establece una relación de confianza entre tu ordenador y el servidor utilizando el par de claves. Si falta una de las claves o hay una discrepancia entre las claves, no se puede establecer una conexión.

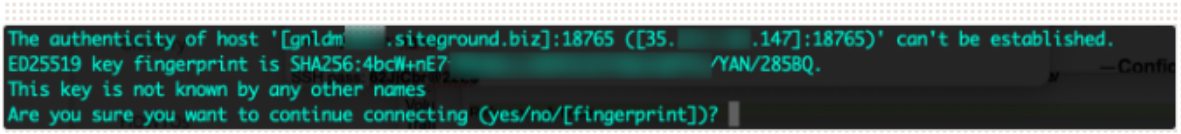
Arquitectura y componentes de SSH

Secure Shell tiene una arquitectura en capas, que encapsula 3 capas principales: ***transporte***, ***autenticación*** y ***conexión***.

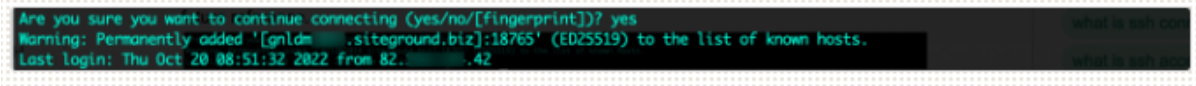
Capa de transporte

La ***capa de transporte*** usa el paquete de protocolos de Internet (**TCP/IP**) Protocolo de Control de Transmisión en el número de puerto SSH predeterminado **22.** Esta capa se encarga del intercambio de claves inicial y la autenticación, verifica su integridad e inicia el cifrado/descifrado. También comprime los datos transmitidos para acelerar el proceso. Por lo tanto, juega un papel importante en el intercambio de información segura entre hosts remotos.

Durante el transcurso de la fase de intercambio de claves, el servidor se identifica ante el cliente utilizando una ***clave de host*** . Si se conecta a ese servidor por primera vez, el cliente le preguntará si acepta esta clave de host y, si lo hace, el cliente guardará una copia localmente.



Si confirmas que deseas continuar, el cliente almacena la copia en un archivo ***claves de host conocidas*** para futura referencia.



Capa de autenticación

Cuando la capa de transporte ha configurado el cifrado, se solicita al cliente que se autentique utilizando uno de los métodos admitidos. La ***capa de autenticación de usuario*** proporciona un conjunto de algoritmos de autenticación y tiende a la autenticación del cliente.

CLAVES SSH

Un par de claves SSH consta de claves públicas y privadas utilizadas en un método de autenticación de clave SSH pública. En este método de autenticación, un archivo (conocido como clave privada) generalmente se guarda en el lado del cliente, y el otro archivo (conocido como clave pública) se almacena en el lado del servidor. Cada par de claves SSH es único, lo que garantiza que solo los usuarios con el par correcto tengan acceso.

- ➔ Las **claves públicas** permiten a los usuarios acceder a un servidor remoto y los servidores las usan para cifrar los datos. Prácticamente cualquier persona que tenga la clave pública SSH del par puede cifrar los datos, pero solo el usuario con la clave privada puede descifrarlos.

Cuando el cliente envía la clave pública al servidor SSH, y el servidor confirma su autenticidad, el servidor marca la clave como autorizada. Por lo tanto, las claves públicas también se denominan claves autorizadas y se almacenan en el ***archivo_autorizadas*** en el directorio de inicio de la cuenta de usuario.

- ➔ Las **claves privadas** también se denominan claves de identidad ya que son una prueba de la identidad del usuario. Un usuario solo puede ser autenticado correctamente por el servidor si el usuario tiene la clave privada correspondiente a la clave pública. Los usuarios deben mantener la confidencialidad de sus claves privadas y evitar compartirlas con otros.
- ➔ Una **clave de sesión** es generada colectivamente por el cliente SSH y el servidor. Esta clave simétrica se usa para cifrar toda la sesión SSH. Ambas entidades acuerdan usar una clave de sesión basada en los datos de la clave pública y privada para generar un “secreto compartido”. Es compartido por las

dos partes de forma segura y se utiliza para cifrar y descifrar los datos intercambiados (es decir, **cifrado simétrico**).

De esta manera, uno puede interceptar los datos en tránsito; cuando se cierra la sesión, la clave de la sesión se destruye.

Capa de conexión

Cuando el proceso de autenticación se completa con éxito, se inicia una conexión multiplexada (forma de enviar múltiples señales o flujos de información a través de un enlace de comunicaciones, al mismo tiempo en forma de una única y compleja señal) al servidor en múltiples canales. Cada uno de estos canales lógicos transfiere datos en ambas direcciones, lo que permite que muchas sesiones provengan de una sola conexión SSH.

Uno de estos canales es el Secure File Transfer Protocol (SFTP), que te permite acceder y transferir archivos de forma segura a través de una conexión SSH.