República Bolivariana de Venezuela

Ministerio del Poder Popular Para la Defensa

Universidad Nacional Experimental Politécnica de la

Fuerza Armada Nacional Bolivariana

Ensayo SSH

Profesor:

Ing. Jesús Méndez

Estudiantes:

YUSBELYS SOTO

YARELIS GODOY

Redes de comunicaciones

8vo semestre de telecom.

Tinaquillo, Noviembre del 2024.

Principalmente, la era digital es donde la información se transmite a través de redes cada vez más complejas y vulnerables donde nuestra seguridad de los datos y la comunicación se han convertido en una prioridad fundamental para cada uno de nosotros. Para la seguridad de los datos han surgido diferentes herramientas y protocolos para resguardar la integridad y confidencialidad de los datos, el Secure Shell (SSH) destaca por su robustez y versatilidad.

Desde una perspectiva más personal, el SSH es un protocolo que nos permite establecer una comunicación entre dos sistemas, el mismo surge como medida para los accesos remotos no seguros. Asimismo, el SSH es una medida por decirlo de este modo, que usa encriptación para proporcionar una conexión segura que intercambie información entre cliente y servidor, esta va cifrando la información que vamos intercambiando durante el proceso.

Es necesario saber, que SSH tiene diferentes funciones con las cuales podemos interactuar e intercambiar información de forma segura desde un acceso remoto que nos permite acceder a servidores y otros dispositivos de manera segura, dándonos las oportunidades de ejecutar comandos, transferir archivos. De igual forma, en palabras simples nos permite el intercambio de nuestra información sin la mera preocupación de que no estamos resguardados, como tal siempre va a mantener la integridad de los datos que estemos intercambiando.

Este protocolo nos permite establecer comunicación usando diferentes técnicas para así resguardar la información, donde dichas técnicas van desde la autenticación de usuarios, claves públicas, privadas y configuración de políticas de seguridad, que no dejan de faltar en ningún dominio o página web ya que estas nos permiten mantener la integridad, confidencialidad y disponibilidad de nuestra información en cualquier sistema.

En consecuencia, queda expresar que SSH es crucial y necesario para asegurar las comunicaciones y la administración remota en un mundo donde la ciberseguridad es cada vez más importante. Hay que destacar, que la versatilidad de este protocolo y robustez lo convierten en una herramienta esencial para cualquier administrador de sistemas e incluso cualquier persona que requiera usarlo.

Por otro lado, el SSH a diferencia de otros protocolos más antiguos este utiliza técnicas avanzadas para asegurar que toda la información intercambiada esté protegida contra interceptaciones y ataques maliciosos. Además, de la conexión a otros dispositivos SSH permite copiar datos de forma segura como: archivos sueltos, simular sesiones cifradas y gestionar claves para no escribir contraseñas al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH y también puede redirigir el tráfico del (Sistema de Ventanas X) para poder ejecutar programas gráficos remotamente. El puerto TCP asignado es el 22.

El SSH cifra la información que se envía y recibe, asegurando que solo el destinario previsto pueda leer los datos esto lo logra mediante el uso de algoritmos; además una de las principales ventajas es su capacidad para autenticar a los usuarios de manera segura, el proceso se basa en contraseñas, claves públicas y privadas. Este proceso garantiza que solo los usuarios autorizados puedan acceder a los sistemas remotos, reduciendo significativamente el riesgo de accesos no autorizados.

En relación, el funcionamiento de SSH se basa en un proceso de autenticación y encriptación que garantiza la seguridad de la conexión, cuando un usuario inicia una sesión SSH el cliente y el servidor negocian para proteger la comunicación. Luego, el usuario debe autenticarse generalmente mediante una combinación de nombre de usuario y contraseña; una vez establecida la conexión el usuario puede ejecutar comandos en el servidor remoto como si estuviera físicamente presente.

Se destaca, que el SSH no se limita a la administración remota de servidores, también es ampliamente utilizado para la transferencia segura de archivos mediante otros protocolos que permiten copiar archivos entre dispositivos de manera segura, protegiendo los datos durante la transferencia. En términos de seguridad, el SSH ofrece una protección contra ataques cibernéticos por lo que proporciona una capa adicional se seguridad para las comunicaciones remotas, sin embargo es importante mantener las prácticas de seguridad adecuadas como el uso de contraseñas fuertes y la actualización regular de software para minimizar la protección que ofrece SSH.

En definitiva, la importancia de SSH es su capacidad para proteger datos sensibles y garantizar la integridad de las comunicaciones remotas, el uso del mismo es esencial para prevenir accesos no autorizados y proteger la información crítica de las organizaciones. Sin más que agregar, el SSH permite la tunelización de datos, lo que facilita la transferencia segura de archivos y la gestión de infraestructuras complejas desde cualquier ubicación.

De igual forma, su capacidad para encriptar comunicaciones y autenticar usuarios de manera robusta lo convierte en una opción preferida para profesionales y administradores de sistemas. Finalmente, al adoptar SSH las organizaciones pueden mejorar significativamente su postura de seguridad y proteger sus activos digitales contra amenazas potenciales.