RESEÑA CAPÍTULO 1 Y 2 SSH MASTERY

Capítulo 1 – Introducing OpenSSH

En los últimos diez años, OpenSSH se ha convertido en el Herramienta estándar para la gestión remota de sistemas similares a Unix. OpenSSH tiene muchas potentes funciones que facilitarán la administración de sistemas si se toma el tiempo para aprender sobre ellos Encontrarás información y tutoriales sobre OpenSSH todo a través de Internet. Algunos de ellos están mal escritos, o sólo se aplican a muy Escenarios específicos. Muchos están bien escritos, pero tienen diez años y están cubiertos. Problemas resueltos por una actualización de software hace nueve años. El autor describe algunos conceptos, entre ellos el SSH, OpenSSH, SSH Server, SSH Clients, SSH Protocol Versions, aborda lo que puedes ver en este libro, también lo que no se vera o no se trata el libro.

Capitulo 2 – Encryption, Algorithms, and Keys

En este capítulo lo que más resalta es como OpenSSH encripta el trafico y los algoritmos encriptados al igual que como SSH usa la encriptación. OpenSSH encripta el tráfico. ¿Qué significa eso y cómo funciona? El cifrado transforma el texto sin formato legible en texto cifrado ilegible que Los atacantes no pueden entender. El descifrado invierte la transformación, produciendo texto legible de galimatías aparentes. Un algoritmo de cifrado es el exacto Método para realizar esta transformación. La mayoría de los niños descubren el código que sustituye números por letras, de modo que A = 1, B = 2, Z = 26 y así sucesivamente. Esto es un algoritmo de cifrado simple. Modernos algoritmos de cifrado controlados por computadora. Trabaja en trozos de texto a la vez y realiza mucho más complicado transformaciones. La mayoría de los algoritmos de cifrado utilizan una clave; un trozo de texto, números, símbolos o Datos utilizados para cifrar mensajes. La clave puede ser elegida por el usuario o al azar. generado. El algoritmo de cifrado usa la clave para encripta el texto, lo que hace que sea más difícil para un forastero descifrar. Incluso si tú Si conoce el algoritmo de cifrado, no puede descifrar el mensaje sin la clave secreta de cifrado.

El autor hace una referencia astuta del cifrado “Piense en un algoritmo de cifrado como un tipo de bloqueo, y la clave como un específico llave. Las cerraduras vienen en muchos tipos diferentes: puertas de casa, bicicletas, fábricas, y así en. Cada uno usa un tipo de llave determinado: la llave de su puerta probablemente tenga la forma incorrecta Para adaptarse a cualquier ignición del vehículo. Pero una clave del tipo adecuado todavía no funcionará la cerradura equivocada La llave de la puerta delantera desbloquea la puerta frontal y solo la delantera puerta. Las claves de cifrado funcionan de manera similar”.

Los algoritmos de cifrado vienen en dos variedades, simétrica y asimétrica. Un algoritmo simétrico usa la misma clave para el cifrado y descifrado Los algoritmos simétricos incluyen, pero no se limitan a los avanzados Estándar de cifrado (AES), Blowfish, 3DES e IDEA. La sustitución del niño. El código es un algoritmo simétrico. Una vez que sepas que A = 1 y así sucesivamente, puedes cifrar y descifrar mensajes. Algoritmos simétricos (más sofisticados que la sustitución simple) puede ser muy rápida y segura, siempre que solo esté autorizada la gente tiene la llave Y ese es el problema: un extraño que obtiene la llave puede Lee tus mensajes o sustitúyelos por los suyos. Debes proteger la llave. Enviar la clave sin cifrar a través de Internet es como estar parado en el parque infantil gritando "A es 1, B es 2." Cualquiera que escuche la clave puede leer su mensaje privado. Un algoritmo asimétrico utiliza diferentes claves para el cifrado y descifrado.

El cifrado simétrico es rápido, pero no ofrece una forma segura para que los hosts intercambiar llaves El cifrado asimétrico permite a los hosts intercambiar claves públicas, pero es Lento y computacionalmente caro. Pero, ¿cómo se puede cifrar de manera eficiente una Sesión entre dos hosts que nunca se han comunicado previamente? Cada servidor SSH tiene un par de claves. Cada vez que un cliente se conecta, el servidor y el cliente utiliza este par de claves para negociar un par de claves temporal compartido solo entre esos dos anfitriones El cliente y el servidor utilizan esta clave temporal para derivar un clave simétrica que utilizarán para intercambiar datos durante esta sesión, así como Claves relacionadas para proporcionar integridad de conexión.