INSTITUTO TECNOLOGICO DE CULIACAN

INGENIERIA EN SISTEMAS COMPUTACIONALES

ADMINISTRACION DE REDES

RESEÑA CAPITULOS 1 Y 2 SSH MASTERY

***ALUMNO**:*

ROSALES CORVERA HERNAN ENRIQUE

***DOCENTE**: LUIS ERNESTO LIZARRAGA BOLAÑOS*

CULIACAN SINALOA, 02 DE JULIO DEL 2019

CHAPTER 1: INTRODUCING OPENSSH

En los últimos diez años, OPEN SSH se ha convertido en laherramienta estándar para la gestión de sistemas Unix-like y muchos dispositivos de red. OpenSSH tiene muchas características poderosas que harán la gestión de sistemas más fácil si se toma el tiempo para aprender acerca de ellos. Secure Shell (SSH) es un protocolo para crear un canal de comunicaciones encriptado entre dos hosts en red. SSH protege los datos que pasan entre dos máquinas para que otras personas no puedan espiar en él. OpenSSH es la implementación más extendida del protocolo SSH. Comenzó como un derivado de una versión libremente-licenciada del software SSH original, pero ha sido fuertemente reescrito, ampliado, y actualizado. Un servidor SSH escucha en la red las peticiones SSH entrantes, autentica esas peticiones, y proporciona un indicador de comandos del sistema. Nosotros accedemos mediante un cliente de SSH, como putty.

Obtener una comprensión en profundidad de la forma subyacente de funcionamiento de SSH puede ayudarles a los usuarios a comprender los aspectos de seguridad de esta tecnología. La mayoría de la gente considera este proceso extremadamente complejo y poco comprensible, pero es mucho más simple de lo que la mayoría piensa.

CHAPTER 2: ENCRYPTION, ALGORITHMS, AND KEYS

El cifrado transforma texto plano legible en texto cifrado ilegible que los atacantes no pueden entender. Decryption invierte la transformación, produciendo texto legible a partir de galimatías aparentes. La mayoría de los algoritmos de encriptación utilizan una clave; un trozo de texto, números, símbolos o datos utilizados para encriptar mensajes. La clave puede ser elegida por el usuario o generada aleatoriamente. El algoritmo de encriptación utiliza la clave para encriptar el texto, lo que hace más difícil para un extraño desencriptar.

Los algoritmos de cifrado vienen en dos variedades, simétricas y asimétricas

Un algoritmo simétrico utiliza la misma clave para encriptar y descifrar

Un algoritmo asimétrico utiliza diferentes claves para encriptar y descifrar. Se encripta un mensaje con una clave, y luego desencriptarlo con otra.

El cifrado simétrico es rápido, pero no ofrece a los anfitriones la posibilidad de intercambiar llaves de forma segura. El cifrado asimétrico permite a los anfitriones intercambiar llaves públicas, pero es lento y computacionalmente caro.

Cada servidor SSH tiene un par de llaves. Cada vez que un cliente se conecta, el servidor y el cliente utilizan este par de llaves para negociar un par de llaves temporal compartidas sólo entre esos dos hosts. SSH soporta muchos algoritmos de encriptación simétricos y asimétricos. El cliente y el servidor negocian algoritmos mutuamente aceptables en cada conexión.