CURSOS INTERSEMESTRALES

PROTECO

Ciberseguridad

Secure Shell (SSH)

Breve Historia de SSH

- Se creo en 1995.
- SSH fue desarrollado por Tatu Ylönen, un programador de origen Finlandés.
- En un inicio comenzó bajo licencia libre.
- Tiempo después se patento SSH y se creo la empresa (SSH Communications Security)
- Un equipo de OpenBSD comenzó a desarrollar una versión libre de nombre OpenSSH.

PROTECO

¿Qué es SSH?

- Es un protocolo de acceso remoto y seguro.
- Es un programa que permite realizar conexiones entre máquinas a través de una red abierta de forma segura, así como ejecutar programas en una máquina remota y copiar archivos de una máquina a otra.
- Nace como un reemplazo a telnet, ftp, rlogin, rsh, y rcp.
- Existen dos versiones para el protocolo SSH.

PROTECO

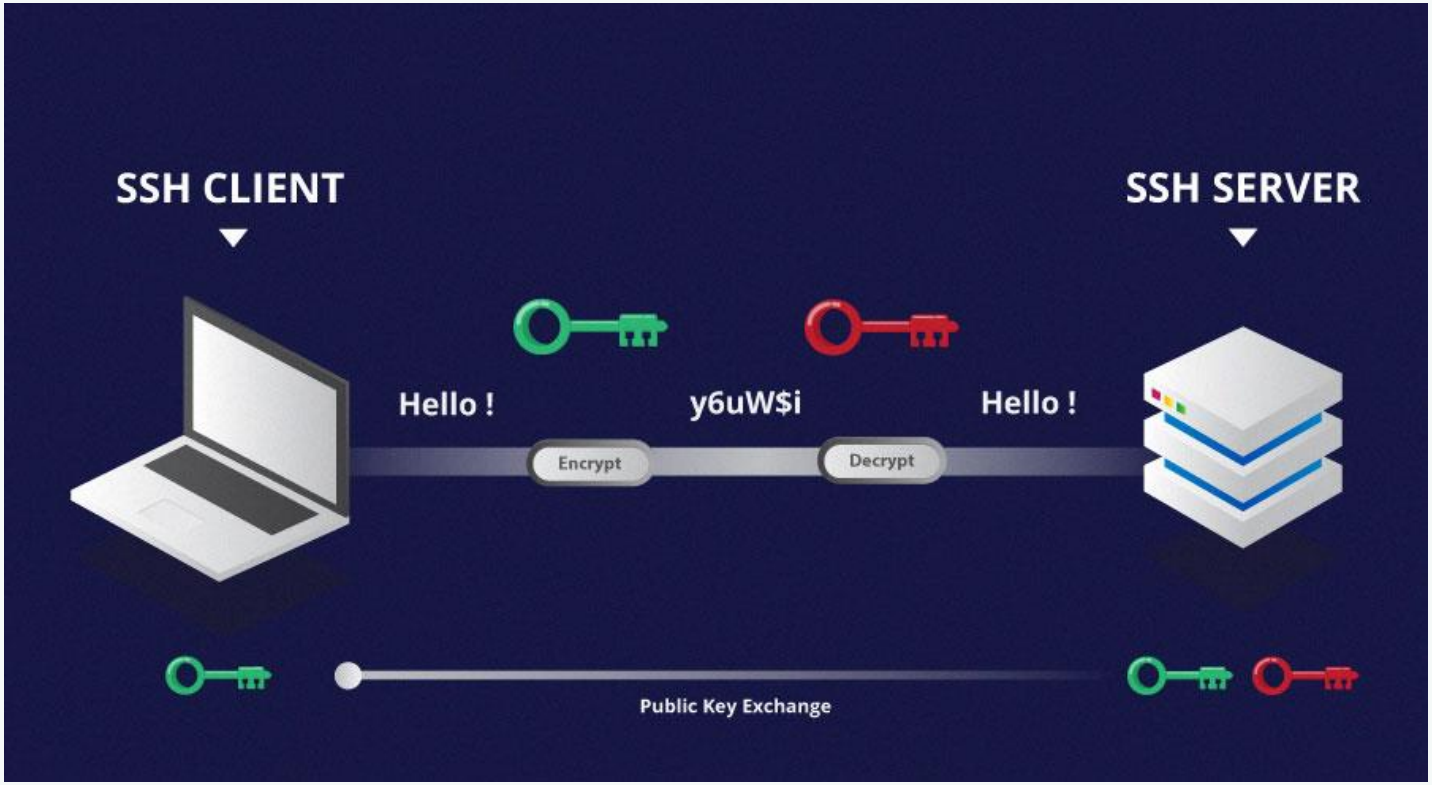
¿Qué es SSH?

SSH nos permite:

- Login en servidores remotos.
- Ejecución de comando de manera remota.
- Realizar túneles IP cifrados.
- Transferencia de archivos desde un ordenador remoto.
- Conexiones seguras y rápidas.
- Backups remotos.

PROTECO

¿Cómo funciona Secure Shell?



PROTECO

¿Cómo funciona Secure Shell?

- El cliente abre una conexión TCP al puerto 22 del host servidor.
- El cliente y el servidor acuerdan la versión del protocolo a utilizar, de acuerdo a su configuración y capacidades.
- El servidor posee un par de claves pública/privada de RSA (llamadas "claves de host"). El servidor envía al cliente su clave pública.

PROTECO

¿Cómo funciona Secure Shell?

- El cliente compara la clave pública de host recibida con la que tiene almacenada, para verificar su autenticidad. Si no la conociera previamente, pide confirmación al usuario para aceptarla como válida.
- El cliente genera una clave de sesión aleatoria y selecciona un algoritmo de cifrado simétrico.
- El cliente envía un mensaje conteniendo la clave de sesión y el algoritmo seleccionado, cifrado con la clave pública de host del servidor usando el algoritmo RSA.

PROTECO

¿Cómo funciona Secure Shell?

- En adelante, para el resto de la comunicación se utilizará el algoritmo de cifrado simétrico seleccionado y clave compartida de sesión.
- Luego se realiza la autenticación del usuario. Aquí pueden usarse distintos mecanismos.
- Finalmente se inicia la sesión.

PROTECO

Autenticación de usuarios

Existen varios métodos que pueden utilizarse para autenticar usuarios.

Aunque son mutuamente excluyentes, tanto el cliente como el servidor pueden soportar varios de ellos.

Existen dos métodos en SSH:

- Autenticación con contraseña.
- Autenticación con clave publica.

PROTECO

Autenticación de usuarios

Autenticación con contraseña:

- Es el método mas común de autenticación.
- El cliente solicita el ingreso y es necesario una contraseña de usuario
- El servidor recibe y valida la contraseña.

PROTECO

Autenticación de usuarios

Autenticación con clave pública:

- El usuario debe tener un par de claves pública/privada.
- La clave publica debe estar en el servidor.
- Una vez establecida la conexión, el servidor genera un "desafío", éste es cifrado con RSA o DSA
- El cifrado es enviado al cliente, posteriormente se descifra con la clave privada y se devuelve al servidor.

PROTECO

El cifrado de Secure Shell

Este hace posible que un cliente (un usuario o un equipo) inicie una sesión interactiva en una máquina remota (servidor) para enviar comandos o ficheros a través de un canal seguro.

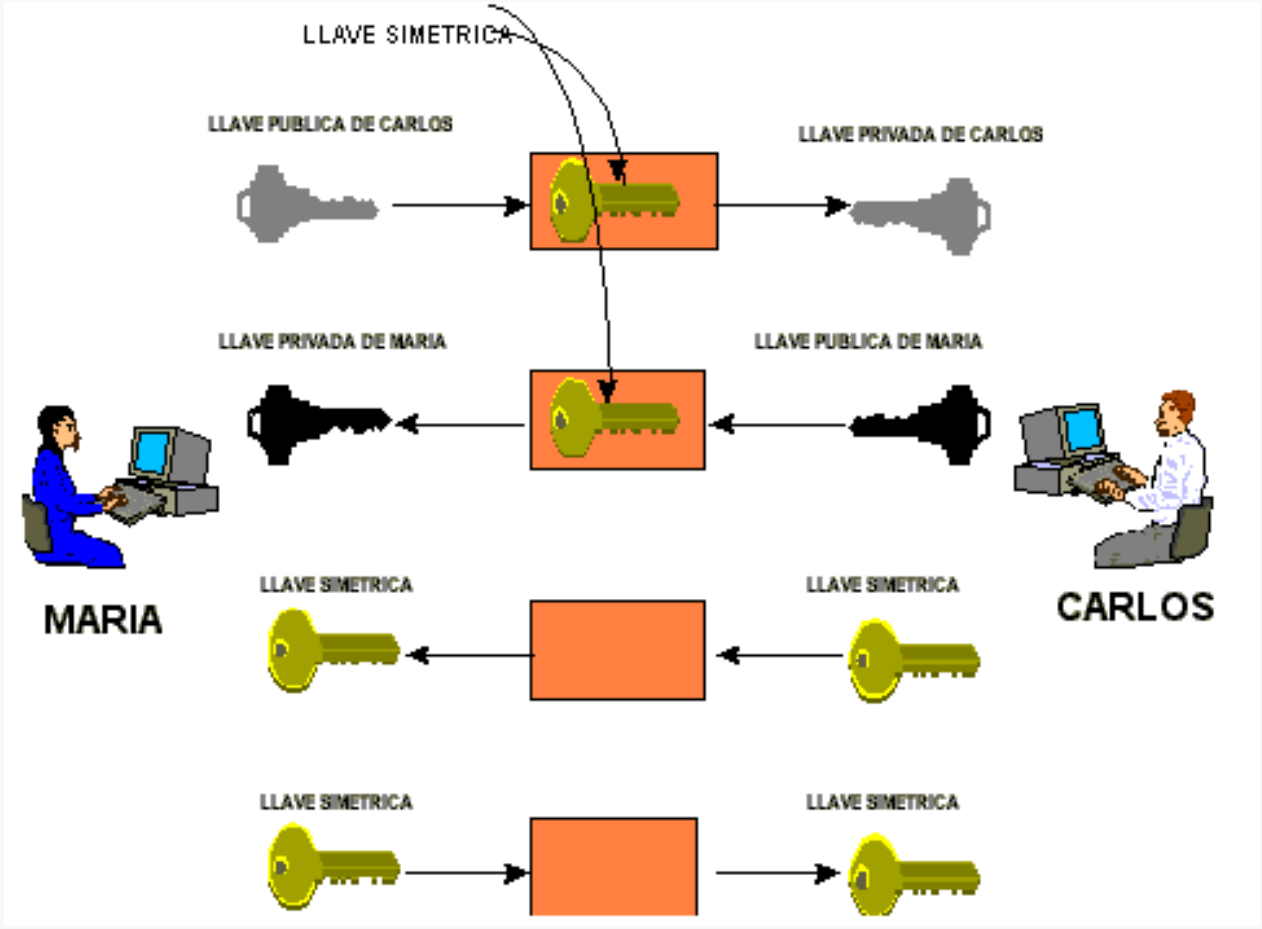
- Los datos que circulan entre el cliente y el servidor están cifrados y esto garantiza su confidencialidad
- El cliente y el servidor se autentifican uno a otro para asegurarse que las dos máquinas que se comunican son, de hecho, aquellas que las partes creen que son.

PROTECO

¿QUÉ ES EL RSA?

- Inventado en 1977 por Ron **R**ivest, Adi **S**hamir, y Leonard **A**dleman, el RSA es un algoritmo criptográfico, funciona basándose en una clave pública y privada.
- La clave pública se usa para cifrar los datos antes de enviarlos al servidor donde se encuentra el certificado.
- La clave privada se emplea para descifrar los datos cifrados con la clave pública.

PROTECO


LLAVE SIMETRICA
LLAVE PUBLICA DE CARLOS
LLAVE PRIVADA DE CARLOS
LLAVE PRIVADA DE MARIA
LLAVE PUBLICA DE MARIA
MARIA
CARLOS
LLAVE SIMETRICA
LLAVE SIMETRICA
LLAVE SIMETRICA
LLAVE SIMETRICA

PROTECO

Ataques a Secure Shell

¿Qué es un ataque?

- Es una ofensiva hacia una computadora o servidor con el fin de comprometer la integridad, confidencialidad y la información.

- Uso no autorizado de una computadora para el procesamiento de datos.
- Obtener o intentar el acceso a un sistema no autorizado.

PROTECO

Ataques a Secure Shell

Entre los ataques más comunes que nos previenen Secure Shell están:

- Sniffering(Captura de trafico)
- IP Spoofing
- MACpoofing
- DNS Spoofing
- Telnet Hickjacking
- ARP Spoofing
- IP Routing Spoofing

PROTECO

Ataques a Secure Shell

Un ataque muy común a un servicio SSH es por fuerza bruta.

Consiste en obtener una clave (contraseña) probando con todas las combinaciones posibles hasta encontrar la correcta.

Herramientas :

- Hydra
- Ncrack
- Medusa

PROTECO

Ataques a Secure Shell

¿Cómo protegerse de este ataque?

- Ejecute SSH en un puerto no estándar. (que no sea el puerto 22).
- Bloquear el inicio de sesión SSH para el usuario *root*.
- Limitar los intentos de inicio de sesión del usuario.

PROTECO

Hardening de un servidor Secure Shell

¿Qué es el Hardening?

- También se le conoce como endurecimiento.
- Consisten en asegurar un sistema.
- Reduce las vulnerabilidades.
- Se trabajan en prevenir los ataques mas típicos.

PROTECO

Hardening de un servidor Secure Shell

Existen varias maneras de implementarlo:

- Instalar un detector de intrusos.
- Firewall
- Cerrar puertos abiertos.
- Herramientas
  - Lynis.
  - Bastille Linux.
  - JASS.
  - Apache/PHP Hardener.

PROTECO