I.E.S. Fernando Aguilar Quignon
C/Conil de la Frontera, 3
CP 11010, Cádiz

Administración de Sistemas Operativos - 1ª Evaluación (RA 4 – CE d, e, f)

Unidad Didáctica 4. Configuración multiusuario centralizada

Ejercicio 1. Emplear un cliente ssh de OpenSSH sobre GNU/Linux para efectuar una conexión ssh contra un servidor, indicando su dirección IP, pero sin indicar expresamente el algoritmo asimétrico a emplear. Observar detenidamente el mensaje que informa de que se trata de un host desconocido, y como se muestra el fingerprint recibido de él (se indica también el algoritmo asimétrico de la clave pública empleada para hacer la conexión: la clave pública de dicho algoritmo será la que se habrá usado para generar el fingerprint). Comprobar que el fingerprint recibido por el cliente se almacena en ~/.ssh/known_hosts, asociado a la IP del servidor.

Para estos ejercicios puede ser útil configurar a "no" la opción HashKnownHost de /etc/ssh/ssh_config, de manera que no se hashee ni el nombre ni la IP de los equipos almacenados en ~/.ssh/known_host

Para poder comparar el fingerprint almacenado en ~/.ssh/known_host del cliente con el que se muestra durante la primera conexión:

ssh-keygen -l -f ~/.ssh/known_hosts

Para poder comparar el fingerprint almacenado en ~/.ssh/known_host del cliente con el que se genera a partir de la clave pública del servidor:

ssh-keygen -l -f ~/.ssh/known_hosts (en lado cliente)

ssh-keygen -l -f /etc/ssh/ssh_host_ecdsa_key.pub (en lado servidor)

Ejercicio 2. Efectuar nuevas conexiones contra el mismo servidor del primer ejercicio, de nuevo indicando su dirección IP, pero sin indicar expresamente el algoritmo asimétrico a emplear (por lo que se empleará el mismo algoritmo que en la primera conexión). En estas nuevas conexiones ya no se debe mostrar mensaje alguno, ya que ahora se trata de un host conocido

Ejercicio 3. Emplear la sintaxis apropiada del comando "ssh-keygen" para eliminar la entrada del fingerprint en el fichero ~/.ssh/known_hosts del lado cliente.

Ejercicio 4. Repetir los dos primeros ejercicios, pero indicando al cliente ssh el nombre del servidor, en lugar de su IP.

Ejercicio 5. Preparar escenarios para forzar avisos "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! [...] Someone could be eavesdropping on you right now (man-in-the-middle attack)!":

- Caso 1: Habiéndose almacenado en una primera conexión solo la IP (no el nombre), asociada al fingerprint, borra (y purga) el servidor OpenSSH, vuélvelo a instalar y realiza la conexión nuevamente.
- Caso 2: Habiéndose almacenado en una primera conexión solo el nombre de equipo (no la IP), asociado al fingerprint, realizamos una segunda conexión indicando el mismo nombre. Si la resolución de nombres (/etc/hosts, DNS, etc.) nos fuerza a conectar con otro equipo, recibiremos la indicación por parte de SSH.
- Caso 3: Habiéndose almacenado en una primera conexión solo la IP (no el nombre), asociada al fingerprint, en una segunda conexión se proporciona al cliente ssh la misma dirección IP que en la primera conexión, pero la IP está ahora asignada (por el motivo que sea) a un equipo distinto, lo cual nos lleva a tratar de conectar con un equipo distinto (que lógicamente tendrá un fingerprint distinto al de la primera conexión).

- Caso 4: Habiéndose almacenado en una primera conexión el nombre o la IP, asociada al fingerprint, en una segunda conexión se proporciona al cliente ssh el mismo nombre o IP que se empleó en la primera conexión, pero el cliente ssh indica que quiere emplear ahora un algoritmo asimétrico distinto del empleado en la primera conexión: como el fingerprint se genera a partir de la clave pública del algoritmo asimétrico empleado, el fingerprint almacenado durante la primera conexión no coincidirá con el fingerprint proporcionado por el servidor durante la segunda conexión. **Para este último caso revisa la opción HostKeyAlgorithms**.