📁 LPIC-2 / 🔒 Tema 212 - La seguridad del sistema

7.6.3 212.3 Secure Shell (SSH) (peso: 4)

Teoría

Secure Shell (SSH) es un protocolo de red criptográfico utilizado para operar servicios de red de forma segura sobre una red no segura. Los usos más comunes incluyen inicio de sesión remoto seguro, ejecución de comandos remotos y transferencia segura de archivos (SFTP y SCP).

Componentes de OpenSSH (la implementación más común):

- `sshd`: El demonio del servidor OpenSSH. Escucha las conexiones entrantes.
- `ssh`: El programa cliente OpenSSH. Se utiliza para iniciar conexiones seguras a un servidor SSH.
- `scp`: Utilidad para copiar archivos de forma segura a través de SSH.
- `sftp`: Programa cliente para transferencia de archivos interactiva y segura (SFTP - SSH File Transfer Protocol) a través de SSH.

Configuración del Servidor OpenSSH (`sshd`):

La configuración principal del servidor SSH se encuentra en:

- `/etc/ssh/sshd_config` (Ubicación estándar en ambas ramas Debian/Red Hat).

Los cambios en este archivo requieren que se reinicie o recargue el servicio `sshd`.

Directivas de Configuración Clave en `sshd_config` (con Enfoque de Seguridad):

- `Port <puerto>`: El puerto TCP en el que el servidor `sshd` escucha las conexiones entrantes. El valor por defecto es 22. Cambiarlo puede ser una medida de "seguridad por oscuridad", pero no protege contra escaneos completos de puertos.
- `ListenAddress <ip>`: Especifica la(s) dirección(es) IP en la(s) que el servidor debe escuchar. Por defecto, escucha en todas las interfaces.
- `Protocol 2`: Especifica la versión del protocolo SSH a usar. **Siempre debe configurarse en `2`** para deshabilitar la versión 1 (insegura).
- `PermitRootLogin yes/no/prohibit-password/without-password`: Controla si el usuario `root` puede iniciar sesión directamente a través de SSH. **Configurarlo a `no` o `prohibit-password` (preferible, permite login root solo con clave) es una medida de seguridad muy importante** para mitigar ataques de fuerza bruta contra la cuenta root. El acceso root se logra mejor iniciando sesión como usuario normal y usando `su` o `sudo`.
- `PasswordAuthentication yes/no`: Si se permite la autenticación basada en contraseña. **Configurarlo a `no` es una medida de seguridad clave** cuando se utiliza la

autenticación basada en clave pública, ya que elimina el riesgo de ataques de fuerza bruta o de diccionario contra contraseñas débiles.

- `PubkeyAuthentication yes/no`: Si se permite la autenticación basada en clave pública. Debe ser `yes` si `PasswordAuthentication` es `no`.
- `AuthorizedKeysFile .ssh/authorized_keys`: La ubicación (relativa al directorio home del usuario) del archivo que contiene las claves públicas autorizadas para ese usuario. El valor por defecto es correcto.
- `AllowUsers <user1> <user2> ...`: Una lista separada por espacios de usuarios a los que se les permite iniciar sesión. Si se especifica, solo estos usuarios pueden acceder.
- `DenyUsers <user1> <user2> ...`: Una lista de usuarios a los que se les deniega explícitamente el inicio de sesión.
- `AllowGroups <group1> <group2> ...`: Una lista de grupos cuyos miembros pueden iniciar sesión.
- `DenyGroups <group1> <group2> ...`: Una lista de grupos cuyos miembros tienen denegado explícitamente el inicio de sesión.
- `PermitEmptyPasswords yes/no`: Si se permite iniciar sesión con una contraseña vacía. **Debe configurarse a `no`**.
- `ChallengeResponseAuthentication yes/no`: Deshabilita la autenticación interactiva (no basada en contraseña), a menudo se establece en `no`.
- `UsePAM yes/no`: Controla si `sshd` utiliza PAM para la autenticación. Generalmente se deja en `yes` para integrar con políticas de sistema (límites, logs, etc. - Revisado 210.2).
- `MaxAuthTries <número>`: Número máximo de intentos de autenticación permitidos por conexión. Un valor bajo (ej: 3-5) ayuda a mitigar ataques de fuerza bruta.
- `LoginGraceTime <segundos>`: Tiempo que el servidor espera a que el cliente se autentique.
- `Banner <ruta_archivo>`: Muestra el contenido de un archivo al cliente antes de la autenticación (ej: aviso legal).
- `SyslogFacility AUTH` / `LogLevel INFO`: Configura dónde y con qué detalle se registran los eventos de sshd (útil para monitorizar intentos de login fallidos).

Autenticación Basada en Clave Pública:

- **Concepto:** En lugar de una contraseña, se utiliza un par de claves criptográficas: una **clave privada** (secreta, solo en el cliente) y una **clave pública** (compartida con el servidor). El servidor puede verificar que el cliente posee la clave privada correspondiente sin que la clave privada abandone nunca el cliente.
- **Generación de Claves:** Se utiliza el comando `ssh-keygen` en el cliente para generar un par de claves (ej: RSA de 2048 o 4096 bits, o Ed25519 - más moderno). Por defecto, crea `~/.ssh/id_rsa` (privada) y `~/.ssh/id_rsa.pub` (pública). **Protege la clave privada con una frase de paso (passphrase).**

- **Instalación de la Clave Pública en el Servidor:** La clave pública del cliente debe copiarse al servidor y añadirse al archivo `~/.ssh/authorized_keys` del usuario con el que se desea iniciar sesión.
- **`ssh-copy-id`:** La herramienta más sencilla para copiar la clave pública al servidor. `ssh-copy-id usuario@servidor`. Se conecta por SSH (usando password authentication la primera vez) y añade la clave pública al archivo `authorized_keys` con los permisos correctos.
- **Instalación Manual:** Crear el directorio `~/.ssh` en el servidor (si no existe), crear/editar el archivo `~/.ssh/authorized_keys` y pegar el contenido de la clave pública (`~/.ssh/id_rsa.pub` del cliente).
- **Permisos de Archivos (¡CRUCIAL para la autenticación por clave!):**
    - Directorio `~/.ssh`: Permisos `700` (solo el propietario tiene acceso).
    - Archivo `~/.ssh/authorized_keys`: Permisos `600` (solo el propietario tiene acceso de lectura/escritura).
    - El directorio home del usuario (`~`) debe tener permisos `755` o más restrictivos (no `777`).
    - Si los permisos son demasiado amplios, `sshd` IGNORARÁ la autenticación por clave por seguridad.

Configuración del Cliente SSH (`ssh`):

- La configuración principal del cliente SSH se encuentra en:
    - `/etc/ssh/ssh_config` (Configuración a nivel de sistema para todos los usuarios).
    - `~/.ssh/config` (Configuración a nivel de usuario, anula la configuración del sistema).
- **Directivas Comunes en `ssh_config`:** `Hostname` (nombre real del host remoto si es diferente al nombre del alias), `Port` (puerto remoto si es diferente a 22), `User` (usuario remoto si es diferente al usuario local), `IdentityFile <ruta_clave_privada>` (especifica qué clave privada usar para un host). Útil para definir alias o configuraciones predeterminadas para hosts específicos.

Firewall:

- El firewall del servidor SSH debe permitir el tráfico TCP entrante al puerto configurado para SSH (por defecto 22).
- El firewall del cliente SSH debe permitir el tráfico TCP saliente al puerto SSH del servidor.