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

*Nota: Estos ejercicios implican configurar el acceso remoto. Realízalos **SIEMPRE en una VM de prueba dedicada** con al menos otra VM para usar como cliente. **Mantén una sesión de consola directa en la VM servidora** mientras realizas cambios que puedan bloquear el acceso SSH. Necesitarás privilegios de superusuario (`sudo`).*

**Ejercicio 12.3.1: Instalando OpenSSH Server y Cliente**

- **Objetivo:** Asegurarse de que el software SSH está instalado.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet. **VM de prueba (servidor y cliente).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM servidora y en la VM cliente.
    2. **En la VM servidora, instala el servidor:** `sudo apt update && sudo apt install openssh-server` (Debian/Ubuntu) o `sudo dnf install openssh-server` (Red Hat/CentOS/Fedora).
    3. **En la VM cliente, instala el cliente (a menudo ya está instalado):** `sudo apt update && sudo apt install openssh-client` (Debian/Ubuntu) o `sudo dnf install openssh-clients` (Red Hat/CentOS/Fedora).
    4. **En la VM servidora, verifica el estado del servicio `sshd`:** `systemctl status sshd.service`. Debería estar `active (running)`.

**Ejercicio 12.3.2: Verificando Reglas de Firewall para SSH**

- **Objetivo:** Asegurarse de que el firewall permite el tráfico SSH.
- **Requisitos:** Privilegios de superusuario (`sudo`). Identificar la herramienta de firewall activa (Ej. 12.2.1). Puerto SSH (22 TCP por defecto). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM servidora.
    2. **Si usas `firewalld`:** Ejecuta `sudo firewall-cmd --zone=<zona> --list-services` o `sudo firewall-cmd --zone=<zona> --list-ports`. Busca el servicio `ssh` o el puerto `22/tcp`. Si no está en la zona relevante, añádelo: `sudo firewall-cmd --zone=<zona_interfaz> --add-service=ssh --permanent` y `sudo firewall-cmd --reload`.
    3. **Si usas `ufw`:** Ejecuta `sudo ufw status`. Busca reglas para el puerto 22 TCP. Si no están, añádelas: `sudo ufw allow 22/tcp` o `sudo ufw allow ssh`.
    4. **Si usas `iptables` directamente:** Ejecuta `sudo iptables -L -v -n`. Busca reglas que permitan el tráfico TCP entrante al puerto 22 en la cadena `INPUT` (y `FORWARD` si actúas como router).

**Ejercicio 12.3.3: Localizando y Explorando el Archivo de Configuración del Servidor SSH**

- **Objetivo:** Encontrar y ver las directivas clave en `sshd_config`.

- **Requisitos:** Servidor SSH instalado. Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM servidora.
    2. **Localiza el archivo:** `/etc/ssh/sshd_config`.
    3. **Crea una copia de seguridad:** `sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig`. **CRUCIAL.**
    4. **Visualiza el contenido:** Ejecuta `sudo less /etc/ssh/sshd_config`. Observa las directivas comentadas y los valores por defecto.
    5. **Busca las directivas de seguridad clave:** `Port`, `PermitRootLogin`, `PasswordAuthentication`, `PubkeyAuthentication`, `AllowUsers`, `AllowGroups`. Anota sus valores actuales.

**Ejercicio 12.3.4: (Conceptual) Modificando Configuraciones de Seguridad en `sshd_config`**

- **Objetivo:** Entender cómo aplicar endurecimiento básico a la configuración de SSH.
- *Requisitos:* Privilegios de superusuario (`sudo`). `sshd_config`. **VM de prueba (servidor). Mantén sesión de consola.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal en la VM servidora. **(¡Desde la consola directa si es posible!)**
    2. **Edita `sshd_config`:** Ejecuta `sudo vi /etc/ssh/sshd_config`.
    3. **Modifica o añade directivas clave (descomenta si están comentadas):**
        - Para deshabilitar login directo de root: `PermitRootLogin no` o `PermitRootLogin prohibit-password`.
        - Para deshabilitar autenticación por password (si vas a usar solo claves): `PasswordAuthentication no`.
        - Para permitir autenticación por clave: `PubkeyAuthentication yes`.
        - Para cambiar el puerto por defecto (ej: a 2222): `Port 2222`. (Si cambias el puerto, **debes actualizar la regla del firewall** Ej. 12.3.2).
        - Para limitar usuarios/grupos (ej: solo permitir a `usuario_admin` y miembros del grupo `sudo`): `AllowUsers usuario_admin` y `AllowGroups sudo`. (Usa solo uno de `AllowUsers`/`AllowGroups` o una combinación cuidadosa).
    4. **Guarda y sal.**
    5. **Verifica la sintaxis de la configuración:** Ejecuta `sudo sshd -t`. Si hay errores, corrígelos.
    6. **Recarga el servicio sshd:** Ejecuta `sudo systemctl reload sshd`.
    7. **(Para probar):** Desde la VM cliente, intenta conectar con la configuración antigua y la nueva para verificar que los cambios (ej: login root, password auth) se aplican según lo esperado. Si cambiaste el puerto, especifícalo en el cliente: `ssh -p 2222 usuario@servidor`. Si algo falla y te quedas fuera, usa la sesión de consola en el servidor para restaurar `/etc/ssh/sshd_config.orig` y reiniciar `sshd`.

**Ejercicio 12.3.5: Generando un Par de Claves SSH**

- **Objetivo:** Crear las claves pública y privada para la autenticación por clave.
- **Requisitos:** Acceso a la línea de comandos en la VM cliente. Paquete `openssh-client` instalado.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM cliente.
    2. **Genera las claves:** Ejecuta `ssh-keygen -t rsa -b 4096`.
        - `-t rsa`: Especifica el tipo de clave (RSA). `ed25519` es una alternativa más moderna y a menudo preferida.
        - `-b 4096`: Especifica el tamaño de la clave (para RSA, 4096 bits es un tamaño seguro común).
    3. **Te pedirá dónde guardar la clave:** El valor por defecto (`~/.ssh/id_rsa`) es usualmente correcto.
    4. **Te pedirá una frase de paso (passphrase):** Es **muy recomendable** usar una frase de paso para proteger la clave privada. La tendrás que introducir cada vez que uses la clave privada por primera vez en una sesión (puedes usar `ssh-agent` para gestionarla).
    5. **Verifica los archivos generados:** Ejecuta `ls -l ~/.ssh/`. Deberías ver `id_rsa` (privada) y `id_rsa.pub` (pública).
    6. **Verifica permisos (deberían ser correctos por defecto):** `ls -l ~/.ssh/`. `id_rsa` debe tener permisos `600` o `400`. `id_rsa.pub` puede ser más permisivo (ej: `644`).

**Ejercicio 12.3.6: (Conceptual) Instalando la Clave Pública en el Servidor**

- **Objetivo:** Copiar la clave pública del cliente al servidor para permitir el login.
- *Requisitos:* Par de claves generado (Ej. 12.3.5). Acceso al servidor SSH con password authentication (al menos la primera vez). Un usuario en el servidor donde instalarás la clave. **VM de prueba (cliente y servidor).**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal en la VM cliente.
    2. **Usa `ssh-copy-id` (método recomendado):** Ejecuta `ssh-copy-id <usuario_servidor>@<IP_servidor>`. Te pedirá la contraseña del usuario en el servidor. Copiará automáticamente la clave pública por defecto (`~/.ssh/id_rsa.pub`) al archivo `~/.ssh/authorized_keys` en el servidor con los permisos correctos.
    3. **(Alternativa Manual):** Si no usas `ssh-copy-id`:
        - Copia el contenido de tu clave pública (`cat ~/.ssh/id_rsa.pub`) en el cliente.
        - Conéctate al servidor (con password auth): `ssh <usuario_servidor>@<IP_servidor>`.

- Crea el directorio `.ssh` en tu home si no existe: `mkdir ~/.ssh`.
- Establece permisos restrictivos: `chmod 700 ~/.ssh`.
- Añade la clave pública al archivo `authorized_keys` (usa `>>` para añadir si el archivo ya existe): `echo "<pega_contenido_clave_publica>" >> ~/.ssh/authorized_keys`.
- Establece permisos restrictivos en `authorized_keys`: `chmod 600 ~/.ssh/authorized_keys`.
- Sal de la sesión SSH.

**Ejercicio 12.3.7: Probando Autenticación por Clave Pública**

- **Objetivo:** Iniciar sesión SSH sin necesidad de contraseña (usando la clave).
- **Requisitos:** Clave pública instalada en el servidor con permisos correctos (Ej. 12.3.6). Clave privada en el cliente. Si usas frase de paso, recuérdala. Autenticación por clave habilitada en `sshd_config`. **VM de prueba (cliente y servidor).**
- **Desarrollo Paso a Paso:**
  1. Abre una terminal en la VM cliente.
  2. **Intenta conectar al servidor (usa el usuario donde instalaste la clave):** Ejecuta `ssh <usuario_servidor>@<IP_servidor>`.
  3. **Si configuraste frase de paso:** Te pedirá la frase de paso para desbloquear la clave privada.
  4. **Si todo está correcto (clave coincide, permisos correctos, frase de paso correcta),** deberías iniciar sesión en el servidor SIN que te pida la contraseña del usuario en el servidor. Si aún te pide la contraseña, algo no está bien configurado (revisa permisos, contenido de `authorized_keys`, y logs de `sshd` en el servidor).

**Ejercicio 12.3.8: Explorando el Archivo de Configuración del Cliente SSH**

- **Objetivo:** Localizar y ver el contenido de `ssh_config`.
- **Requisitos:** Cliente SSH instalado. Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
  1. Abre una terminal en la VM cliente.
  2. **Visualiza el archivo de configuración a nivel de sistema:** Ejecuta `less /etc/ssh/ssh_config`.
  3. **Visualiza el archivo de configuración a nivel de usuario (si existe):** Ejecuta `ls -l ~/.ssh/config`. Si no existe, puedes crearlo (`touch ~/.ssh/config`).
  4. **(Contexto):** Puedes usar estos archivos para definir atajos o configuraciones predeterminadas para hosts. Por ejemplo, en `~/.ssh/config`:

```
Host myserver
    Hostname 192.168.1.100
    Port 2222
    User myuser
    IdentityFile ~/.ssh/id_rsa
```

Con esto, simplemente ejecutando `ssh myserver` usarás la IP 192.168.1.100, puerto 2222, usuario myuser y la clave id_rsa.