Guía de estudio - Gestión de claves SSH, parte II

¡Hola! Te damos la bienvenida a esta nueva guía de estudio.

¿En qué consiste esta guía?

En la primera parte de esta serie, exploramos la creación, distribución y gestión de claves SSH. En esta continuación, profundizaremos en la implementación de la autenticación basada en claves SSH. Este método reemplaza la autenticación mediante contraseñas, ofreciendo un mecanismo mucho más seguro para el acceso remoto. La autenticación basada en claves se fundamenta en el uso de pares de claves (pública y privada), donde la clave pública se almacena en el servidor y la clave privada se conserva de manera segura en el cliente.

A lo largo de esta guía, aprenderás a configurar el servidor para que acepte únicamente autenticaciones basadas en claves, a deshabilitar los métodos de autenticación por contraseña y a realizar pruebas y diagnósticos para asegurar una implementación exitosa.

¡Vamos con todo!

Tabla de contenidos

¡Comencemos!

Fundamentos de la autenticación basada en claves SSH

Ventajas y principios

- **Seguridad mejorada:**
  Al eliminar la autenticación por contraseña, se reduce la vulnerabilidad ante ataques de fuerza bruta y otros métodos de intrusión. Las claves SSH, en combinación con una passphrase, ofrecen una doble capa de seguridad.

- **Integridad y confianza:**
  La autenticación por clave se basa en un par criptográfico. El servidor almacena la clave pública en el archivo authorized_keys y, durante el proceso de conexión, utiliza algoritmos criptográficos para verificar que el cliente posee la clave privada correspondiente.

- **Gestión centralizada:**
  Permite la administración centralizada de accesos en entornos multiusuario. Además, facilita la revocación o rotación de claves en caso de que se comprometa alguna.

Configuración en el servidor SSH

La implementación de la autenticación basada en claves implica modificar algunos parámetros en el archivo de configuración del servidor SSH, generalmente ubicado en /etc/ssh/sshd_config.

Ajustes recomendados en sshd_config

Habilitar la autenticación por clave:

Asegúrate de que la autenticación mediante clave esté activada (por defecto suele ser así):

```
PubkeyAuthentication yes
```

Deshabilitar la autenticación por contraseña:

Para reforzar la seguridad, se recomienda desactivar el método de autenticación por contraseña:

```
PasswordAuthentication no
ChallengeResponseAuthentication no
```

Verificar otros parámetros de seguridad:

- PermitRootLogin no:
  Evita el acceso directo del usuario root, obligando a la conexión mediante un usuario normal y el uso de `sudo` para acciones privilegiadas.
- StrictModes yes:
  Garantiza que los permisos de los archivos y directorios relacionados con SSH sean correctos, lo que previene vulnerabilidades por configuraciones inadecuadas.

Pasos para aplicar la configuración

Editar el archivo de configuración:

Abre el archivo `sshd_config` con tu editor de texto favorito:

```
sudo nano /etc/ssh/sshd_config
```

Realiza las modificaciones:

Asegúrate de que las siguientes líneas estén configuradas según lo recomendado:

```
PubkeyAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no
PermitRootLogin no
StrictModes yes
```

Guardar y reiniciar el servicio SSH:

Una vez realizados los cambios, guarda el archivo y reinicia el servicio para aplicar la nueva configuración:

```
sudo systemctl restart sshd
```

Verificar los registros:

Consulta los logs del sistema para asegurarte de que no existan errores:

```
sudo tail -f /var/log/auth.log
```

Nota: La ubicación de los logs puede variar según la distribución.

Actividad guiada: Configuración del servidor para autenticación basada en claves

1. **Iniciar la máquina virtual con Rocky Linux.**
2. **Accede al archivo de configuración:**

Abre el archivo `/etc/ssh/sshd_config` con:

```
sudo nano /etc/ssh/sshd_config
```

3. **Habilita la autenticación por clave y desactiva la autenticación por contraseña:**

Asegúrate de que las siguientes líneas estén presentes y configuradas:

```
PubkeyAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no
PermitRootLogin no
```

Guarda y cierra el editor.

4. **Reinicia el servicio SSH:**

Ejecuta:

```
sudo systemctl restart sshd
```

5. **Verifica la configuración:**

Intenta conectarte al servidor desde otro terminal utilizando tu clave SSH:

```
ssh usuario@direccion_del_servidor
```

Confirma que la conexión se establece sin solicitar la contraseña del sistema (aunque podría pedir la passphrase si se configuró).

¡Manos a la obra! - Diagnóstico y resolución de problemas

1. **Prueba de conexión:**

Si la conexión falla, revisa los permisos del directorio `~/.ssh` y del archivo `authorized_keys` en el servidor:

```
ls -ld ~/.ssh
ls -l ~/.ssh/authorized_keys
```

Los permisos recomendados son `700` para el directorio y `600` para el archivo.

2. **Revisión de Logs:**

Consulta los registros para identificar posibles errores:

```
sudo tail -f /var/log/auth.log
```

Busca mensajes que indiquen problemas con la autenticación por clave.

3. Ajusta la Configuración según Sea Necesario:
    - Si detectas errores de permisos o configuraciones, corrige y reinicia el servicio nuevamente.

Reflexiona:

- ¿Qué beneficios concretos encuentras al deshabilitar la autenticación por contraseña en comparación con el uso de claves SSH?
- ¿Por qué es crucial mantener permisos estrictos en los directorios y archivos relacionados con SSH (por ejemplo, ~/.ssh y authorized_keys)?
- ¿Cómo afecta la implementación de la autenticación por clave a la administración de accesos en entornos multiusuario?
- ¿Qué medidas de recuperación o fallback podrías implementar en caso de que un usuario pierda su clave privada?

La implementación de la autenticación basada en claves SSH es un paso decisivo para reforzar la seguridad de las conexiones remotas. Al desactivar los métodos de autenticación por contraseña y asegurar que solo se utilicen claves criptográficas, se reduce significativamente la vulnerabilidad a ataques de fuerza bruta y otros tipos de intrusiones.