Seguridad y administración de acceso remoto en Linux

Configuración básica de SSH y OpenSSH Server

{desafío} latam_

¿Qué aprenderás en esta sesión?

Configurar y administrar SSH en un entorno Linux, aplicando medidas de seguridad para proteger el acceso remoto.

{desafío}
latam_

¿Qué diferencias percibes entre acceder a un servidor físicamente y hacerlo de forma remota?

{desafío} latam_

/* Configuración básica de SSH y OpenSSH Server */

Contexto

El protocolo SSH (Secure Shell) es una herramienta esencial para la administración remota de servidores y sistemas basados en Unix/Linux.
Su importancia radica en ofrecer un canal seguro de comunicación, encriptando los datos que se transmiten a través de la red y evitando accesos no autorizados.

Instalación y configuración inicial de OpenSSH Server

Instalación

Verifica el gestor de paquetes de tu distribución:

- En distribuciones basadas en Debian/Ubuntu, utiliza apt.
- En distribuciones basadas en RedHat/CentOS, emplea yum o dnf.

Ejemplo de instalación en Debian/Ubuntu:
Abre una terminal y ejecuta:

```
sudo apt-get update
sudo apt-get install openssh-server
```

- Con estos comandos actualizas los repositorios e instalas el paquete necesario.

Verificación del servicio:
Comprueba el estado del servicio con:

```
systemctl status sshd
```

- Debes ver que el servicio está activo y corriendo.

Instalación y configuración inicial de OpenSSH Server

Configuración inicial del servicio

Archivo de configuración principal:

- El archivo de configuración de OpenSSH se encuentra generalmente en */etc/ssh/sshd_config*.
- Este archivo controla el comportamiento del servidor SSH y permite personalizar aspectos críticos de seguridad y comunicación.

Reinicio del servicio:

Cada vez que realices cambios en sshd_config, es necesario reiniciar el servicio:

```
sudo systemctl restart sshd
```

Actividad guiada: Instalación y verificación del servicio

Instrucciones

1. Inicia la máquina virtual Rocky Linux.
2. Ejecuta el comando de instalación correspondiente.
3. Usa systemctl status sshd para confirmar que el servicio esté activo.
4. Comprueba la conexión desde la máquina tutora con un cliente ssh como por ejemplo Putty.

Ajustes en el Archivo sshd_config

Es el corazón de la configuración del servidor SSH

A. Cambio de puerto

El puerto por defecto de SSH es el 22, lo que lo hace un blanco frecuente de ataques automatizados. Cambiar el puerto puede reducir el número de intentos maliciosos.

- Abre el archivo con un editor de texto (por ejemplo, nano o vim): `sudo nano /etc/ssh/sshd_config`
- Busca la línea que dice `#Port 22.`
- Descomenta la línea (elimina el símbolo #) y cambia el número a otro puerto, por ejemplo: `Port 2222`
- Guarda los cambios y reinicia el servicio SSH.

Ajustes en el Archivo sshd_config

Es el corazón de la configuración del servidor SSH

B. Selección de protocolos permitidos

Existen distintas versiones del protocolo SSH; sin embargo, la versión 2 es la más segura y recomendada. Limitar la conexión a este protocolo refuerza la seguridad.

- En el mismo archivo `/etc/ssh/sshd_config`, busca la línea relacionada con el protocolo: `#Protocol 2,1`
- Modifica la línea para que solo permita la versión 2: `Protocol 2`
- Guarda y reinicia el servicio.

Ajustes en el Archivo sshd_config

Es el corazón de la configuración del servidor SSH

C. Deshabilitar el acceso directo de Root

Permitir el inicio de sesión directo del usuario root incrementa los riesgos en caso de ataques de fuerza bruta o vulnerabilidades. Es preferible que los usuarios inicien sesión con un usuario normal y luego utilicen `sudo` para obtener privilegios administrativos.

- Abre nuevamente el archivo `/etc/ssh/sshd_config.`
- Busca la línea que dice: `#PermitRootLogin prohibit-password`
- Cámbiala a: `PermitRootLogin no`
- Guarda el archivo y reinicia el servicio SSH.

¡Manos a la obra!

Configuración del protocolo y deshabilitación de Root

Instrucciones

1. Inicia la máquina virtual Rocky Linux.
2. Editar Configuración:
    - Abre /etc/ssh/sshd_config.
3. Ajustar Protocolos:
    - Modifica la línea para permitir solo Protocol 2.
4. Deshabilitar Root Login:
    - Cambia la línea correspondiente a PermitRootLogin a no.
5. Guardar y Reiniciar:
    - Guarda los cambios y reinicia el servicio.
6. Verificación:
    - Intenta conectarte como root para confirmar que el acceso está bloqueado.

Resumen

Ideas principales

- La correcta configuración de OpenSSH Server es crucial para garantizar la seguridad y estabilidad de cualquier sistema remoto.
- Mediante la instalación adecuada, la personalización del archivo sshd_config y la aplicación de buenas prácticas como cambiar el puerto, limitar los protocolos a la versión 2 y deshabilitar el acceso directo de root– se reducen significativamente las vulnerabilidades frente a ataques externos.

¿Qué otras medidas de seguridad podrías implementar en un servidor SSH además de las presentadas en la clase?

Próxima sesión...

Creación, distribución y gestión de claves públicas y privadas.

{desafío} latam_

{desafío}
latam_

Academia de
talentos digitales