Guía de estudio - Políticas de autenticación y acceso, parte I

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

¿En qué consiste esta guía?

En entornos multiusuario y en servidores accesibles remotamente, es fundamental implementar políticas de autenticación y acceso que garanticen que solo usuarios y grupos autorizados puedan conectarse.

Esta guía se enfoca en la configuración de acceso restringido mediante la definición de permisos específicos por usuario y grupo. Al aplicar estas políticas, se refuerza la seguridad del sistema, se limita la superficie de ataque y se facilita la administración de los accesos.

¡Vamos con todo!

Tabla de contenidos

¡Comencemos!

Fundamentos y conceptos clave

Antes de proceder a la configuración, es importante comprender los siguientes conceptos:

- **Usuarios y grupos:**
  Cada usuario en un sistema Unix/Linux tiene un identificador único, y estos pueden agruparse para facilitar la administración de permisos y políticas de acceso.

- **Directivas de SSH para acceso:**
  El archivo de configuración de OpenSSH (/etc/ssh/sshd_config) permite especificar quiénes pueden o no acceder mediante las siguientes directivas:
  - AllowUsers: Permite definir una lista de usuarios autorizados.
  - DenyUsers: Especifica usuarios a los que se les niega el acceso.
  - AllowGroups: Permite que solo los usuarios que pertenezcan a determinados grupos puedan acceder.
  - DenyGroups: Niega el acceso a usuarios pertenecientes a ciertos grupos.

Configuración de acceso restringido

La configuración de acceso restringido se realiza editando el archivo sshd_config y aplicando las directivas adecuadas. A continuación, se describe cómo hacerlo:

Directiva AllowUsers y DenyUsers

AllowUsers:

Permite especificar explícitamente qué usuarios pueden iniciar sesión a través de SSH.
Ejemplo:

```
AllowUsers juan maria admin@192.168.1.*
```

Esto autoriza a los usuarios "juan" y "maria", y al usuario "admin" cuando se conecte desde una IP que coincida con el patrón especificado.

DenyUsers:

Permite denegar el acceso a ciertos usuarios, incluso si se encuentran en listas de usuarios permitidos por otras configuraciones.
Ejemplo:

```
DenyUsers pepe
```

Directiva AllowGroups y DenyGroups

AllowGroups:

Permite que solo los usuarios pertenecientes a los grupos especificados puedan acceder. *Ejemplo:*

```
AllowGroups sshusers admins
```

Esto indica que solo los usuarios que pertenezcan a los grupos "sshusers" o "admins" podrán autenticarse.

DenyGroups:

Similar a DenyUsers, esta directiva deniega el acceso a usuarios que pertenezcan a ciertos grupos. *Ejemplo:*

```
DenyGroups invitados temporales
```

Tabla resumen de directivas

Directiva	Propósito	Ejemplo
AllowUsers	Especificar usuarios autorizados	`AllowUsers juan maria admin@192.168.1.*`
DenyUsers	Denegar acceso a usuarios específicos	`DenyUsers pepe`
AllowGroups	Permitir el acceso solo a usuarios de ciertos grupos	`AllowGroups sshusers admins`
DenyGroups	Denegar acceso a usuarios que pertenezcan a ciertos grupos	`DenyGroups invitados temporales`

Nota: Las directivas se evalúan en orden. Es recomendable probar la configuración en un entorno controlado para evitar bloqueos accidentales.

Actividad guiada: Configuración básica de usuarios permitidos

1. **Inicia la máquina virtual con Rocky Linux.**
2. **Accede al archivo de configuración:**
   Abre el archivo `/etc/ssh/sshd_config` con un editor de texto:

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

3. **Añade o modifica la directiva AllowUsers:**
   Inserta la siguiente línea (o ajusta la existente) para autorizar a usuarios específicos:

```
AllowUsers juan maria
```

Consejo: Puedes incluir patrones de IP si deseas restringir aún más el acceso.

4. **Guarda los cambios y reinicia el servicio:**

```
sudo systemctl restart ssh
```

5. **Prueba la conexión:**
   Desde otro terminal o desde la máquina tutora, utilizando Putty, intenta conectarte con los usuarios especificados:

```
ssh juan@direccion_del_servidor
```

¡Manos a la obra! - Configuración de acceso restringido por grupo

Configura la directiva AllowGroups:
Abre nuevamente `/etc/ssh/sshd_config` y agrega:

```
AllowGroups sshusers
```

Verifica que los usuarios estén en el grupo adecuado:
Comprueba la pertenencia de un usuario al grupo "sshusers":

```
groups juan
```

Si "juan" no aparece en el grupo, agrégalo:

```
sudo usermod -aG sshusers juan
```

Reinicia el servicio SSH y prueba la conexión:

```
sudo systemctl restart ssh
ssh juan@direccion_del_servidor
```

Realiza pruebas con un usuario fuera del grupo:
Intenta conectarte con un usuario que no pertenezca al grupo "sshusers" para confirmar que se deniega el acceso.

Reflexiona:

- ¿Qué ventajas ofrece la configuración de acceso restringido mediante usuarios y grupos en comparación con una política de acceso abierta?
- ¿Cuáles podrían ser las consecuencias de configurar incorrectamente estas directivas en un entorno de producción?
- ¿Cómo facilitaría esta configuración la administración de accesos en un sistema con un gran número de usuarios?
- ¿Qué procedimientos implementarías para validar que la política de acceso restringido funciona correctamente sin afectar a usuarios autorizados?

Implementar políticas de autenticación y acceso mediante restricciones basadas en usuario y grupo es esencial para reforzar la seguridad en sistemas críticos. La correcta configuración de directivas como AllowUsers, DenyUsers, AllowGroups y DenyGroups en el archivo sshd_config te permite controlar de forma granular quién puede acceder a tu sistema.