Configuración de SSH: autenticación por contraseña y fortaleza

Este documento evalúa la configuración de SSH en una máquina Debian y demuestra que el servicio permite autenticación por contraseña (incluyendo acceso como root) sin controles adecuados de fortaleza. Esto habilita el uso de contraseñas débiles y aumenta el riesgo de compromisos por fuerza bruta o reutilización de credenciales.

Resumen de hallazgos

Hallazgo	Evidencia	Riesgo
PasswordAuthentication habilitado	passwordauthentication yes	Fuerza bruta y contraseñas débiles
Root permitido por SSH	permitrootlogin yes + log 'Accepted password for root'	Compromiso total del sistema
No se exige método fuerte	authenticationmethods any	No obliga claves/MFA; se mantiene vector password
Sin política PAM de complejidad	No aparece pam_pwquality/pam_cracklib en common-password	Contraseñas simples son posibles

Alcance y metodología

Alcance: revisión de configuración efectiva de OpenSSH (sshd), archivo sshd_config, módulos PAM asociados a políticas de contraseña, y registros (journald).
Método: comandos locales en Debian para extraer parámetros efectivos y evidencias de autenticación.

Evidencia recopilada

1) Configuración efectiva (sshd -T)

```
Comando:
  sudo sshd -T |
    grep -Ei 'passwordauthentication|pubkeyauthentication|permitrootlogin|'
            'authenticationmethods|maxauthtries|usepam|kbdinteractiveauthentication'

Salida:
usepam yes
maxauthtries 6
permitrootlogin yes
pubkeyauthentication yes
passwordauthentication yes
kbdinteractiveauthentication no
authenticationmethods any
```

2) Parámetros en /etc/ssh/sshd_config

```
Comando:
  sudo grep -nE '^(PasswordAuthentication|PubkeyAuthentication|PermitRootLogin|'
                'AuthenticationMethods|MaxAuthTries|UsePAM|KbdInteractiveAuthentication)\b' \
    /etc/ssh/sshd_config

Salida:
33:PermitRootLogin yes
57:PasswordAuthentication yes
62:KbdInteractiveAuthentication no
85:UsePAM yes
```

3) Política de complejidad en PAM (common-password)

```
Comando:
  sudo grep -nE 'pam_pwquality\.so|pam_cracklib\.so' /etc/pam.d/common-password

Salida:
  (sin salida)

Interpretación:
  Sin coincidencias (no se observan pam_pwquality.so ni pam_cracklib.so en common-password).
```

4) Evidencia en logs (journald)

```
Comando:
  sudo journalctl -u ssh --no-pager | tail -n 80

Líneas relevantes:
  Server listening on 0.0.0.0 port 22.
  Server listening on :: port 22.
  Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
  tail: cannot open '/var/log/auth.log' for reading: No such file or directory
```

Nota: /var/log/auth.log no está disponible; la evidencia de autenticación se obtuvo desde journald.

Análisis de seguridad

• Autenticación por contraseña habilitada: 'passwordauthentication yes' permite acceso con password, por lo que la seguridad depende directamente de la calidad de las contraseñas y de los controles contra fuerza bruta.

• Acceso como root permitido: 'permitrootlogin yes' habilita el objetivo más valioso (root) por SSH. Esto incrementa el impacto de cualquier credencial débil o filtrada.

• No se exige un método fuerte: 'authenticationmethods any' indica que no se impone un esquema como 'publickey' exclusivo o combinaciones tipo 2FA.

• Sin controles PAM visibles de complejidad: al no observarse pam_pwquality/cracklib en common-password, no hay evidencia de requisitos mínimos (longitud, complejidad, repetición) aplicándose al crear contraseñas.

Impacto

Con esta configuración, un atacante puede intentar adivinar contraseñas (fuerza bruta) o reutilizar credenciales robadas. Si obtiene acceso como root (confirmado en logs), el impacto

es compromiso total del sistema: lectura/modificación de datos, instalación de persistencia, movimiento lateral y deshabilitación de controles.

Recomendaciones de mitigación (hardening)

• Deshabilitar login directo de root: establecer PermitRootLogin no y usar sudo con usuarios administrativos.

• Deshabilitar autenticación por contraseña: establecer PasswordAuthentication no y usar llaves SSH (publickey).

• Forzar método de autenticación: configurar AuthenticationMethods publickey (o publickey + MFA si aplica).

• Restringir quién puede acceder: usar AllowUsers o AllowGroups para limitar cuentas permitidas.

• Reducir intentos: bajar MaxAuthTries (por ejemplo, 3) y habilitar protección anti-fuerza bruta (fail2ban).

• Aplicar política de contraseñas: instalar y configurar libpam-pwquality para exigir longitud mínima y complejidad.

Ejemplo de configuración recomendada (referencial)

```
Archivo: /etc/ssh/sshd_config
  PermitRootLogin no
  PasswordAuthentication no
  PubkeyAuthentication yes
  AuthenticationMethods publickey
  MaxAuthTries 3
  AllowUsers <usuario_admin>

Aplicar cambios (referencial):
  sudo systemctl restart ssh
```

Importante: aplica cambios en un entorno controlado y confirma que tienes acceso por llaves antes de deshabilitar contraseñas.