Fail2ban

¿Qué es Fail2Ban?

Fail2Ban es una herramienta de prevención contra intrusiones que supervisa los intentos de conexión sospechosos en los registros del sistema (logs) y que puede implementarse en su infraestructura local.

¿Qué bloquea exactamente?

Fail2Ban protege principalmente contra ataques de tipo **«Brute Force»** (fuerza bruta).

Para decidir si una actividad es maliciosa, Fail2Ban analiza los intentos de conexión e identifica patrones específicos. Estos son los errores comunes que desencadenan una alerta y un bloqueo:

- ◦ `Usuario no válido`**:** alguien intenta iniciar sesión con nombres aleatorios (por ejemplo: `admin`, `root`, `test`, `guest`). Es el indicio típico de un bot que prueba diccionarios de nombres.
  - ◦ `Contraseña incorrecta`**:** existe un usuario conocido**,** pero la contraseña introducida es incorrecta. Un número excesivo de intentos indica un ataque de fuerza bruta.
  - ◦ `Authentication failure` **(Error de autenticación):** Un error general que se produce cuando las credenciales proporcionadas no coinciden con ninguna entrada de la base de datos segura del servidor.
  - ◦ `Failed public key authentication` **(Autenticación de clave pública fallida):** Aunque utilices claves de seguridad (más seguras que las contraseñas), Fail2Ban bloquea a quienes intentan presentar claves no autorizadas repetidamente.

Si una IP genera 5 fallos en un intervalo de 10 minutos, se bloquea durante 10 minutos.

Revision #1
Created 2026-04-30 07:40:59 UTC by Adrien Thaissen
Updated 2026-04-30 07:40:59 UTC by Adrien Thaissen