Investigación de intentos SSH fallidos – host Kali

Fecha: 2025-11-06

Resumen

Se detectaron intentos de autenticación SSH fallidos en el host 'kali'. Se identificaron las IPs 203.0.113.45 y 203.0.113.46, intentando acceder a los usuarios 'testuser' y 'root'. Este comportamiento es típico de ataques de fuerza bruta y requiere mitigación inmediata.

Evidencia

Archivo: ~/practice_logs/auth.log
Nov 06 12:00:01 kali sshd[1234]: Failed password for testuser from 203.0.113.45 port 54321
Nov 06 12:01:02 kali sshd[1235]: Failed password for root from 203.0.113.46 port 54322

Acciones realizadas

1. Contabilización de intentos por IP. 2. Revisión de logins exitosos (no se detectaron accesos aceptados). 3. Preparación para bloqueo de IPs maliciosas.

Recomendaciones

- Bloquear las IPs en firewall (ufw o iptables). - Implementar fail2ban para proteger SSH automáticamente. - Monitorear logs adicionales para detectar patrones similares.

Comandos usados

grep "Failed password" ~/practice_logs/auth.log
grep -oE '([0-9]{1,3}\.){3}[0-9]{1,3}' | sort | uniq -c | sort -nr
sqlite3 ~/logins.db "SELECT ip_address, COUNT(*) FROM logins WHERE status='failed' GROUP BY ip_address;"