Reporte de Incidencia – Intento de Ataque por Fuerza Bruta en SMTP

1. Resumen del incidente

Se detectó un intento de ataque de fuerza bruta (SMTP brute force attack) dirigido al servidor de correo electrónico, con el objetivo de obtener acceso no autorizado para el envío de correos maliciosos.

---

2. Descripción del evento

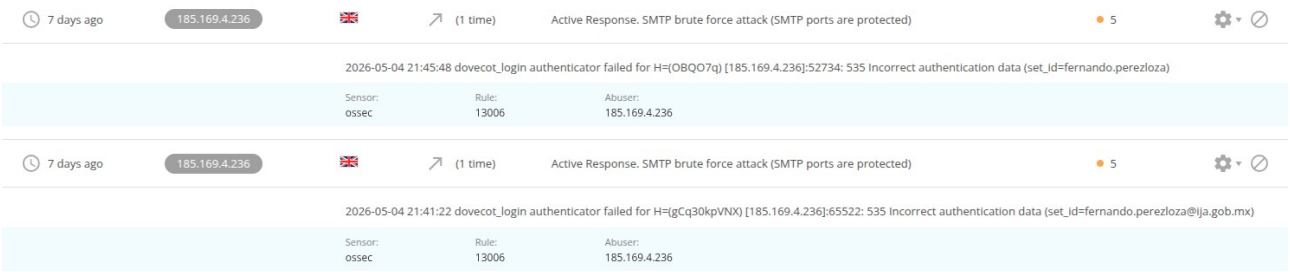
El sistema de seguridad del servidor identificó múltiples intentos de autenticación fallidos utilizando credenciales de acceso antiguas, las cuales ya habían sido previamente deshabilitadas y dadas de baja.

El atacante intentó comprometer el servicio SMTP mediante el uso repetitivo de estas credenciales, buscando vulnerar el sistema para el envío de correos electrónicos no autorizados o maliciosos.

---

3. Detección

El incidente fue detectado de manera oportuna por el firewall del servidor, el cual activó las alertas correspondientes ante el patrón inusual de intentos de autenticación fallidos.



---

4. Impacto

- No se logró acceso al sistema .
- No se enviaron correos electrónicos maliciosos.
- Se revisaron los logs de envío de correos y el uso de API Keys, confirmando que todo se encuentra en estado normal y sin actividad sospechosa.

---

6. Estado actual

No se han observado actividades sospechosas posteriores.

---

8. Posibles causas del incidente

Este tipo de ataques de fuerza bruta contra servicios SMTP suelen presentarse debido a una combinación de factores relacionados con exposición de credenciales y automatización de ataques. Entre las causas más comunes se encuentran:

- **Filtración de credenciales (data leaks):**
  Credenciales antiguas o deshabilitadas pueden haber sido expuestas previamente en brechas de seguridad de terceros, repositorios públicos o bases de datos comprometidas. Estas credenciales suelen ser reutilizadas por atacantes en intentos automatizados.
- **Uso de diccionarios de contraseñas filtradas:**
  Los atacantes emplean listas masivas de usuarios y contraseñas obtenidas de filtraciones anteriores (credential stuffing), probando combinaciones comunes o previamente comprometidas contra servicios SMTP.
- **Contraseñas débiles o reutilizadas:**
  En algunos casos, credenciales antiguas pueden haber sido simples o reutilizadas en múltiples sistemas, lo que incrementa la probabilidad de que formen parte de listas de ataque.
- **Escaneo automatizado de servicios expuestos:**
  Bots y herramientas automatizadas escanean constantemente Internet en busca de servicios SMTP accesibles para intentar autenticación mediante fuerza bruta.
- **Credenciales históricas no completamente retiradas del ecosistema:**
  Aunque las cuentas hayan sido deshabilitadas, en algunos escenarios pueden existir referencias residuales en sistemas, logs o integraciones antiguas que los atacantes intentan explotar.