**Caso 1: Acceso Fallido a RDP desde una IP Externa**

- **Contexto**: Una alerta indica múltiples intentos de acceso fallido a RDP desde una IP externa.
- **Datos disponibles**:
    - Logs del firewall muestran intentos de conexión recurrentes al puerto 3389.
    - [2025-01-23 14:32:10] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:15] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:20] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:25] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:30] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:35] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:40] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:45] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:50] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.
    - [2025-01-23 14:32:55] [INFO] [Firewall] Intento de conexión entrante desde 203.0.113.45 al puerto 3389.

El sistema Windows muestra eventos 4625 de fallos de inicio de sesión.

[2025-01-23 14:32:10] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:15] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:20] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:25] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:30] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:35] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:40] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:45] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:50] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

[2025-01-23 14:32:55] [ERROR] [Windows Security] Evento 4625: Intento de inicio de sesión fallido para el usuario 'admin' desde la dirección IP 203.0.113.45. Motivo: Contraseña incorrecta.

- **Tareas**:

1.

a. Analiza los logs del firewall y del sistema Windows.
b. Identifica si la IP debe ser bloqueada y otras medidas necesarias.
c. Propón una respuesta y documenta tus hallazgos.

Claro la ip debe ser bloqueada puesto que esta intentando acceder por RDP, lo cual puede generar un ataque por fuerza bruta.

**Caso 2: Tráfico Sospechoso desde un Servidor Interno**

- **Contexto**: Una alerta del firewall indica tráfico inusual desde un servidor interno hacia una IP maliciosa.
- **Datos disponibles**:
  - Logs del firewall muestran conexiones HTTPS hacia la IP 198.51.100.50.
  - 2025-01-23 14:32:50 | ALERTA | 10.0.0.15 -> 198.51.100.50 | HTTPS | Conexión permitida
  - Acción: Permitida
  - Descripción: Conexión HTTPS desde el servidor interno 10.0.0.15 hacia la IP maliciosa 198.51.100.50. No se reportan procesos nuevos en el sistema.
  - Estado: Activa
  - Puerto de destino: 443

2025-01-23 14:33:10 | ALERTA | 10.0.0.15 -> 198.51.100.50 | HTTPS | Conexión permitida

Acción: Permitida

Descripción: Reintento de conexión HTTPS a la misma IP maliciosa 198.51.100.50. Sin procesos nuevos en el sistema.

Estado: Activa

Puerto de destino: 443

2025-01-23 14:33:30 | ALERTA | 10.0.0.15 -> 198.51.100.50 | HTTPS | Conexión permitida

Acción: Permitida

Descripción: Conexión HTTPS reestablecida hacia la IP 198.51.100.50. Sin procesos nuevos identificados.

Estado: Activa

Puerto de destino: 443

2025-01-23 14:34:00 | ALERTA | 10.0.0.15 -> 198.51.100.50 | HTTPS | Conexión permitida

Acción: Permitida

Descripción: Conexión HTTPS establecida correctamente hacia la IP maliciosa 198.51.100.50, sin procesos nuevos.

Estado: Activa

Puerto de destino: 443

2025-01-23 14:35:01 | ALERTA | 10.0.0.15 -> 198.51.100.50 | HTTPS | Conexión terminada

Acción: Permitida

Descripción: Conexión HTTPS terminada sin actividad de procesos nuevos.

Estado: Terminada

Puerto de destino: 443

- **Tareas**:

1.
    a. Analiza el tráfico registrado en el firewall.
    b. Sugiere pasos para investigar el servidor y asegurar su integridad.
    c. Define acciones correctivas para mitigar la amenaza.

Estos registros muestran conexiones HTTPS repetidas desde el servidor interno 10.0.0.15 hacia la IP maliciosa 198.51.100.50, esto es super alarmante puesto que se puede enviar datos de manera encriptada y evadir detección. Además, las conexiones están siendo permitidas por el firewall, lo que indica que no esta siendo bloqueado. Esto aumenta el riesgo que el servidor este comprometido y este enviado información confidencial

Se reporta que no hay procesos nuevos es decir que el código malicioso puede estar oculto o ejecutándose en manera discreta en el servidor.