Informe de Incidente de Ciberseguridad

1. Identificación del tipo de ataque.

El apretón de manos TCP en tres pasos (Three-Way Handshake)

1. **SYN**: El cliente envía un paquete SYN al servidor para solicitar una conexión.
2. **SYN-ACK**: El servidor responde con un paquete SYN-ACK para confirmar la solicitud.
3. **ACK**: El cliente responde con un paquete ACK, completando el establecimiento de la conexión.

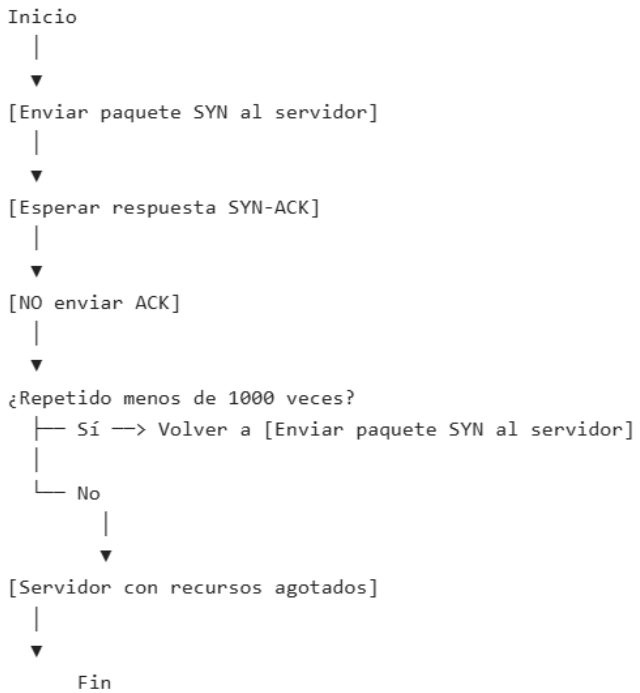
El incidente corresponde a un ataque de *denegación de servicio (DoS),* específicamente un ataque SYN Flood.

¿Qué sucede en un ataque SYN Flood?

En un ataque SYN Flood, un atacante envía una gran cantidad de paquetes SYN **sin completar el apretón de manos TCP**.

Como resultado, el servidor mantiene abiertas múltiples conexiones incompletas en su tabla de conexiones, **agotando la memoria y los recursos disponibles**, lo que lleva al **bloqueo del servicio** para nuevos usuarios legítimos.

Se diferencia de un ataque DDoS en que este proviene de una *única IP* o un número reducido de ellas, mientras que un DDoS proviene de *múltiples orígenes*.



2. Explicación del impacto del ataque en el sitio web

Durante la tarde del 10 de mayo de 2025, la agencia de viajes ficticia "Viajes Sol y Mar S.A." experimentó una interrupción crítica en su servidor web.

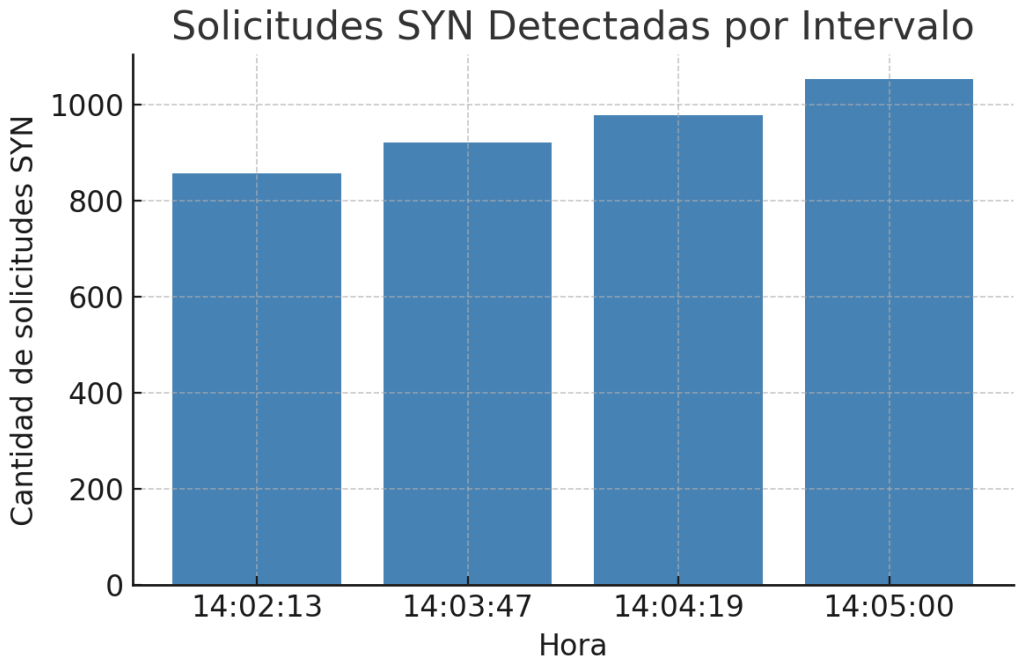
Los empleados reportaron que no podían acceder a la página de promociones, y se recibió una alerta automática del sistema de monitoreo.

Al revisar el tráfico de red con Wireshark, se detectó un número masivo de paquetes TCP SYN provenientes de una dirección IP sospechosa.

Datos técnicos del ataque

Tabla 1: Solicitudes TCP SYN detectadas

Hora	Dirección IP Origen	Número de Solicitudes SYN
14:02:13	192.168.45.101	856
14:03:47	192.168.45.101	921
14:04:19	192.168.45.101	978
14:05:00	192.168.45.101	1052



El ataque SYN Flood causó que el servidor web se viera desbordado, acumulando conexiones semiabiertas.

Esto resultó en la incapacidad del servidor para procesar nuevas solicitudes, mostrando errores de 'tiempo de espera de conexión'.

La operación interna de los empleados se vio afectada, provocando una caída en la productividad y potencial pérdida de ventas. También afectó la percepción de fiabilidad del sitio por parte de los clientes.

3. Impacto:

3.1 Operativo:

- 2h 23min de inactividad del sitio web
- Bloqueo del acceso a promociones y sistema de reservas

3.2 Económico:

- Pérdida estimada: ~15,200 EUR (ventas promedio en ese horario)

3.3 Reputacional:

- 42 quejas de clientes en redes sociales
- Caída del 30% en visitas las 24h posteriores

Medidas inmediatas:

- Desconectar el servidor para su recuperación.
- Bloquear temporalmente la IP atacante desde el firewall.
- Activación de una página estática de emergencia.

4. Recomendaciones para Mitigar y Prevenir Futuros Ataques

Para el equipo técnico:

Corto Plazo(48h):

- Implementar protección contra DoS/DDoS en el firewall y el servidor web.
- Usar técnicas como SYN cookies en Apache.
- Establecer límites de conexiones simultáneas por IP.
- Activar alertas tempranas en caso de tráfico anómalo.

Medio Plazo (2 semanas):

- Contratar servicio Cloudflare Pro (mitigación DDoS)
- Simulación de ataque con herramientas como hping3

Largo Plazo (1 mes):

- Capacitación obligatoria en seguridad para todo el personal
- Implementar ISO 27001 como estándar de seguridad

Para la dirección de la empresa:

- Invertir en infraestructura de ciberseguridad moderna y escalable.
- Establecer un plan de respuesta ante incidentes y comunicarlo a todo el personal.
- Realizar capacitaciones regulares de concienciación sobre seguridad para empleados.
- Asegurar la contratación de servicios de alojamiento web que incluyan mitigación DDoS.
- Incluir la ciberseguridad como parte del plan estratégico de la empresa.

En caso de sufrir un ataque **SYN Flood** o cualquier otro incidente de ciberseguridad, es crucial informar a las entidades adecuadas para cumplir con la ley, mitigar daños y prevenir futuros ataques.

- **INCIBE (Instituto Nacional de Ciberseguridad)**:
  📌 Formulario de Reporte de Incidentes
  📞 Teléfono: **017** (Servicio gratuito para empresas y ciudadanos).
  Obligatorio si el ataque afecta a datos personales (LOPDGDD) o infraestructuras críticas.

- **AEPD (Agencia Española de Protección de Datos)**:
  📌 Solo si se filtran datos personales (RGPD).
  ✉ canaletico@aepd.es.

Autoridades Policiales (Si hay delito)

- **Guardia Civil (España) - Grupo de Delitos Telemáticos**:
  📌 Formulario online.

Clientes y Afectados

- **Comunicación Transparente**:
  Si el ataque afectó a usuarios (ej: caída del servicio), enviar un email o anuncio explicando lo ocurrido y medidas tomadas.
  📌 Ejemplo:

"El [fecha], nuestro sitio experimentó interrupciones por un ataque cibernético. Hemos mitigado el problema y reforzado la seguridad. Lamentamos las molestias."