# Cybersecurity Incident Report

| Section 1: Identify the type of attack that may have caused this  network interruption | |
| --- | --- |
| Desde el equipo de seguridad después de realizar las comprobaciones necesarias podemos ver que el cliente de la empresa no puede acceder a la página de ventas. Un individuo antes de que el cliente hiciera la petición, el servidor recibió una gran cantidad de paquetes con peticiones SYN lo que provocó que este dejará de funcionar.  Hemos hecho una revisión de los logs de registro de la red usando la herramienta Wireshark, esta herramienta efectivamente nos confirma que han tenido lugar diferentes eventos a la misma hora repetidas veces por el mismo puerto 443 desde el puerto 54770,  con insignificante diferencia horaria entre ellos, provocando la saturación del servidor hasta provocar un registro en la página de ventas con un página de estado “HTTP 200” para indicar la caída del servicio que queríamos acceder. No solo esto nos indica un mala conexión con el servidor si no podemos ver la existencia de RST - ACK en los paquetes analizados indicando tardanza en las próximas peticiones.  Este evento es claramente un ataque DoS, clasificado como “SYN Flood” debido a la cantidad de intentos de conexión para obtener comunicación con el servidor de tipo “SYN ACK”. | |
|

| Section 2: Explain how the attack is causing the website to malfunction |
| --- |
| 1. Primero tenemos la solicitud de conexión por parte del atacante al servidor:   54770->443 [SYN] Seq=0 Win=5792 Len=0…   1. Seguidamente obtenemos la respuesta del servidor al cliente indicando mensajes RST - ACK debido a la congestión y tardanza en dar las respuestas: 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... 2. Por último, tenemos el registro de que la petición por parte del servidor a llegado al cliente que ataca de manera repetida al servidor con las solicitudes: 54770->443 [SYN] Seq=0 Win=5792 Len=0… |
| Cuando un ciberdelincuente envía repetidos paquetes tcp SYN, el servidor espera una solicitud con un ACK final pero este nunca aparece provocando un corte en la solicitud de manera directa. Estas solicitudes se guardan dentro de una tabla de conexiones dentro del servidor que llenan su almacenamiento si se realizan de manera masiva. El agotamiento de los recursos del servidor provocará que el servidor caiga.  Los logs nos indican un masiva campaña de solicitudes SYN por parte del ciberdelincuente, provocando que el servidor se quede sin recursos y haciendo que el equipo caiga por sobrecarga. |