Cybersecurity Incident Report

Sección 1: Identificar el tipo de ataque que ha causado esta interrupción de la red
Basado en el análisis de los síntomas y el registro de Wireshark, parece que la red está experimentando un **ataque de Denegación de Servicio Distribuida (DDoS)**. Un ataque DDoS inunda un servidor o red objetivo con una gran cantidad de tráfico malicioso proveniente de múltiples fuentes, lo que provoca una interrupción significativa en los servicios. En este caso, el sitio web presenta tiempos de carga extremadamente lentos y errores de "tiempo de espera de conexión agotado". Estos son síntomas clásicos de un ataque DDoS, donde los usuarios legítimos no pueden acceder al servicio debido a que el servidor está sobrecargado con una avalancha de solicitudes. Los registros de Wireshark muestran patrones inusuales de tráfico provenientes de una gran cantidad de direcciones IP en un corto período de tiempo, todas apuntando al mismo servidor web. El volumen y la distribución del tráfico indican un ataque coordinado desde varias fuentes, lo que confirma un ataque DDoS.

Sección 2: Explicación de cómo el ataque está afectando el funcionamiento del sitio web
El ataque DDoS está afectando el sitio web al sobrecargar el servidor con solicitudes falsas o maliciosas, lo que impide que los usuarios legítimos accedan a la página. El servidor no puede procesar todas las solicitudes simultáneas, lo que causa retrasos y, eventualmente, el agotamiento de recursos del sistema, resultando en errores de tiempo de espera. Este tipo de ataque afecta negativamente al rendimiento de la red, ya que el tráfico legítimo no puede ser procesado debido a la congestión artificial creada por los atacantes. Las consecuencias de este ataque incluyen la interrupción de los servicios en línea de la organización, pérdida de ingresos, daño a la

reputación y posibles costos de recuperación y mitigación.

Es crucial implementar medidas de defensa como el uso de firewalls avanzados, herramientas de monitoreo de tráfico, y sistemas de mitigación de DDoS para prevenir futuros incidentes similares.