Informe sobre incidentes de ciberseguridad

Sección 1: Identifica el tipo de ataque que puede haber causado esta interrupción de la red
El tipo de ataque que se observó para que los servidores se cayeran se denomina Ataque de Denegación de Servicio (DoS). Observando más a detalle, el tipo de ataque específico sería una inundación sincronizada (SYN flood). Este ataque satura el servidor con paquetes SYN, dejando las conexiones semiabiertas y consumiendo recursos. Se espera que al configurar el firewall para mitigar este ataque, el atacante intente burlarlo mediante la suplantación de IP, cambiando su dirección IP para continuar el ataque.

Sección 2: Explica cómo el ataque está provocando que el sitio web no funcione como debería
Un ataque de Denegación de Servicio (DoS) se da cuando un servidor recibe múltiples solicitudes, incrementando significativamente el tráfico de datos. El objetivo de este ataque es saturar la red con solicitudes falsas, sobrecargando así el servidor. Un tipo específico de este ataque es la inundación sincronizada (SYN flood), que simula una conexión TCP/IP enviando múltiples paquetes SYN. Este ataque afecta considerablemente porque, al iniciar una conexión TCP/IP, el atacante envía paquetes SYN y el servidor responde con paquetes SYN-ACK. El servidor espera recibir un paquete ACK para completar la conexión, pero el atacante no lo envía. Esto deja las conexiones semiabiertas, consumiendo recursos y manteniendo los puertos ocupados, lo que puede ralentizar el servidor o incluso causarle una caída. Para mitigar esta amenaza, los firewalls pueden bloquear la IP del atacante. Sin embargo, esto puede llevar al atacante a usar un método conocido como suplantación de IP, donde cambia su IP para hacerse pasar por una IP autorizada y continuar el ataque. Es esencial implementar técnicas adicionales, como el uso de SYN cookies y límites de tasa de conexiones, para proteger eficazmente el servidor contra estos ataques.