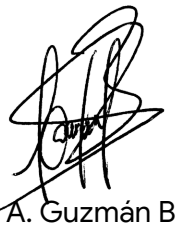
Reporte- Análisis del Incidente de Incidente

Resumen	Esta mañana, se notificó al departamento de IT un problema para ingresar a la red interna de la empresa, lo cual se pudo verificar que ningún empleado puede tener acceso. Visto esto el departamento de ciberseguridad se puso manos a la obra para realizar los análisis y pruebas pertinentes para detectar cuál es la causa de esta anomalía. El resultado de este análisis fue el descubrimiento de un hallazgo preocupante: un ataque tipo DDoS (denegación de servicios distribuido.
Identificar	El equipo de ciberseguridad realizó análisis y pruebas en la red interna para identificar por qué ocurre esto. Se identificó el fallo de seguridad debido a un firewall mal configurado.
Proteger	Para hacer frente a este problema de seguridad, el equipo de seguridad de red implementó lo siguiente: - Una nueva regla en el firewall para limitar la tasa de paquetes ICMP entrantes. - La verificación de la dirección IP de origen en el firewall para comprobar si hay direcciones IP falsas en los paquetes ICMP entrantes. - Un software de monitoreo de red para detectar patrones de tráfico anómalos. - Un sistema IDS/IPS para filtrar parte del tráfico ICMP basándose en características sospechosas.
Detectar	El equipo de ciberseguridad de la empresa realizó una investigación, donde se determinó que un actor malicioso había enviado una avalancha de pings ICMP a la red de la empresa a través de un firewall no configurado. Esta vulnerabilidad permite a los atacantes saturar la red de la empresa mediante un ataque de denegación de servicios distribuido (DDoS)

Responder	En un futuro, ante el aviso en el Firewall que ya estará configurado de manera correcta para evitar estos ataques, avisará si hay algún intento de envíos de paquetes masivos levantando la sospecha de que sea otro ataque DDoS, con el software de monitoreo habrá una mejor visión para poder tomar precauciones, y usaremos filtros a través del IDS/IPS instalado. Luego el personal encargado deberá escalar el caso y reportar el intento como un incidente el cuál será revisado de cerca para evitarlo o de ser necesario. Así el equipo de gestión de incidentes responderá oportunamente bloqueando paquetes ICMP entrantes sospechosos, se detendrán todos los servicios de red no críticos fuera de línea y se reestablecerán los servicios de red críticos.
Recuoerar	En este caso, no hay nada que recuperar ya que el daño se basó únicamente en la caida de la red privada de la empresa.

Nota: Este caso nos deja como aprendizaje el mantener siempre actualizadas nuestras políticas de ciberseguridad, el apego a marcos de ciberseguridad como el CSF proporcionadas por el NIST. La salud de nuestros activos digitales es parte fundamental de la empresa y debemos cuidarlos como se debe a través de reglas y marcos de seguridad que, si bien no podremos quizá evitar un ataque al 100%, sí disminuye muchísimo la posibilidad de que un actor malicioso obtenga información indebida y nos haga daño.

Esta vez no hay nada que lamentar sino tan solo el hecho de haber recibido un ataque, pero pudo ser peor, por eso de ahora en adelante seremos más empáticos y estricos a la vez con los temas de seguridad para evitar futuros ataques



Luis A. Guzmán B

Programador y
Analista de Ciberseguridad