**Incidente análisis de informes**

|  |  |
| --- | --- |
| **Resumen** | Es una empresa multimedia (me reservo el nombre) que ofrece servicios de diseño web, diseño gráfico y soluciones de Marketing en redes sociales a pequeñas empresas. Su organización ha sufrido recientemente un ataque DDoS, que ha puesto en peligro la red interna durante dos horas hasta que se ha resuelto. |
| Identificar | Investigue el incidente de seguridad. Descubriendo que un actor malicioso había enviado una avalancha de pings ICMP a la red de la empresa a través de un cortafuegos no configurado. Esta vulnerabilidad permitió al agresor abrumar la red de la empresa mediante un ataque de denegación de servicio distribuido (DDoS). |
| Proteger | * Una nueva regla de cortafuegos para limitar la tasa de paquetes ICMP entrantes * Verificación de la dirección IP de origen en el cortafuegos para comprobar si hay direcciones IP falsificadas en los paquetes ICMP entrantes * Software de Monitoreo de red para detectar patrones de tráfico anormales * Un sistema IDS/IPS para filtrar parte del tráfico ICMP basado en características sospechosas |
| Detectar | Posibles incidentes de seguridad y mejorar las capacidades de supervisión para aumentar la rapidez y eficacia de las detecciones. |
| Responder | Para contener, neutralizar y analizar incidentes de seguridad; implantar mejoras en el proceso de seguridad. |
| Recuperar | El funcionamiento normal de los sistemas afectados y restaurar los datos y/o activos de los sistemas que se hayan visto afectados por un incidente. |

|  |
| --- |
| Reflexiones/Notas: |