**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | Se ha identificado que los servicios de red de la organización dejaron de responder repentinamente debido a una avalancha de paquetes ICMP entrantes, a través de un cortafuegos no configurado lo que un actor malicioso aprovecho para enviar una avalancha de pings ICMP.  Se identifico que fue un ataque de denegación de servicio distribuido (DDoS).  Tanto el equipo como los clientes a los que se les ofrece el servicio se han visto afectados para acceder al sistema.  El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos. |
| Identify | Un actor malisioso se dirigió a la empresa con un ataque de inuncación ICMP. Toda la red se vio afectada. |
| Protect | Para hacer frente a este problema de seguridad, el equipo de Seguridad de red implementó:   * Una nueva regla de cortafuegos para limitar la tasa de paquetes ICMP entrantes * Un sistema IDS/IPS para filtrar parte del tráfico ICMP basado en características sospechosas   El equipo de seguridad debe estar actualmente formado para identificar con eficacia ataques futuros. |
| Detect | * 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 |
| Respond | Se deben de establecer protocolos de respuesta, los cuales deben ser actualizados constantemente para saber que acciones tomar en caso de un determinado incidente.  Para futuros eventos de seguridad, el equipo de ciberseguridad aislará los sistemas afectados para evitar más interrupciones en la red. Intentarán restaurar los sistemas y servicios críticos que se vieron interrumpidos por el evento. Luego, el equipo analizará los registros de la red para verificar si hay actividad sospechosa y anormal. El equipo también informará de todos los incidentes a la alta dirección y a las autoridades legales correspondientes, si procede. |
| Recover | Para recuperarse de un ataque DDoS por inundación ICMP, el acceso a los servicios de red debe restaurarse a un estado de funcionamiento normal. En el futuro, los ataques de inundación ICMP externos se pueden bloquear en el firewall. A continuación, todos los servicios de red no críticos deben detenerse para reducir el tráfico de red interno. A continuación, primero se deben restaurar los servicios de red críticos. Finalmente, una vez que se ha agotado el tiempo de espera de la avalancha de paquetes ICMP, todos los sistemas y servicios de red no críticos pueden volver a estar en línea. |

|  |
| --- |
| Reflections/Notes:  Se recomienda:  Mantenimiento de cortafuegos, implica comprobar y actualizar las configuraciones de seguridad con regularidad.  Privilegios de acceso a la red, implican permitir, limitar y/o bloquear privilegios de acceso a los activos de la red para personas, roles, grupos, direcciones IP, direcciones MAC, etc. Reduce el riesgo de que usuarios no autorizados y tráfico externo accedan a la red interna. |

CASO:

Usted es un analista de ciberseguridad que trabaja para una empresa multimedia 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.

Durante el ataque, los servicios de red de su organización dejaron de responder repentinamente debido a una avalancha de paquetes ICMP entrantes. El tráfico normal de la red interna no podía acceder a ningún recurso de la red. El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos.

A continuación, el equipo de ciberseguridad de la empresa investigó el incidente de seguridad. Descubrieron 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).

Para hacer frente a este problema de seguridad, el equipo de Seguridad de red implementó:

* 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

Como analista de ciberseguridad, se le ha encomendado la tarea de utilizar este evento de seguridad para crear un plan que mejore la seguridad de la red de su empresa, siguiendo el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). Utilizarás el CSF para ayudarte a navegar a través de los diferentes pasos del análisis de este evento de ciberseguridad e integrar tu análisis en una estrategia de seguridad general. Hemos dividido el análisis en diferentes partes en la plantilla que figura a continuación. Puede explorarlas aquí:

* **Identificar** los riesgos de seguridad mediante auditorías periódicas de las redes internas, los sistemas, los dispositivos y los privilegios de acceso para identificar posibles brechas en la seguridad.
* **Proteger** los activos internos mediante la aplicación de políticas, procedimientos, formación y herramientas que ayuden a mitigar las amenazas a la ciberseguridad.
* **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.