Análisis Incidente Seguridad: Ping Flood ICMP 15-05-2024 #1

Globe Sistemas - Av. Libertador Jardin America

Descripción General del Reporte

Se analizará la situación utilizando el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF). El CSF es un marco voluntario que consta de estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad.

Se creará un informe de incidentes de ciberseguridad de calidad y se aplicará el CSF para demostrar un enfoque proactivo de la seguridad, mejorar la comunicación y la transparencia con las partes interesadas y mejorar las prácticas de seguridad dentro de la organización. El CSF es escalable y se puede aplicar en una amplia variedad de contextos.

Se identificará qué medidas de seguridad se deben aplicar en respuesta a las necesidades comerciales y se determinará cuáles son las mejores opciones disponibles en lo que respecta a la seguridad de la red.

Contexto

El contexto del escenario se detalla a continuación:

Se realizó un reporte de análisis de incidente como analista de ciberseguridad externo para la empresa Globe Sistemas que ofrece servicios de diseño web, desarrollos de apps, ecommerce y soluciones de marketing en redes sociales a pequeñas empresas. Su organización experimentó recientemente un ataque DDoS que comprometió la red interna durante dos horas hasta que se resolvió.

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

Como analista, investigué el evento de seguridad. Descubrí 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 permitió al atacante malintencionado invadir la red de la empresa mediante un ataque distribuido de denegación de servicio (DDoS).

Para abordar este evento de seguridad, como medida de seguridad de la red implementé:

* Una nueva regla de firewall para limitar la tasa de paquetes ICMP entrantes
* Verificación de la dirección IP de origen en el firewall 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 en función de características sospechosas

Como analista, utilicé este evento de seguridad para crear un plan para mejorar la seguridad de la red y crear una estrategia de seguridad general para la empresa, siguiendo el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). He dividido el análisis en diferentes partes:

* Identificar riesgos de seguridad mediante auditorías periódicas de redes internas, sistemas, dispositivos y privilegios de acceso para identificar posibles brechas de seguridad.
* Proteger los activos internos mediante la implementación de políticas, procedimientos, capacitación y herramientas que ayudarán a mitigar las amenazas a la ciberseguridad.
* Detectar posibles incidentes de seguridad y mejorar las capacidades de monitoreo para aumentar la velocidad y eficiencia de las detecciones.
* Responder para contener, neutralizar y analizar incidentes de seguridad; implementar mejoras al proceso de seguridad.
* Recuperar los sistemas afectados para su funcionamiento normal y restaurar los datos y/o activos de los sistemas que han sido afectados por un incidente.

| **Resumen** | La empresa experimentó un problema de seguridad cuando todos los servicios de red dejaron de responder repentinamente. El equipo de sistemas descubrió que la interrupción fue causada por un ataque de denegación de servicios distribuidos (DDoS) a través de una avalancha de paquetes ICMP entrantes. El equipo respondió bloqueando el ataque y deteniendo todos los servicios de red no críticos, para poder restaurar los servicios de red críticos. | | |
| --- | --- | --- | --- |
| **Identificar** | Uno o varios actores maliciosos atacaron a la empresa con un ataque de inundación ICMP. Toda la red interna se vio afectada. Todos los recursos críticos de la red debían protegerse y restaurarse a un estado funcional. | | |
| **Proteger** | El equipo de ciberseguridad implementó una nueva regla de firewall para limitar la velocidad de los paquetes ICMP entrantes y un sistema IDS/IPS para filtrar parte del tráfico ICMP en función de características sospechosas. | | |
| **Detectar** | El equipo de ciberseguridad configuró la verificación de la dirección IP de origen en el firewall para verificar si hay direcciones IP falsificadas en los paquetes ICMP entrantes e implementó un software de monitoreo de red para detectar patrones de tráfico anormales. | | |
| **Responder** | Para futuros eventos de seguridad, el equipo de ciberseguridad aislará los sistemas afectados para evitar mayores interrupciones en la red. Intentarán restaurar cualquier sistema y servicio crítico que haya sido interrumpido por el evento. Luego, el equipo analizará los registros de la red para detectar actividades sospechosas y anormales.. El equipo también informará todos los incidentes a la alta dirección y a las autoridades legales correspondientes, si corresponde. | | |
| **Recuperar** | Para recuperarse de un DDoS ataque 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 podrán bloquear en el firewall. Luego, se deben detener todos los servicios de red no críticos para reducir el tráfico de la red interna. A continuación, primero se deben restaurar los servicios de red críticos. Finalmente, una vez que se agota 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. | | |