

RESUMEN DE LA INCIDENCIA

Descripción del suceso

La red interna de la empresa multimedia fue blanco de un ataque de denegación de servicio (DoS). Durante un periodo de dos horas, los servicios de red dejaron de responder debido a una saturación masiva de tráfico.

Análisis del suceso

- **Causa raíz:** Un actor malicioso explotó un cortafuegos no configurado para enviar una avalancha de pings ICMP.
- **Origen del ataque:** Tráfico ICMP entrante desde fuentes externas que aprovecharon la falta de límites de velocidad en el firewall.
- **Sistemas atacados:** La infraestructura de red interna y los servicios de red críticos y no críticos.

Impacto

- **Disponibilidad:** Los servicios de red quedaron completamente inaccesibles para el tráfico normal.
- **Operatividad:** El personal no pudo acceder a los recursos de la red interna durante el tiempo que duró el ataque.
- **Duración:** El compromiso de la red se mantuvo por un espacio de dos horas hasta su resolución.

Respuesta y Mitigación

- El equipo de gestión de incidentes aplicó las siguientes medidas reactivas y proactivas:
 - **Contención inmediata:** Se bloquearon los paquetes ICMP entrantes y se desconectaron los servicios no críticos para estabilizar la red.
 - **Recuperación:** Se restablecieron los servicios de red críticos una vez que el tráfico malicioso fue neutralizado.
 - **Mejores Técnicas (Post-incidente):**
 - Implementación de **limitaciones de tasa (rate limiting)** para paquetes ICMP.
 - Activación de **verificación de IP de origen** para prevenir direcciones falsificadas (spoofing).
 - Instalación de software de **supervisión de red** y un sistema **IDS/IPS** para detectar y filtrar patrones anómalos en el futuro.

IDENTIFICACIÓN DEL ATAQUE Y SISTEMAS AFECTADOS

- **Tipo de ataque:** Se produjo un ataque de Denegación de Servicio (DoS).
- **Método de exploración:** El atacante utilizó una inundación de paquetes ICMP aprovechando un **cortafuegos mal configurado**.
- **Sistemas afectados:**

- **Red interna:** El tráfico de la red interna se vio comprometida y dejó de responder.
 - **Servicios de red:** Tanto los servicios críticos como los no críticos quedaron fuera de línea.
 - **Dispositivos de seguridad:** El cortafuegos perimetral fue el punto de entrada debido a su vulnerabilidad de configuración.
- **Actor y procesos identificados:**
- **Activos de hardware:** Sistemas de red y el hardware del firewall.
 - **Procesos empresariales:** Se interrumpieron los servicios de diseño web, diseño gráfico y soluciones de marketing en redes sociales para los clientes.
- **Brecha de seguridad:** Se identificó que la falta de límites en la tasa de paquetes y la falta de verificación de IPs permitieron la saturación de los recursos.

PROTEGER: Plan de acción

Basado en las vulnerabilidades identificadas durante el ataque, el plan de acción inmediato incluye las siguientes actualizaciones y modificaciones:

- Configuración de cortafuegos:**
Implementar una nueva regla de cortafuegos diseñada específicamente para limitar la tasa (rate-limiting) de paquetes ICMP entrantes, evitando así que una inundación sature la red.
- Verificación de identidad de red:**
Configurar la verificación de la dirección IP de origen en el firewall para detectar y bloquear paquetes ICMP con direcciones falsificadas (spoofing).
- Tecnología de protección:**
Invertir e implementar un sistema de prevención de intrusiones (IPS) que permite filtrar tráfico basado en características sospechosas antes de que impacte la red interna.
- Gestión de parches y mantenimiento:**
Realizar una revisión y actualización de los sistemas operativos y el software del firewall para asegurar que no existan otras vulnerabilidades de configuración conocidas.
- Concienciación y formación:**
Desarrollar programas de formación para el personal sobre la naturaleza de estos ataques y cómo informar anomalías de red detectadas de forma temprana.
- Políticas de acceso:**
Revisar quién tiene permisos para modificar las configuraciones de los dispositivos de red perimetrales para asegurar que solo el personal de seguridad autorizado pueda realizar cambios.

DETECTAR: Capacidades de supervisión y análisis

Siguiendo las directrices del NIST CSF y los hallazgos del incidente, la organización debe implementar las siguientes medidas de detección:

- **Supervisión continua de la seguridad:**

Implementar software de supervisión de red dedicado para analizar el tráfico en tiempo real y establecer una línea base de comportamiento normal, lo que permitirá detectar patrones de tráfico anómalos de forma inmediata.

- **Sistemas de Detección de Intrusiones (IDS):**

Configurar un IDS para monitorear el tráfico entrante desde Internet, específicamente diseñado para identificar y alertar sobre firmas de ataques de inundación ICMP y otros eventos de seguridad sospechosos.

- **Análisis de Registros (Logging):**

Utilizar herramientas de registro en el cortafuegos para rastrear el flujo del ataque a través de la red interna y documentar intentos de acceso desde direcciones IP no fiables o falsificadas.

- **Detección de Anomalías y Eventos:**

Evaluar la implementación de una herramienta de Gestión de Información y Eventos de Seguridad (SIEM) para centralizar las alertas, facilitando la detección de actividades inusuales en cuentas de usuario y el seguimiento de accesos no autorizados.

- **Control de Cuentas y Usuarios:**

Realizar auditorías periódicas de los privilegios de acceso para identificar intentos de inicio de sesión inusuales o brechas de seguridad en las credenciales de los empleados.

RESPONDER: Plan de acción ante incidentes



Siguiendo el marco NIST CSF y los procedimientos de manejo de incidentes, el plan se estructura de la siguiente manera:

- **Contención de Incidentes:**
 - Implementar el bloqueo inmediato de paquetes ICMP entrantes desde el cortafuegos para detener la saturación de la red.
 - Aislar o desconectar recursos no críticos de la red para reducir la superficie de ataque y preservar el ancho de banda para servicios esenciales.
- **Neutralización de la Amenaza:**
 - Activar las reglas de limitación de tasa (rate-limiting) en el cortafuegos para filtrar el exceso de tráfico malicioso automáticamente.
 - Utilizar la verificación de IP de origen para identificar y descartar paquetes con direcciones falsificadas (spoofing) [escenario].
- **Análisis del Incidente:**
 - Utilizar los registros (logs) del cortafuegos y del sistema IDS/IPS para rastrear el flujo del ataque a través de la red interna.
+1
 - Analizar las métricas del software de supervisión de red para determinar el volumen del ataque y los patrones de tráfico anómalos detectados.

- **Comunicación y Mejora:**
 - Establecer canales de comunicación claros para informar al personal de TI y a los usuarios finales afectados sobre el estado de la red.
 - Realizar una sesión de "lecciones aprendidas" para identificar qué mejoras son necesarias en los procedimientos de respuesta actuales y actualizar el plan de acción.

RECUPERACIÓN: Restauración y continuidad del negocio

Esta fase asegura que la organización regrese a su estado normal de funcionamiento de manera segura y eficiente.

- **Sistemas a restaurar inmediatamente:**

Se deben restablecer todos los servicios de red críticos que fueron pausados para detener el ataque, permitiendo que el tráfico normal de los clientes vuelva a fluir hacia los servicios de diseño web y marketing.

- **Procesos de recuperación:**

- Validación de integridad: Verificar que los sistemas operativos y el hardware del cortafuegos funcionen correctamente con las nuevas reglas de limitación de tasa (rate-limiting) implementadas.
- Monitoreo post-incidente: Mantener una supervisión intensiva durante las primeras horas tras la restauración utilizando el nuevo software de monitoreo para asegurar que la inundación de paquetes ICMP no se reinicie.

- **Comunicación interna y externa:**

- Informar al personal de TI y a los departamentos de diseño que la red interna vuelve a ser segura para el acceso a recursos.
- Notificar a la gerencia sobre la resolución del incidente y el tiempo total de inactividad (dos horas) para evaluar el impacto económico.

- **Mejoras estratégicas:**

Actualizar los planes de recuperación ante desastres para incluir respuestas específicas contra ataques DoS, asegurando que la próxima vez la neutralización sea más veloz que en este evento.