**Title:** Use the NIST Cybersecurity Framework to respond to a security incident.  
**Analyst:** José Escamilla  
**Date:** 26/07/2024

#### **Incident Documentation**

**Incident Description:**

On [Date of Incident], a Distributed Denial of Service (DDoS) attack was detected impacting our internal network for a duration of two hours. The attack was characterized by a massive influx of ICMP packets, which caused network services to become unresponsive. Normal network traffic was unable to access network resources due to the overwhelming volume of malicious traffic.

**Incident Details:**

* **Type of Attack:** DDoS Attack
* **Attack Vector:** ICMP Flood
* **Duration:** 2 hours
* **Initial Response:** Blocking ICMP packets, taking non-critical services offline, and restoring critical network services.
* **Root Cause:** A misconfigured firewall allowed the attack to exploit the network.

**Post-Incident Measures Implemented:**

* **New Firewall Rule:** Implemented to limit the rate of incoming ICMP packets.
* **IP Verification:** Enabled on the firewall to check for spoofed IP addresses in ICMP packets.
* **Network Monitoring Software:** Deployed to detect anomalous traffic patterns.
* **IDS/IPS System:** Installed to filter suspicious ICMP traffic based on characteristic anomalies.

#### **NIST Cybersecurity Framework Functions and Recommendations**

#### **1. Identify**

##### **Risks Identified:**

* **Misconfigured Firewall:** Allowed unrestricted ICMP traffic, leading to the DDoS attack.
* **Lack of Network Visibility:** Insufficient monitoring tools to detect and analyze traffic anomalies.

##### **Recommendations:**

* **Conduct Regular Risk Assessments:** Regularly perform audits of the network and associated systems to identify vulnerabilities, such as misconfigured firewalls or inadequate traffic filtering.
* **Asset Management:** Maintain an up-to-date inventory of network devices, services, and configurations. Ensure critical assets are classified and protected according to their sensitivity and importance.
* **Access Control:** Review and enforce network access policies, ensuring only authorized personnel can modify firewall configurations and network settings.

#### **2. Protect**

##### **Risks Identified:**

* **Unprotected Network Ports:** Lack of firewall rules allowed excessive ICMP traffic to enter the network.
* **Inadequate Rate Limiting:** Absence of controls to limit the volume of incoming traffic contributed to the attack's impact.

##### **Recommendations:**

* **Configure Firewalls Properly:** Ensure firewalls are configured to handle various types of traffic and are regularly updated to protect against known attack vectors. Implement rate limiting and rules to block excessive traffic, such as ICMP floods.
* **Implement Rate Limiting:** Apply rate-limiting controls to mitigate the impact of large-scale attacks by restricting the volume of traffic that can enter the network.
* **Employee Training:** Educate employees on cybersecurity best practices and incident response procedures to reduce the risk of human error contributing to security vulnerabilities.

#### **3. Detect**

##### **Risks Identified:**

* **Delayed Detection:** Insufficient monitoring tools led to a delay in detecting the abnormal traffic patterns.
* **Limited Visibility into Traffic Patterns:** Lack of real-time traffic analysis capabilities hampered quick identification of the attack.

##### **Recommendations:**

* **Deploy Network Monitoring Tools:** Utilize network monitoring software to detect and alert on anomalous traffic patterns indicative of potential DDoS attacks. Ensure monitoring tools are configured to analyze traffic volume and behavior.
* **Enhance IDS/IPS Capabilities:** Implement and regularly update Intrusion Detection/Prevention Systems (IDS/IPS) to identify and respond to suspicious network traffic in real-time.
* **Regular Log Analysis:** Continuously analyze network logs and traffic data to identify unusual patterns or potential signs of an ongoing attack.

#### **4. Respond**

##### **Risks Identified:**

* **Inadequate Initial Response:** The initial response was delayed due to the lack of predefined procedures for handling such attacks.
* **Insufficient Containment Measures:** Limited immediate actions to contain and mitigate the attack.

##### **Recommendations:**

* **Develop an Incident Response Plan:** Create and regularly update an incident response plan to address various types of network attacks, including DDoS. Ensure the plan includes procedures for containing, mitigating, and communicating about the attack.
* **Establish Communication Protocols:** Set up clear communication channels for reporting and managing incidents, both internally and with external stakeholders.
* **Conduct Post-Incident Reviews:** After an attack, perform a thorough review to understand what happened, evaluate the effectiveness of the response, and identify areas for improvement.

#### **5. Recover**

##### **Risks Identified:**

* **Service Disruption:** The attack caused significant downtime, affecting the availability of critical network services.
* **Data Integrity Concerns:** Potential concerns about data integrity and system availability during and after the attack.

##### **Recommendations:**

* **Restore Systems and Services:** Develop and test procedures for restoring network services and systems to normal operations after an incident. Ensure backups are current and can be used to recover lost or damaged data.
* **Review and Update Security Policies:** Based on lessons learned from the incident, revise security policies and procedures to address any identified gaps and prevent similar incidents in the future.
* **Improve Resilience:** Invest in network resilience measures, such as redundant systems and load balancing, to minimize the impact of future attacks and ensure continued service availability.

#### **Conclusion:**

The recent DDoS attack highlighted significant vulnerabilities in our network security posture. By applying the NIST Cybersecurity Framework, we have outlined key measures to strengthen our defenses and mitigate future threats.

#### **Recommendations:**

1. **Regularly Update and Configure Firewalls:** Ensure ongoing protection and proper traffic management.
2. **Enhance Monitoring and Detection:** Implement and maintain robust monitoring systems to detect and respond to potential threats in real-time.
3. **Strengthen Incident Response and Recovery:** Develop and regularly test incident response plans and recovery procedures to improve overall network resilience.

This structured approach will help us better protect our network and enhance our cybersecurity practices moving forward.

**Título:** Usa el Marco de Ciberseguridad del NIST para responder a un incidente de seguridad   
**Analista:** José Escamilla  
**Fecha:** 26/07/2024

#### **Documentación del Incidente (spanish)**

**Descripción del Incidente:**

El [Fecha del Incidente], se detectó un ataque de Denegación de Servicio Distribuido (DDoS) que afectó nuestra red interna durante una duración de dos horas. El ataque se caracterizó por una avalancha masiva de paquetes ICMP, lo que provocó que los servicios de red se volvieran no respondientes. El tráfico normal de la red no pudo acceder a los recursos de la red debido al abrumador volumen de tráfico malicioso.

**Detalles del Incidente:**

* **Tipo de Ataque:** Ataque DDoS
* **Vector del Ataque:** Inundación de ICMP
* **Duración:** 2 horas
* **Respuesta Inicial:** Bloqueo de paquetes ICMP, desactivación de servicios de red no críticos y restauración de los servicios de red críticos.
* **Causa Raíz:** Un firewall mal configurado permitió que el ataque explotara la red.

**Medidas Implementadas Posteriormente:**

* **Nueva Regla de Firewall:** Implementada para limitar la tasa de paquetes ICMP entrantes.
* **Verificación de IP:** Habilitada en el firewall para verificar direcciones IP falsas en los paquetes ICMP.
* **Software de Monitoreo de Red:** Desplegado para detectar patrones de tráfico anómalos.
* **Sistema IDS/IPS:** Instalado para filtrar el tráfico ICMP sospechoso basado en anomalías características.

#### **Funciones del Marco de Ciberseguridad (NIST) y Recomendaciones**

#### **1. Identificar**

##### **Riesgos Identificados:**

* **Firewall Mal Configurado:** Permitió tráfico ICMP no restringido, lo que contribuyó al ataque DDoS.
* **Falta de Visibilidad de la Red:** Insuficientes herramientas de monitoreo para detectar y analizar anomalías en el tráfico.

##### **Recomendaciones:**

* **Realizar Evaluaciones de Riesgos Periódicas:** Realizar auditorías regulares de la red y los sistemas asociados para identificar vulnerabilidades, como firewalls mal configurados o filtrado de tráfico inadecuado.
* **Gestión de Activos:** Mantener un inventario actualizado de dispositivos de red, servicios y configuraciones. Asegurar que los activos críticos se clasifiquen y protejan de acuerdo a su sensibilidad e importancia.
* **Control de Acceso:** Revisar y hacer cumplir las políticas de acceso a la red, asegurando que solo el personal autorizado pueda modificar configuraciones de firewall y ajustes de red.

#### **2. Proteger**

##### **Riesgos Identificados:**

* **Puertos de Red No Protegidos:** La falta de reglas de firewall permitió un tráfico ICMP excesivo en la red.
* **Falta de Control de Tasa:** Ausencia de controles para limitar el volumen de tráfico contribuyó al impacto del ataque.

##### **Recomendaciones:**

* **Configurar Adecuadamente los Firewalls:** Asegurar que los firewalls estén configurados para manejar diferentes tipos de tráfico y se actualicen regularmente para proteger contra vectores de ataque conocidos. Implementar limitación de tasa y reglas para bloquear tráfico excesivo, como inundaciones de ICMP.
* **Implementar Control de Tasa:** Aplicar controles de limitación de tasa para mitigar el impacto de ataques a gran escala restringiendo el volumen de tráfico que puede ingresar a la red.
* **Capacitación de Empleados:** Educar a los empleados sobre las mejores prácticas de ciberseguridad y procedimientos de respuesta a incidentes para reducir el riesgo de errores humanos que contribuyan a vulnerabilidades de seguridad.

#### **3. Detectar**

##### **Riesgos Identificados:**

* **Detección Retrasada:** Herramientas de monitoreo insuficientes llevaron a una demora en la detección de los patrones de tráfico anómalos.
* **Visibilidad Limitada en Patrones de Tráfico:** Falta de capacidad de análisis en tiempo real de tráfico dificultó la identificación rápida del ataque.

##### **Recomendaciones:**

* **Desplegar Herramientas de Monitoreo de Red:** Utilizar software de monitoreo de red para detectar y alertar sobre patrones de tráfico anómalos indicativos de posibles ataques DDoS. Asegurar que las herramientas de monitoreo estén configuradas para analizar volumen y comportamiento del tráfico.
* **Mejorar Capacidades IDS/IPS:** Implementar y actualizar regularmente Sistemas de Detección/Prevención de Intrusiones (IDS/IPS) para identificar y responder al tráfico de red sospechoso en tiempo real.
* **Análisis Regular de Registros:** Analizar continuamente los registros de red y los datos de tráfico para identificar patrones inusuales o posibles señales de un ataque en curso.

#### **4. Responder**

##### **Riesgos Identificados:**

* **Respuesta Inicial Inadecuada:** La respuesta inicial se retrasó debido a la falta de procedimientos predefinidos para manejar tales ataques.
* **Medidas de Contención Insuficientes:** Acciones inmediatas limitadas para contener y mitigar el ataque.

##### **Recomendaciones:**

* **Desarrollar un Plan de Respuesta a Incidentes:** Crear y actualizar regularmente un plan de respuesta a incidentes para abordar varios tipos de ataques a la red, incluyendo DDoS. Asegurar que el plan incluya procedimientos para contener, mitigar y comunicar sobre el ataque.
* **Establecer Protocolos de Comunicación:** Configurar canales de comunicación claros para informar y gestionar incidentes, tanto interna como externamente.
* **Realizar Revisiones Post-Incidente:** Después de un ataque, realizar una revisión exhaustiva para entender lo que ocurrió, evaluar la efectividad de la respuesta y identificar áreas de mejora.

#### **5. Recuperar**

##### **Riesgos Identificados:**

* **Interrupción del Servicio:** El ataque causó una interrupción significativa, afectando la disponibilidad de servicios críticos de red.
* **Preocupaciones sobre la Integridad de los Datos:** Posibles preocupaciones sobre la integridad de los datos y la disponibilidad del sistema durante y después del ataque.

##### **Recomendaciones:**

* **Restaurar Sistemas y Servicios:** Desarrollar y probar procedimientos para restaurar los servicios y sistemas de red a operaciones normales después de un incidente. Asegurar que las copias de seguridad estén actualizadas y puedan usarse para recuperar datos perdidos o dañados.
* **Revisar y Actualizar Políticas de Seguridad:** Basado en las lecciones aprendidas del incidente, revisar las políticas y procedimientos de seguridad para abordar cualquier brecha identificada y prevenir incidentes similares en el futuro.
* **Mejorar la Resiliencia:** Invertir en medidas de resiliencia de la red, como sistemas redundantes y balanceo de carga, para minimizar el impacto de futuros ataques y asegurar la disponibilidad continua del servicio.

#### **Conclusión:**

El reciente ataque DDoS destacó vulnerabilidades significativas en nuestra postura de seguridad de red. Al aplicar el Marco de Ciberseguridad del NIST, hemos delineado medidas clave para fortalecer nuestras defensas y mitigar amenazas futuras.

#### **Recomendaciones:**

1. **Actualizar y Configurar Regularmente los Firewalls:** Asegurar una protección continua y una adecuada gestión del tráfico.
2. **Mejorar Monitoreo y Detección:** Implementar y mantener sistemas de monitoreo robustos para detectar y responder a amenazas potenciales en tiempo real.
3. **Fortalecer Respuesta a Incidentes y Recuperación:** Desarrollar y probar planes de respuesta a incidentes y procedimientos de recuperación para mejorar la resiliencia general de la red.

Este enfoque estructurado nos ayudará a proteger mejor nuestra red y mejorar nuestras prácticas de ciberseguridad en el futuro.