Informe de Incidente de Ciberseguridad: Ataque de Inundación SYN

1. Resumen del Incidente

- **Tipo de Incidente:**
  Ataque de Denegación de Servicio (DoS) mediante Inundación SYN
- **Descripción del Incidente:**
  El servidor web experimentó errores de tiempo de espera de conexión debido a una gran cantidad de paquetes SYN maliciosos que lo abrumaron. Esto impidió que el servidor procesara el tráfico, provocando errores HTTP 504 (Gateway Timeout) y afectando a los usuarios legítimos que intentaban acceder al sitio.

2. Cronología del Incidente

- **Fecha y Hora del Incidente:**
  17/09/2019
- **Duración del Incidente:**
  El incidente estuvo activo durante varias horas antes de ser identificado y mitigado.

3. Descripción del Ataque: Inundación SYN

Un Ataque de Inundación SYN es un tipo de Denegación de Servicio (DoS) en el que el atacante envía una gran cantidad de paquetes SYN al servidor, sin completar el protocolo de enlace TCP. Esto hace que el servidor dedique recursos a cada conexión incompleta, sobrecargándolo y haciéndolo incapaz de manejar tráfico legítimo.

Detalles del Ataque:

- Inundación SYN Detectada:
  Los registros del servidor revelaron un volumen inusualmente alto de paquetes SYN provenientes de una dirección IP maliciosa: 203.0.113.0, dirigidos al puerto 443 (HTTPS) del servidor web.
- Respuesta del Servidor:
  Inicialmente, el servidor respondió a las solicitudes SYN enviando paquetes SYN-ACK, intentando establecer conexiones legítimas. Sin embargo, el atacante siguió enviando más paquetes SYN sin completar el proceso, sobrecargando al servidor.
- Impacto en el Tráfico Legítimo:
  Los usuarios legítimos que intentaban acceder al sitio web durante el ataque no pudieron establecer conexiones exitosas. Los registros muestran numerosos errores HTTP 504 Gateway Timeout y paquetes [RST, ACK], lo que indica que el servidor no podía completar las conexiones debido a la sobrecarga.

4. Explicación Técnica: Protocolo TCP y Ataque SYN

El ataque se aprovechó del proceso de enlace TCP, que normalmente sigue estos pasos:

1. Solicitud SYN (Synchronize):
   El cliente (visitante del sitio) envía un paquete SYN al servidor, solicitando establecer una conexión.
2. Respuesta SYN-ACK (Synchronize-Acknowledge):
   El servidor responde con un paquete SYN-ACK, confirmando que está listo para establecer la conexión.
3. Confirmación ACK (Acknowledge):
   El cliente responde con un paquete ACK, completando el enlace TCP y estableciendo una conexión completa.

Escenario del Ataque:

Durante un ataque de Inundación SYN, el atacante envía muchas solicitudes SYN pero no completa el proceso. Como resultado:

- El servidor reserva recursos para cada solicitud, pero al no recibir las respuestas ACK, queda saturado.
- Cuando el volumen de solicitudes SYN excede la capacidad del servidor, éste no puede manejar nuevas conexiones legítimas, lo que provoca errores de tiempo de espera.

5. Análisis de Registros y Detección del Ataque

Los registros del servidor proporcionan las siguientes pruebas del ataque:

- Aumento de Paquetes SYN:
  Un volumen inusualmente alto de paquetes SYN provenientes de la IP maliciosa 203.0.113.0, dirigidos al puerto 443 del servidor.
- Errores de Tiempo de Espera:
  Se observó un número significativo de errores HTTP 504 Gateway Timeout, lo que indica que el servidor no pudo procesar las solicitudes de los usuarios debido a la sobrecarga.
- Paquetes TCP RST (Reset):
  Los registros también muestran paquetes [RST, ACK], lo que sugiere que el servidor tuvo que restablecer las conexiones debido a la saturación de los recursos.

6. Evaluación del Impacto

- Sistemas Afectados:
  Servidor Web: Principal objetivo, afectado por la sobrecarga de recursos debido al ataque SYN.
- Impacto en los Usuarios:
  Los visitantes legítimos del sitio web experimentaron errores de tiempo de espera de conexión y no pudieron acceder al sitio. El servidor no pudo gestionar el tráfico legítimo mientras se encontraba abrumado por las solicitudes SYN maliciosas.
- Tiempo de Inactividad:
  El ataque provocó X horas de inactividad en el acceso legítimo antes de ser mitigado.

7. Medidas de Mitigación

Acciones Inmediatas:

1. Bloqueo de la IP Maliciosa:
   Se bloqueó la dirección IP maliciosa 203.0.113.0 en el firewall para detener el tráfico SYN malicioso.
2. Limitación de la Tasa de Conexiones:
   Se aplicaron políticas de limitación de conexiones para restringir la cantidad de paquetes SYN que el servidor puede recibir desde una sola fuente en un período determinado, evitando así la saturación.
3. Activación de SYN Cookies:
   Se activaron SYN cookies en el servidor, una técnica que ayuda a mitigar ataques de inundación SYN al no asignar recursos hasta que se completa el enlace TCP.

Medidas Preventivas Futuras:

- Monitoreo de Tráfico y Alertas:
  Implementar monitoreo en tiempo real del tráfico de red con alertas automáticas cuando se detecten patrones anómalos, como un aumento repentino de paquetes SYN.
- Protección contra Denegación de Servicio (DDoS):
  Desplegar un servicio de protección DDoS para detectar y mitigar ataques de inundación SYN antes de que lleguen a la infraestructura del servidor.
- Endurecimiento del Servidor:
  Aplicar técnicas de endurecimiento del servidor, como limitar el número de conexiones simultáneas y reducir el tiempo de espera de las conexiones TCP, para minimizar el impacto de la saturación de recursos.

8. Lecciones Aprendidas

- Monitoreo Proactivo:
  Un monitoreo continuo del tráfico de red podría haber permitido la detección más temprana del ataque, reduciendo el tiempo de inactividad.
- Políticas de Limitación de Tasa:
  La implementación de políticas de limitación de conexiones es esencial para evitar que futuros ataques SYN inunden el servidor.

9. Plan de Acción

1. Investigación Adicional:
   Continuar la investigación para identificar posibles otros vectores de ataque y analizar el origen del tráfico malicioso.
2. Implementación de Medidas de Seguridad Avanzadas:
   Desplegar medidas como SYN cookies, protección DDoS y limitación de la tasa de conexiones para mitigar ataques de inundación SYN de forma continua.
3. Monitoreo Continuo y Respuesta Rápida:
   Establecer un sistema de monitoreo y respuesta ante incidentes en tiempo real, utilizando herramientas avanzadas de análisis de tráfico y firewalls con detección de intrusiones.