### **Security incident: network attack Analysis Report**

#### **Problem Summary**

The identified problem is a SYN flood attack, a type of denial of service (DoS) attack. This attack floods the company's web server with a large number of TCP SYN requests, preventing the server from adequately responding to legitimate user requests.

#### **Incident Analysis**

**Name of Attack:** SYN Flood Attack

**Affected Network Protocol:** The affected protocol is TCP (Transmission Control Protocol).

**Description of the Attack:** The SYN flood attack negatively impacts network performance by sending a large number of SYN requests to the server, overwhelming it and consuming its resources. The server attempts to respond to each SYN request with a SYN-ACK packet, but without receiving the final ACK response back, it remains waiting, which consumes memory and processing resources. This excessive volume of requests prevents the server from handling legitimate requests, resulting in timeouts and connection errors for users.

**Description of Captured Traffic:** Using a packet sniffer, a high volume of TCP SYN requests from an unknown IP address was observed. This suggests that the server is under attack by a malicious actor attempting to overwhelm the system with a SYN flood attack.

**Impact of the Attack:** The web server was losing its ability to respond to legitimate requests due to the incoming traffic volume, resulting in connection timeout errors in users' browsers. This issue affected both company employees and customers, preventing them from accessing the sales page.

#### **Response and Mitigation**

**Time of Incident:** The incident was detected in the afternoon through an automated alert from the monitoring system.

#### **Captured Traffic Log**

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150

**Detection and Initial Response:**

1. **Detection:** An automated alert from the monitoring system indicated a problem with the web server.
2. **Investigation:** Using a packet sniffer, a large number of TCP SYN requests from an unknown IP address were identified.
3. **Immediate Action:** The server was temporarily disconnected to allow it to recover and return to a normal operating state.
4. **Temporary Mitigation:** The company's firewall was configured to block the IP address sending the SYN requests.

**Key Findings:**

* **Affected Protocol:** TCP
* **Type of Attack:** SYN flood
* **Attacker's IP:** A specific IP address was identified sending the malicious traffic.
* **Impact:** Disruption of access to the web server, affecting employees and customers.

**Likely Cause:** The most likely cause of the incident is a SYN flood attack by a malicious actor attempting to overwhelm the web server with an excessive volume of SYN requests.

### **Conclusion and Recommendations**

#### **Conclusion:**

The company's web server was the victim of a SYN flood attack, a type of denial of service attack. This attack flooded the server with a large number of TCP SYN requests, preventing the server from responding to legitimate requests. This incident highlights the importance of having robust security measures and incident response protocols in place to mitigate the impact of such attacks.

#### **Recommendations:**

1. **Implement Additional Protection Measures:** Configure protection mechanisms such as dynamic blacklists, intrusion detection and prevention systems (IDS/IPS), and next-generation firewalls (NGFW).
2. **Review and Update Security Policies:** Ensure that security policies are up to date and include specific measures to mitigate SYN flood attacks.
3. **Continuous Monitoring:** Continue to monitor network traffic in real-time to detect and respond quickly to any suspicious activity.
4. **Training and Awareness:** Provide ongoing training to employees about cybersecurity and raise awareness of the types of attacks and how they can affect the company.

### **Incidente de seguridad: ataque a la red Informe de análisis (spanish)**

#### **Resumen del Problema**

El problema identificado es un ataque de inundación SYN, que es un tipo de ataque de denegación de servicio (DoS). Este ataque está inundando el servidor web de la empresa con un gran número de solicitudes TCP SYN, impidiendo que el servidor pueda responder adecuadamente a las solicitudes legítimas de los usuarios.

#### **Análisis del Incidente**

**Nombre del Ataque:** Ataque de inundación SYN (SYN flood attack).

**Protocolo de Red Afectado:** El protocolo afectado es TCP (Protocolo de Control de Transmisión).

**Descripción del Ataque:** El ataque de inundación SYN afecta negativamente al rendimiento de la red al enviar una gran cantidad de solicitudes SYN al servidor, abrumándolo y consumiendo sus recursos. El servidor intenta responder a cada solicitud SYN con un paquete SYN-ACK, pero al no recibir la respuesta final (ACK) de vuelta, queda esperando, lo que consume memoria y recursos de procesamiento. Este volumen excesivo de solicitudes provoca que el servidor no pueda manejar solicitudes legítimas, resultando en tiempos de espera y errores de conexión para los usuarios.

**Descripción del Tráfico Capturado:** Utilizando un detector de paquetes, se observó un gran volumen de solicitudes TCP SYN procedentes de una dirección IP desconocida. Esto sugiere que el servidor está siendo atacado por un actor malicioso que intenta abrumar el sistema con un ataque de inundación SYN.

**Impacto del Ataque:** El servidor web estaba perdiendo su capacidad para responder a las solicitudes legítimas debido al volumen de tráfico entrante, lo que provocó un tiempo de espera de conexión en los navegadores de los usuarios. Este problema afectó tanto a los empleados de la empresa como a los clientes, impidiéndoles acceder a la página de ventas.

#### **Respuesta y Mitigación**

**Hora del Incidente:** El incidente fue detectado en la tarde, a través de una alerta automatizada del sistema de monitoreo.

#### **Registro de Tráfico Capturado**

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150

**Detección y Respuesta Inicial:**

1. **Detección:** Se recibió una alerta automatizada del sistema de monitoreo indicando un problema con el servidor web.
2. **Investigación:** Utilizando un detector de paquetes, se identificó un gran número de solicitudes TCP SYN procedentes de una dirección IP desconocida.
3. **Acción Inmediata:** Se desconectó temporalmente el servidor para que el equipo pudiera recuperarse y volver a un estado de funcionamiento normal.
4. **Mitigación Temporal:** Se configuró el firewall de la empresa para bloquear la dirección IP que estaba enviando las solicitudes SYN.

**Hallazgos Clave:**

* **Protocolo Afectado:** TCP.
* **Tipo de Ataque:** Inundación SYN.
* **IP Atacante:** Se identificó una dirección IP específica que estaba enviando el tráfico malicioso.
* **Impacto:** Interrupción del acceso al servidor web, afectando a empleados y clientes.

**Causa Probable:** La causa más probable del incidente es un ataque de inundación SYN por parte de un actor malicioso que intenta abrumar el servidor web con un volumen excesivo de solicitudes SYN.

### **Conclusión y Recomendaciones**

#### **Conclusión:**

El servidor web de la empresa fue víctima de un ataque de inundación SYN, que es un tipo de ataque de denegación de servicio. Este ataque inundó el servidor con un gran número de solicitudes TCP SYN, impidiendo que el servidor pudiera responder a las solicitudes legítimas. Este incidente resalta la importancia de tener medidas de seguridad robustas y protocolos de respuesta a incidentes en lugar para mitigar el impacto de tales ataques.

#### **Recomendaciones:**

1. **Implementar Medidas de Protección Adicionales:** Configurar mecanismos de protección como listas negras dinámicas, sistemas de detección y prevención de intrusiones (IDS/IPS) y firewalls de última generación (NGFW).
2. **Revisar y Actualizar Políticas de Seguridad:** Asegurarse de que las políticas de seguridad estén actualizadas y que incluyan medidas específicas para mitigar ataques de inundación SYN.
3. **Monitoreo Continuo:** Continuar monitoreando el tráfico de red en tiempo real para detectar y responder rápidamente a cualquier actividad sospechosa.
4. **Capacitación y Concienciación:** Proporcionar capacitación continua a los empleados sobre ciberseguridad y concienciarlos sobre los tipos de ataques y cómo pueden afectar a la empresa.