Soluciones para protección frente a ataques DoS.

Implementación para el Ministerio de Defensa y posible evolución.

Autor: Rodríguez Ortega, Juan José

Director/es: Zamorano Pinal, Carlos y Álvarez Sabucedo, Luis.

Contacto: jrodort@fn.mde.es / juanjo1972ad@gmail.com

Resumen:

El objetivo del trabajo es proporcionar un acercamiento a los ataques tipo Denegación de Servicios comúnmente conocidos por su acrónimo de inglés Denial of Services DoS, como podemos protegernos frente a ellos y cuál es el Estado del Arte actualmente en cuanto a medidas de protección existentes.

A través de la TAXONOMIA de referencia desarrollada por el CCN, se introduce en los diferentes tipos de que ataque DoS/DDoS que podemos encontrarnos, lo que nos ayudará a entender mejor las distintas formas en las que se puede producir un ataque de denegación de servicios y como protegernos frente a estas amenazas.

Se realizará un recorrido por el Estado del Arte, en cuanto a medios y medidas de protección frente a estos ataques disponibles en el mercado actual, así como las herramientas que el CCN-CERT pone a disposición de las AA.PP. y empresas que quieren cumplir con los estándares del ENS.

Dar una visión de la estrategia que emplea en Ministerio de Defensa (MINISDEF) para hacer frente a ataques del tipo DoS. Solución implementada en ámbito del MINISDEF para defenderse de estos ataques, que mecanismos y procedimientos operativos se emplean en el MINISDEF a día de hoy para luchar contra ellos.

Para finalizar se detallarán las conclusiones a que nos ha llevado este trabajo en lo referente a protección frente a DoS y específicamente en el ámbito del Ministerio de Defensa.

Palabras clave: DoS, DDoS, denegación de servicios, ataque, tráfico legítimo, spoofing, flood.

1. Introducción

1.1. Introducción

Existe múltiples tipos de amenaza en el ciberespacio, algunas de ellas van encaminadas al robo de información, otras a la escalada de privilegios para sabotear un sistema o tomar su control, otras van dirigidas a la destrucción de la información o los sistemas de información, etc.

La denegación de servicios más conocida por sus siglas en inglés DoS (Denial of Services), es un tipo de ataque dirigido a la fuente de la información o al canal de transmisión, impidiendo el acceso a un recurso informático por parte de los usuarios legitimados para el acceso al sistema o la información que en él se almacena, la navegación web, realizar operaciones de banca, uso del correo electrónico, etc.

Cuando estos ataques en lugar de realizarse desde una única fuente se realizan desde múltiples fuentes en la misma o diferentes ubicaciones, nos estamos refiriendo entonces a ataques del tipo DDoS (Distributed Denial of Services) mucho más perjudiciales y peligrosos que los primeros, si bien el objetivo de estos sigue siendo el mismo, la interrupción de un servicio o lo que es lo mismo la denegación de este a los usuarios.

1.2. Atacantes potenciales o actores relacionados con los ciber ataques.

Las Tecnologías de la Información han dado entrada a nuevas actividades y formas de negocio. De igual manera que el ciberespacio ha representado una oportunidad de expansión para la sociedad digital, también puede ser explotado con fines malintencionados o delictivos, debido a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación [1].

Como en cualquier otro tipo de ciber ataques, en los DoS/DDoS podemos encontrarnos con múltiples agentes de muy diversa índole y con motivaciones de todo tipo [2]. En muchos casos la peligrosidad de estos agentes estará en función de los recursos a su disposición, lo podemos clasificarlos de la siguiente manera:

- Estados,
- Grupos Terroristas,
- Organizaciones Criminales,
- Hackativistas,
- Ciberdelincuentes e
- Insider.

1.3. Taxonomía de ataques de Denegación de Servicio propuesta por el CCN [3].

El Centro Criptológico Nacional (CCN) propone en su guía sobre la seguridad de las Tecnologías de la Información número 820 (CCN-STIC-820) una TAXONOMÍA genérica, que se ha adoptado en el ámbito del Ministerio de Defensa para clasificar y analizar las características de los ataques DoS.

Afrontar de forma eficaz un ataque de Denegación de Servicio ya sea distribuido o no, requiere entender sus características el ***objetivo***, su ***origen***, el ***impacto*** que genera, su método de ***propagación***, las ***vulnerabilidades que explota***, etc. Los ataques DoS pueden afectar a diferentes capas del modelo de referencia OSI y hacerlo de formas diversas.

1.4. Categorías de ataques DoS.

Como norma general y para poder facilitar la categorización de los distintos tipos de ataques DoS, podemos distinguir entre tres tipos distintos de categoría de ataque DoS.

1) **Volumétricos** o por inundación [4], que tienen como objetivo principal el consumo del ancho de banda de la víctima.
2) **Ataques reflexivos (DrDoS)** [5] representa un 20% del total de los casos de DDoS, se enfoca a debilidades en las capas de *red* (capa 3) y de *transporte* (capa 4) del modelo OSI. El ataque explota el proceso de protocolo de enlace o *handshake* del Protocolo de Control de Transmisión (TCP).
3) **Agotamiento de recursos** el atacante se dirige contra los recursos de un sistema, genera tráfico fragmentado o mal formado, peticiones invalidas o sin sentido, el servidor intenta resolver todas estas peticiones inútilmente.

1.5. Métodos más comunes para ejecutar un DoS.

Algunos de los métodos más comúnmente empleados para desarrollar ataques de Denegación de Servicios son [6]:

1) **Ping de la muerte** [7]**.** El Ping de la Muerte o "Ping of Death" se hizo famoso en la década de los 90, cuando un ataque a base de paquetes ICMP pesados conseguía bloquear el Sistema. El atacante crea un paquete ICMP que supera el tamaño máximo permitido para estos paquetes de datos.
2) **ICMP Flood.** También conocido como Ping Flood, es un tipo de ataque en el que se intenta sobrecargar a la víctima con paquetes de peticiones de echo ICMP, provocando que el objetivo se vuelva inaccesible para el tráfico licito [4].
3) **Smurf** [8]**.** El atacante realiza peticiones ping (echo-request) a una o más redes de dispositivos, falsificando la dirección IP de la víctima (IP spoofing) los dispositivos que han recibido la solicitud de ping envían sus respuestas a la dirección IP de la víctima, amplificando el tráfico inicial del ataque.
4) **Buffer overflow** [9]**.** Este tipo de ataque consiste en enviar una cantidad de tráfico a los recursos de una red que exceda la capacidad por defecto de procesamiento del Sistema, cargando el búfer con más datos de los que puede contener.
5) **Ataque de fragmentación de paquetes IP** [10]**.** Es un tipo de ataque en el que la víctima recibe un flujo de fragmentos de tamaño pequeño sin que ninguno de ellos tenga desplazamiento de cero, el objetivo podría colapsar al intentar reconstruir el datagrama a partir de los paquetes recibidos. Se pueden mitigar de diferentes formas, siendo en la mayoría de los casos, el asegurar que los paquetes maliciosos no lleguen nunca a su objetivo.
6) **Ataques de Amplificación** [11]**.** En ellos se utiliza un factor de amplificación para aumentar el efecto del ataque cuando este se ejecuta con un número limitado de recursos. El DNS (Domain Name Service) Amplificaton attack es el más común de estos ataques.
7) **SYN attack** [4]**.** Es un ataque DDoS que explota parte del proceso denominado *conexión en tres pasos* el protocolo TCP para consumir recurso en la maquina objetivo con el fin de dejarla fuera de servicio.
8) **UDP Flood** [12]**.** Es un tipo de denegación de servicio que explota el *User Datagram Protocol (UDP)* enviando un elevado número de estos paquetes a la víctima con la intención de saturar la capacidad de proceso y respuesta de ésta.
9) **HTTP Flood** [4]**.** Este ataque está diseñado para que la víctima destine el mayor número de recursos posible para hacer frente a las solicitudes que recibe, el atacante intenta saturar

al objetivo con una inundación de cuantas más solicitudes de procesado intensivo como le sea posible.

10) **Mac Flood** [13]**.** A diferencia de otros ataques, el MAC flood no va dirigido contra host u otras máquinas que alojan distintos servicios, en su lugar va dirigido a comprometer la seguridad de los dispositivos de conmutación de red (switch).
11) **Slowloris** [4]**.** Este tipo de ataque utiliza solicitudes HTTP parciales para abrir una conexión con un servidor web y mantenerla abierta tanto tiempo como le sea posible con el fin de sobrecargar y ralentizar a la maquina objetivo.
12) **NTP Amplification** [12]. Se basa en un ataque volumétrico de reflexión, el atacante aprovecha el protocolo de tiempo *Network Time Protocol (NTP)* para desbordar a la víctima con una cantidad amplificada de tráfico UDP, lo que hace que el objetivo y su infraestructura circundante quede inaccesible al tráfico legítimo.
13) **Zero-day DDoS Attack** [14]**.** Generalmente el termino Zero-day hace referencia a ataques que explotan una nueva vulnerabilidad del software de la cual no la comunidad no tiene conocimientos aún. Puede pasar mucho tiempo desde que un atacante detecta este tipo de vulnerabilidades hasta que la comunidad la descubre y lanza una actualización para solucionar la vulnerabilidad.

1.6. Mirai, la red Zombie.

En octubre de 2016 tuvo lugar un ciberataque contra Dyn, compañía estadounidense dedicada a soluciones DNS en direcciones IP dinámicas en Internet.

Se trato de un DDoS que colapso los servicios de Dyn, fue un ataque masivo a la infraestructura básica de internet ejecutado por millones de dispositivos del Internet de la Cosas (IoT).

Mirai es un malware de la familia de los botnets, destinado a infectar equipos del IoT, el objeto principal de este malware es la infección de routers y cámaras IP. Se cree que Mirai ha sido empleada para atacar a la web Krebs on Security y la francesa OVH cloud-computing service además de Dyn [15].

Mirai afecto a millones de usuarios, por más de dos horas provocó la imposibilidad de acceder a recursos de Internet tales como Twitter, CNN, ediciones digitales de periódicos de tirada nacional, Amazon, Reddit, Tumblr, PayPal, etc.

2. Desarrollo

A la hora de tomar medidas preventivas a los DoS/DDoS debemos tener en cuenta los distintos vectores que un atacante puede aprovechar para lanzar su ataque, quizás el primer vector que debemos contemplar al implementar las distintas capas de seguridad es nuestra infraestructura de red que nos dan conectividad hacia el exterior, otro vector lo conforman las infraestructuras que componen nuestra red interna (routers, switches y servidores) y un tercer vector lo componen nuestras aplicaciones web.

El CCN ofrece a la AGE y a las empresas que quieran cumplir con el ENS una soluciones, con el fin de incrementar el grado de protección de estos organismos y su eficacia en la respuesta y mitigación de incidentes de seguridad. Podemos encontrar, desde la el Sistema de Alerta Temprana de la red SARA, a herramientas de seguridad del tipo de LUCIA (gestión de incidentes de seguridad tipo RT-IR), o INES (para verificar el grado de cumplimiento de las organizaciones del ENS)

Existen en el mercado multitud de empresas y dispositivos dedicados a la protección anti-DoS, sus productos y soluciones están específicamente diseñadas para la prevención y mitigación de estos ataques.

2.1. Imperva [16].

Es una empresa de servicios y software de ciberseguridad, que ofrece protección a los datos y al software de aplicaciones de multitud de empresas y organizaciones gubernamentales. Por lo tanto, podemos encasillar a Imperva dentro del grupo de Proveedores de Servicios de Seguridad. Imperva es líder mundial entre los proveedores de soluciones DDoS según informe de Forrester Research.

Imperva ofrece soluciones de protección contra ataques DDoS para sitios web, redes, servidores de aplicaciones, DNS e IPs individuales. Entre sus éxitos Imperva ha mitigado el ataque más grande producido hasta el momento, de forma inmediata y sin incurrir apenas en aumento de la latencia ni interfiriendo en el tráfico de usuarios legítimos. Las soluciones Imperva están diseñadas para encontrar las necesidades específicas del cliente, las opciones ofrecidas se ajustan a los clientes.

2.2. Netscout Arbor [10].

A diferencia de Imperva, Netscout Arbor, está centrada principalmente a la venta de soluciones de seguridad hardware y/o software, pero no proporciona servicios de protección contra incidentes.

La solución propuesta por Arbor, se basa en la inteligencia obtenida mediante el escaneo de la red del cliente y en la detección de anomalías en a la gestión de amenazas de primera categoría, detectando así un posible agotamiento volumétrico, de estado de las conexiones TCP y por último a nivel de aplicación. Adicionalmente, Arbor dispone de ATLAS, una red global de inteligencia que nutre las bases de datos de Arbor Network en beneficio directo de sus productos de protección.

2.3. Neustar [17].

Neustar tiene una solución contra DDoS capaz de mitigar ataques que superen los 12 Tbps a través de una de las redes de depuración de datos más grandes del mundo.

Las soluciones Neustar ofrecen a sus clientes servicios 24/7, protección en las capas 3 a 7 del modelo OSI. Implantación sin necesidad de despliegue de hardware o software en las redes del cliente, años de experiencia en el sector.

2.4. ELK Stack [18].

Uso de Machine Learning asociado a la seguridad frente a DoS/DDoS, integrando plataformas como ELK Stack.

El plugging de Machine Learning del ELK, nos sirve para identificar patrones y ver anomalías en estos patrones, podemos ejecutar este plugging en nuestro sistema, para que aprenda cual es el funcionamiento normal del mismo a lo largo un periodo de tiempo, por ejemplo, así podrá distinguir cual es el volumen de tráfico, los eventos generados, las llamadas a los servicios que desplegamos, etc.

3. Resultados y discusión

En el tratamiento de un incidente DoS se establen típicamente tres fases (*DETECCIÓN, AUTORIZACIÓN y MITIGACIÓN*). En CESTIC la gestión de un incidente DoS corresponde a la subunidad de Internet de la Unidad de Redes de la División de Operaciones (DIVOPER) y la operadora adjudicataria del contrato de servicios del Nodo de Interconexión.

El MINISDEF identifica como activos críticos a proteger frente a amenazas DoS *Servicios* y *Redes*, estableciendo unas prioridades en cuanto al nivel de protección.

CESTIC adopta una serie de medidas preventivas agrupada en tres aspectos diferenciados (Organización, Técnicos y Monitorización y Control) para luchar contra los ataques DoS.

La mitigación de los ataques DoS, se realiza activamente a través de las medidas reactivas y dentro del marco del contrato vigente con el operador de servicios, se solicita la provisión de un servicio de mitigación contra ataques DoS que incluye la inspección de todo el tráfico cursado por las líneas de acceso a Internet conectadas al MINISDEF en los centros principales y de respaldo.

Este servicio permite configurar una serie de alertas para que detecten la existencia de un ataque y dependiendo del tipo, iniciar de manera automática determinadas contramedidas. Es lo que se conoce como ***auto-mitigación***.

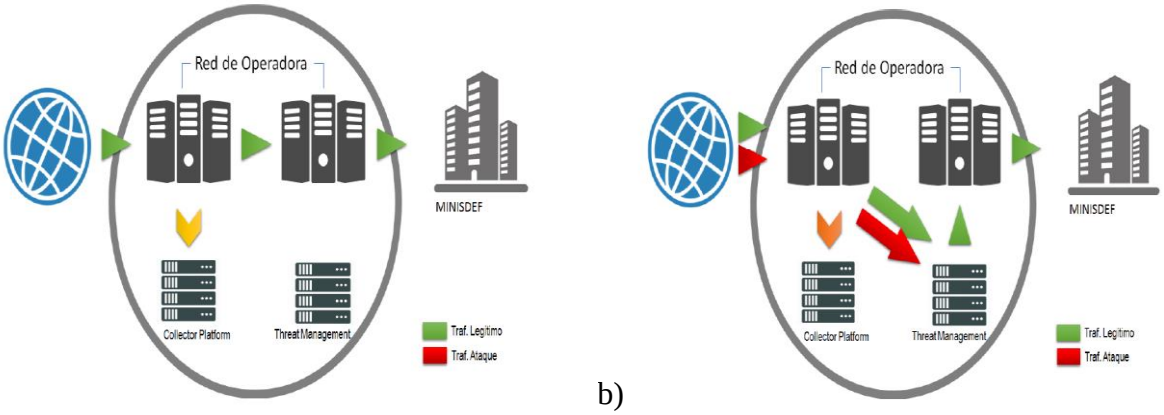

Figura 1. a) Tráfico normal. b) Tráfico mitigado.

Se define la siguiente operativa asociada frente a un ataque DoS:

- El Sistema Autónomo envía un resumen de 1/2000 paquetes del tráfico a la sonda colectora que monitoriza el servicio, este envío se realiza por SNMP.

- El servicio, comprueba si se está rebasando el consumo de ancho de banda habitual, más un tanto por ciento acordado (en previsión de noticias, campañas o actividades que puedan exceder el consumo habitual).

- Superado los valores establecidos, si este consumo anómalo se mantiene durante un tiempo preestablecido, se generan las alertas.

- Cada alerta generará automáticamente una notificación a los equipos de operación tanto en el C-SOC de la Operadora, como al equipo que da soporte en las instalaciones del Ministerio.

- Tras la alerta, ambos equipos de operación realizan un seguimiento de la alerta, pendientes de su evolución.

- Si el evento llega al umbral de ALARMA:

  - La Operadora modificará el protocolo de routing (BGP) para hacer pasar el tráfico por las herramientas anti-DoS.
  - El TMS se intercalará entre el Sistema Autónomo de la Operadora y el Sistema Autónomo del MINISDEF.
  - Se ejecutan las contramedidas automáticas acordadas.
  - Se registra una incidencia en el sistema ITSM SCAN.

- Si la automitigación no da resultado, lo operadores del C-SOC solicitan autorización a los responsables del MINISDEF, la ejecución de contramedidas adicionales (estas medidas pueden afectar al tráfico legítimo, con la consiguiente pérdida de información).

- Finalizado el ataque, se restablece el servicio.

4. Conclusiones

El Ministerio de Defensa ha optado por una solución hibrida en cuanto a la defensa y prevención de ataques del tipo DoS/DDoS, dividiendo la carga de la gestión frente a este tipo de incidentes entre las responsabilidades del ISP, mediante la adecuada contratación del servicio y el establecimiento de un SLA, que permita o garantice la continuidad del servicio del MINISDEF a sus usuarios aun estando siendo objeto de un ataque de Denegación de Servicios, y los equipos de defensa interna gestionados por el grupo de explotación de seguridad del CESTIC a través de la implementación de FIREWALL, IDS, IPS y configuraciones seguras en los distintos servicios que se han identificado como críticos.

La configuración adecuada de firewall, IDS, IPS y el establecimiento de mailguard que limiten o filtren el tráfico de correos recibidos y enviados, así como la limitación en el número de destinatarios posibles o limitar el número de direcciones de correo que puedan formar parte de una lista de distribución, limitar las conexiones a los servicios web tanto en el número como en el tiempo que se pueden mantener activas, etc., son medidas que deben implementarse por parte del MINISDEF.

La evolución de los sistemas de defensa contra DoS/DDoS pasa actualmente por un incremento en el desarrollo de técnicas de **IA** y ***MACHINE LEARNING*** en los distintos dispositivos empleados para la prevención de estos incidentes.

Agradecimientos

A mi esposa Alejandra y a mis hijas Rocío, Emma y Sofía, por apoyarme y aguantar mis malos ratos y padecer el tiempo que les he hurtado con alegría y buenas caras.

Sin vuestro cariño y apoyo no habría podido terminar este trabajo.

Referencias

[1] Estrategía de Seguridad Nacional 2017.

[2] Estrategía Nacional de Ciberseguriad 2019.

[3] Guía sobre la Seguridad de las Tecnologías de la Información número 820 (CCN-STIC-820).

[4] «Wikipedia,» [En línea]. Available: https://en.wikipedia.org/wiki/.

[5] «unaaldia.hispasec.com,» [En línea]. Available: https://unaaldia.hispasec.com/2018/03/hablemos-de-drdos.html.

[6] «Openwebinars.Net,» [En línea]. Available: https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/.

[7] «Informática para tu negocio.,» [En línea]. Available: https://www.informaticaparatunegocio.com/blog/significa-ping-funciona/.

[8] «Kaspersky,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack.

[9] «OWASP.ORG,» [En línea]. Available: https://owasp.org/www-community/attacks/Buffer_overflow_attack.

[10] «NETSCOUT,» [En línea]. Available: https://www.netscout.com/what-is-ddos/ip-icmp-fragmentation.

[11] «Centro de Gestión de Incidentes Informáticos,» [En línea]. Available: https://www.cgii.gob.bo/es/publicaciones/ataque-de-amplificacion-de-servidor-de-nombre-de-dominio-dns-recursivo.

[12] «Cloudflare,» [En línea]. Available: https://www.cloudflare.com/.

[13] «Interserver.Net,» [En línea]. Available: https://www.interserver.net/tips/kb/mac-flooding-prevent/.

[14] «INCIBE,» [En línea]. Available: https://www.incibe.es.

[15] «McAfee Labs Threats Report 2017».

[16] «Imperva,» [En línea]. Available: https://www.imperva.com/.

[17] «Neustar,» [En línea]. Available: https://www.home.neustar/.

[18] «Elastic,» [En línea]. Available: https://www.elastic.co/.