TALLER APLICADO DE SEGURIDAD DE LA INFORMACIÓN

Máquinas virtuales

Unidad 2

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Eder Moran Heredia

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar: Alex Flores Fuentealba

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

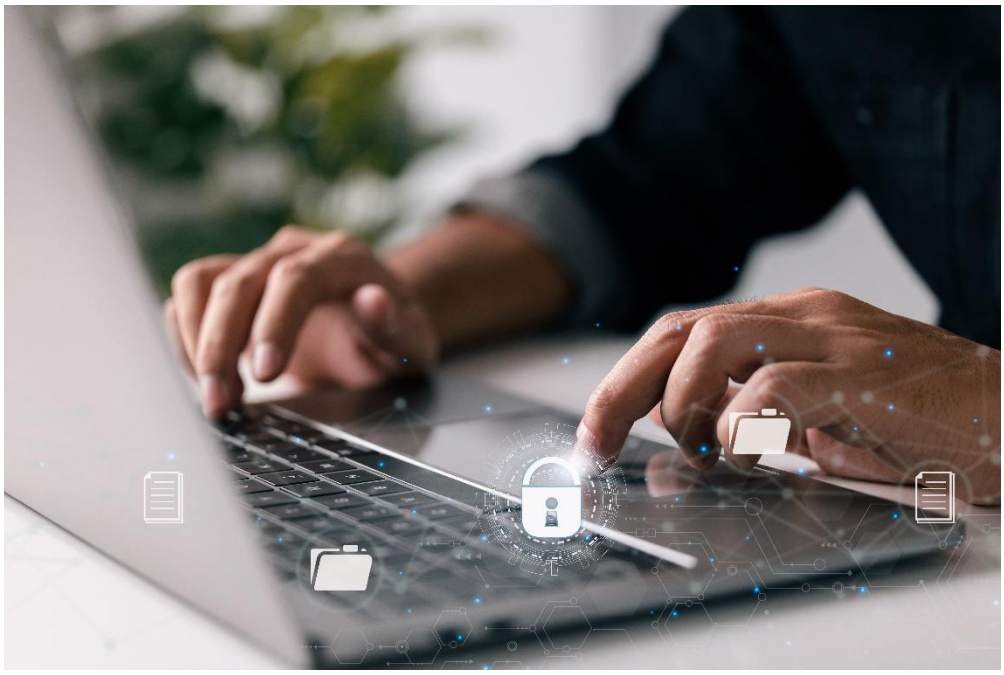
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Utilizan técnicas de DoS/DDoS, considerando Ethical Hacking y requerimientos actuales de la industria.



Introducción

En septiembre de 2017 ocurrió el mayor ataque DDoS de la historia. Implicó 2,54 Tbps y fue dirigido a los servicios de Google. Google Cloud informó de este ataque en octubre de 2020.

Se logró mediante el envío de paquetes falsificados a 180.000 servidores web, que respondieron a Google. Los atacantes habían dirigido varios ataques DDoS a la infraestructura de Google en los seis meses anteriores al incidente por lo que no fue un hecho aislado.

En febrero de 2020 AWS informó de que había mitigado un ataque DDoS masivo. En un momento, el ataque generó 2,3 terabits por segundo (Tbps). AWS no quiso revelar a quien iba dirigido el ataque.

Esta vez se utilizó servidores web que fueron pirateados con protocolo ligero de acceso a directorios sin conexión (CLDAP). El CLDAP es un protocolo enfocado a directorios de usuarios. Como alternativa existe el LDAP, una versión anterior del protocolo. El CLDAP últimamente ha sido ocupado en varios ataques DDoS.

De la experiencia comentada, es importante que en esta semana podamos estudiar los conceptos relacionados a los ataques DDoS y sus técnicas.

1. Conceptos de DoS/ DDoS

Existen dos técnicas conocidas para realizar ataques de Ethical hacking, DoS o ataque de denegación de servicio (por sus siglas en inglés, Denial of Service) y por otro lado DDos o ataque distribuido de denegación de servicio (por sus siglas en inglés, Distributed Denial of Service).

1.1 Ataque DoS o denegación de servicios

Ésta técnica se utiliza para inhabilitar la utilización de un sistema, un computador o una aplicación, afectando a cualquiera de las instancias de comunicación, desde el origen de la información hasta la red informática de donde proviene. Se caracteriza por efectuarse los ataques desde una máquina o dirección IP.

1.2 Ataque DoS o denegación de servicios distribuido

Esta técnica se utiliza para inhabilitar la utilización de un sistema, un computador o una aplicación, afectando a cualquiera de las instancias de comunicación, desde el origen de la información hasta la red informática de donde proviene. Se caracteriza por efectuarse los ataques desde grandes cantidades de máquinas o direcciones IP.

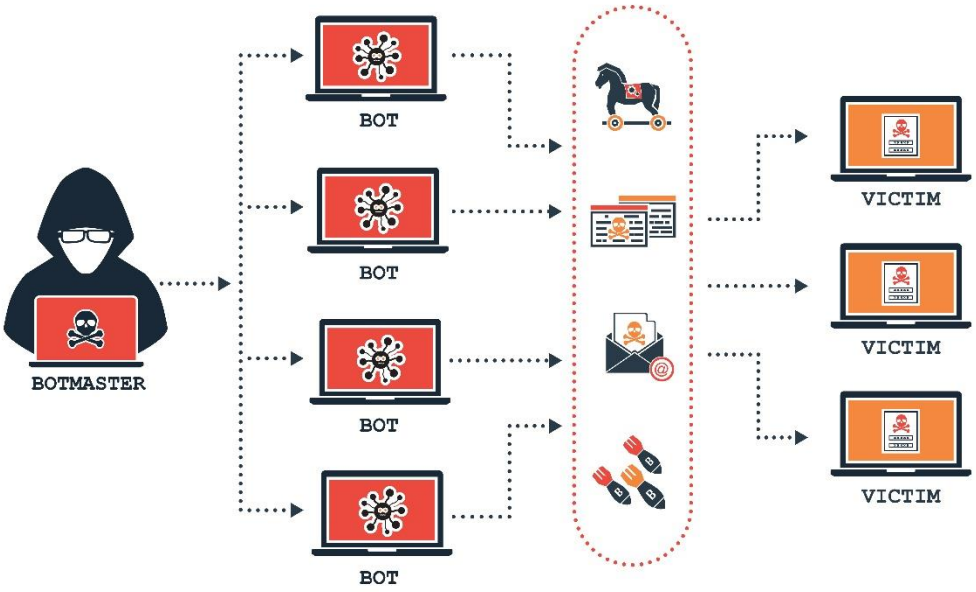


Figura 1. Ataque DoS

Fuente: Osi.es (2018)

2. Técnicas de ataques de DoS DDoS

Como vimos anteriormente, los ataques de denegación de servicio (DoS) y denegación de servicio distribuido (DDoS) acciones maliciosas de que buscan interrumpir las operaciones normales de un servidor, un servicio o simplemente una red objetivo a través de una saturación de tráfico de Internet. Pueden ser ataques sin gran sofisticación desde un solo equipo, tales como enviar al servidor objetivo gran más solicitudes

de ICMP (ping) de las que puede procesar y controlar, lo que produce una baja del servicio.

Los ataques DDoS, en cambio, utilizan más de un equipo para enviar lograr el objetivo. Por lo general, esos equipos forman parte de una red de bots (botnet), y como su nombre lo dice es un conjunto de dispositivos u ordenadores que han sido infectados con malware y que, por lo mismo, pueden ser controlados a distancia por un atacante particular.

Los ataques DDoS son mucho más dañinos y frecuentes en la actualidad por dos razones: Existen nuevas herramientas de seguridad que han idi evolucionando para detener ciertos ataques DoS habituales. En cambio, las herramientas de ataque DDoS son relativamente baratas y fáciles de usar.

2.1 Vectores de ataques básicos DoS/DDoS

Hay una gran diversidad de herramientas que pueden adaptarse para realizar ataques DoS/DDoS o que simplemente fueron diseñadas para ese fin. Las que fueron diseñadas se conocen como "agentes estresantes", es decir, tienen como fin ayudar a los ingenieros de redes e investigadores de seguridad a realizar pruebas de estrés aplicadas en sus propias redes, pero que también pueden ser utilizadas para realizar ataques reales.

Existen herramientas de ataque especializadas y solo se centran en una capa del modelo OSI. Existen otras que permiten múltiples vectores de ataque. Estas herramientas incluyen:

Herramientas para ataques lentos que consumen poco ancho de banda

Así como indica su nombre, estas herramientas de ataque se valen de un bajo volumen de datos y operan muy lentamente. Funcionan enviando cantidades pequeñas de datos a través de múltiples conexiones, así se puede mantener abiertos los puertos del objetivo todo el tiempo posible. Adicionalmente, continúan usando recursos del servidor hasta que logran impedir que pueda establecer y mantener otras conexiones. Para ser más específicos, estos ataques pueden ser efectivos incluso cuando no se esté utilizando una botnet, con frecuencia se realizan con un solo equipo.

Herramientas para ataques contra la capa de aplicación (capa 7)

En la capa 7 del modelo OSI, se realizan solicitudes que se basan en Internet como el HTTP. Esto se logra por un ataque de inundación HTTP para saturar al servidor atacado con solicitudes del tipo HTTP GET y POST, en este ataque de tráfico es difícil distinguir entre las solicitudes maliciosas de las solicitudes normales.

Herramientas para ataques a las capas de protocolo y transporte (capas 3/4)

Aquí comúnmente se usan protocolos UDP para enviar gran volumen de tráfico a un servidor, por ejemplo, durante una inundación UDP. Por lo general estos ataques no son efectivos si se hacen de forma individual, por lo que realizan como ataques DDoS, de esta forma su efecto aumenta cuantos más equipos se encuentren atacando.

Herramientas DoS/DDoS

Mencionaremos las herramientas más utlizadas:

LOIC: Abreviación del término "Low Orbit Ion Cannon**".** Es una herramienta fácil de utilizar por principiantes para el envío de solicitudes UDP, TCP y HTTPS a un servidor blanco.

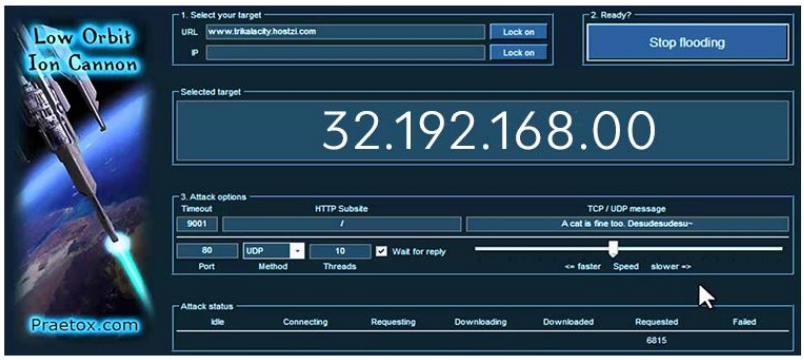


Figura 2. LOIC

Fuente: Wallarm.com (s.f)

HULK: abreviatura de "HTTP Unbearable Load King", fue diseñada para investigación, y por lo mismo es frecuentemente elegida por delincuentes informáticos utiliza el protocolo HTTP, y evita el paso por el motor de caché y así genera tráfico fantasma.

Tor's Hammer: "El martillo de Tor" es una herramienta de trafico bajo para realizar ataques DDoS, esto se logra activando conexiones muertas a través de la 7ma capa del modelo OSI, y así la red se confunde

mostrando resultados. Se considera una herramienta poco eficaz al funcionar con tráfico lento.

RUDY: abreviatura de la frase en inglés ¿"R.U. Dead Yet"? (¿áun no te mueres?). Reemplaza encabezados HTTP por HTTP POST. Así logra llenar la red con ataques coordinados de DoS.

HOIC: Acrónimo de "High Orbit Ion Cannon". Es una versión superior de LOIC y se usa para ataques más voluminosos, refinados e intensos. Funciona mandando una infinidad de paquetes HTTP POST y HTTP GET al servidor objetivo. Este tipo de ataques es muy difícil de detectar y bloquear, por eso es el mecanismo favorito de Anonymous para ataques DDoS.

2.2 UDP flood attack

Un ataque por inundación UDP es un DoS que consiste en enviar un gran número de paquetes del protocolo UDP a un servidor objetivo para así sobrecargar la capacidad de este para procesar y responder. Así mismo el firewall que protege al servidor atacado también puede verse saturado por la inundación UDP, lo que provoca al final la denegación de servicio.

Básicamente esta funciona al aprovecharse de los protocolos que sigue el servidor cuando responde a un paquete UDP recibido. Cuando un servidor recibe un paquete UDP en condiciones normales en un puerto determinado, realiza los siguientes pasos:

- Primero el servidor comprueba si está en ejecución algún proceso que esté escuchando solicitudes en el puerto especificado.

- Si no se está recibiendo paquetes en ese puerto, el servidor responde con un paquete ICMP (ping) y así informa que no se puede llegar a ese destino.

- A medida que el servidor va recibiendo paquetes UDP, y procesa las solicitudes, se van utilizando los recursos del servidor. Cuando se transmiten los paquetes UDP, en cada paquete se incluye las direcciones IP del dispositivo de origen. Pero en estos ataques DDoS, lo normal no se use una dirección IP real por los que se falsea la dirección IP de origen al paquete de UDP, lo que impide obtener la ubicación del atacante y así no se vea saturada con los paquetes de respuesta del servidor atacado.

- Así avanzado el ataque al servidor, este utiliza recursos de sistema para verificar y luego enviar respuesta los paquetes UDP recibidos. Por ello los recursos de los servidores pueden colapsar muy rápido lo que provoca al fin una denegación de servicio al tráfico normal.

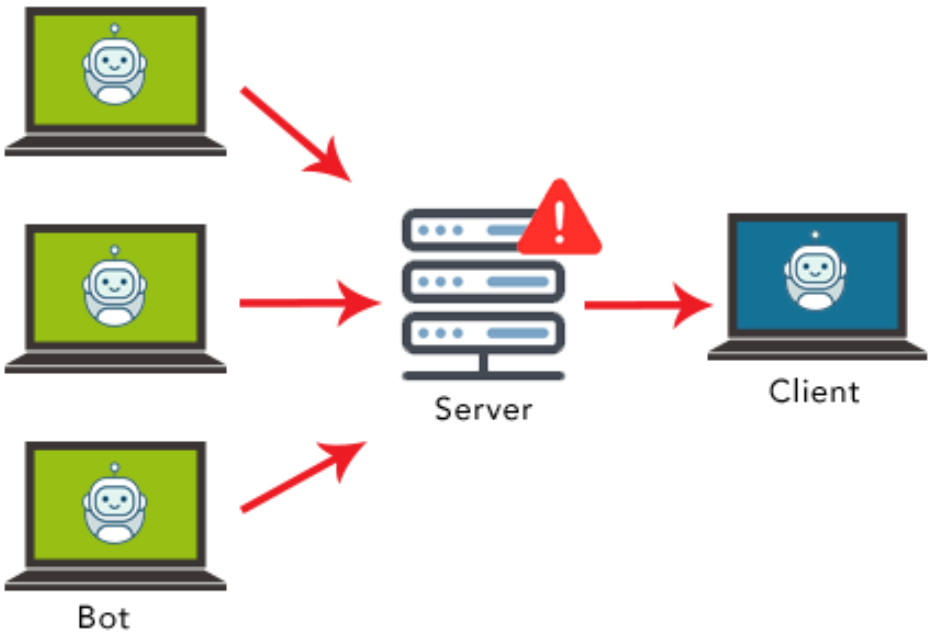


Figura 3. Flood Attack

Fuente: Purevpn.com (s.f)

2.3 ICMP Flood Attack

Un ataque por inundación ICMP es un DoS en que él se pretende sobrecargar un dispositivo con paquetes de solicitud de eco ICMP, entonces se busca que el objetivo sea inaccesible al tráfico normal. Si este ataque se realiza desde múltiples dispositivos se convierte en un ataque DDoS.

El Protocolo ICMP es el que se ocupa en el ataque de inundación de Ping. Estas herramientas de diagnóstico de red Ping y Traceroute funcionan con el protocolo ICMP. Habitualmente, estos mensajes ICMP

se usan para solicitar eco y respuesta a través de un ping a un dispositivo de red, esto tiene como finalidad de diagnosticar conectividad y el estado del dispositivo y la conexión entre el remitente y el dispositivo.

Las solicitudes ICMP requieren recursos del servidor para poder procesar cada solicitud y así enviar una respuesta. También requiere ancho de banda tanto en el mensaje entrante (solicitud de eco) como en la respuesta saliente (respuesta de eco). Este ataque tiene como fin para que el dispositivo no pueda responder al elevado número de solicitudes y/o sobrecargar la conexión de red con tráfico falso. Si se tienen dispositivos en una botnet que se encuentren dirigidos a un mismo componente de infraestructura con solicitudes ICMP, el poder de ataque se incrementa sustancialmente, esto provoca una interrupción de la actividad normal de la red. Si se hace una revisión histórica, antes se solía suplantar una dirección IP falsa para enmascarar el dispositivo emisor. En la actualidad los ataques con botnets, casi no tienen la necesidad de enmascarar la IP del bot ya que confían que la gran red de bots "no suplantados" lograrán denegar el servicio en el objetivo.

El mayor daño de una Inundación de Ping se debe al número de solicitudes que se realizan al servidor atacado. Si los comparamos con los ataques DDoS basados en la reflexión, como la amplificación DNS y la amplificación NTP, El ataque de inundación PING es simétrico; es decir, el tráfico total enviado desde cada bot es igual al recibido.

2.4 Ping of Death and smurf Attack

El conocido Ping de la muerte (PoD) es un antiguo ataque de denegación de servicio (DoS), en este el atacante desestabiliza una máquina al enviar un paquete mayor que el tamaño máximo permitido, esto provoca que el dispositivo atacado deje de funcionar. Este tipo de ataque es poco usual actualmente. Son más frecuentes los ataques de inundación de ICMP.

Los Smurf son ataques DDoS en el que se colapsa un servidor con protocolo ICMP. Como se hacen solicitudes con la dirección IP falsificada del dispositivo atacado a una o más redes informáticas, estas responden al servidor atacado, así se amplifica el tráfico de ataque inicial y se sobrecarga de forma potencial al objetivo, que se vuelve inaccesible. Este vector de ataque ya es considerado como una vulnerabilidad detectada y ya son frecuentes.

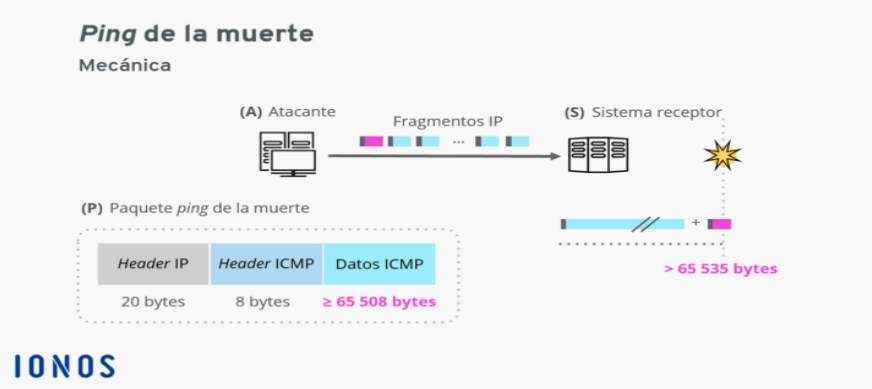


Figura 4. Ping of death

Fuente: ionos.es (2020)

2.5 SYN Flood Attack

Un Ataque de inundación SYN o ataque medio abierto es un tipo de DDoS que trata que el servidor no se encuentre disponible para el tráfico verdadero, ya que consume todos los recursos disponibles. Esto lo logra enviando constantemente paquetes de solicitud de conexión inicial (SYN), así se sobrecargan todos los puertos disponibles en el servidor atacado, esto hace que el dispositivo entregue una respuesta lenta o incluso que no responda en absoluto.

Las inundaciones SYN usan el protocolo de enlace de la conexión TCP. En cuando todo es normal, la conexión TCP muestra 3 procesos para lograrse:

1. Primero el cliente envía un paquete SYN al servidor para iniciar la conexión.

2. Luego, el servidor envía una respuesta a ese paquete inicial con un paquete SYN/ACK y así reconoce la comunicación.

3. Por último, el cliente envía de vuelta un paquete ACK y así confirma que recibió el paquete del servidor. Una vez cumplida esta secuencia, la conexión TCP se abre y es capaz de enviar y recibir datos.

Para crear el DoS, el atacante aprovecha que, después de que se recibió un paquete SYN inicial, el servidor responde con uno o más

paquetes SYN/ACK. Así espera el paso final del protocolo de enlace. Y así funciona:

El host envía un elevado volumen de paquetes SYN al servidor objetivo, casi siempre desde una dirección IP falsificada.

Luego el servidor atacado responde cada una de las solicitudes de conexión y abre un puerto para recibir la respuesta.

En el entretanto el servidor queda en espera de recibir el paquete ACK final, el cual no llegará nunca, entonces el atacante envia más paquetes SYN. Cada nuevo paquete SYN que llega hace que el servidor mantenga por un rato abiertas nuevas conexiones de puerto, una vez que se hayan utilizado todos los puertos disponibles, el servidor ya funcionará con normalidad.

Por lo general, cuando un servidor deja una conexión abierta y la máquina que se contactó no lo hace, la conexión se considera medio abierta. En este tipo de ataque DDoS, el servidor atacado mantiene conexiones abiertas reiteradamente y queda a la espera que cada una de ellas cumpla el tiempo asignado antes de que los puertos estén disponibles de nuevo.

Tipos de Inundaciones SYN

Ataque directo: En este ataque, el atacante no oculta ni falsifica su dirección IP.

Ataque con suplantación: el atacante falsifica la dirección IP en cada paquete SYN enviado para burlar los esfuerzos de mitigación y dificultar que se descubra su identidad.

Ataque distribuido (DDoS): Ataque por Botnet, muy difícil de identificar su fuente de origen.

2.6 Fragmentation Attack

En este tipo de ataque se fragmentan paquetes grandes en varios paquetes IP más pequeños. Cada paquete pequeño lleva una identificación que los vincula entre sí. Así al recibir datos, el servidor los puede ensamblar gracias a los valores de compensación que contienen.

Dentro de estos ataques el más conocido es Teardrop. Básicamente introduce información de compensación falsa en los paquetes fragmentados. Entonces, durante el proceso de reensamblado, van formándose fragmentos vacíos o superpuestos que desestabilizan el sistema. Actualmente no existen sistemas que sean vulnerables a este tipo de ataques.

Cierre

Después de revisado el contenido de la semana, podemos extraer los siguientes factores claves:

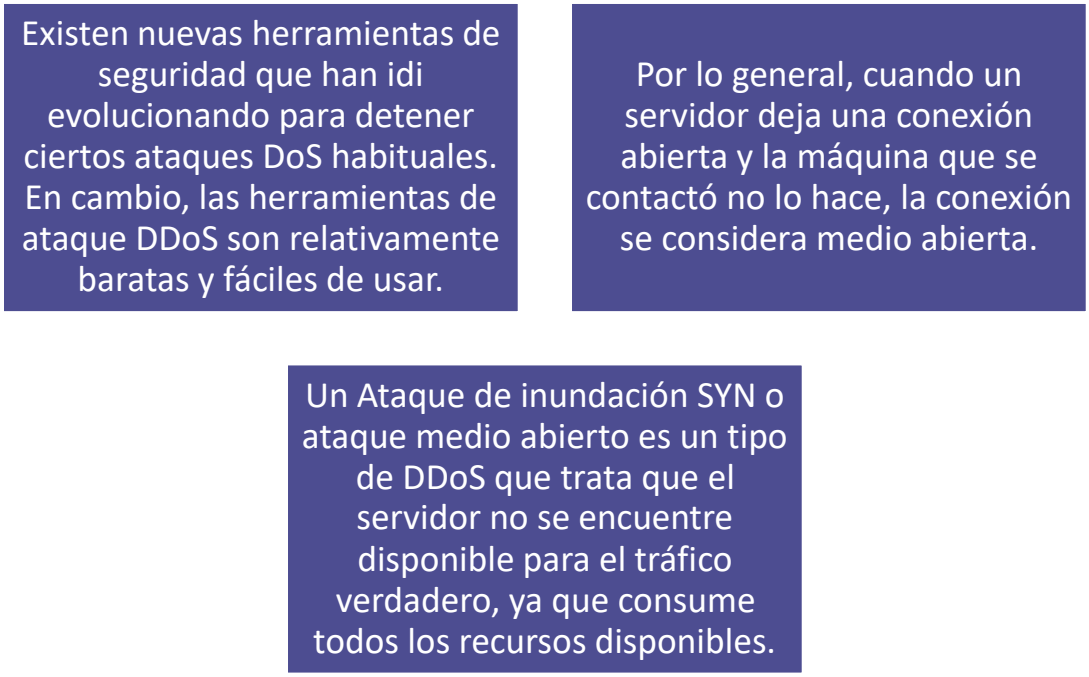


Figura 5. Ideas claves semana 6.

Fuente: Moran, E. (2022)

Referencias

Citelia (s.f.). ¿Qué es ftp o file transfer protocol (protocolo de transferencia de archivos)? Recuperado de https://citelia.es/diccionario/ftp-file-transfer-protocol/#STU

Flores, A. (2021). Qué es HTTP2: el nuevo protocolo de GoogleBot para 2021. Recuperado de https://cmacomunicacion.com/blog/.

Ataques DoS/ DDoS. Recuperado de https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

Díaz Granados, H. (2020). Empresas, principal objetivo de ciberataques en América Latina. Recuperado de https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

Sotnikov, A. (s. f.). Las 10 mejores herramientas para monitorizar aplicaciones y servidores. En Acronis. Recuperado de https://www.acronis.com/es-es/articles/monitoring-tools/

El ping de la muerte: uno de los primeros ataques de red. (s/f). IONOS Digital Guide. Recuperado el 7 de noviembre de 2022, de https://www.ionos.es/digitalguide/servidores/seguridad/ping-de-la-muerte/

¿Qué son los ataques DoS y DDoS? (s/f). Osi.es. Recuperado el 7 de noviembre de 2022, de https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

Wallarm Inc. (s/f). *What is the low Orbit Ion Cannon (LOIC)* ***?***. Wallarm.com. Recuperado el 7 de noviembre de 2022, de https://www.wallarm.com/what/what-is-low-orbit-ion-cannon-loic

(S/f). Purevpn.com. Recuperado el 7 de noviembre de 2022, de https://www.purevpn.com/ddos/http-flood-attack