**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Detección de denegación**

**de**

**servicios**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



**Proyecto de investigación**

**Alejandro Peña Tsukamoto**

**Manuel David Quiceno**

**Ingeniería de Sistemas**

**Facultad de ingeniería**

**Universidad ICESI**

**Colombia, Septiembre 2019**

Resumen

El presente proyecto de investigación tiene como objetivo dar a conocer sobre un tema que está recientemente generando amenazas a nivel de red, los ataques DoS o según sus siglas en inglés (Denial of Service) para posteriormente aprender a defenderse contra ellos. Se hizo énfasis en evitar ataques de denegación de servicio para juegos, los cuales tienden a ser más vulnerables ante estos. Para llevar a cabo el objetivo, se iniciará con el análisis de los términos generales utilizados en dichos ataques, así como su estructura y funcionamiento, se estudiarán a fondo los diferentes tipos de ataques para una vez haberlos entendido, poder diseñar estrategias para contrarrestarlos. (Conclusiones… Aún no tomadas)

**Palabras Clave:** DoS, Detección, Defensa

**Índice General**

1. **Introducción 3**

**1.1** Conceptos generales. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. . **4**

**1.1.1** Detección DoS. . . . . . . . . . . . . . . . . . . . . . . . . . .. . . . . . . . **4**

**1.1.2** Cliente-Servidor . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . **4**

1. **Denegación de servicio 5**

**2.1** Ataques de denegación de servicio . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . **6**

**2.1.1** Ataques de lágrima de fragmentación de red . . . . . . . . . . . .

**2.1.2** Inundación de protocolo de datagramas de usuario . . . . . . . .

**2.1.3** Inundación SYN . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**2.1.4** Ping de la muerte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**2.1.5** Botnets . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**2.1.6** Exploits . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**2.1.7** Armada colectiva . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

1. **Metodología**

**3.1** Métodos De Mitigación

**3.1.1** Ataques de lágrima de fragmentación de red . . . . . . . . . . . .

**3.1.2** Inundación de protocolo de datagramas de usuario . . . . . . . .

**3.1.3** Inundación SYN . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**3.1.4** Ping de la muerte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**3.1.5** Botnets . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**3.1.6** Exploits . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**3.1.7** Armada colectiva . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**Capítulo 1**

**Introducción**

Los ataques de denegación de servicio son los encargados de provocar la falta de disponibilidad de los servicios de red, inundando de manera continua los servidores con tráfico malicioso [[3](#x5q49wrdsds7)]. Hoy en dia en la red se encuentran infinidad de programas de fácil acceso que permiten realizar los ataques de una manera eficaz, esto gracias a la rápida evolución de la tecnología y las formas de acceso al mundo de la internet.

La cantidad de tráfico que se puede concentrar en un sitio web ya es de por sí, una tarea difícil de calcular, ahora las herramientas que existen para detectar dichos ataques y reducir el tráfico no deseado necesitan una infraestructura adicional para que sean efectivas.

Por una cantidad módica de dinero una persona puede comprar puntos de acceso basadas en el 801.11 que permiten extender la conectividad de red hasta por cien metros, sin problema alguno, cabe recalcar que estos pueden ser usados en cualquier tipo de espacio, ya sea doméstico, empresarial o gubernamental. Así mismo como su popularidad aumenta, su atractividad ante los posibles atacantes también lo hará [[2](#ghsar0ijsoxo)].

**1.1 Conceptos Generales**

**1.1.1 DoS**

La detección de denegación de servicios o DoS (por sus siglas en inglés) es el proceso que se encarga de distinguir los ataques de denegación distribuida del tráfico de red para poder mitigarlos de manera efectiva. Su objetivo consiste en limitar el acceso de una aplicación (En este caso juegos online), negándole a los usuarios reales el acceso a sus servicios.

Existen muchos tipos de esquemas actualmente en lo que ataques DoS se refieren, provocando que estos sean más populares, utilizados y cada vez más sofisticados. Lo que hace peligroso estos ataques es la capacidad de generar y atosigar un servicio utilizando una cantidad de miles de solicitudes de fuentes variadas, lo que provoca que sea sumamente difícil poder detener su ataque deteniendo o identificando una sola dirección IP, esto sin tener en cuenta en lo difícil que sería distinguir el tráfico de usuarios reales y los maliciosos.

**1.1.2 Cliente-Servidor**

El modelo de Cliente-Servidor se caracteriza por tener dos partes, por un lado la parte del servidor y por otro la parte de cliente o clientes. Se entiende que el servidor debe ser una máquina con un hardware y software específico para que actúe como un tipo de depósito de datos o funcione como un sistema gestor de base de datos o aplicaciones [[4](#k8mitrak0wsz)].

Los componentes de este modelo son:

Red: Conjunto de clientes, servidores y bases de datos en conjunto de manera física.

Cliente: Se refiere al encargado de demandar los servicios, ya sea un ordenador o una aplicación

Servidor: Se refiere al proveedor de servicios, este servidor también puede ser un ordenador o una aplicación la cual se encargue de mandar la información a los demás

Protocolo: El conjunto de normas o reglas de una manera clara y concreta sobre el flujo de una red estructura.

**Capítulo 2**

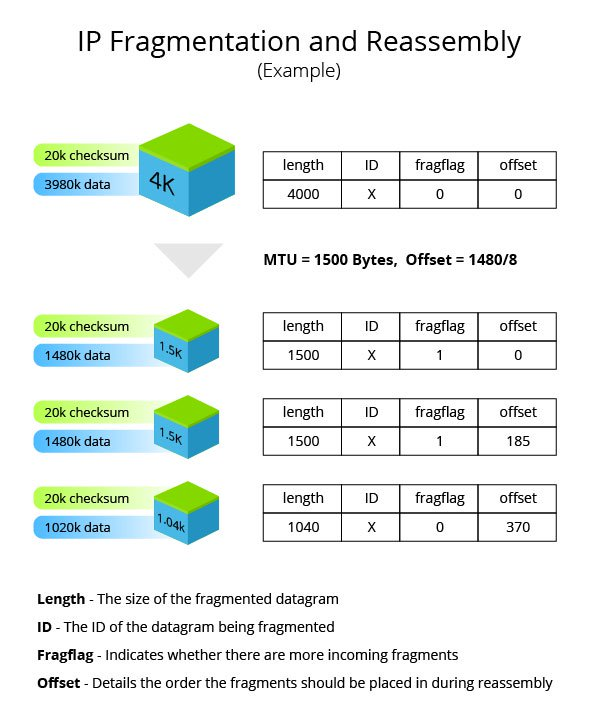
**Denegación de servicio**

Ninguna organización está exenta a sufrir un ataque de denegación de servicio, el cual es en pocas palabras un intento de provocar que un recurso de red o una máquina dejen su correcto funcionamiento hasta poder ser no disponible para los usuarios. Los motivos para llevar a cabo un ataque de este estilo pueden ser muy variados y estos se realizan mediante diferentes métodos. Algunos de ellos son

**2.1 Ataques de denegación de servicio**

**2.1.1 Ataques de lágrima de fragmentación de red**

Consiste básicamente en que el autor se encarga de dominar una red explotando los mecanismos de fragmentación de datagramas, Para entender el ataque primero hay que entender que es la compresión del proceso de fragmentación del protocolo de internet (IP), el cual es un procedimiento en donde los datagramas IP se particionan en pequeños paquetes, los cuales son transmitidos por la red y son re-ensamblados después en el datagrama original.

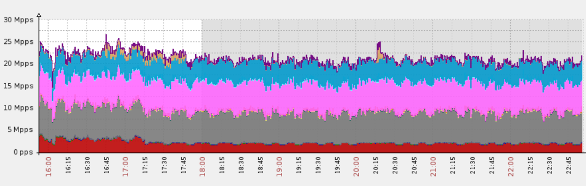
La fragmentación es necesaria para la transmisión de los datos, debido a que toda la red tiene un límite único para el tamaño de los datagramas que pueden procesar. Este límite se conoce como MTU o unidad máxima de transmisión y en caso de que el datagrama que se manda es mayor del que recibe el servidor MTU, él tiene que ser fragmentado para que se pueda transmitir completamente 

**2.1.2 Inundación de protocolo de datagramas de usuario**

Se trata de un protocolo de red sin conexión. Como el UDP o protocolo de datagramas de usuario no necesita un enlace de tres vías como el TCP, puede ser ejecutado con una menor sobrecarga y se usa idealmente para el tráfico que no necesita ser revisado como lo es el chat o el VoIp.

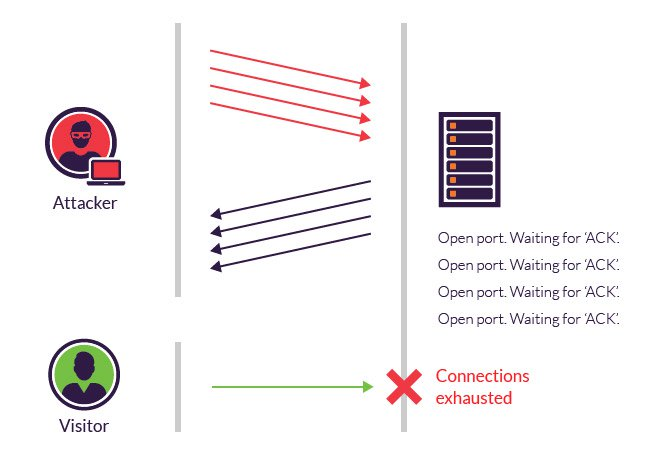
En un principio para establecer una conexión válida, se pueden enviar un gran volumen de tráfico a través de canales UDP a cualquier otro host sin necesidad de tener una protección incorporada para limitar la velocidad de la inundación del ataque, lo que significa que estos ataques son altamente efectivos y también pueden ejecutarse sin necesidad de usar muchos recursos.

Una forma de efectuar este ataque es usando el llamado “Ataque de sopa de letras” , gracias a que UDP no define formatos de paquetes específicos, los atacantes pueden crear paquetes de más de 8KB llenos de texto basura o números para después enviarlos al host víctima



**2.1.3 Inundación SYN**

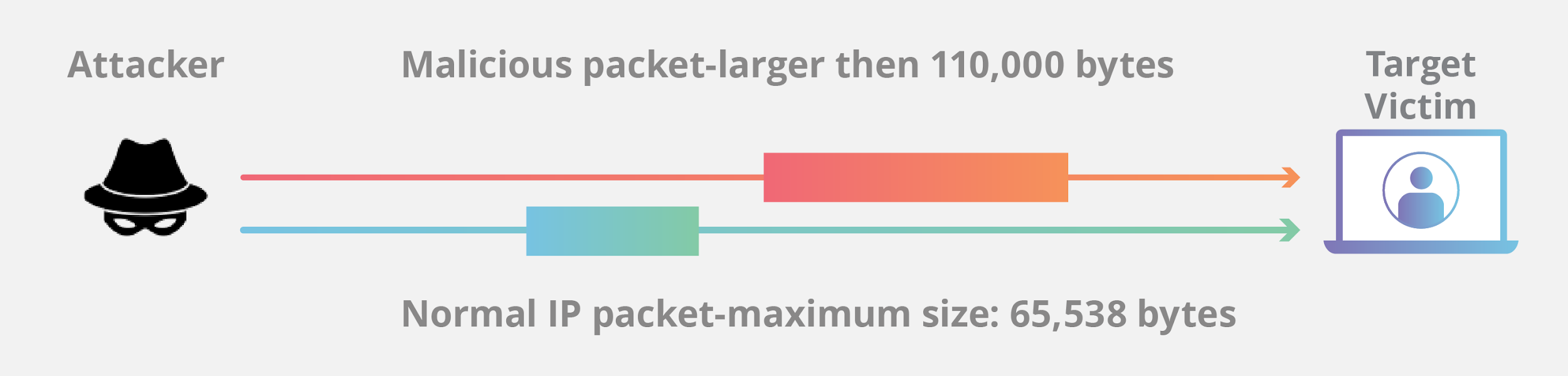
Cuando se establece una conexión cliente servidor se establece un enlace de tres vías o “three-way handshake” como en su traducción al inglés. En un ataque SYN, el atacante envía repetidos paquetes de sincronización a cada puerto del servidor de la víctima usualmente usando una dirección IP falsa. El servidor bajo ataque recibe múltiples y aparentemente peticiones legítimas para establecer la conexión, por lo que devolverá un paquete ACK para cada puerto abierto.



**2.1.4 Ping de la muerte**

El tamaño de un paquete IPv4 correctamente formado, incluido el encabezado IP, es de 65.535 bytes, incluido un tamaño de carga útil total de 84 bytes. Muchos sistemas informáticos históricos simplemente no podrían manejar paquetes más grandes y se bloquearían si recibieran uno.

El envío de un paquete ping de más de 65,535 bytes viola el Protocolo de Internet, los atacantes generalmente envían paquetes mal formados en fragmentos. Cuando el sistema de destino intenta volver a ensamblar los fragmentos y termina con un paquete de gran tamaño, puede producirse un desbordamiento de memoria y provocar varios problemas del sistema, incluido el bloqueo. Los ataques de ping de la muerte fueron particularmente efectivos porque la identidad del atacante podría ser fácilmente suplantada. Además, un atacante Ping of Death no necesitaría un conocimiento detallado de la máquina que estaba atacando, a excepción de su dirección IP.

****

**2.1.5 Botnets**

**2.1.6 Exploits**

**2.1.7 Armada colectiva**

**Capítulo 3**

**Metodología**

**3.1 Métodos de mitigación**

**3.1.1 Ataques de lágrima de fragmentación de red**

Los ataques de fragmentación de IP se mitigan de varias maneras diferentes, según el tipo y la gravedad del ataque. La mayoría de los métodos de mitigación aseguran que los paquetes de datos maliciosos nunca lleguen a sus destinos de destino. El más común consiste en inspeccionar los paquetes entrantes por violaciones de las reglas de fragmentación (por ejemplo, usando un enrutador o un proxy seguro).

**3.1.2 Inundación de protocolo de datagramas de usuario**

En el nivel más básico, la mayoría de los sistemas operativos intentan mitigar los ataques de inundación UDP limitando la tasa de respuestas ICMP. Sin embargo, este filtrado indiscriminado tendrá un impacto en el tráfico legítimo.

Tradicionalmente, el método de mitigación UDP también se basaba en firewalls que filtraban o bloquear paquetes UDP maliciosos. Sin embargo, estos métodos ahora se están volviendo irrelevantes, ya que los ataques modernos de alto volumen pueden simplemente superar los cortafuegos, que no están diseñados teniendo en cuenta el exceso de aprovisionamiento.

**3.1.3 Inundación SYN**

Si bien los sistemas operativos modernos están mejor equipados para administrar recursos, lo que dificulta el desbordamiento de las tablas de conexión, los servidores aún son vulnerables a los ataques de inundación SYN.

Existen varias técnicas comunes para mitigar los ataques de inundación SYN, que incluyen:

**Microbloques**: los administradores pueden asignar un microregistro (tan solo 16 bytes) en la memoria del servidor para cada solicitud SYN entrante en lugar de un objeto de conexión completo.

**Cookies SYN**: mediante el uso de hashing criptográfico, el servidor envía su respuesta SYN-ACK con un número de secuencia (seqno) que se construye a partir de la dirección IP del cliente, el número de puerto y posiblemente otra información de identificación única. Cuando el cliente responde, este hash se incluye en el paquete ACK. El servidor verifica el ACK y solo entonces asigna memoria para la conexión.

**Cookies RST**: para la primera solicitud de un cliente determinado, el servidor envía intencionalmente un SYN-ACK no válido. Esto debería dar como resultado que el cliente genere un paquete RST, que le dice al servidor que algo está mal. Si se recibe esto, el servidor sabe que la solicitud es legítima, registra al cliente y acepta las conexiones entrantes posteriores.

**Ajuste de pila**: los administradores pueden ajustar las pilas TCP para mitigar el efecto de las inundaciones SYN. Esto puede implicar reducir el tiempo de espera hasta que una pila libere la memoria asignada a una conexión, o descartar selectivamente las conexiones entrantes.

Obviamente, todos los métodos mencionados anteriormente se basan en la capacidad de la red de destino para manejar ataques DDoS volumétricos a gran escala, con volúmenes de tráfico medidos en decenas de Gigabits (e incluso cientos de Gigabits) por segundo.

**3.1.4 Ping de la muerte**

Para evitar los ataques Ping de Death, y sus variantes, muchos sitios bloquean por completo los mensajes de ping ICMP en sus firewalls. Sin embargo, este enfoque no es viable a largo plazo.

En primer lugar, los ataques de paquetes no válidos pueden dirigirse a cualquier puerto de escucha, como los puertos FTP, y es posible que no desee bloquearlos por razones operativas.

Además, al bloquear los mensajes de ping, evita el uso legítimo del ping, y todavía hay utilidades que dependen del ping para verificar que las conexiones estén activas, por ejemplo.

El enfoque más inteligente sería bloquear selectivamente los pings fragmentados, permitiendo que el tráfico de ping real pase sin obstáculos.

**Bibliografía**

**[****1]**  Dragoș Glăvan, Ciprian Răcuciu, Radu Moinescu, Narcis-Florentin Antonies, “DDoS Detection and Prevention Based on Artificial Intelligence Techniques” Military Technical Academy “Ferdinand I” – Systems Engineering for Defense and Security

**[****2]** John Bellardo, Stefan Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions” - University of California at San Diego. Disponible en: <https://www.usenix.org/legacy/event/sec03/tech/full_papers/bellardo/bellardo_html/>

**[****3]** Quamar Niyaz , Weiqing Sun, Ahmad Y Javaid “A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)” The University of Toledo. Disponible en: <https://arxiv.org/pdf/1611.07400.pdf>

**[****4]** Andrés Schiaffarino “Modelo cliente servidor” Tutoriales de Hosting. Disponible en

“<https://blog.infranetworking.com/modelo-cliente-servidor/>”