UNIVERSIDAD DE GRANADA

ATAQUES DDOS

Servidores Web de Altas Prestaciones
Curso 2023/2024

Juan Luis Torres Ramos
Javier García Pérez
Miguel Torres Alonso

Índice

1. Introducción **3**
1.1. Motivación . . . 3

2. Fijando objetivos **4**
2.1. Metas Específicas . . . 4
2.2. Tendencias actuales: . . . 4

3. ¿Qué son los ataques DDoS? **5**
3.1. Concepto de DoS y diferencias con DDoS. . . . 5

4. Contextualizando el peligro **6**
4.1. Botnets . . . 6
4.2. Historia de los ataques DDoS . . . 6

5. Desarrollo y análisis DDoS en profundidad **7**
5.1. Creación de Botnets . . . 7
5.2. Tipos de Botnets . . . 7
5.3. Funcionamiento de una Botnet . . . 7
5.4. Estrategias para ataques DDoS . . . 7
5.5. Protección para ataques DDoS . . . 7

6. Despliegue de la demo **8**
6.1. Setup de la demo . . . 8
6.2. HTTP Flood . . . 11
6.3. Slowloris . . . 13
6.4. Connection flood . . . 15

7. Conclusiones **17**

1. Introducción

A día de hoy no es difícil notar que vivimos en una sociedad donde cualquier persona es poseedora de al menos un dispositivo electrónico, el cual en gran parte beneficia al usuario en gran cantidad de aspectos como por ejemplo trabajar o simplemente comunicarse a distancia. Esta constante conexión puede conllevar a varios inconvenientes, siendo uno de ellos la existencia de riesgo de recibir ataques usando multitud de estrategias que pueden comprometer la información personal de un usuario o, como vamos a ver más adelante, pueden reducir o incluso interrumpir la disponibilidad de servidores web, pudiendo generar pérdidas de datos y/o económicas.

De entre las estrategias usadas para llevar a cabo este último propósito mencionado, destacan los ataques DDoS, llevados a cabo en multitud de ocasiones a lo largo de la historia relativamente breve de internet, con una efectividad aún a día de hoy bastante alta y cuyo fin es claramente malicioso. En este trabajo se verá con detalle el concepto de ataque DDoS, cómo funcionan, diferentes tipos y una demostración práctica mediante el uso de *'botnets'*.

1.1. Motivación

Cuando se desarrollan aplicaciones web, se debe de tener en cuenta que se está expuesto a Internet y las consecuencias que ello acarrea, tanto positivas como negativas. Aunque normalmente se piense en una página web como un recurso donde únicamente acceden simples usuarios sin ninguna mala intención, como ingenieros informáticos es preciso ser precavido y saber emplear técnicas, estrategias y configuraciones disponibles a la hora de levantar servidores web de tal manera que se minimice el daño de cualquier tipo causado por posibles ataques.

El problema surge cuando debido al "anonimato" que proporciona Internet, algunos usuarios se aprovechan de ello para llevar a cabo ataques DDoS con un motivo determinado ya sea económico, por ocio, venganza... etc. Por esto, para poder defenderse de posibles amenazas, es importante aprender a fondo el mecanismo de las mismas, funcionamiento, fortalezas, debilidades... Es entonces cuando conociendo ciertos patrones o singularidades de este tipo de ataque se podría disminuir la efectividad del mismo. Por ejemplo, reconociendo o detectando a tiempo se podrían tomar decisiones muy importantes de cara a disminuir las consecuencias negativas en base a lo que requiera el caso que esté sucediendo o usando cierto tipo de configuraciones de un servidor o firewalls para que actúen de cierta manera al detectar un número de solicitudes elevado en un corto periodo de tiempo, por ejemplo.

2. Fijando objetivos

El objetivo principal del proyecto es comprender y mitigar los riesgos asociados con los ataques de Denegación de Servicios Distribuidos (DDoS). Al conocer en profundidad cómo operan estos ataques, estaremos mejor preparados para anticiparlos y neutralizarlos eficazmente, fortaleciendo así la seguridad y continuidad de nuestros sistemas y servicios.

2.1. Metas Específicas

Durante el proyecto abordaremos los siguientes puntos:

1. **Explicación del Funcionamiento de los Ataques DDoS.**
   - Diferencia entre DoS y DDoS.
   - Concepto de botnet.
   - Historia de los Ataques DDoS.
   - Estrategias Utilizadas en Ataques DDoS.
   - Tendencias Actuales.
2. **Demostración de un ataque DDoS.**
   - Proceso de creación y Activación de una Botnet.
   - Realización de ataques Específicos (Slowris, HTTP FLood, Connection Flood).
   - Análisis y comprensión en la Máquina Objetivo.

Las botnet juegan un papel crucial en la ejecución de ataques DDoS. Podemos destacar varias tendencias y desafíos actuales relacionados con el uso de botnets en estos ataques.

2.2. Tendencias actuales:

- **Aumento en la sofisticación:** Cada vez las botnets se vuelven mucho más sofisticadas, empleando técnicas avanzadas de evasión para evitar la detección y la mitigación. Esto incluye la capacidad de cambiar rápidamente sus patrones de ataque y aplicar métodos de cifrado para esconder su tráfico.
- **Uso de dispositivos IoT:** Con la proliferación de dispositivos IoT, los atacantes aprovechan las vulnerabilidades de las pobres medidas de seguridad de la mayoría de IoT con el objetivo de crear botnets masivas. Estos dispositivos son especialmente atractivos debido a su gran número y a su conexión constante a internet.
- **Servicios de Botnet como Servicio (BaaS):** Estos últimos años se ha visto un incremento en el modelo de negocio conocido como "Botnet como Servicio", donde los atacantes alquilan botnets para poder hacer ataques DDoS sin necesidad de construir su propia botnet. Esto ha democratizado el acceso a las capacidad¡es de ataque DDoS, haciéndolos más accesibles incluso para actores con pocos recursos técnicos.
- **Mobile Botnets:** Se ha observado un creciente uso de botnets móviles, que consisten en una red de smartphones comprometidos controlados remotamente por un botmaster a través de canales de C&C. Los dispositivos móviles son particularmente atractivos para los atacantes debido a su alta penetración en el mercado, conectividad constante y la frecuencia de medidas de seguridad insuficientes en las aplicaciones móviles.

3. ¿Qué son los ataques DDoS?

Existen multitud de formas de llevar a cabo ataques informáticos, ya sea a servidores o a equipos personales, normalmente con fines maliciosos aunque también con fines lúdicos o preventivos siempre y cuando se lleven a cabo en entornos controlados y aislados de manera que no pueda descontrolarse y por tanto causar daños no intencionados. Una de ellas es el **"ataque de denegación de servicio distribuido"**, conocido por sus siglas en inglés "DDoS" **(Distributed Denial of Service)**.

Los ataques "DDoS" son un intento **malintencionado** de ralentizar o interrumpir el tráfico normal de un servidor mediante la sobrecarga del mismo utilizando varios equipos organizados o infectados, pudiendo existir varias metodologías con este fin. Esto se consigue, resumidamente, de la siguiente manera: se generan una cantidad masiva de peticiones al servicio desde varias máquinas o direcciónes IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta debido a la sobrecarga, comienza a rechazar peticiones y por tanto, se materializa la denegación del servicio.

3.1. Concepto de DoS y diferencias con DDoS.

No podemos olvidar mencionar que también existen los ataques DoS (Denial of Service), donde el objetivo es el mismo, bloquear el servicio para el que un sistema o aplicación está destinado, pero con la diferencia del número de ordenadores o direcciones IP destinadas al ataque. Es importante entender la diferencia entre el concepto DoS y DDoS, pues ahí radica una de las claves por las que DDoS es más difícil de detectar y por ende más peligroso.

En el momento en el que se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP y pueda darse la denegación de servicio, el administrador puede bloquear la IP que está realizando las peticiones. Esto mismo es más difícil de detectar en el caso de los ataques DDoS porque las peticiones provienen de direcciones IP diferentes.

Por lo general, una 'botnet' posee mayor efectividad que una sola máquina (DoS) a la hora de realizar un ataque DDoS por cuestiones obvias.

4. Contextualizando el peligro

4.1. Botnets

En la mayoría de casos reales y para la demostración práctica de este trabajo se ha decidido hacer uso de una 'botnet', por lo cual es necesario entender su significado y funcionamiento. Botnet proviene de la combinación de las palabras robot y red. Es un conjunto de dispositivos infectados con malware, llamados bots, que son controlados remotamente por un atacante para llevar a cabo actividades delictivas. En este trabajo se usa el concepto de Botnet pero se utiliza realmente una simulación de la misma.

El control sobre las máquinas infectadas varía según el tipo de malware, desde simples solicitudes a una dirección IP concreta hasta la capacidad de descargar y ejecutar archivos o iniciar una shell remota.

Existen varios roles o papeles de bots dentro de una Botnet, los cuales llamaremos 'slaves' y 'master':

- Los 'slaves' simplemente se encuentran en un estado de letargo hasta recibir órdenes del master.
- Los 'masters' se encargan de dar órdenes a los bots slaves o incluso a otros master.

La efectividad de una botnet depende de la disponibilidad de un dispositivo en la red, la cual a su vez depende de su conexión a la misma y encendido. Por este motivo es conveniente para un atacante infectar el mayor número de dispositivos para aumentar la potencia del ataque y para aumentar el porcentaje de disponibilidad total de la red.

4.2. Historia de los ataques DDoS

El primer ataque DDoS de los que se tiene constancia fue a "Panix", el 3º mayor ISP (Proveedor de Servicios de Internet) de la época, el cual sufrió una inundación de paquetes SYN. Esto produjo la caída de sus servicios durante varios días, mientras la reconocida mundialmente empresa "Cisco", que se encargaba en aquel entonces del hardware de la red, encontraba una solución.

Uno de los primeros ataques DDoS conocidos mundialmente fue el de un chico canadiense de 15 años que en el año 2000 lanzó un ataque que consistió en sobrecargar los servidores de varios sitios web de gran popularidad, como Yahoo!, CNN, eBay, Amazon y Buy.com, con un tráfico de datos masivo, lo que provocó su caída y la imposibilidad de acceder a ellos durante varias horas. Lo consiguió gracias al uso de una red de miles de ordenadores infectados con malware (botnet) para generar una avalancha de solicitudes HTTP. El ataque generó millones de euros en pérdidas en total y puso de manifiesto la clara vulnerabilidad de Internet ante este tipo de ataques y la necesidad de mejorar las medidas de seguridad.

Posteriormente han seguido habiendo ataques DDoS mundialmente famosos, tanto a organizaciones gubernamentales, como fue el caso del gobierno de Estonia en el año 2007 (según ciertas teorías conspirativas llevado a cabo por el gobierno ruso), como a empresas multinacionales como GitHub, AWS, Wikipedia, Google... etc. A la vista está que, a sabiendas del riesgo de recibir este tipo de ataques y aún habiendo tomado medidas de seguridad, toda precaución es poca en el mundo de la informática y ningún servicio o servidor es infranqueable al 100 %.

5. Desarrollo y análisis DDoS en profundidad

Ahora que sabemos qué son las botnets y los ataques DDoS, vamos a estudiar en profundidad cómo funcionan, qué tipos de Botnets existen y cómo protegerse de estos ataques maliciosos. Este análisis abarca desde la creación de una botnet hasta las estrategias empleadas en los ataques DDoS y las medidas de protección más efectivas.

5.1. Creación de Botnets

La creación de una botnet comienza con la infección de dispositivos mediante técnicas como phishing, explotación de vulnerabilidades de software y descargas involuntarias de malware. Los dispositivos infectados se conectan a un servidor de comando y control (C&C), permitiendo al atacante coordinar las acciones de todos los dispositivos afectados.

5.2. Tipos de Botnets

Existen varios tipos de botnets con diferentes características y mecanismos de control. Las botnets centralizadas son las más comunes, donde todos los bots se conectan a un servidor C&C central. Las botnets descentralizadas o P2P no dependen de un único punto de control y son más resistentes a interrupciones, ya que en estas, los bots se comunican entre sí.

Una botnet diseñada para ataques DDoS es Mirai. Mirai infecta dispositivos IoT (Internet de las Cosas), como cámaras de seguridad y routers domésticos. Utiliza estos dispositivos para lanzar ataques volumétricos masivos, saturando el ancho de banda del objetivo. Se destaca por infectar rápidamente una gran cantidad de dispositivos, aprovechando las credenciales determinadas y vulnerabilidades comunes.

5.3. Funcionamiento de una Botnet

El funcionamiento de una botnet en un ataque DDoS implica varias etapas. Primero, el botmaster prepara la botnet y selecciona el objetivo de ataque. Luego se envían comandos a los bots para que inicien la generación de tráfico hacia el objetivo. Durante la ejecución los bots inundan el objetivo con un volumen masivo de tráfico, sobrecargando su capacidad de procesamiento y red. El botmaster monitorea el ataque en tiempo real, ajustando las tácticas según sea necesario para maximizar el impacto y evadir las medidas de defensa del objetivo.

5.4. Estrategias para ataques DDoS

Los ataques DDoS se pueden clasificar en tres categorías principales. Los ataques de volumen buscan consumir todo el ancho de banda disponible del objetivo mediante la generación de tráfico masivo, como los ataques UDP Flood y ICMP Flood. Los ataques de protocolo se enfocan en agotar los recursos de los servidores y dispositivos de red explotando debilidades en los protocolos, como los ataques SYN Flood y Ping of Death. Finalmente, los ataques a la capa de aplicación tienen como objetivo aplicaciones específicas, enviando solicitudes que parecen legítimas pero que sobrecargan la aplicación, como los ataques HTTP Flood y Slowloris.

5.5. Protección para ataques DDoS

Para protegerse contra ataques DDoS es crucial implementar una combinación de medidas preventivas y reactivas. Entre las medidas preventivas se incluyen el filtrado de tráfico mediante firewall y sistemas de detección y prevención de intrusiones (IDS/IPS). En términos de medidas reactivas, se pueden emplear técnicas como blackholing y sinkholing para redirigir el tráfico a un “agujero negro”, limitación de la tasa de solicitudes permitidas en un periodo de tiempo determinado, y el análisis continuo del trafico para identificar y responder rápidamente a patrones sospechosos.

6. Despliegue de la demo

Para la demostración, planeamos llevar a cabo tres ataques contra nuestra granja web de prácticas, centrándonos especialmente en el balanceador, simulando los comportamientos de una botnet centralizado. Para ejecutar el ataque, utilizaremos una botnet desarrollada en Python. Comenzaremos configurando el servidor C&C local y creando los bots correspondientes. Después, procederemos con los ataques Slowris, HTTP, Connection flood.

El objetivo de esta demostración es ilustrar los riesgos asociados con los ataques de botnet y resaltar la importancia de implementar medidas efectivas de seguridad cibernética para proteger nuestra infraestructura contra tales amenazas.

6.1. Setup de la demo

1. Vamos a nuestra carpeta Granja Web y desplegamos nuestra granja que hemos realizado en prácticas. 'Granja Web' y desplegamos la infraestructura que hemos configurado durante nuestras prácticas. He añadido una imagen en el archivo .php para potenciar la efectividad frente a ataques DDoS (figura 1). Ahora, procedemos a lanzar nuestra granja web utilizando el siguiente comando:

```
docker compose up -d
```

   Una vez desplegada, la granja web estará disponible en los siguientes enlaces:

   - HTTPS: `https://localhost:4000/`
   - HTTP: `https://localhost:3000`

   Vamos a lanzar nuestro ataque contra el servidor HTTP.

2. Nos vamos a la carpeta botnet y ejecutamos el siguiente comando para iniciar el servidor de control y comandos C&C para luego controlar los bots. Iniciamos el servidor en el puerto 1337.

```
sudo python3 cnc.py 1337
```

3. Una vez que el servidor C&C está en funcionamiento, puedes conectarte a él utilizando Telnet. Telnet es un protocolo que permite establecer una conexión de terminal remota con otro sistema. En este caso, estás estableciendo una conexión a la dirección IP local (127.0.0.1) en el puerto 1337, donde se encuentra ejecutándose nuestro servidor C&C. Para entrar en el servidor el usuario es rootz la contraseña es root"(figura 2).

```
telnet 127.0.0.1 1337
```

4. Ahora vamos a inicializar los bots. Abre otra terminal y ejecuta el siguiente comando para lanzar 4 bots.

```
python3 ejecutarBots.py
```

Vemos en la figura 4 cómo responde el servidor C&C ante la llegada de los bots y comprobamos que están operativos.
Tenemos 4 bots operativos, procedemos a realizar los ataques y hacer un monitoreo de la máquina objetivo:

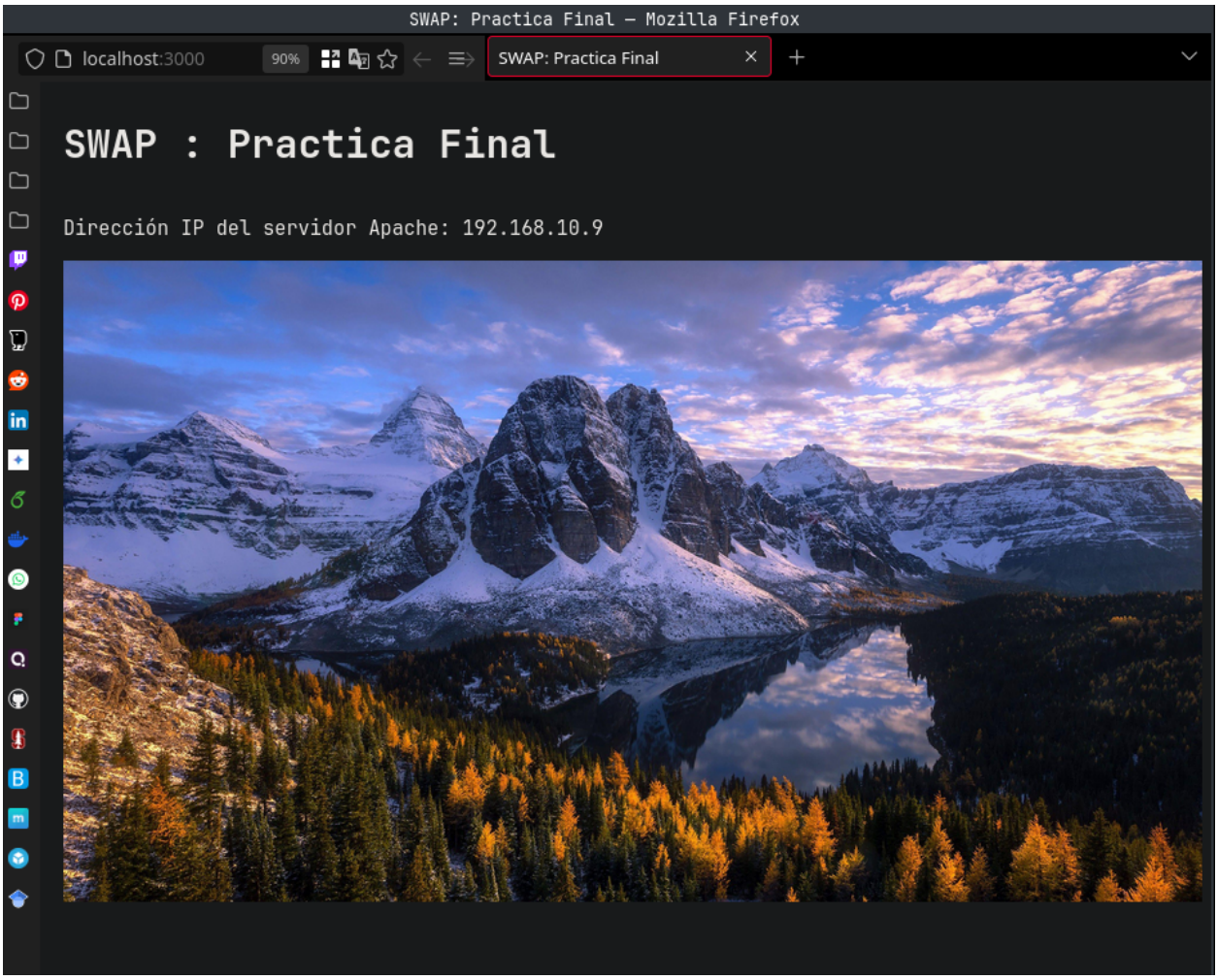

Figura 1: Aspecto de la página que sirve nuestra granja web.

Figura 2: Introducción de los comandos anteriores.

Figura 3: Terminal de Aoyama.

Figura 4: Salida por terminal de eventos.

Figura 5: Disponemos de 4 bots.

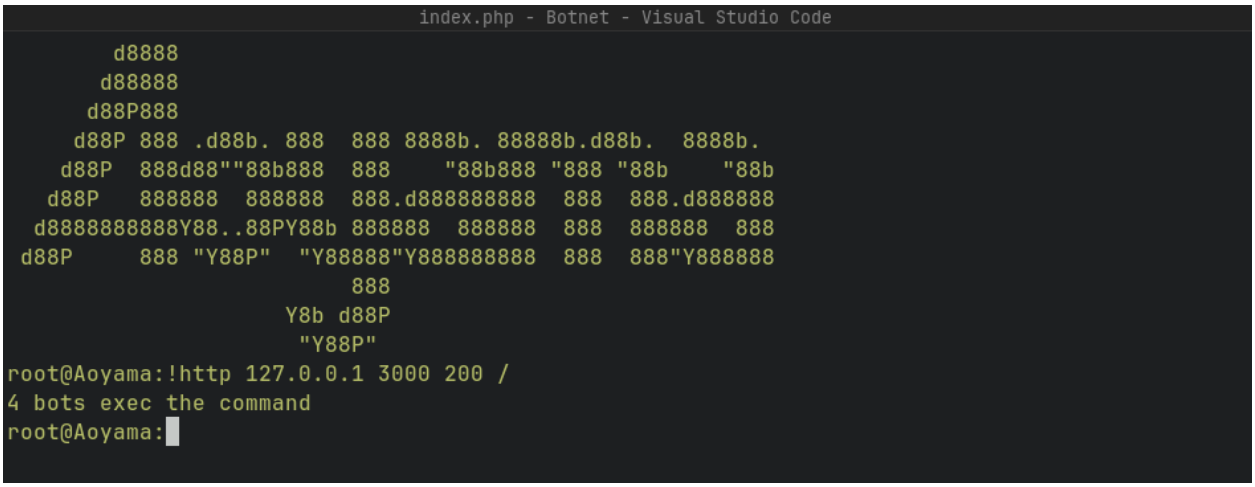

Figura 6: Lanzamos la botnet.

6.2. HTTP Flood

Se llevará a cabo un gran volumen de solicitudes HTTP enviadas simultáneamente al servidor web con el propósito de sobrecargarlo y volverlo inaccesible para los usuarios legítimos.

Si un balanceador de carga es vulnerable a un ataque HTTP flood, es probable que su capacidad para mantener la disponibilidad y el rendimiento del servicio se vea gravemente comprometida. Esto podría ocasionar una interrupción en el servicio o incluso exponerlo a riesgos de seguridad.

Procedemos a realizar este comando en la terminal C&C (figura 6).

```
!http 127.0.0.1 3000 200 /
```

- 127.0.0.1:3000 es la dirección IP y el puerto de la máquina objetivo.
- 200 es el número de hebras que se utilizarán para ejecutar el ataque.
- / indica que el ataque se dirigirá a la raíz del archivo index.php en el servidor objetivo.

Para parar luego el ataque haremos un *!Stop*

Vemos que el balanceador queda inoperativo (fig. 7) y, si accedemos a los log que tenemos configurados en *var/log/nginxnginx_juanluis.access.log* dentro de la terminal del balanceador y ejecutamos:

```
tail -f nginx_juanluis.access.log
```

Monitoreamos los logins que acceden y vemos que se han inundado de peticiones GET (fig. 8).
Los registros muestran claramente un patrón consistente con un ataque de HTTP flood en nuestro balanceador. La gran cantidad de solicitudes GET recibidas en un corto período de tiempo indica una actividad anormal que supera con creces la carga típica del servidor.

Es importante tener en cuenta que, mientras algunas solicitudes resultan en respuestas exitosas (código de estado 200), otras generan errores (código de estado 400). Esto indica que el servidor está teniendo dificultades para manejar eficientemente la abrumadora carga de solicitudes, lo que puede resultar en una degradación del rendimiento y una posible indisponibilidad para los usuarios legítimos.

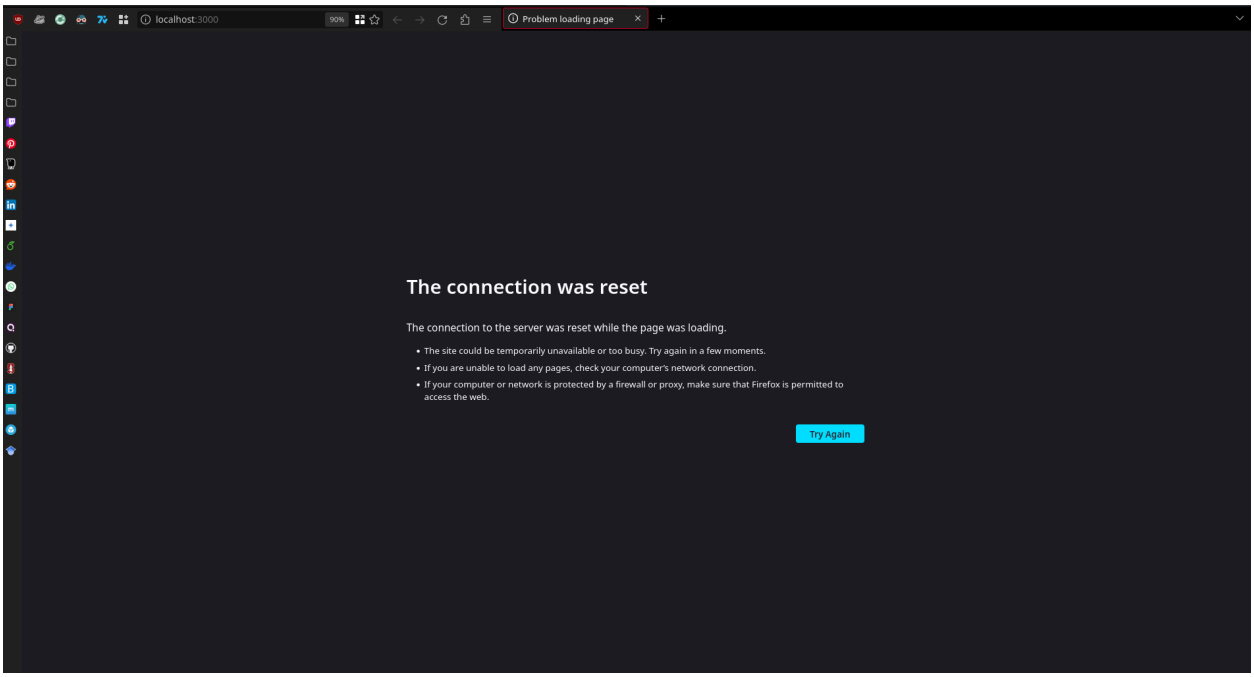

Figura 7:

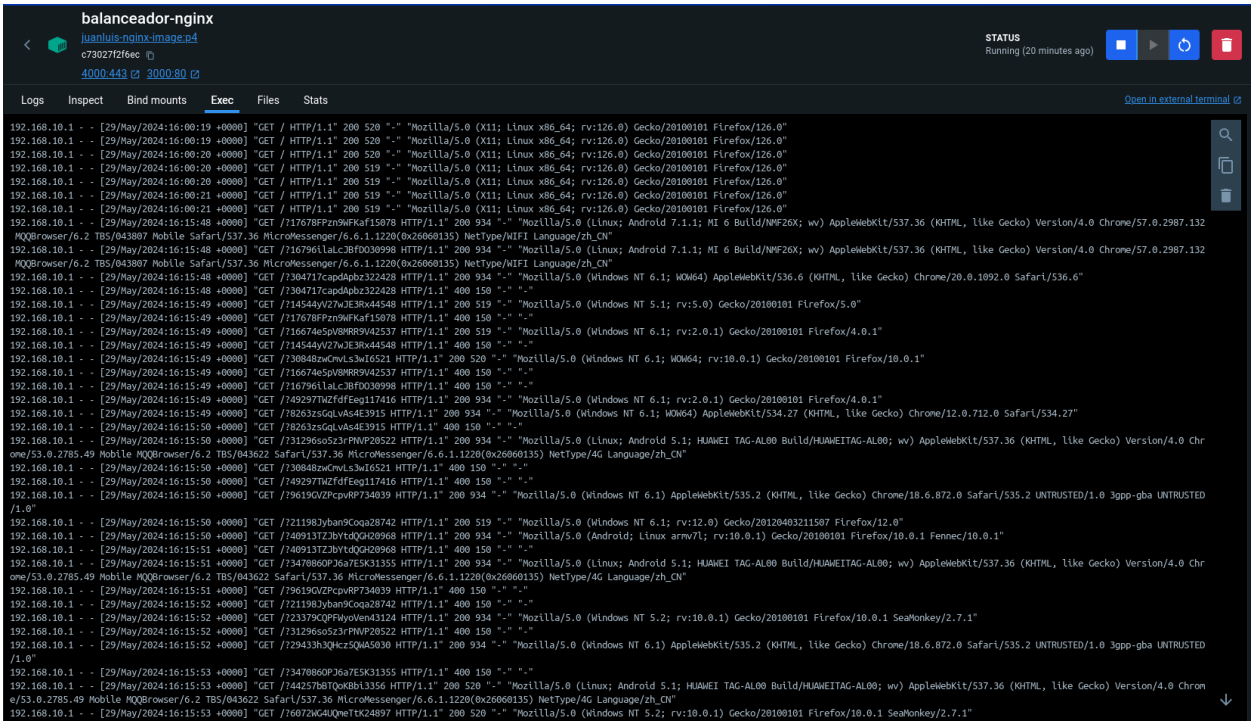

Figura 8: Monitorización de los logins.

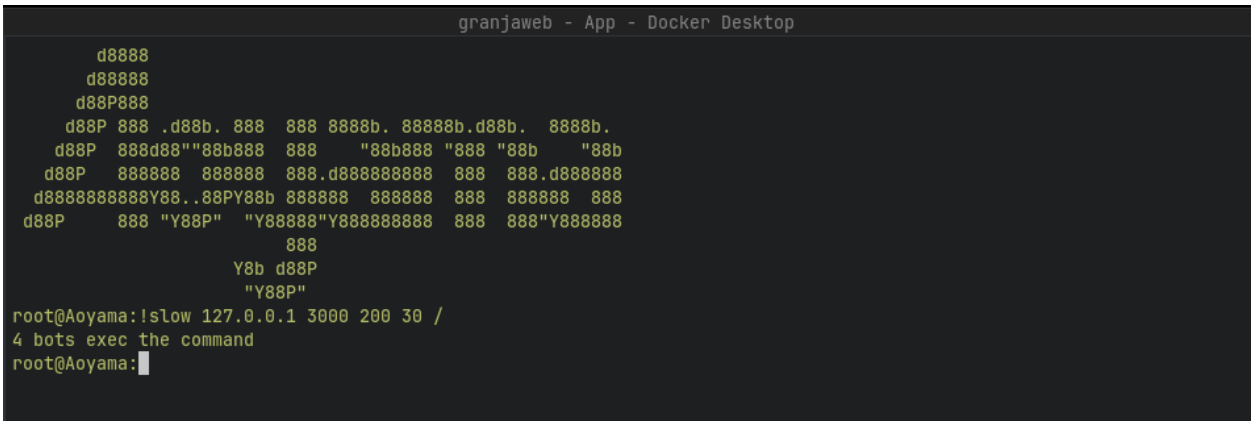

Figura 9: Ejecución del comando para Slowloris.

6.3. Slowloris

El ataque Slowloris se caracteriza por el envío de múltiples solicitudes HTTP incompletas al servidor objetivo, manteniéndose abiertas por un largo tiempo para consumir sus recursos. Si un balanceador de carga es vulnerable a este tipo de ataque, es probable que su respuesta sea similar a la observada en un ataque HTTP flood: una disminución en el rendimiento del servidor y, en casos extremos, la indisponibilidad del servicio para los usuarios legítimos.

Procedemos a realizar este comando en la terminal C&C

```
!slow 127.0.0.1 3000 200 30  /
```

- 127.0.0.1:3000 es la dirección IP y el puerto de la máquina objetivo.
- 200 es el número de hebras que se utilizarán para ejecutar el ataque.
- 30 Es el tiempo que cada conexión mantendrá abierta la solicitud HTTP (30 segundos).
- / indica que el ataque se dirigirá a la raíz del archivo index.php en el servidor objetivo.

A diferencia de HTTP Flood en un ataque Slowloris, el servidor experimenta una carga más sutil pero persistente, ya que las conexiones HTTP incompletas se mantienen abiertas y consumen recursos del servidor durante un período de tiempo prolongado.
Lanzamos el comando (fig. 9), para pararlo luego ejecutaremos un *!Stop*:
Podemos ver que el balanceador se queda esperando indefinidamente como se muestra en la figura 10.
Podemos verificar que una vez finalizado el ataque Slowloris, el servidor continúa estando inoperativo debido al impacto persistente del ataque hasta que todas las conexiones activas se cierren.
Monitorizamos los logins que acceden (fig. 11).
Al igual que en el caso del ataque HTTP Flood, el balanceador se ve inundado por conexiones GET durante un ataque Slowloris.

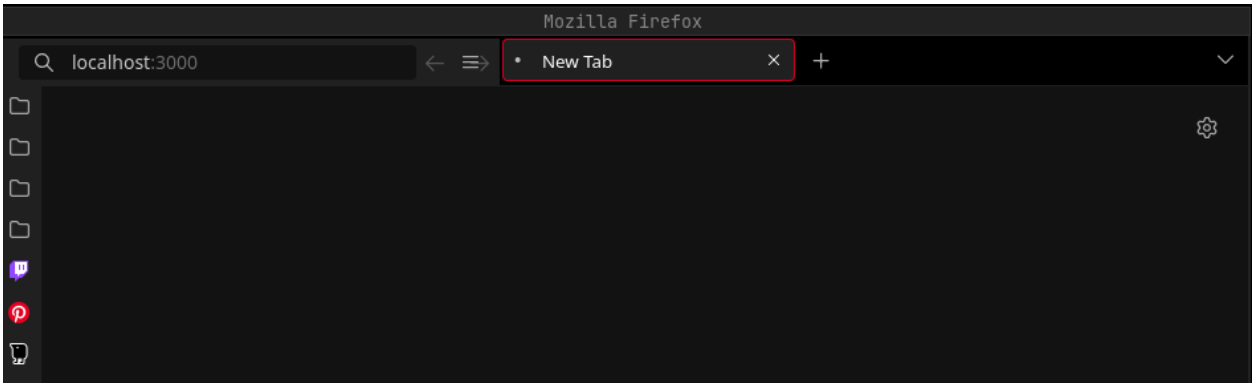

Figura 10: El balanceador se queda esperando indefinidamente.

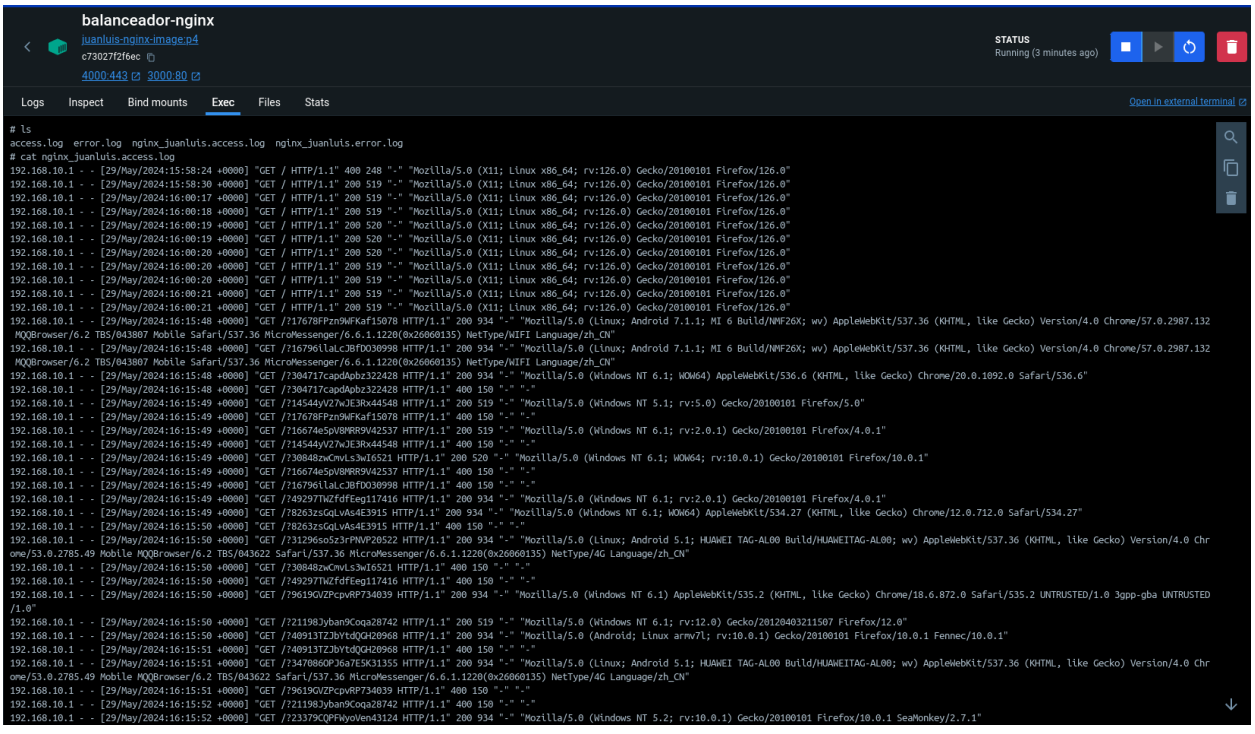

Figura 11: Monitorización de los logins.

Figura 12: Ejecución del comando para connection flood.

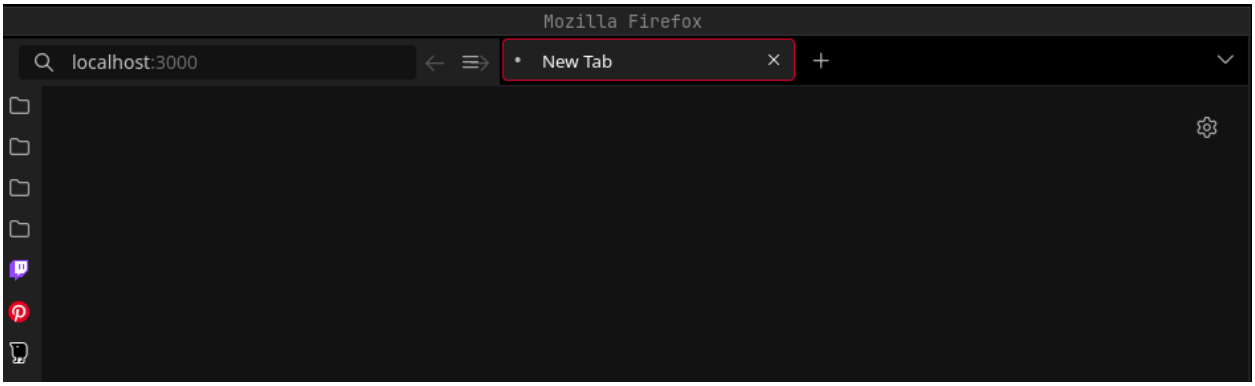

Figura 13: Caída del servidor.

6.4. Connection flood

Un ataque de 'Connection Flood' implica abrumar un servidor con un gran número de conexiones TCP simultáneas, agotando así sus recursos de red. A diferencia del ataque Slowloris, donde se mantienen conexiones TCP abiertas durante un largo período, en un ataque de Çonnection Flood"se establecen muchas conexiones simultáneas, pero no se mantienen abiertas. Esto puede sobrecargar rápidamente el servidor y dificultar el procesamiento de conexiones legítimas.

Procedemos a realizar este comando en la terminal C&C (fig. 12):

```
!cc 127.0.0.1 3000 200
```

- 127.0.0.1:3000 es la dirección IP y el puerto de la máquina objetivo.
- 200 es el número de hebras que se utilizarán para ejecutar el ataque.

Vemos en la figura 13 que el servidor vuelve a quedar inoperativo.

Estudiamos la interfaz "loütilizando Wireshark (fig. 14). La interfaz 'lo' se refiere a la interfaz de bucle invertido (loopback) en los sistemas operativos, que permite que la máquina local se comunique consigo misma. En Linux y otros sistemas Unix, la dirección IP 127.0.0.1 está asociada con esta interfaz.

La captura de tráfico sugiere un ataque de Connection Flood debido a la gran cantidad de paquetes TCP con conexiones repetidas y constantes, dirigidas a la interfaz "lo"(127.0.0.1). Esto indica un intento de consumir los recursos de la máquina objetivo manteniendo muchas conexiones abiertas al mismo tiempo.

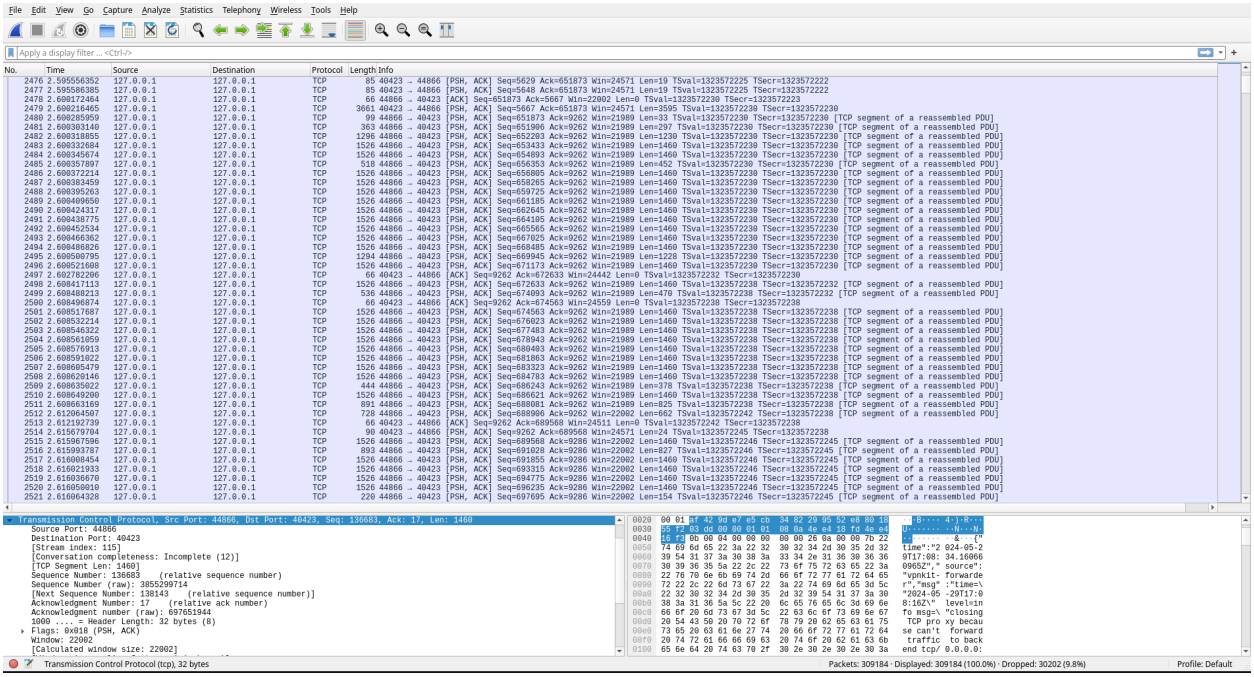

Figura 14: Interfaz 'loopback' desde WireShark.

7. Conclusiones

En conclusión este trabajo nos ha proporcionado una visión exhaustiva sobre los ataques de DDoS, destacando su evolución, funcionamiento y sus diversas estrategias empleadas para su ejecución. Hemos explorado en detalle como los ataques DDoS, representan una amenaza significativa para la disponibilidad de los servicios en línea. A través de nuestra investigación y la demostración práctica, hemos logrado cumplir con los objetivos planteados, entendiendo no solo el concepto y la diferencia entre DoS y DDoS, sino también las complejidades que envuelven la creación y operación de botnets.

En resumen, la comprensión y mitigación de los ataques DDoS son aspectos críticos en la seguridad de las aplicaciones y servicios en línea. Los ingenieros informáticos deben estar constantemente actualizados sobre las técnicas utilizadas por los atacantes, así como en las mejores prácticas de defensa. Este trabajo nos ha proporcionado una base sólida para entender los peligros de los ataques DDoS y como prepararse eficazmente para reducir su impacto, contribuyendo así a la protección de nuestros sistemas digitales.

Referencias

[1] N. Z. Bawany, J. A. Shamsi, and K. Salah. Ddos attack detection and mitigation using sdn: Methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 2017.

[2] Chad Kime. Complete guide to the types of ddos attacks, 2022. Accedido: 28 mayo 2024. URL: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/.

[3] CloudFlare. Ataque ddos de ping de la muerte, 2024. Accedido: 28 mayo 2024. URL: https://www.cloudflare.com/es-es/learning/ddos/ping-of-death-ddos-attack/.

[4] CloudFlare. Ataques ddos más conocidos — los mayores ataques ddos de la historia, 2024. Accedido: 28 mayo 2024. URL: https://www.cloudflare.com/es-es/learning/ddos/famous-ddos-attacks/.

[5] CloudFlare. What is a ddos attack?, 2024. Accedido: 28 mayo 2024. URL: https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/.

[6] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita. Botnet in ddos attacks: Trends and challenges. *IEEE Communications Surveys Tutorials*, 17(4):2242–2270, 2015. doi:10.1109/COMST.2015.2457491.

[7] INCIBE. ¿qué son los ataques dos y ddos? — ciudadanía, 2018. Accedido: 28 mayo 2024. URL: https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos.

[8] INCIBE. Ataques ddos: ¿qué son y qué puedo hacer para proteger mi empresa?, 2023. Accedido: 28 mayo 2024. URL: https://www.incibe.es/empresas/blog/ataques-ddos-que-son-y-que-puedo-hacer-para-proteger-mi-empresa.

[9] Leeon123. Aoyama, 2019. Accedido: 28 mayo 2024. URL: https://github.com/Leeon123/Aoyama.

[10] Tibor Moes. Botnet examples (2024): The 6 worst attacks of all time, 2024. Accedido: 28 mayo 2024. URL: https://softwarelab.org/blog/botnet-examples/.

[11] Wikipedia. Ataque de denegación de servicio, 2024. Accedido: 28 mayo 2024. URL: https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio.