

## **Ataques de denegación de servicio**

### **Distributed Denial of Service Attack (DDoS)**

Autores: Antonio Jesús Peláez Priego

Francisco José Pimentel Moreno

#### **Índice**

- Que es un ataque DDoS
- Tipos de ataques DDoS
- Ataques realizados más famosos y sus consecuencias
- Sanciones, legalidad y leyes
- Quienes pueden realizar este tipo de ataques y como lo hacen
- Como defenderte

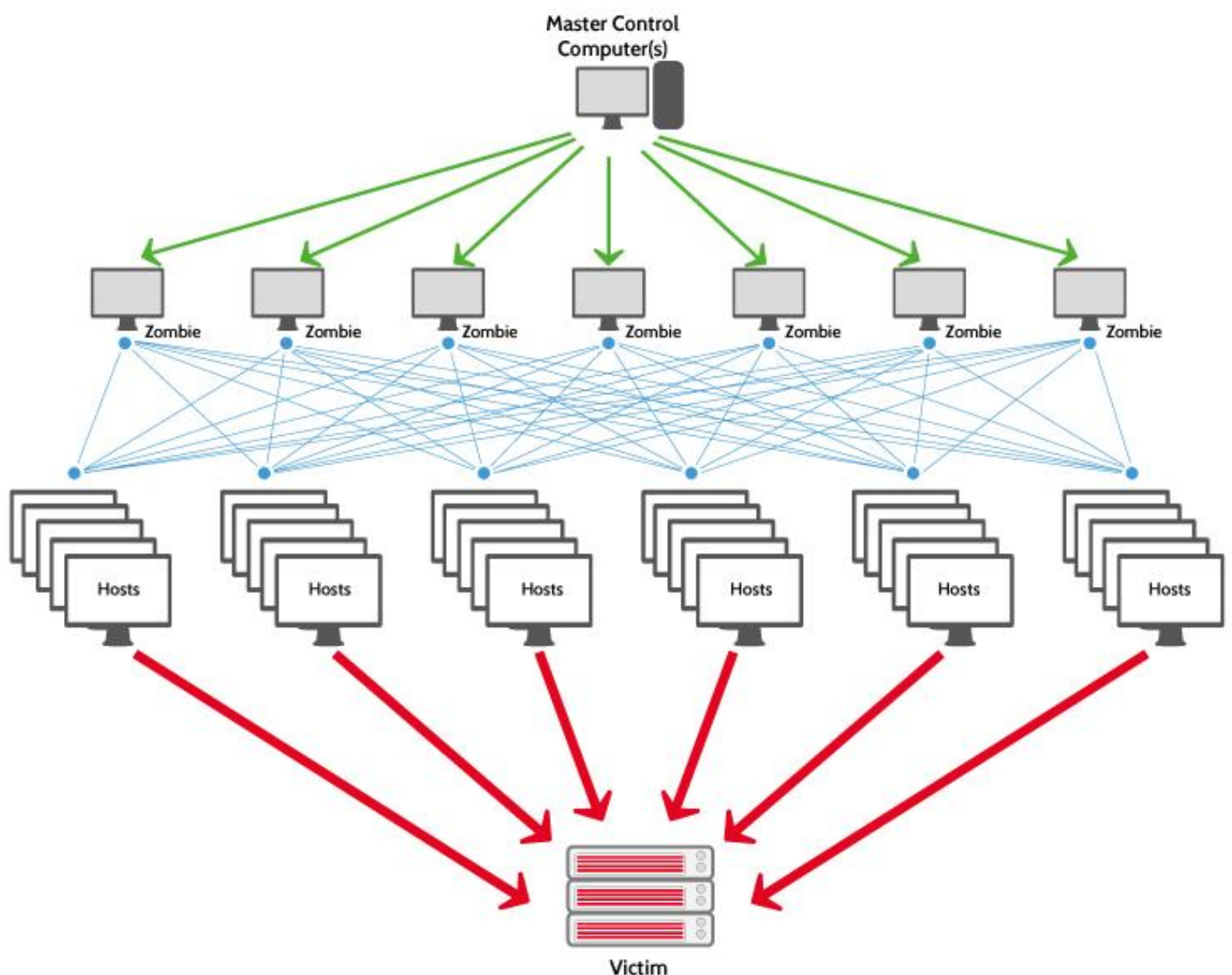
## Que es un ataque DDoS

Seguro que con una simple búsqueda en google encuentras millones de definiciones y descripciones de que es y en que consiste un ataque DDoS. Por lo que nosotros te lo vamos a explicar de la forma más sencilla posible, y desde nuestro punto de vista.

El **objetivo principal** de estos ataques es inhabilitar nuestro servidor para que deje de ofrecer los distintos servicios que estaba sirviendo, además existe la posibilidad de pérdida de datos durante un ataque.

Esto **se consigue** sobrecargando el ancho de banda del servidor o capando sus recursos hasta agotarlos. Se puede hacer de diversas formas, básicamente el funcionamiento es el siguiente:

Se envían multitud de peticiones simultáneamente desde múltiples puntos de la red, estos “puntos” pueden ser ordenadores o servidores infectados (wordpress desactualizados, ordenadores personales infectados...) que alguien utiliza como “zombies” usando parte de su ancho de banda para lanzar el ataque con todos estos “puntos” a la vez, también estos “puntos” pueden ser servidores comprados y programados para este propósito normalmente con una muy buena conexión.



## Tipos de ataques DDoS

Existen tres estrategias que pueden inhabilitar un sitio web, servidor o infraestructura:

- **Ancho de banda:** Ataque que consiste en saturar la capacidad de la red del servidor, haciendo que sea imposible llegar a él.
- **Recursos:** Ataque que consiste en agotar los recursos del sistema de la máquina, impidiendo que esta pueda responder a las peticiones legítimas.
- **Explotación** de fallos de software: Categoría de ataque que explota fallos en el software que inhabilitan el equipo o toman su control.

Aunque realmente, dentro de estos tres tipos mencionados anteriormente encontramos muchos subtipos de ataques, y cada día aparecen nuevos tipos.

Ahora debemos recordar el modelo OSI, estos ataques operan en varias de las capas de este modelo:

- **Capa 3:** Capa de red encargada del direccionamiento y encontrar la mejor ruta.
- **Capa 4:** Capa de transporte.
- **Capa 7:** Capa de aplicación.

Nombre del ataque	Capa	Tipo	Explicación del ataque
ICMP echo request flood	3	Recursos	También denominado Ping Flood. Envío masivo de paquetes (ping), que implican una respuesta por parte de la víctima (pong) con el mismo contenido que el paquete de origen.
IP Packet Fragment Attack	3	Recursos	Envío de paquetes IP que remiten voluntariamente a otros paquetes que nunca se envían, saturando así la memoria de la víctima.
SMURF	3	Ancho de banda	Ataque por saturación ICMP que usurpa la dirección de origen para redirigir las múltiples respuestas hacia la víctima.
IGMP Flood	3	Recursos	Envío masivo de paquetes IGMP (protocolo de gestión de grupos de internet)
Ping of Death	3	Explotación	Envío de paquetes ICMP que explotan fallos del sistema operativo
TCP SYN Flood	4	Recursos	Envío masivo de solicitudes de conexión TCP
TCP Spoofed SYN Flood	4	Recursos	Envío masivo de solicitudes de conexión TCP usurpando la dirección de origen
TCP SYN ACK Reflection Flood	4	Ancho de banda	Envío masivo de solicitudes de conexión TCP a un gran número de máquinas, usurpando la dirección de origen por la dirección de la víctima. En ancho de banda de la víctima queda saturada por las respuestas a dichas peticiones
TCP ACK Flood	4	Recursos	Envío masivo de acuses de recibo de segmentos TCP
TCP Fragmented Attack	4	Recursos	Envío de segmentos TCP que remiten voluntariamente a otros que nunca se envían, saturando la memoria de la víctima
UDP Flood	4	Ancho de banda	Envío masivo de paquetes UDP (sin necesidad de establecer conexión previa)
UDP Fragment Flood	4	Recursos	Envío de datagramas que remiten voluntariamente a otros datagramas que nunca se envían, saturando así la memoria de la víctima.
Distributed DNS Amplification Attack	7	Ancho de banda	Envío masivo de peticiones DNS usurpando la dirección de origen de la víctima hacia un gran número de servidores DNS legítimos. Como la respuesta tiene un mayor volumen que la pregunta, el ataque se amplifica.
DNS Flood	7	Recursos	Ataque de un servidor DNS mediante el envío masivo de peticiones.
HTTP(S) GET/POST Flood	7	Recursos	Ataque de un servidor web mediante el envío masivo de peticiones.
DDoS DNS	7	Recursos	Ataque de un servidor DNS mediante el envío masivo de peticiones desde un gran número de máquinas controladas por el atacante.

## Ataques realizados más famosos y sus consecuencias

### Los hackers toman la bandera de Wikileaks y piratean Visa, Mastercard y Paypal.

En diciembre de 2010... Ataques y contraataques a favor y en contra de Wikileaks a través de internet se pusieron en marcha por un grupo voluntarios de piratas informáticos. Ese miércoles, consiguieron bloquear los sistemas informáticos de Visa y Mastercard, después de que ambos bloqueasen los pagos a Wikileaks.

La 'Operación vengar a Assange' organizada por Anonymus a raíz del cerco aplicado a Wikileaks y su creador consiguió derribar parte de los sistemas informáticos de Mastercard.

Los hackers informaban, a través de un canal denominado IRC (Internet Relay Chat) desde el que se dirigió el ataque a mastercard, que más de 1.800 bots estaban inundando con ataques distribuidos de denegación de servicio (DDOS) a [www.mastercard.com](http://www.mastercard.com). Y la empresa reconocía dificultades en algunos de sus servicios.

Pero la guerra no acaba aquí, mientras otros usuarios del canal informaban del progreso del ataque con mensajes sobre el estado de las operaciones de Mastercard en países como Suecia, Sri Lanka o México o sobre la evolución de las acciones de la compañía de tarjetas de crédito en la Bolsa de Nueva York. Los responsables de del grupo Anonymous anunciaron a última hora del día que el nuevo objetivo a atacar era Visa.

Efectivamente, se anunciaba por medio de las redes sociales (Twitter en este caso) que la página de VISA se había caído.

Paypal también se vio afectada por un ataque de estos hackers, aunque tras el ataque, Paypal entregó a Wikileaks el dinero de las donaciones que le había retenido. Según Paypal, su decisión se basó únicamente en la deontología profesional amparada bajo su código de conducta.

Paypal señaló que el ataque DDOS contra [ThePayPalblog.com](http://ThePayPalblog.com) durante 8 horas causó que el blog sufriese 75 interrupciones de servicio.

**Como consecuencia** de estos ataques bajo la popularidad de las tarjetas de crédito especialmente de las mencionadas anteriormente como Visa y MasterCard produciendo un grave malestar a sus clientes y la pérdida de confianza en las tarjetas de crédito. También se comentó que se pudieron filtrar algunos datos personales de los clientes, pero la misma mastercard lo negó en un comunicado. Paypal también perdió popularidad, esto hizo que emitieran un comunicado en el que exponían que se limitaban a cumplir la ley de los EEUU, ya que dicho departamento de estado había afirmado que las actividades de wikileaks eran ilegales. Esto también influye en una pérdida de dinero que no se puede estimar ya que no sabemos cuánto tiempo estuvo el servicio caído.

## Ataque a PlayStation Network

La razón de este ataque contra Sony vino a raíz de la puesta en marcha por parte de la compañía de acciones judiciales contra los usuarios Geohot y Graf-Chokolo, quienes habían logrado “hackear” la PS3; en el caso del primero, Sony le reclama 750.000 euros de multa.

Esto llamo la atención de Anonymous que actúan allí donde consideran que se ha vulnerado algún derecho del usuario. Anonymous considero como un “abuso judicial” lo que Sony pedía a sus amigos de Geohot y Graf-Chokolo y decidieron intervenir por ellos en un comunicado en el que se podía leer: “Felicitaciones Sony, lograste llamar la atención de Anonymous. Tus recientes acciones legales contra nuestros queridos hackers, GeoHot y Graf\_Chokolo, nos han alarmado y difícilmente serán olvidados”. A partir de aquí los ataques no se hicieron esperar y es que la noche del 5 de abril de 2011, Sony.com cayó de manera intermitente, mientras PlayStation.com se mantenía más o menos estable.

El lunes 11 de abril los usuarios manifestaban las dificultades que tenían para entrar en la plataforma de PSN. Sony lo achacaba a un problema de mantenimiento y que pronto cesaría el problema, pero desde Anonymous comunicaban que eran ellos los causantes pero que cesarían la actividad por no entrar en su estrategia. Caso que no sucedió con un cese de las hostilidades del famoso grupo de hacktivistas contra la multinacional japonesa que siguió con los ataques hasta verse satisfecho con el resultado.

Así fue el 21 de abril Sony cerraba PlayStation Network por mantenimiento. El día antes, el miércoles 20 de abril, los usuarios experimentaron problemas de estabilidad en sus conexiones, e incluso algunos no podían acceder al servicio con normalidad. Eran los primeros síntomas de lo que estaba por venir.

Una semana más tarde, y sin el servicio restaurado, Sony informa a los usuarios de que ha habido una vulnerabilidad en la seguridad del servicio, y que sus datos personales y financieros podrían haber sido accedidos por un atacante externo.

Finalmente, el martes 26 de abril, Sony anunciaba que cerraba el servicio de PlayStation Network debido a la intrusión en su sistema.

**Consecuencias:** incertidumbre entre los usuarios por la protección de sus datos personales y tarjetas de crédito durante casi el mes que tardó Sony en restaurar el servicio. Esto conlleva a la pérdida de usuarios por parte de la marca japonesa. Sin hablar del coste económico tanto por reanudar el servicio como por luchar contra el ataque.

## Un niño canadiense hackea sitios gubernamentales por encargo de Anonymous

Un niño de 12 años de edad de Montreal, Canadá, ha reconocido que hackeó sitios web del Gobierno y la Policía como parte de una operación de Anonymous que tuvo lugar en 2012.

Al parecer, el muchacho ha hackeado varios sitios web comerciales, el del Instituto de Salud Pública de Quebec, el de la policía de Montreal y el sitio de una organización gubernamental de Chile. El daño que causó se ha estimado en alrededor de 60.000\$ (41.700€).

El joven hacker, cuyo nombre no ha sido revelado, es un estudiante de 5º grado. Él ha sido un apasionado de los ordenadores desde que tenía nueve años.

Sus acciones no fueron motivadas políticamente. En cambio, ofreció información a los hacktivistas de Anonymous a cambio de videojuegos, según informa Toronto Sun.

Las autoridades dicen que el niño lanzó ataques distribuidos de denegación de servicio (DDOS), alteró sitios web y filtró datos de sus servidores.

Él se ha declarado culpable de tres cargos relacionados con el hacking. Otros individuos también fueron arrestados en relación con los ataques de Anonymous. Sin embargo, parece que el muchacho de 12 años de edad fue el que ayudó a los demás a penetrar en los sitios web.

## Sanciones, legalidad y leyes

Este tipo de ataques lo suelen realizar grupos organizados y son difíciles de capturar debido a la organización que tienen. Pero cuando se logra capturar al infractor y atribuirle los cargos por este tipo de ataques las sanciones que se les imponen no son excesivamente grandes. Nunca o casi nunca pasan de una mera sanción económica por el daño causado o en casos más graves a esta sanción económica se le añade de 6 meses a tres años de cárcel.

Con los cambios en la ley que limita el uso de los datos que los prestadores están obligados a preservar a efectos de identificar al abonado y el acceso a ellos por parte de un determinado cargo dentro del sistema. La legalidad de estos ataques está penada cosa que antes no lo estaba. Aunque actualmente se debate la ilegibilidad de estos ataques. Aunque está penado en el código penal a nivel de España.

La ley por la que se rige y juzga estos ataques queda reflejada en:

El Código Penal por la Ley Orgánica 5/2010, de 22 de junio, y establece el siguiente redactado para el artículo 264, apartados 1 y 2:

1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.
2. El que, por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

## Quienes pueden realizar este tipo de ataques y como lo hacen

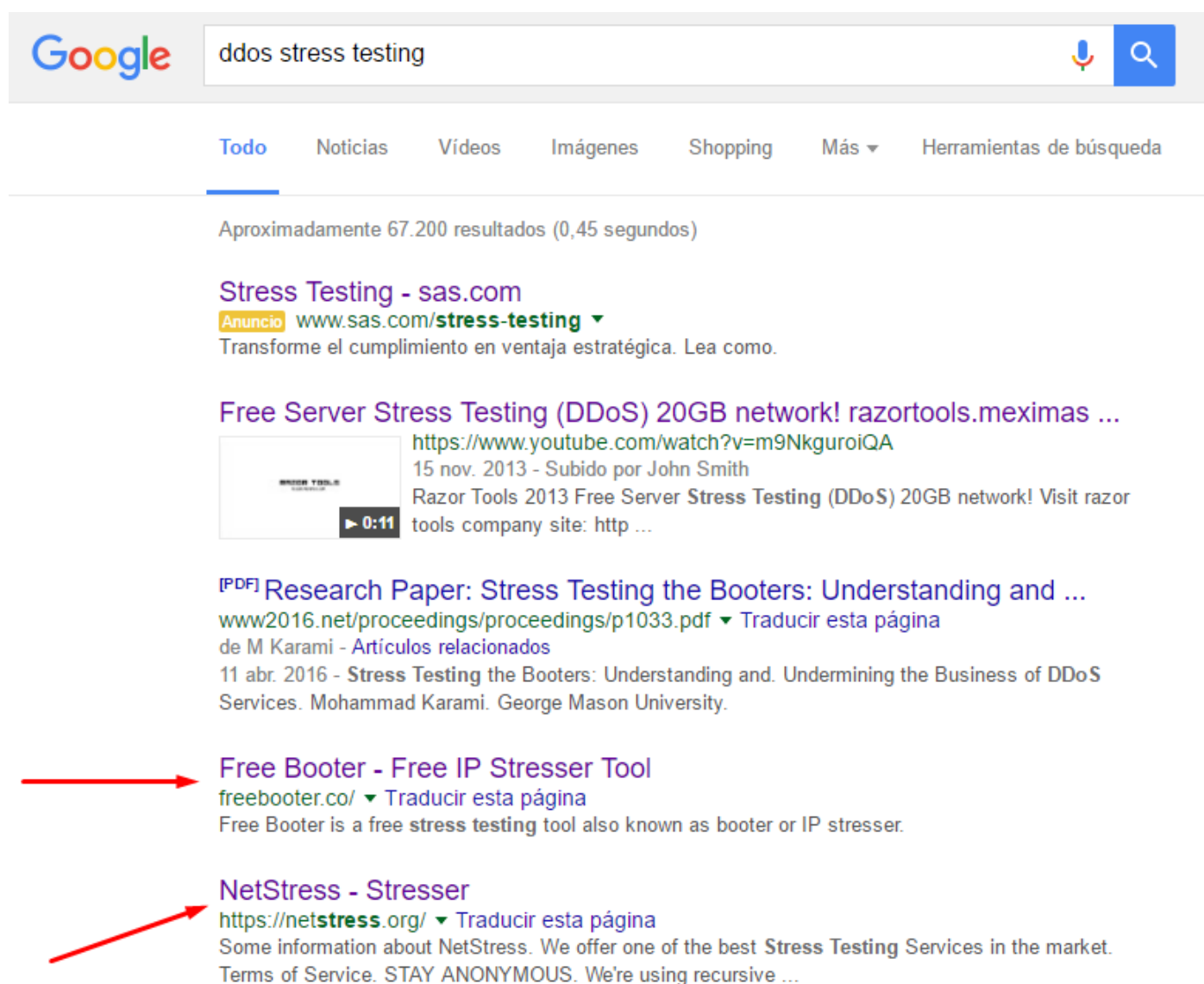
Hace unos años este tipo de ataques eran realizados por expertos, hackers, gente con conocimiento en el área de la informática.

Pero claro, esto era hace unos años, y como todo, las cosas evolucionan a veces a peor y a veces a mejor. Hoy día cualquiera con conexión a internet y un par de euros en bitcoin o paypal puede realizar este tipo de ataques.

Y os preguntareis... **¿cómo?**

Actualmente los ataques de denegación de servicio se han convertido en un producto muy demandado por internet, y me aventuraría a decir que ya hay miles de sitios donde por 2-5€ podemos empezar a lanzar ataques de gran envergadura.

Pongamos un ejemplo de una simple búsqueda en google:



Google search results for "ddos stress testing".

Approximately 67.200 results (0,45 segundos)

**Stress Testing - sas.com**  
Anuncio [www.sas.com/stress-testing](http://www.sas.com/stress-testing) ▾  
Transforme el cumplimiento en ventaja estratégica. Lea como.

**Free Server Stress Testing (DDoS) 20GB network! razortools.meximas ...**  
<https://www.youtube.com/watch?v=m9NkguroiQA>  
15 nov. 2013 - Subido por John Smith  
Razor Tools 2013 Free Server Stress Testing (DDoS) 20GB network! Visit razor tools company site: http ...

**[PDF] Research Paper: Stress Testing the Booters: Understanding and ...**  
[www2016.net/proceedings/proceedings/p1033.pdf](http://www2016.net/proceedings/proceedings/p1033.pdf) ▾ Traducir esta página  
de M Karami - Artículos relacionados  
11 abr. 2016 - Stress Testing the Booters: Understanding and. Undermining the Business of DDoS Services. Mohammad Karami. George Mason University.

**Free Booter - Free IP Stresser Tool**  
[freebooter.co/](http://freebooter.co/) ▾ Traducir esta página  
Free Booter is a free stress testing tool also known as booter or IP stresser.

**NetStress - Stresser**  
<https://netstress.org/> ▾ Traducir esta página  
Some information about NetStress. We offer one of the best Stress Testing Services in the market. Terms of Service. STAY ANONYMOUS. We're using recursive ...

Solo en la primera página de google nos encontramos con más de 2 sitios que ofrecen "stress test", incluso uno lo hace gratuitamente.



Bueno, esto no es todo, investigemos un poco más, vamos a un foro de hackers a ver que se cuece por allí con este tema, visitaremos hackforums.net.

Welcome to HackForums.net Current time: 05-18-2016, 09:19 AM

# Hack Forums

Packets, Punks, and Posts

Home Upgrade Search Members Extras Wiki Help Follow Contact

Welcome back, **pessadillas**. You last visited: 04-15-2016, 06:25 AM (**User CP** — Log Out)  
View New Posts | Your Threads | Your Posts | Private Messages (Unread 0, Total 0) Open Buddy List

## Hack Forums

Common Hack Tech Code Game Groups Web GFX **Market** Money

### Marketplace

Forum	Threads/Posts	Last Post
<b>Marketplace Discussions</b> This is to be used for rules, policies, feedback, and general discussions about the HF Marketplace. Please read the stickies in this section before conducting business here. Moderated By: Diabolic Free Services and Giveaways Deal Disputes Appraisals and Pricing	196,663 2,630,225	<b>Make Easy Money [15 minut...</b> Today 09:13 AM by Jacoder23
<b>Premium Sellers Section</b> This area is only for upgraded member sales threads. Server Stress Testing Cryptography and Encryption Market	80,790 1,550,910	<b>[LEARN HOW TO DOX] Privata...</b> Today 08:56 AM by Mouse♥
<b>Secondary Sellers Market</b> This is a sellers section open to all members. We advise extreme caution in all deals here. Sales threads must follow the policies of HF and we expect you to read them in the help documents. Virtual Game Items Traders Topics Member Auctions	201,108 1,217,280	<b>CS:GO items for RS Gold</b> Today 09:10 AM by Pimp.
<b>Online Accounts</b> If you're selling an OG internet account this is your section. Top sellers include social networking accounts, popular IM names, and excellent email addresses. Non-Free Accounts Gamertags	44,836 513,979	<b>Need this tag [From the r...</b> Today 09:18 AM by Sevn Alias

Una sección dedicada para la venta de servicios para realizar ataques...

Pages (200): 1 2 3 4 5 ... 200 Next >

### Server Stress Testing

SYT Mark

Thread / Author	Replies	Rating	Last Post [asc]
<b>Important Threads</b>			
<b>SYNSTRESS.NET</b> (Pages: 1 2 3 4 ... 49 ) Joey	480	4.5	Today 04:41 AM Last Post: Klaus
<b>THUNDER STRESS // Mobile APP // 500G + 500K RS / 100% Custom / RAW Methods / BEST VIP</b> (Pages: 1 2 3 4 ... 37 ) Taranis	363	4.5	Yesterday 02:50 PM Last Post: Taranis
<b>[CLICKBOOT] ~ MOST RELIABLE BOOTER   195+ Gbps / 20+k R/s TN   100% Uptime   Autobuy</b> (Pages: 1 2 3 4 ... 11 ) Tando	102	4.5	Yesterday 02:27 PM Last Post: Tando
<b>**New Source**[Vouched] Str3ssed Networks   1+ Year Running   210Gbps+TN   L4&amp;L7</b> (Pages: 1 2 3 4 ... 32 ) AnonNinja™	318	4.5	Yesterday 10:35 AM Last Post: AnonNinja™
<b>Normal Threads</b>			
<b>CriticalBOOT   MOST POWERFUL   Stop/Resume/Renew   VIP   TCP-FLAG OVH ABUSE   300Gbps</b> (Pages: 1 2 3 4 ... 101 ) Stratos	1,009	4.5	Today 08:07 AM Last Post: Moeseeph
<b>vDos Stresser 300Gbps+TN L4&amp;L7 CC/BTC 17 Attack methods! VIP Nodes Since 2012!</b> (Pages: 1 2 3 4 ... 34 ) Apple J4ck.	330	4.5	Today 07:55 AM Last Post: Klaus
<b>Selling IRC Spots:: Nulls NFO, Downs Staminus, Hyperfilter, wreks everything!!!!</b> Layer7 Attacks	6	4.5	Today 07:53 AM Last Post: Virgin Retard
<b>KRONOS BOOTER   L4-L7   10G +25 k r/s PER ATK  JSBYPASS   POSTDATA   INSTANT DELIVERY</b> (Pages: 1 2 3 4 ... 6 )	56	4.5	Today 05:54 AM Last Post: MeNoSkidPls

Más de **200 páginas** ofreciendo el mismo tipo de servicios, y echadle un ojo a la potencia de los ataques...

Pero claro, diréis eso costará una pasta y solo lo podrá hacer gente con mucho dinero para quitarse de en medio a la competencia... Veamos si es cierto, vamos a ver cuanto cuesta alguno de los que ofrecen en la sección de importantes.

The screenshot shows the HUNDRETTRESS website with a dark theme. The navigation bar includes links for HOME, ABOUT, WHY US, PRICING, CONTACT, BLOG, and LOGIN. The main content area features three pricing plans, each with a 'Sign Up' button. The 'Basic' plan is highlighted with a red box around its price.

Plan	Starting Price	Features
Basic	Starting from \$13	Mobile APP & Target Tracking 1 Concurrent Attack 800 Seconds Boot time 400Gbps + 500k R/S Network Methods : All basic L4 + L7
Pro	Starting from \$25/mo	Mobile APP & Target Tracking 1 Concurrent Attack 1800 Seconds Boot time 400Gbps + 500k R/S Network Methods : L4/L7 Basic + Custom Methods
Elite	Starting from \$56	Mobile APP & Target Tracking 1 Concurrent Attack 3600 Seconds Boot time 500Gbps + 800k R/S + Private Network Methods : All L4/L7 and Raw Methods

Por 13 dólares tenemos la capacidad de lanzar ataques de **400Gbps** de potencia o **500 mil** peticiones por segundo durante algo mas de 5 minutos. Además incluye aplicación para el móvil para un día que nos apetezca estar atacando continuamente estemos donde estemos...

Y ahora seguramente os estéis preguntando... **¿Por qué no cierran estas webs si supuestamente este tipo de ataques son ilegales?**

La mayoría de estos sitios incluyen algo como esto en sus términos de uso:

The screenshot shows the 'TERMS & CONDITIONS' page. It lists seven terms, with the first three underlined in red. A close button (X) is visible in the top right corner.

- 1.) This professional stress testing service can ONLY be used to test your own servers' strengths against DDOS attacks.
- 2.) We won't be liable for any damages caused with the attacks you send using Nulled Network, it is at your OWN risk.
- 3.) You're not allowed to attack any website which ends with .gov or .edu, is associated with any Federal Bureau of Investigation or any other government websites.
- 4.) You're not allowed to 'hack' accounts or attempt to brute force any accounts with any means. This means using a dictionary attack list.
- 5.) You're not allowed to access the website using TOR. This causes issues with your IP address and we may by mistake ban you thinking you have shared your account.
- 6.) You're not allowed to re-sell your account for any currency, including crypto currency.
- 7.) You're not allowed to use this service to exploit any of our features. This includes Cross Site Scripting vulnerabilities or any vulnerabilities of the sort. If you find one and report one - we'll gladly give you an upgrade.

Se supone, que ellos te ofrecen el servicio para que tú pruebes la protección de tu propio servidor, pero claro ellos no saben si la IP o la web que pones como objetivo es tuya o es de tu competencia o es de tu primo. Por lo que se lavan las manos y no se hacen responsable del daño que puedas hacer con esto. ¿Interesante verdad? Solo se preocupan si atacas webs del gobierno, en cuyo caso ellos podrían ser parcialmente responsables del ataque.

Y en resumen, así funciona esto, por lo que, si aún no has sido atacado, es raro, empieza a montar tu defensa ya antes de que sea tarde.

## Como defenderte

Como dijimos anteriormente cuando explicábamos quien puede realizar ataques DDoS, las cosas evolucionan, y al mejorar la facilidad para hacer ataques, también han mejorado los métodos para protegernos contra estos ataques.


Por internet podemos encontrar muchísimo material para proteger nuestro servidor contra ataques, además de que también podemos encontrar muchísimas empresas que se dedican a hacer ese trabajo por ti.

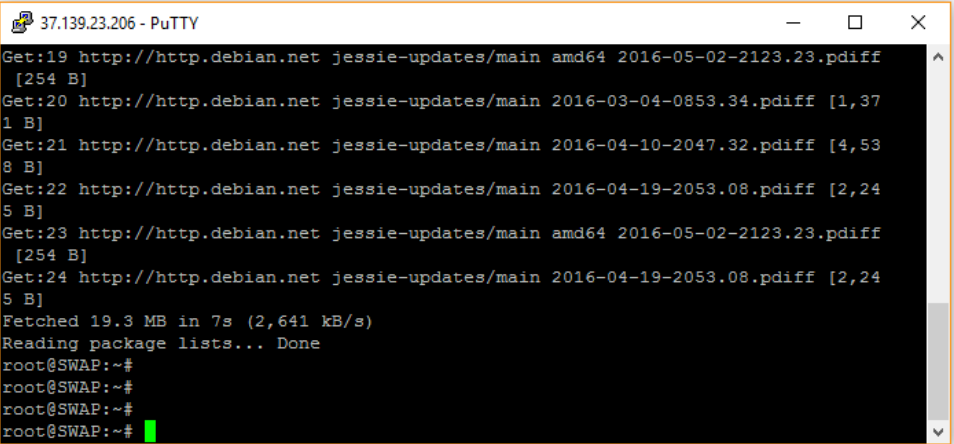
Con lo que os voy a ofrecer 3 opciones:

- Contratar un servicio de protección a alguna de las muchas empresas que lo ofrecen y despreocuparnos del tema.
- Configurar por nosotros mismos la protección
- Combinar las dos anteriores

Esta claro que lo mejor es la última opción, nosotros aquí os vamos a mostrar como configurar una protección más o menos decente y como combinarla con la primera opción.

Las pruebas las haremos en un servidor virtual que hemos comprado en digital ocean.

Img	Name	IP Address	Created
	<b>SWAP</b> 1 GB Memory / 30 GB Disk / AMS2	37.139.23.206	2 minutes ago <a href="#">More</a>

En primer lugar instalaremos apache, para dejar nuestro servidor web funcionando.

Ahora lo que haremos sera bloquear todas las conexiones a nuestro servidor, dejando únicamente abiertos los puertos 80 y 22.

Todo esto lo haremos por medio de IPTABLES y creando un script bash que ejecute todas nuestras reglas:

Versión 1 del script:

<http://pastebin.com/2PTF9UYD>

Para la versión 2 vamos a agregar más reglas y restricciones (10 conexiones tcp por minuto) a nuestro script:

<http://pastebin.com/jiLHceYq>

Para la versión 3 agregaremos reglas para bloquear los ataques más comunes y otros un poco más específicos:

<http://pastebin.com/jj0iXHnh>

Ahora vamos a pasar a la práctica:

Con el comando:

```
netstat -na | awk '{print $5}' | cut -d. -f1-4 | sort -n | uniq -c | sort -n
```

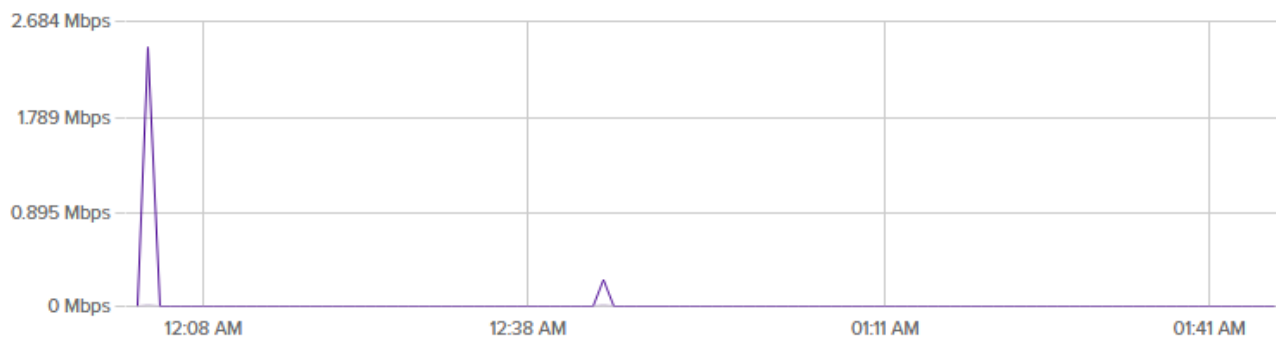
Obtenemos las Ips que estan conectadas a nuestro servidor:

```
37.139.23.206 - PuTTY
root@SWAP:~# netstat -na | awk '{print $5}' | cut -d. -f1-4 | sort -n | uniq -c | sort -n
 1 217.216.34.60:54189
 1 Address
 1 and
 1 (servers
 1 State
 6 ]
 7 :::*
 7 0.0.0.0:*
13 DGRAM
16 STREAM
root@SWAP:~#
```

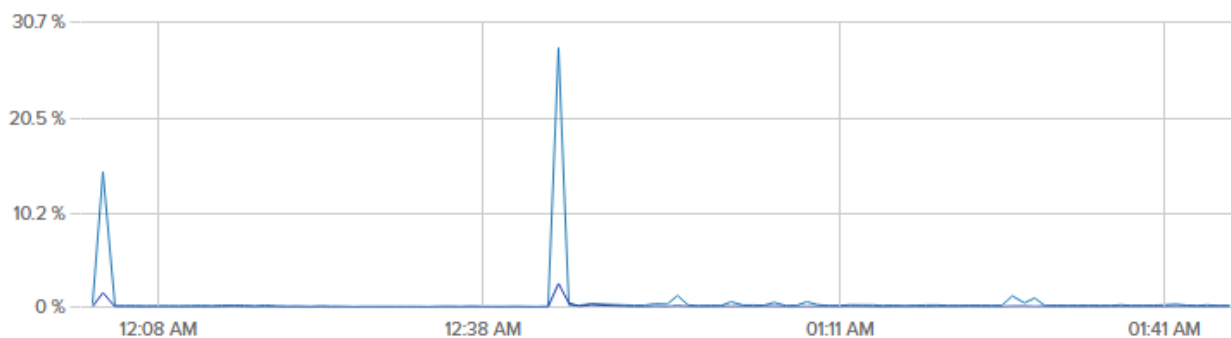
También mostraremos las gráficas de uso de red proporcionadas por Digital Ocean:

## Bandwidth - Public

6 hours



## CPU



Como vemos ahora mismo solo esta conectada mi IP, ahora probaremos a tirar un ataque sin IP tables.

Lo primero desactivamos nuestras reglas:

```
iptables -F
```

```
iptables -X
```

```
iptables -t nat -F
```

```
iptables -t nat -X
```

```
iptables -t mangle -F
```

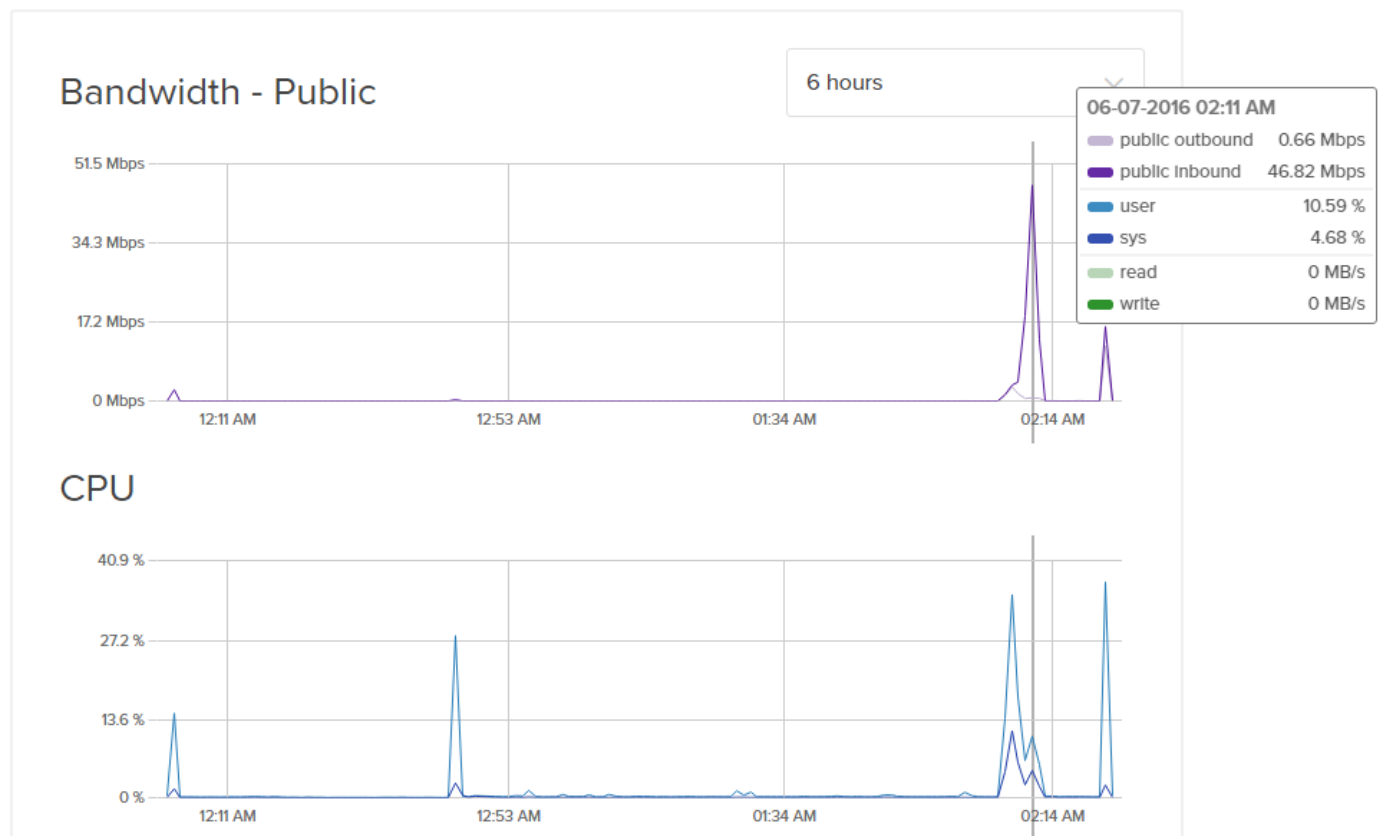
```
iptables -t mangle -X
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

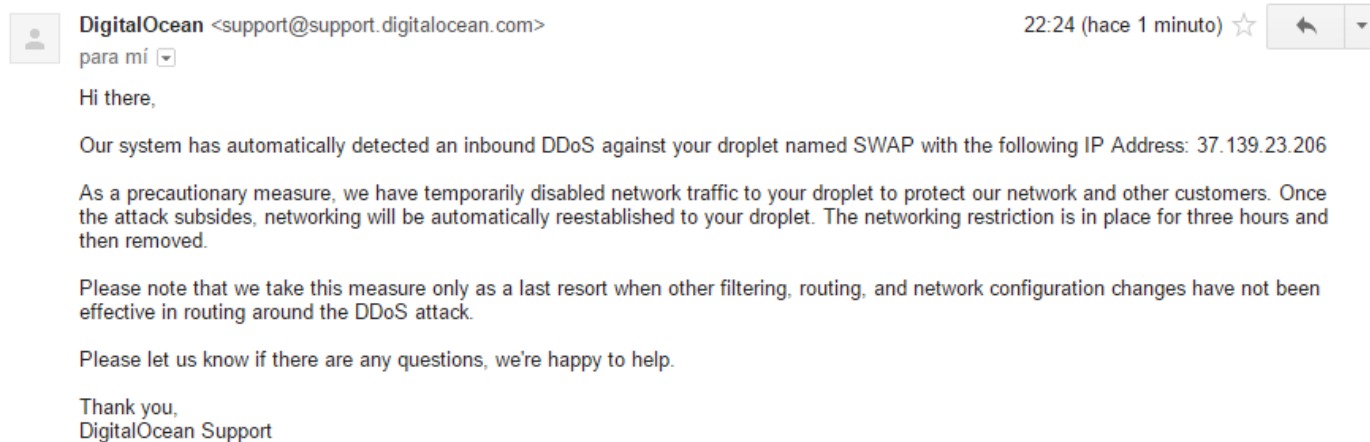
```
iptables -P FORWARD ACCEPT
```

Y bueno como era de esperar... tras lanzar el ataque al servidor nos quedamos sin conexion y no podemos ver las Ips que teniamos conectadas, asi que dejo la grafica de digitalocean:



Ahora vamos a lanzar el mismo ataque con nuestras iptables activadas tras ejecutar el script 3.

Aunque ahora sera complicado hacer esto porque hemos recibido un bonito correo de nuestro proveedor DigitalOcean:



Debido a este inconveniente, continuaremos las pruebas en otro servidor virtual adquirido en la empresa OVH.

Ahora vamos a lanzar el mismo ataque con nuestras iptables activadas tras ejecutar el script 3.

Aunque también perdemos la conexión, y recibimos otro bonito correo.



Por lo menos no han cortado la conexión del vps.

Agregaremos algunas configuraciones en el kernel para ver si así podemos contener el ataque:

Para esto debemos modificar el fichero `/etc/sysctl.conf`

Y para aplicar las estas configuraciones ejecutamos: `sysctl -p`

Aquí dejamos el fichero con las configuraciones: <http://pastebin.com/PytT3mtc>

Pues nada seguimos igual... se ve que el “stress test” que compramos es muy potente.

Así que vamos a comenzar con la opción de combinar la protección que nos ofrece cloudflare más la que hemos instalado que parece que no funciona adecuadamente.

Para esto hemos registrado el dominio `swapddostest.ml` y lo hemos registrado en cloudflare, además hemos modificado el archivo `virtualhost` de nuestro vps para que sirva el contenido de esta web.

Ahora modificaremos nuestro firewall para permitir conexiones entrantes desde las Ips de cloudflare:

Las Ips las podemos consultar aquí: <https://www.cloudflare.com/ips/>

Y probamos a atacar de nuevo...

Ahora no notamos nada y la web funciona correctamente.



## Cloudflare resolver

Aunque existen herramientas llamadas cloudflare resolver, por ejemplo: <http://iphostinfo.com/cloudflare/>



[Ip Lookup](#) | [Cloudflare IP Resolver](#) | [FAQ](#) | [Contact](#)

### CloudFlare IP Resolver

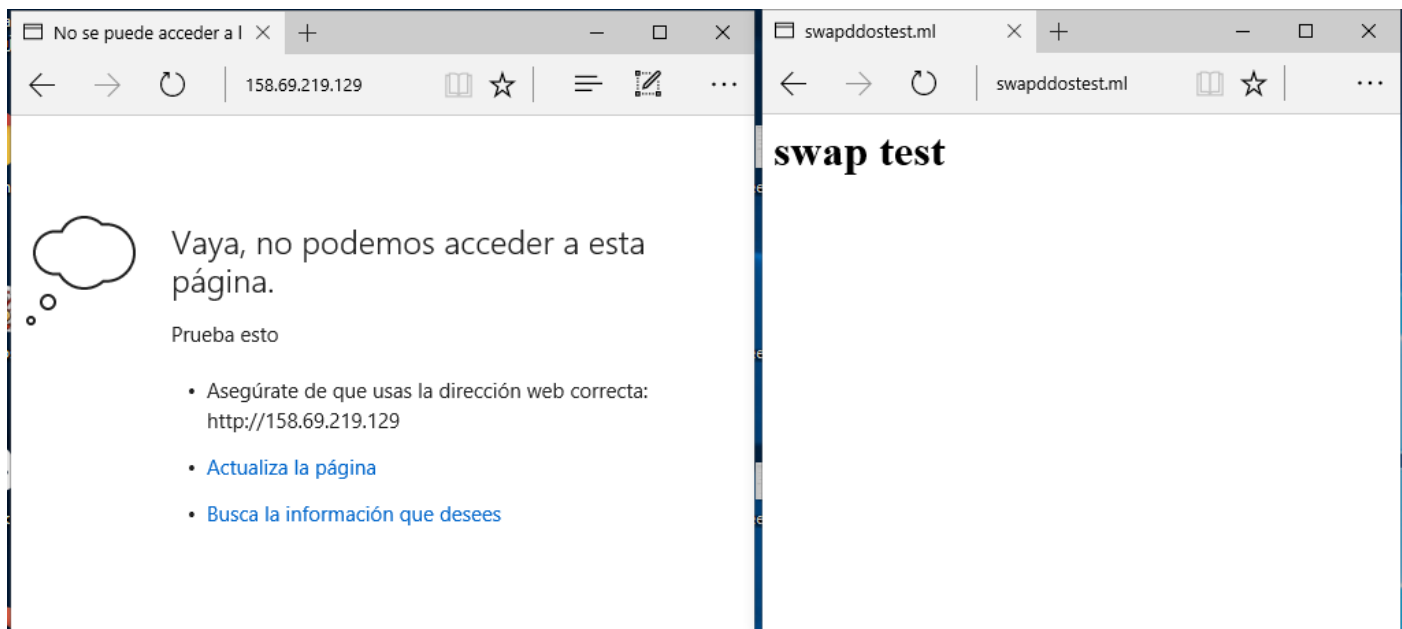
**Domain: swapddostest.ml**

DNS	IP
mail.swapddostest.ml	158.69.219.129
direct.swapddostest.ml	No DNS record
direct-connect.swapddostest.ml	No DNS record
cpanel.swapddostest.ml	No DNS record
ftp.swapddostest.ml	158.69.219.129
admin.swapddostest.ml	No DNS record
pop.swapddostest.ml	No DNS record
imap.swapddostest.ml	No DNS record
forum.swapddostest.ml	No DNS record
admin.swapddostest.ml	No DNS record
beta.swapddostest.ml	No DNS record
portal.swapddostest.ml	No DNS record

Con esta herramienta podemos obtener la IP del servidor que esta sirviendo la web, y “saltarnos” la protección de cloudflare atacando directamente a este servidor.

Para evitar esto, deberiamos bloquear todo el tráfico del servidor, y permitir únicamente el tráfico entrante desde las Ips de cloudflare, con esto nuestras reglas quedarían asi:

<http://pastebin.com/U7e15b36>



Como comprobamos la IP de nuestro servidor no esta disponible puesto que solo admite tráfico entrante desde cloudflare, por lo que el dominio si que funciona correctamente.

Con lo que llegamos a la conclusión de que la mejor opción para evitar este tipo de ataques es:

- Blindar al máximo tu servidor (cerrar todos los puertos)
- Contratar un servicio de protección anti DDoS, como el del cloudflare que tiene un plan gratuito.
- En el servidor web, tener solo la web. (No servir correo, dns...)
- Esconder la IP de tu servidor lo máximo posible.
- No poner restricciones a las Ips de cloudflare.
- Ver la IP del usuario real haciendo uso de mod\_cloudflare en apache (asi podremos poner limites y bloquear dichas Ips desde nuestras iptables)

Empresas similares a cloudflare:

<https://www.incapsula.com/>

<http://cloudlayer.com/>

<https://www.hyperfilter.com/>

<https://blazingfast.io/>

<https://javapipe.com/>

<https://www.staminus.net/>