



# Ataques de denegación de servicio



Antonio Jesús Peláez Priego  
Francisco José Pimentel Moreno



# Que os vamos a contar

Os vamos a dar una visión general de que son los ataques DDoS y os contaremos aspectos muy interesantes sobre estos.

- Qué 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

# ¿Qué es un ataque DDoS?

Seguro que con una simple búsqueda en google encuentras millones de definiciones y descripciones de qué es y en qué 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.

# ¿Cómo consiguen inhabilitar nuestro servidor?

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...

Master Control  
Computer(s)



Zombie



Zombie



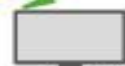
Zombie



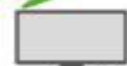
Zombie



Zombie



Zombie



Zombie



Hosts



Hosts



Hosts



Hosts



Hosts



Hosts



Victim

**PC Zombies**

**Atacado**



**Atacante**

**Usuario Normal**

# Tipos de ataques

**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.

# Tipos de ataques

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.



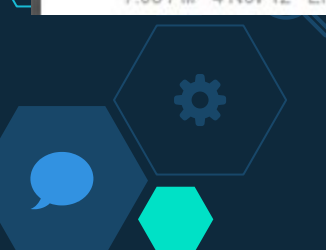


# Ataques famosos

Y sus consecuencias...



## A decorative graphic in the bottom right corner featuring a lightbulb icon inside a hexagon, surrounded by other hexagons in various shades of blue and green.




Target: 


## TARGET THESE IP's

204.152.204.166

195.74.38.17

**FREEDOM**  
is  
**PRICELESS**  
for everything else there is...



 **OPERATION PAYBACK**  
<http://anonops.net/>

**DEFEND WIKILEAKS**  
**DEFEND FREEDOM**



Everyone's attacking [www.paypal.com](http://www.paypal.com) port 443 right now. So keep firing at #Paypal. #ddos #payback #wikileaks

via Chromed Bird ☆ Favorite ↕ Retweet ↩ Reply

# PlayStation Network y su caída de servicio durante casi un mes



PSN currently undergoing sporadic maintenance. Access to the PSN may be interrupted throughout the day. We apologize for any inconvenience.

57 minutes ago via CoTweet ☆ Favorite ↻ Retweet ↩ Reply

Retweeted by AmonLau and 93 others



**Anonymous**  
@YourAnonNews

Twitter Suivre



.@Sony Hacked, @PlayStation Network Pwned | [pastebin.com/HUjZPaF3](https://pastebin.com/HUjZPaF3) | #PSN | #Anonymous

← Répondre ↻ Retweeter ★ Favori

414  
RETWEETS

46  
FAVORIS



Voir ce Tweet



**PlayStation®  
Network**



Un niño canadiense  
hackea sitios  
gubernamentales

“





# Sanciones, legalidad y leyes

- ◇ En un principio las sanciones para este tipo de ataques no eran penales, simplemente eran sanciones económicas.
- ◇ Ahora, ante el crecimiento de estos ataques, se penan con entre 6 meses a 2 años de cárcel según la ley española.
- ◇ Estos ataques están penados por la ley pero en la red abundan.





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

## Antes

Realizados por expertos, hackers, gente con conocimiento en el área de la informática.

## Ahora

Cualquiera con conexión a internet y un par de euros en bitcoin o paypal

Las cosas evolucionan a veces a peor y a veces a mejor.





# Seguro que ahora os estais preguntando... ¿Cómo?

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

Ahora os voy a explicar el proceso...



[Todo](#)[Noticias](#)[Vídeos](#)[Imágenes](#)[Shopping](#)[Más ▾](#)[Herramientas de búsqueda](#)

Aproximadamente 67.200 resultados (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 ...](http://razortools.com)

## [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 ...



# 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 <ul style="list-style-type: none"><li>Free Services and Giveaways</li><li>Deal Disputes</li><li>Appraisals and Pricing</li></ul>	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. <ul style="list-style-type: none"><li>Server Stress Testing</li><li>Cryptography and Encryption Market</li></ul>	80,790 1,550,910	<b>[LEARN HOW TO DOX] Privat...</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. <ul style="list-style-type: none"><li>Virtual Game Items</li><li>Traders Topics</li><li>Member Auctions</li></ul>	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. <ul style="list-style-type: none"><li>Non-Free Accounts</li><li>Gamertags</li></ul>	44,836 513,979	<b>Need this tag [From the r...</b> Today 09:18 AM by Sevn Alias

## Server Stress Testing





[SYT](#) [Mark](#)

Thread / Author Replies Rating Last Post [asc]

### Important Threads

	<a href="#">▶ SYNSTRESS.NET</a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">49</a> ) Joey	480	<div><div></div><div></div><div></div><div></div><div></div></div>	Today 04:41 AM Last Post: Klaus
	<a href="#">▶ THUNDER STRESS // Mobile APP // <u>500G + 500K RS</u> / 100% Custom / RAW Methods / BEST VIP</a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">37</a> ) Taranis	363	<div><div></div><div></div><div></div><div></div><div></div></div>	Yesterday 02:50 PM Last Post: Taranis
	<a href="#">▶ [CLICKBOOT] ~ MOST RELIABLE BOOTER   <u>195+ Gbps</u> / 20+k R/s TN   100% Uptime   Autobuy</a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">11</a> ) Tando	102	<div><div></div><div></div><div></div><div></div><div></div></div>	Yesterday 02:27 PM Last Post: Tando
	<a href="#">▶ <b>**New Source**</b>[Vouched] Str3ssed Networks   1+ Year Running   <u>210Gbps+TN</u>   L4&amp; L7</a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">32</a> ) AnonNinja™	318	<div><div></div><div></div><div></div><div></div><div></div></div>	Yesterday 10:35 AM Last Post: AnonNinja™

### Normal Threads

	<a href="#">▶ CriticalBOOT   MOST POWERFUL   Stop/Resume/Renew   VIP   TCP-FLAG OVH ABUSE   <u>300Gbps</u></a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">101</a> ) Stratos	1,009	<div><div></div><div></div><div></div><div></div><div></div></div>	Today 08:07 AM Last Post: Moeseeph
	<a href="#">▶ vDos Stresser <u>300Gbps+TN</u> L4&amp;L7 CC/BTC 17 Attack methods! VIP Nodes Since 2012!</a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">34</a> ) Apple J4ck.	330	<div><div></div><div></div><div></div><div></div><div></div></div>	Today 07:55 AM Last Post: Klaus
	<a href="#">▶ Selling IRC Spots:: Nulls NFO, Downs Staminus, Hyperfilter, wreks everything!!!!</a> Layer7 Attacks	6	<div><div></div><div></div><div></div><div></div><div></div></div>	Today 07:53 AM Last Post: Virgin Retard
	<a href="#">▶ KRONOS BOOTER   L4-L7   <u>10G +25 k r/s PER ATK</u>  JSBYPASS   POSTDATA   INSTANT DELIVERY</a> (Pages: <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ... <a href="#">6</a> )	56	<div><div></div><div></div><div></div><div></div><div></div></div>	Today 05:54 AM Last Post: MeNoSkidPls



### 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

 Sign Up



### 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

 Sign Up



### 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

 Sign Up

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...



¿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...



- 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.



# ¿Vacio legal?

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 responsables 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.

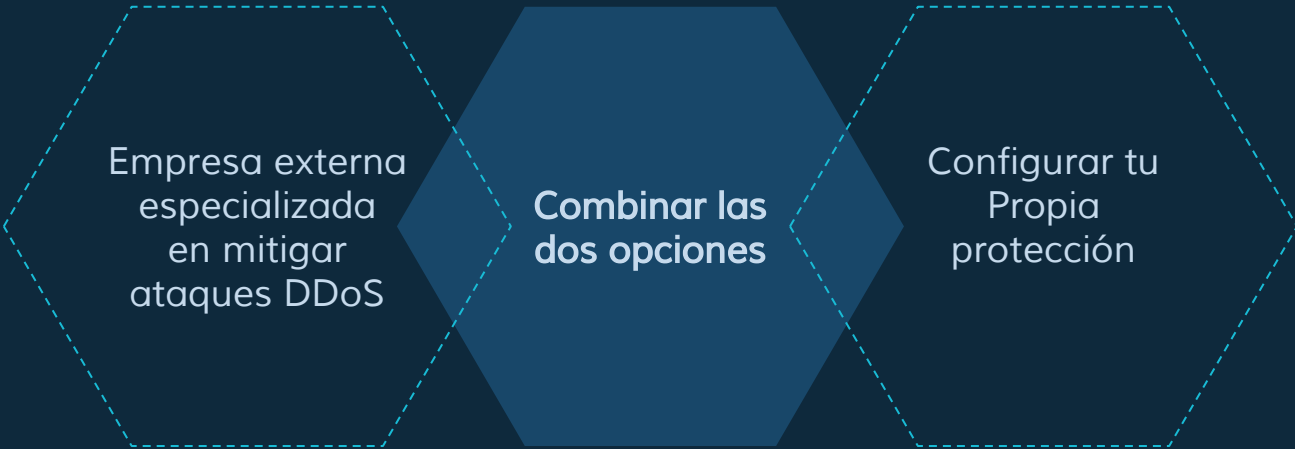


Y en resumen, así funciona esto, por lo que, si aún no has sido atacado, es raro, o has tenido suerte, empieza a montar tu defensa ya antes de que sea tarde.





# Como defenderte




Empresa externa  
especializada  
en mitigar  
ataques DDoS

**Combinar las  
dos opciones**

Configurar tu  
Propia  
protección







SUCCESS: Login Successful. Redirecting... x


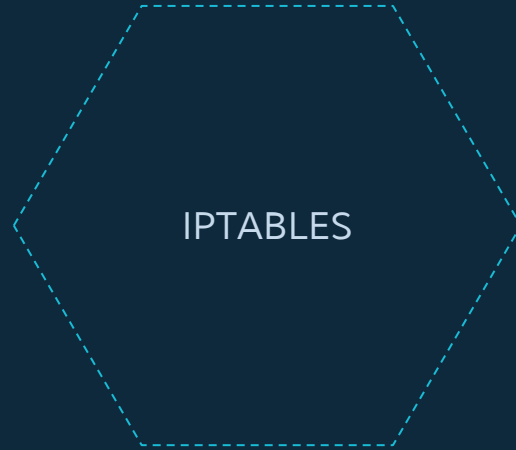
### Sign in

[Sign in](#)

[Create an account](#)

© All Rights Reserved EagleStresser 2016

VS



Massive use of this service - Ban 1 Day

**cacatua**  
Active Membership

- Home
- Stresser
- SmS-Bomber [PREMIUM]
- SmS-Bomber [FREE]
- ToS
- Support

## Hub

Stress Test Your Network!

DASHBOARD > HUB

### Launch Attack

Host:  Port:

Seconds:


Method:


[Launch](#)

### Manage Attacks

TARGET	PORT	METHOD	EXPIRES	ACTION
104.27.170.83	80	SynAck : TCP	Expired	<a href="#">Renew</a>
158.69.219.129	80	SynAck : TCP	Expired	<a href="#">Renew</a>
158.69.219.129	80	SynAck : TCP	Expired	<a href="#">Renew</a>
158.69.219.129	80	SynAck : TCP	Expired	<a href="#">Renew</a>
158.69.219.129	80	SynAck : TCP	Expired	<a href="#">Renew</a>




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>


 37.139.23.206 - PuTTY

```
Get:19 http://http.debian.net jessie-updates/main amd64 2016-05-02-2123.23.pdiff [254 B]
Get:20 http://http.debian.net jessie-updates/main 2016-03-04-0853.34.pdiff [1,371 B]
Get:21 http://http.debian.net jessie-updates/main 2016-04-10-2047.32.pdiff [4,538 B]
Get:22 http://http.debian.net jessie-updates/main 2016-04-19-2053.08.pdiff [2,245 B]
Get:23 http://http.debian.net jessie-updates/main amd64 2016-05-02-2123.23.pdiff [254 B]
Get:24 http://http.debian.net jessie-updates/main 2016-04-19-2053.08.pdiff [2,245 B]
Fetched 19.3 MB in 7s (2,641 kB/s)
Reading package lists... Done
root@SWAP:~#
root@SWAP:~#
root@SWAP:~#
root@SWAP:~#
```

Servidor privado virtual en DigitalOcean



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>

 37.139.23.206 - PuTTY

```
Get:19 http://http.debian.net jessie-updates/main amd64 2016-05-02-2123.23.pdiff [254 B]
Get:20 http://http.debian.net jessie-updates/main 2016-03-04-0853.34.pdiff [1,371 B]
Get:21 http://http.debian.net jessie-updates/main 2016-04-10-2047.32.pdiff [4,538 B]
Get:22 http://http.debian.net jessie-updates/main 2016-04-19-2053.08.pdiff [2,245 B]
Get:23 http://http.debian.net jessie-updates/main amd64 2016-05-02-2123.23.pdiff [254 B]
Get:24 http://http.debian.net jessie-updates/main 2016-04-19-2053.08.pdiff [2,245 B]
Fetched 19.3 MB in 7s (2,641 kB/s)
Reading package lists... Done
root@SWAP:~#
root@SWAP:~#
root@SWAP:~#
root@SWAP:~#
```

Servidor privado virtual en DigitalOcean





# Primeros pasos

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

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

```
#!/bin/sh
# Server ip
SERVER_IP="37.139.23.206"
# Limpiar reglas
iptables -F
iptables -X
# Denegar cualquier conexion
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# Permitir todas las conexiones para localhost
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# Permitir conexiones al puerto 22 y 80
iptables -A INPUT -p tcp -s 0/0 -d $SERVER_IP --sport 513:65535 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -s $SERVER_IP -d 0/0 --sport 22 --dport 513:65535 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d $SERVER_IP --sport 513:65535 --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -s $SERVER_IP -d 0/0 --sport 80 --dport 513:65535 -m state --state ESTABLISHED -j ACCEPT
# Nos aseguramos de bloquear conexiones
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

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

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



# Mejorando nuestro script

V2 : más reglas y restricciones (10 conexiones tcp por minuto) a nuestro script:

<http://pastebin.com/jiLHceYq>

V3: reglas para bloquear los ataques más comunes y otros un poco más específicos

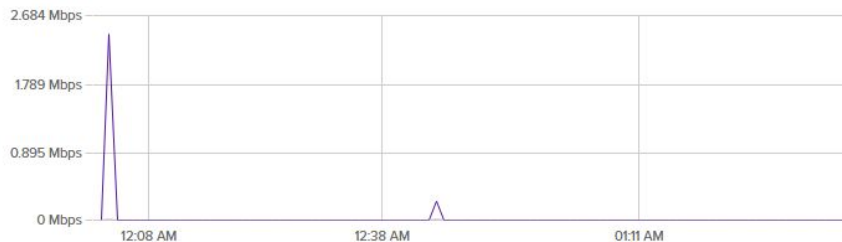
<http://pastebin.com/jj0iXHnh>

# Comienza la acción

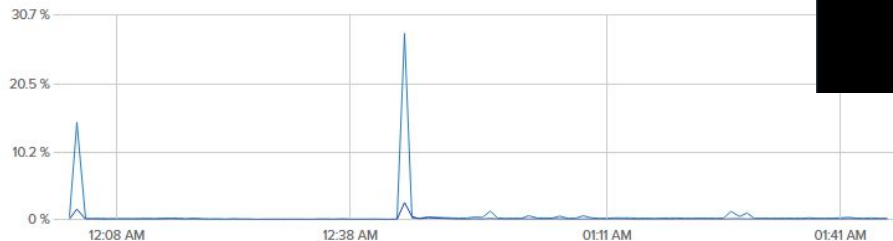
`netstat -na | awk '{print $5}' | cut -d. -f1-4 | sort -n | uniq -c | sort -n`

Bandwidth - Public

6 hours



CPU



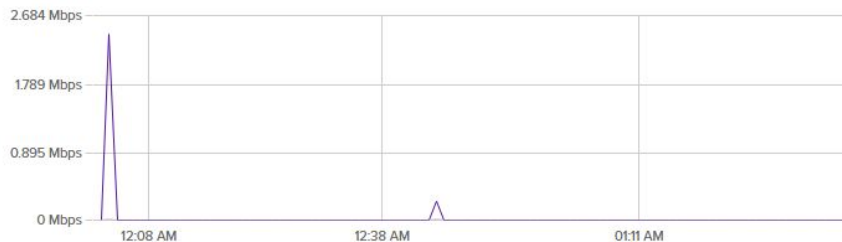
```
37.139.23.206 - PuTTY
root@SWAP:~# netstat -na | awk '{print $5}' | cut -d. -f1-4 | sort -n | uniq -c | sort -n
  1 217.216.34.60:54189
  1 Address
  1 and
  1 (servers
  1 State
  6 ]
  7 :::*
  7 0.0.0.0:*
 13 DGRAM
 16 STREAM
root@SWAP:~#
```

# Comienza la acción

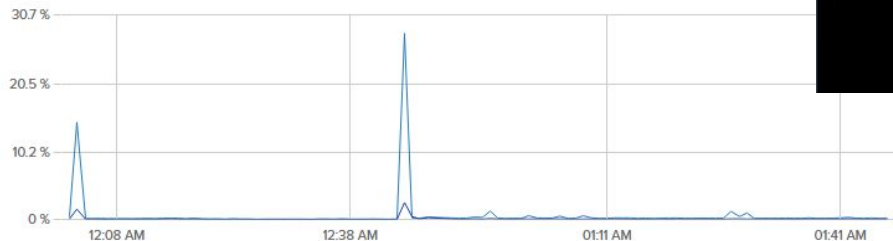
`netstat -na | awk '{print $5}' | cut -d. -f1-4 | sort -n | uniq -c | sort -n`

Bandwidth - Public

6 hours



CPU



```
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:~#
```



# Primera prueba

`iptables -F`

`iptables -X`

`iptables -t nat -F`

`iptables -t nat -X`

`iptables -t mangle -F`

`iptables -t mangle -X`

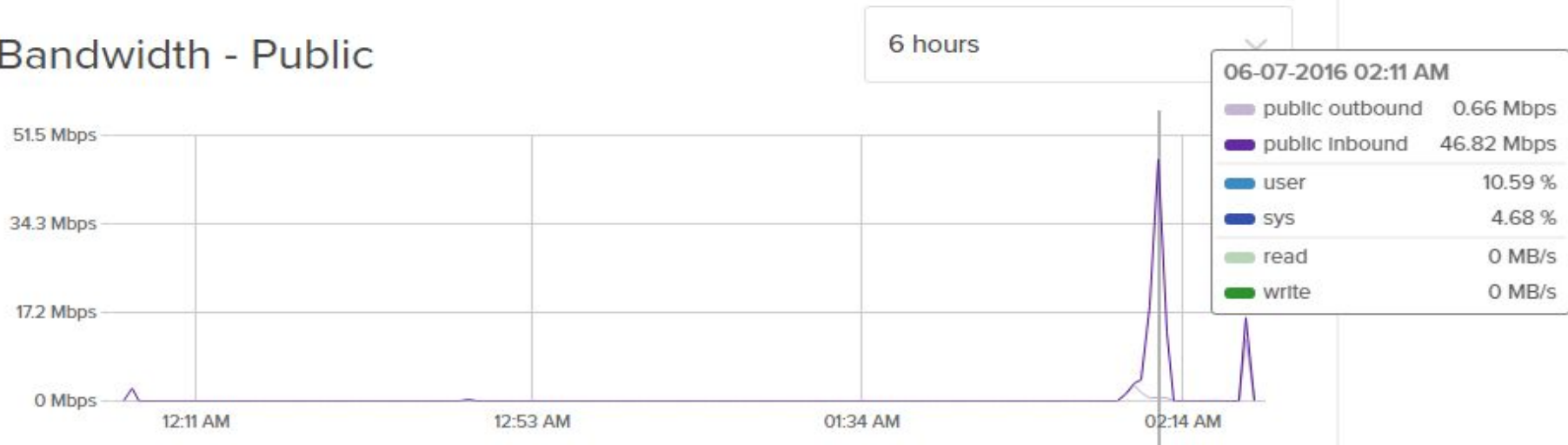
`iptables -P INPUT ACCEPT`

`iptables -P OUTPUT ACCEPT`

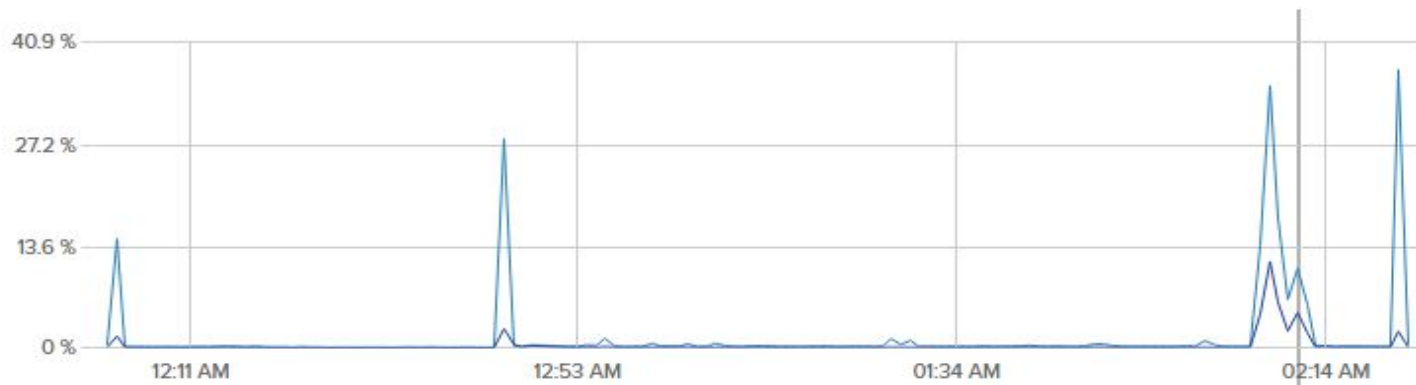
`iptables -P FORWARD ACCEPT`



## Bandwidth - Public



## CPU



# Primera prueba



**DigitalOcean** <support@support.digitalocean.com>

para mí ▾

22:24 (hace 1 minuto) ☆



Hi there,

Our system has automatically detected an inbound DDoS against your droplet named SWAP with the following IP Address: 37.139.23.206

As a precautionary measure, we have temporarily disabled network traffic to your droplet to protect our network and other customers. Once the attack subsides, networking will be automatically reestablished to your droplet. The networking restriction is in place for three hours and then removed.

Please note that we take this measure only as a last resort when other filtering, routing, and network configuration changes have not been effective in routing around the DDoS attack.

Please let us know if there are any questions, we're happy to help.

Thank you,  
DigitalOcean Support



# Segunda prueba

Después de adquirir un nuevo servidor en otra empresa, OVH...

Ejecutamos nuestro script v3 para lanzar nuestras reglas creadas para IPtables

Resultado...

**Soporte OVH** a través de undelivered.ovh.net

0:27 (hace 0 minutos) ☆



🔒 para mí ▾



español ▾



inglés ▾

[Traducir mensaje](#)[Desactivar para: español](#) x

OVH HISPANO S.L.U.  
C/ Alcalá 21, 5º dcha.  
28014 Madrid  
España

Estimado/a cliente:

Acabamos de detectar un ataque sobre la dirección IP 158.69.219.129.

Con el fin de proteger su infraestructura, hemos desviado su tráfico hacia nuestra infraestructura de mitigación.

De esta manera, todo ataque será filtrado por nuestra infraestructura y sólo el tráfico legítimo llegará a sus servidores.

Cuando finalice el ataque, su infraestructura será inmediatamente retirada de la mitigación.

Más información sobre la infraestructura de mitigación de OVH:

<http://www.ovh.es/anti-ddos/>

Atentamente,

Atención al Cliente de OVH



# Tercera prueba

Por lo menos no han cortado la conexión del vps.

(En digital ocean han tardado 3 horas en reactivar el vps aunque solo lo atacamos 30 segundos)

Seguiremos trabajando con el vps de OVH, ahora modificaremos algunas configuraciones del kernel para mejorar nuestra protección.

Modificamos el fichero `/etc/sysctl.conf`

<http://pastebin.com/PytT3mtc>

`Sysctl -p`

Resultado...

## Cannot Connect to Server

Sorry about that. Maybe if you  
hit retry...

Retry





# Cuarta prueba

- Usaremos cloudflare.
- Registramos el dominio: swapddostest.ml
- Le asignamos las dns de cloudflare.
- Modificamos los registros A para que apunten a nuestro vps

Type	Name	Value	TTL	Status
A	swapddostest.ml	points to 158.69.219.129	Automatic	 
CNAME	www	is an alias of swapddostest.ml	Automatic	 

Advanced ▶ API ▶ Help ▶

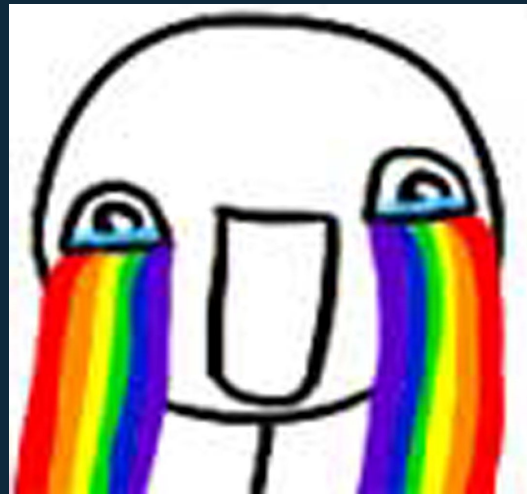
# Cuarta prueba

- Creamos el virtual host en nuestro servidor apache para que sirva swapddostest.ml
- Agregamos a la whitelist de nuestro firewall las IPs de cloudflare: <https://www.cloudflare.com/ips/>

Lanzamos el ataque...

Resultado...

La web sigue online!







# Pero aún hay un problemilla

Nuestro problema ahora es, cloudflare resolver:

<http://iphostinfo.com/cloudflare/>



## CloudFlare IP Resolver

### Domain: swapddostest.ml

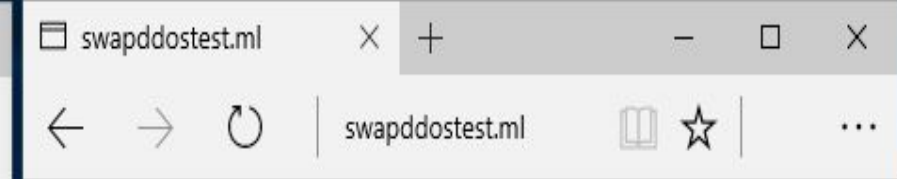
DNS	IP
mail.swapddostest.ml	<b>158.69.219.129</b>
direct.swapddostest.ml	No DNS record
direct-connect.swapddostest.ml	No DNS record
cpanel.swapddostest.ml	No DNS record
ftp.swapddostest.ml	<b>158.69.219.129</b>
admin.swapddostest.ml	No DNS record
pop.swapddostest.ml	No DNS record
imap.swapddostest.ml	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



# ¿Cómo lo evitamos?

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

<http://pastebin.com/U7e15b36>



**swap test**



# Conclusiones

- 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 límites y bloquear dichas Ips desde nuestras iptables)



# Alternativas a cloudflare

<https://www.incapsula.com>

<http://cloudlayer.com>

<https://www.hyperfilter.com>

<https://blazingfast.io>

<https://javapipe.com>

<https://www.staminus.net>



# ¡Gracias!

## ¿Alguna pregunta?

Puedes encontrar el trabajo completo en:

[https://github.com/ajpelaiez/SWAP/tree/master/trabajo\\_final](https://github.com/ajpelaiez/SWAP/tree/master/trabajo_final)

