Como hacer ataques DDoS – Nivel principiante en CMD

Chuiso agosto 2, 2013 64 comentarios Black Hat, Fraudes, SEO

¿Cómorrrr? **¿Ataques DDoS, Chuiso?** Sí, señores, hay que saber de todo en esta cibervida, por eso hoy empiezo la primera parte de una serie de artículos en la que os hablaré de los distintos tipos de ataques DDoS que existen, cómo se realizan y con qué herramientas. En la medida de lo posible os enseñaré a realizar ataques de este tipo y os explicaré cómo funcionan. ¿Por qué? Sencillo, si eres un bastardo sin escrúpulos quizás quieres usarlos para fastidiar a alguien… Y si eres un webmaster cauteloso querrás saber en qué consisten este tipo de amenazas hacias nuestras webs y **como subsanarlas**. Lógicamente ni yo ni nadie va a tocar Quondos (mirar viñeta), porque es más sagrado que la Santísima Trinidad jejeje, pero fue lo primero que se me vino a la mente

Yo, **Chuiso Chuisez**, prometo, confirmo y aseguro haber sufrido **malditos ataques DDoS** en alguna web en algún momento de mi vida. La sensación de impotencia es indescriptible, sobretodo si ves que esto te está haciendo perder dinero. También recuerdo casos curiosos de ataques DDoS completamente cabrones, como el que sufrió **Alex Navarro** de Vivirdelared.com poco antes de que se eligiese el ganador del concurso Seorimícuaro, con cerca de 2.500 dólares en juego. Sí, señores, si tienes una competencia fuerte y hay mucho dinero en juego (o un enemigo de

esos de película), no descartes sufrir ataques DDoS. Hoy en día están muy al alcance de la mano y, aunque son relativamente fáciles de subsanar, pueden jugarte una mala pasada.

Todo lo que debes saber sobre un DDoS

Un jodido DDos (que viene de Distributed Denial of Service) es un ataque (que se puede realizar de diversas formas) a un sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos (por ejemplo, y en nuestro caso, una página web). Normalmente provoca la pérdida de la conectividad de la red por el **consumo del ancho de banda de la red** de la víctima o sobrecarga de los recursos del sistema de la víctima (incluso aunque tengas un VPS, por ejemplo).
Después de este **copypaste de Wikipedia**, hablemos claro. En estos artículos vamos a hablar de las diversas formas que hay de atacar mediante DDoS, y qué software o medios se emplean. Normalmente la idea básica en nuestra temática la podemos resumir en esto.

__Víctima__ tiene página web -> __Bastardo__ quiere tumbarla -> __Bastardo__ usa un ataque DDoS lo suficientemente potente para que el hosting de la __víctima__ colapse -> Los usuarios que quieren entrar a la web de la __víctima__ se encuentran con que está caída mientras dura el ataque -> __Bastardo__ tiene orgasmos de placer

Como veis un ataque DDoS es una faquinshit. Se pueden citar cientos de formas de atacar una web, sin embargo en la actualidad destacan por su relevancia programas como **LOIC** (que os pasaré y enseñaré a usar), usados por los "Anonymous" para joder al FBI, etc. Como hoy no quiero asustaros con mucha información, vamos a empezar por la base de la pizza... lo más básico en cuánto a ataques DDos. Se llama el **"Ping de la Muerte"** y aunque en la actualidad su funcionalidad no es de gran valor, nos sirve para entender mejor la historia de los ataques DDoS y cómo funcionan.

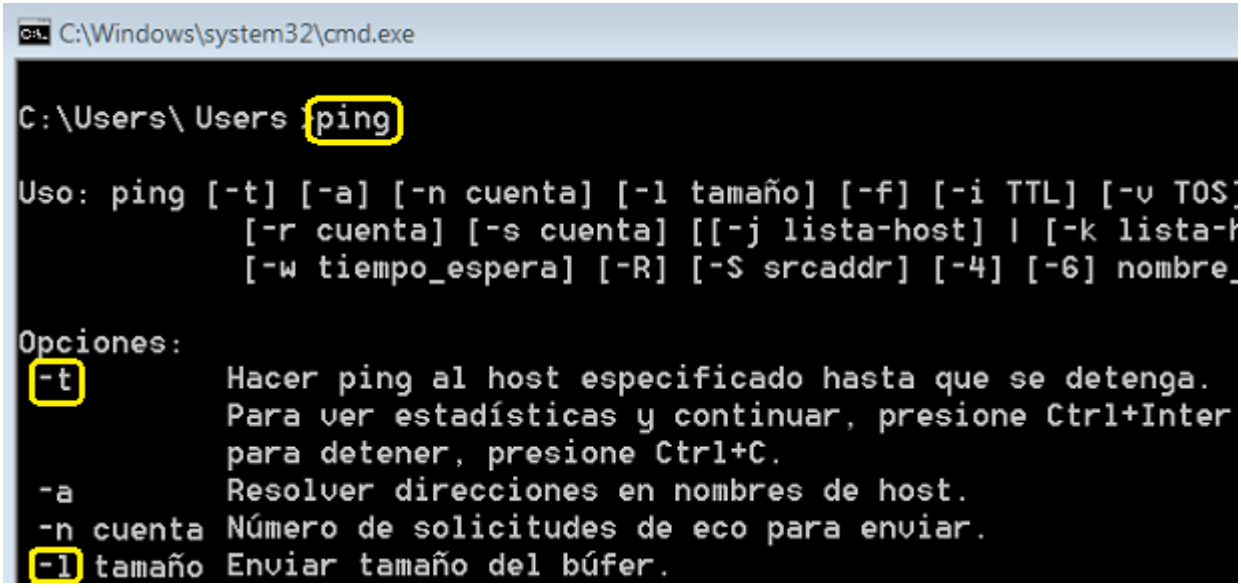
Por cierto, ¿todavía no conoces **TeamPlatino**? **Deberías echarle un vistazo ya**. Es mi curso privado de SEO y monetización y la estamos liando parda

dentro

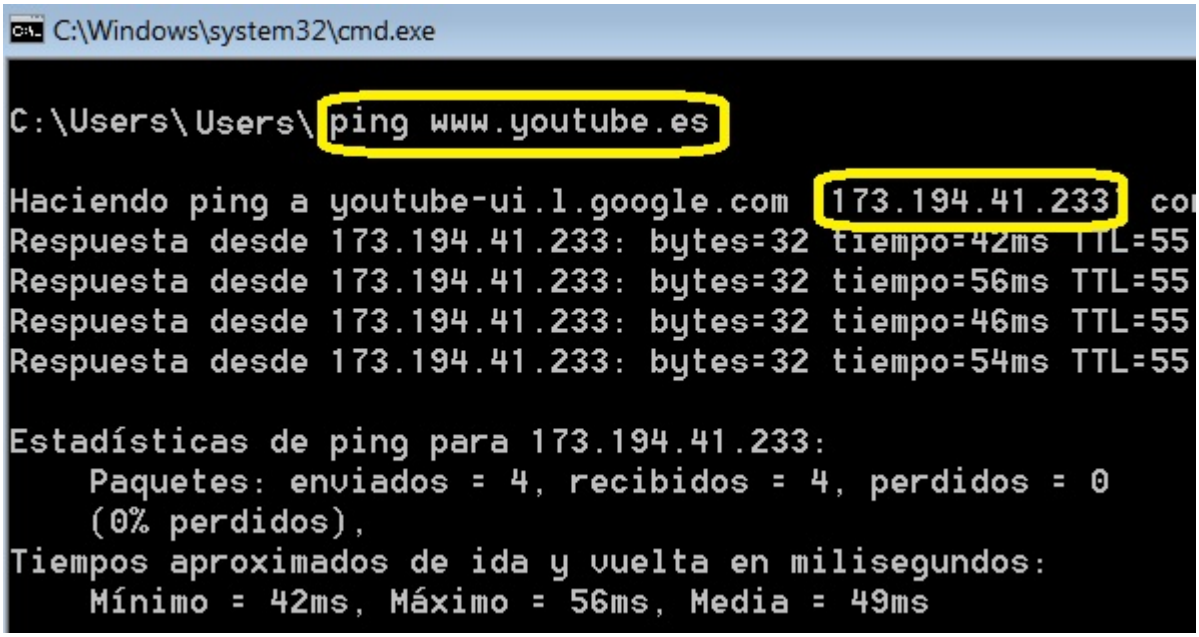
Ataque DDoS en CMD – Ping de la Muerte

Este tipo de ataques se realizaron mucho hace más de 15 años, e hicieron mucho daño en el creciente ambiente cibernético de la época. El sistema consistía en mandar numerosos paquetes **ICMP grandes** (mayores a 65.535 bytes) con el fin de colapsar el sistema atacado. Todo ello se realizaba a través de pings deformados con tamaños mucho mayores a los comunes 64 bytes. Hoy en día realizar dichos ataques DDoS mediante pings **es muy sencillo**, sin embargo todas las redes actuales están protegidas ante dichos ataques tan anticuados, por lo que hace falta mandarlos desde varios ordenadores para que puedan funcionar. Si bien los pings deben tener un **peso de más de 65.535 bytes**, yo no he conseguido mandarlos con más de 15.000 bytes, por lo que necesitaría otros usuarios mandando el mismo ataque DDoS a la misma web para tener la posibilidad de tumbar una página web

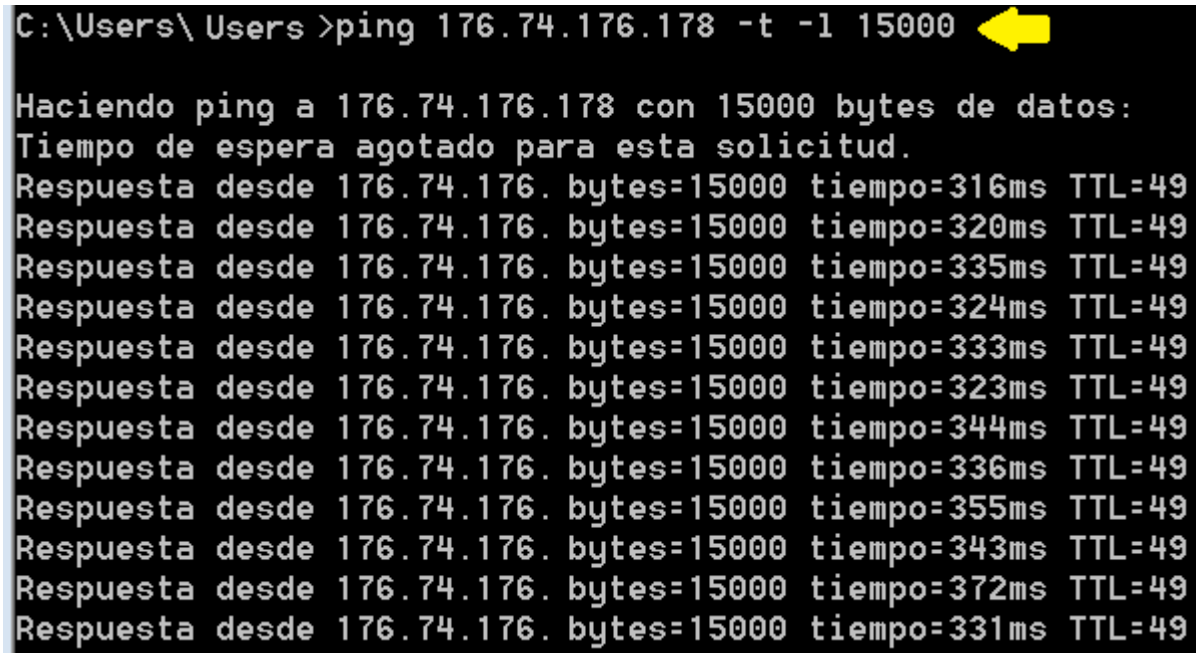
con un hosting normalillo
Ahora explicaré cómo se realiza el ataque. Entramos a nuestro menú de Windows y ejecutamos CMD. Se nos abrirá la típica pantalla de MSDOS en la que, si ponemos ping, veremos las opciones de la función que empleamos. Ahí va pantallazo con lo interesante:



Sobra decir que las opciones que emplearemos para nuestro ping **son "-t" y "-l"**. Con la "-t" mandamos el ping de forma repetida y continuada, y con la "-l" elegimos el peso de cada ping, en este caso búfer. Ahora debemos conocer la IP de la web a la que queremos atacar. Para ello tecleamos un nuevo y simple comando: **"ping www.webqueatacare.com"** y damos a "Intro". En pocos segundos nos dará una IP como veis a continuación:



Ahora, con la IP de nuestra víctima, debemos teclear el nuevo comando que hará temblar la página. Os recomiendo escribirlo en un bloc de notas y luego pegarlo en el **CMD** para que podáis modificarlo rápidamente. El formato debe ser así: **"ping 123.111.23.453 -t -l 15000"**. Lógicamente debéis cambiar la IP por la de vuestra víctima, y la cifra final es la cantidad de bytes que estáis enviando. La "-t" y "-l" son los comandos de ping que empleamos. En la siguiente pantalla podéis ver un ataque de pings exitosos.



Si los pings no dan respuestas y da un mensaje del tipo "Tiempo de espera agotado para esta solicitud", significa que la cantidad de bytes que hemos puesto es muy alta. Debemos ir regulando la cantidad para saber **cuantos bytes soporta por ping**. Una vez sepamos la cifra máxima soportada, es cuanto entra en juego **el trabajo en equipo**. Busca amigos, foreros, webmasters y/u otro tipo de gente que esté dispuesta a ayudarte y facilítales la información, cantidad de bytes y método y poneros a funcionar todos a la vez en la misma web. En función del tipo de hosting que tenga la víctima y la calidad del mismo es posible que podáis tumbar una web

con esta técnica tan simple y antigua
Ahora bien, si te gustó el artículo y quieres que continúe con la segunda

parte, **dame un +1 en Google Plus** y lo haré ¿No tienes cuenta en Google? ¿En qué mundo caótico y cruel vives…? Bueno, también pueden valerme **Facebook,**

Twitter… ¡Si me pongo muy blando me vale hasta Tuenti! Compartir es vivir