Reading Report: Vlajic12

Ricard Medina Amado

April 15, 2023

Upload your report in PDF format.
Use this LaTeX template to format the report, keeping the proposed headers.
The length of the report must not exceed **5 pages**.

1 Content

1.1 Identify the genre[1] of the document, its purpose, and its target audience.

Es tracta d'un paper presentat en la tercera conferència internacional d'Ambient Systems, Networks and Technologies. El seu propòsit és avaluar l'impacte dels DNS TTL values en l'usuari i veure com el sue ús inadequat pot arribar a causar atacs, per exemple de DDOS. Està destinat a gent amb uns coneixements mínims d'informàtica.

1.2 Summarize the document, indicating the key concepts[2].

Els atacs DDoS suposoen un dels majors perills a Internet acutalment. Això es deu a que és un tipus d'atac molt simple d'executar i que té un cost molt baix.Els atacs de DDOS consisteixen en enviar dades de forma massiva a una màquina deixant-la inhabilitada a cuasa de la impossibilitat de respondre totes les prticions fetes. Per executar aquests atacs es poden fer servir xarxes de botnets (conjunts d'ordinadors que efectuen el que els hi diu un ordinador "mare" que els ha infectat). Per evitar els atacs DDoS s'implanten diferents mecanismes com:

- L'ús de firewalls i sistemes de detecció d'intrusos.
- Sobreaprovisionament d'ample de banda.
- L'ús de repliques dels servidors web separades físicament.

Encara així, això no és suficient per a evitar els atacs DDOS, ja que la majoria de problemes són causats a la part del DNS.
Per entendre l'impacte del valor del DNS TTL, primer hem d'entendre com funciona un DNS, aquí un exemple:

- L'usuari proporciona la URL de la web a la que vol accedir.

[1] Genres: book, article, essay, report, review, manual, white paper, data sheet, weblog, etc.
[2] The summary should help you to answer the questions about the reading in the exam.

- La URL és enviada al DNS-resolver per el navegador, el resolver mira si la té a la seva cache, si és així retorna la seva IP, sinó consulta el DNS local.
- El DNS busca si la té a la seva memoria, sinó li fa la consulta a un DNS superior.
- Un cop l'usuari obté la IP de la web s'inicia la connexió HTTP.

Un camp que té molta importància és el TTL, que és la quantitat de temps que es quedarà a la cache. Aquest temps es decideix per varies raons:

- La freqüencia de les actualitzacions del web-site i la seva localització: Les webs amb contingut estàtic normalment escullen uns valors TTL més llargs per aconseguir una velocitat de baixada de la pàgina web més ràpida. Degut a que llargues TTL és probable que les peticions DNS estiguin ja cachejades. En canvi, les webs que solen canviar el contingut de les seves pàgines solen escollir valors curts de TTL per provocar que es refresquin freqüentment els seus registres DNS. D'aquesta forma aconsegueixen que la informació es lliuri de forma precisa i puntual.
- Els sforços per controlar el nombre de DNS-lookup: És un augment de la càrrega de treball en els servidors de DNS. És a dir, amb curt TTLs, els DNS Records caduquen més ràpidament des les memòries cau DNS dels clients, el que provoca un nombre més gran de requests de DNS siguin reenviades als servidors de DNS de més alt nivell.

Normalment els llocs web solen considerar que el TTL ideal està situat entre uns 15 i 30 minuts. Encara que aquesta suposició pot causar desventatges i grans pérdues per l'empresa. Per a entendre com afecta escollir incorrectament el DNS TTL value s'exemplificarà amb un possible atac de DDOS:

- En aquest exemple l'usuari accedeix a una pàgina web i mentre està accedint es produeix un atac DDOS que paralitza el servidor, per el que el servidor acaba migrant a una altra ubicació. Encara així, com el client havia accedit en un TTL vàlid abans de l'atac les seves peticions es segueixen fent a la mateixa ubicació. Aquesta situació s'anomena Faulty-DNS-cache lock. L'única forma d'arreglar aquesta situació és fent un flush de la cache.

Un estudi ha demostrat que entre el 37% i el 49% d'usuaris que tenen problemes al realitzar una operació abandonen el lloc i es poden passar al competidor. Un altre estudi fet per Google i Bing afirma que el 57% dels usuaris abandonen una pàgina desprrés de que no doni servei per més de 3 segons i 8 de cada 10 persones no tornen a utilitzar el servei si no han tingut una bona experiència.
Un estudi fet a 2010 per Forrester Consulting sobre la disponibilitat de banca online afirma que els 75% d'usuaris esperen que hi hagi un 99% de disponibilitat en el servei.
En conclusió els TTL de llarga durada són estadísticament més propensos a posar més màquines de clients enFaulty DNS-Cache Lock. Per un website sota un atac DDoS, molts d'intents de recàrrega per part d'usuaris legítims només agreujarà la congestió de l'amplada de banda i/o la càrrega de processament al servidor, ajudant així l'atacant a aconseguir l' objectiu.
Per una altra part, els Faulty DNS-Cache Lock amb llargs TTL és possible que

desemboquin en conseqüencies negatives a llarg terminidegut a que l'usuari experimenta un lloc web deficient.
Els usuaris que accedeixin a una web normalment s'aprofiten d'una petita part del valor de TTL al registre DNS, degut a que implicaria fer actualitzacions freqüents de les memòries cache DNS dels clients i una bona resistència en cas d'un error del lloc, com podria ser un atac DDOS. Però tenir un TTL petit pot produïr problemes com un atac d'inntoxicació del DNS. Hi ha empreses que com depenen críticament del rendiment dels seus llocs web utilitzen valors de DNS TTL de 0 segons.

Dins de la recerca de Faulty DNS-Cache Locka s'han buscat els valors per a el DNS TTL a alguns bancs eureopeus i d'Estats Units:

- Grup A: 15 bancs d'Estats Units amb millor rendiment segons Forbes.com
- Grup B: 15 grans bancs d'Estats Units, pel que fa al seu actiu total segons Forbes.com
- Grup C: 15 principals bancs de la UE i grups bancaris segons Banks-Daily.com.

Al grup A, 8 dels 15 bancs fan ús de valors DNS TTL de 60 minuts o més. Tots ells utilitzan un únic nom d'adreça IP en els seus registres DNS. Per el que es suposa que cap dels bancs disposa de servidors redundants ni de la capacitat de migrar automàticament els servidors.
Al grup B, 2 de cada 15 bancs utilitzan valors DNS TTL de 60 min i més, i 10 de cada 15 utilitzan valors inferiors a 1 minut. 6 dels 15 bancs utilitzen múltiples noms d'adreces IP en els seus registres DNS, pel que s'entenen que estan preparats per a una possible migración de servidor en cas de que fos necessàri.
Al grup C, 5 dels 15 bancs fan ús de DNS TTL de més de 60 minuts, 4 s'observen utilitzant TTLs inferiors a 1 min, mentre que els altres 6 bancs tenien TTLs d'entre 5 i 30 minuts. S'observen que tres bancs d'aquest grup utilitzen noms d'adreça IP múltiples, mentre que un banc confia en els serveis d'allotjament web d'Akamai CDN.

Alguns dels problemes que encara estan sent investigats relatius al Faulty DNS-Cache lock són:

- La interacció mútua entre els diferents tipus de memòries cau de DNS del navegador i l'impacte que cada memoria podria tenir en situacions de bloqueig de cache DNS defectuós.
- També es segueix intentant trobar quin seria el TTL òptim, ja que depèn de molt altres factors.

2 Assessment

2.1 Rate the readability of the document: easy, readable, difficult, unreadable.

Ha estat un article fàcil de llegir encara que potser una mica més comlpexe que els anteriors.

2.2 Give your opinion of the reading assignment, indicating whether it should be included in next year's course or not.

Ha estat interessant i al no ser molt llarg es fa fàcil de llegir. No veig problema en seguir incluint-lo a les lectures del próxim curs.