Reading Report: Vlajic12

Albert Bausili Fernández

April 17, 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.

This document is an article,and its target audience is all the people with interest in IT and specifically the owners of enterprise nets and/or their admins.

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

Solutions to DDOS attacks usually only mitigate the problem instead of solving it, some examples of those "solutions are the following: Adequate use of firewalls and intrusion-detection system, over-provisioning of bandwidth and deployment of multiple physically and logically separated web-server replicas.

How DNS work: 1. The browser recieve a simbolic name (URL) 2. The browser sends the simbolic name to the local (OS) resolver 3. The local DNS looks up its own cache if no match is found the query is forwarded to a higher DNS server, finally the mapping is returned to the browser 4. The browser establishes a HTTP connection with the provided IP

An important component of DNS is the time-to-live (TTL). THis value is controlled by the original (authoritative) DNS server, the servers and applications are allowed to store the given DNS Record before they must discart it and needed to request a new copy. The main parameter in order to configure this TTL is the frequency of updates in the web-site's content and/or the location of the host server. In order to avoid collapsing DNS, many web-sites opt to use long TTL times as a mechanism of DNS-load balancing, as shorter TTL's increse the workload of DNS server, especially autorative ones.

If the TTL is too large the users that want to connect during a DDOS atack may not be able to do so for the next TTL seconds as the DNS still redirects

[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.

them to the old server. It could be solved by the user flushing their DNS cache, however this is not somthing that an average user would do and the other solutions that that type of user may try, such as cnaging tabs, changing of browser window, etc, are mostly unefective to deal with the given problem.

DDOS attacks in faulty TTL configured websites tend to be more effective.

Shorter TTL imply better resilience against for example, DDOS attacks, on the other hand, shorter TTL also increases the riscks of a successfully conducted DNS Poisoning Attack.

A good solution to increase resilence instead of shortening the TTLs is having multiple replicas of the server with different IPs and in different locations. This is the solution used in CDN and it is the heart of their strategy of achieving load-balancing and fault-tolerance for hosted web-sites.

2 Assessment

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

Easy.

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

Simple, concise and enjoyable, those are the three words that I would use to describe this document. I think it should be included in next year.