ISSN 2047-3338

An Overview of DNS Poisoning and a Possible Solution

Manan Lalaji[1], Mangesh Bhangare[2] and Jaison Manitharavely[3]
[1,2,3]St.Francis Intitute of Technology, Mumbai University, India

***Abstract*– It is the DNS which makes away remembering strings of illogical numbers to use the internet. Converting readable names into their allotted IP is the basic function of a DNS server. Hence, it provides a very useful and a critical function to the users all over the world. Therefore, any unethical changes in a DNS server can make users not able to reach their desired sites. Hackers can then redirect the users to their malicious sites. This is an example of DNS poisoning. In this paper, we propose a possible solution to DNS poisoning by using multiple DNS servers.**

***Index Terms*– DNS, DNS Poisoning, Internet and IP Address**

I. INTRODUCTION

IP addresses are difficult for people to remember. It is not feasible for people to remember or make a document and copy and paste the IP address from the document every time they wish to visit a web site. Also, even after remembering the IP address, if someone enters an IP address and that particular website changes its servers, then, people will need to again remember another IP address to visit the same website e.g., A user types 207.241.148.80 in the address bar to access http://www.about.com. Now, if the website changes it server hosts, then not only the user will not able to access the website, he will have to remember another IP address [6].

The basic function of the DNS server is to avoid the need of remembering complex IP addresses. The user enters a name of a website in the address bar. This string goes to the DNS server, where, the DNS server sends back the associated IP address to the user's browser enabling the client browser to direct to the desired web server.

The working of the DNS server can be summarized as shown in the Fig. 1.

1. The user enters an easy to remember name of a website in the address bar. The name is then sent to a DNS server.
2. The domain name is matched with pre-fed IP addresses in the lookup table (Fig. 2).
3. The matched IP address is then returned to the user's web browser and then the browser is directed to the required web server.

The service provided by the DNS-Domain Name System is very critical to users and applications on the Internet. It basically consists of a root DNS server which point to the top level DNS servers in the DNS hierarchy.

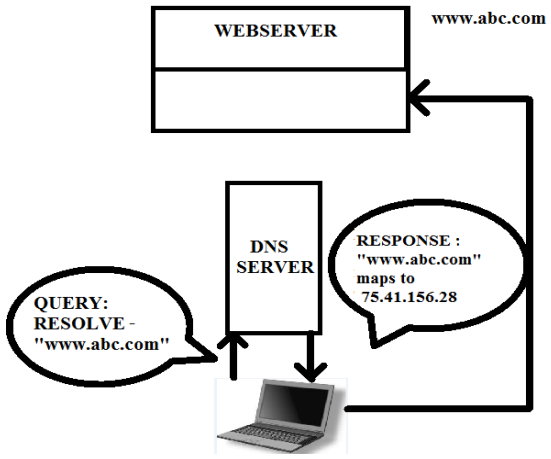

Fig. 1: Basic DNS Processing

102.4.23.122	www.abc.com
103.23.34.133	www.xyz.com
•	
•	
104.6.32.11	www.sfit.com

Fig. 2: A Lookup table

II. DNS POISONING

A table stored in the DNS server basically stores the human readable names along with their dotted decimal notations. A hacker or a user with a malicious intent may gain access to the DNS server through unethical means and modify the stored IP addresses to point them. Hence, now the user will not be directed to the desired site but to the site pointed by the modified IP address. The hacker's website may then impersonates the original website in its services and functions and may get private and confidential details like passwords, credit card numbers, (Phishing). Or simply the hacker may erase the IP address and deny any user wanting to visit the original web site.

III. A POSSIBLE SOLUTION

We can make the use of multiple DNS servers, consider a user's web browser sends human readable form of a website address to two distinct DNS servers. Now, If the user's web browser receives the same IP addresses, then, we can say that the IP addresses will direct the user to the desired web site because two DNS servers sending modified addresses is very rare.

Now consider that the user's web browser receives two different IP addresses from two distinct DNS servers. Hence, we may infer that the one of the DNS server has been infected maliciously [1]. As, now we don't have a majority, the user's web browser will send the human readable website address a third distinct DNS server. The returned IP address is then matched with the first two IP addresses, and then the web browser is directed to the IP address sent by two similar of the three DNS servers.

Algorithm 1: Iterative Multiple DNS Server

Step 1:
Send request to 2 DNS servers
n=4
If *(2 DNS servers return a similar IP address)*
Then *go to step 4*
Else
Go to *step 2*
Step 2:
Set n=3
Step 3:
If *(n/2 DNS servers return a similar IP address)*
Then *go to step 4*
Else
n=n+1
Go to *step 3*
Step 4:
Go to *the IP address sent by at least n/2 DNS servers.*

Consider that a web browser is not able to go to step 4 after receiving IP addresses from 2 DNS servers. Now, the Web Browser will send the human readable address to a third DNS server. The reply received by the web browser will be matched with the IP addresses received by the earlier DNS servers. Now, if the condition in the step 3, i.e., if at least n/2 (where n is the number of DNS servers) servers send the same IP address, then, the IP address can be assumed to be safe and the web browser directs to the above IP address.

Else, we approach another DNS server with the human readable IP address name and the cycle continues until we meet the condition in step 3.

IV. CONCLUSION

This method using the described algorithm gives an easy to implement, efficient solution to overcome the problem of DNS Poisoning. Given the currently available networking and hardware capabilities, the above solution is feasible to implement.

REFERENCES

[1] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in dns and dnssec", in Proceedings of the the Second International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society, 2007, pp. 335–342.
[2] [Online]. Available http://portal.acm.org/citation.cfm?id=1249254.1250514W.-K.
[3] Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
[4] [Online]. http://www.secmaniac.com/dns.htm
[5] [Online]. http://www.computer-network-security-training.com/what-is-a-dns-poisoning-attack/
[6] Behrouz A. Forouzan, "TCP/IP Protocol Suite", fourth edition, Tata McGraw-Hill.