BOOK CHAPTER | Domain Name System Security

Performance Evaluation of Domain Name System (DNS) Security

[1]Arinze, U.C., [2]Eneh, A.H. & [3]Longe, O.B.
[1&2] Department Computer Science, University of Nigeria, Nsukka, Nigeria
[3]Computational Sciences & informatics Academic City University College, Accra, Ghana
Email: [1]arinzeuchechukwu@gmail.com , [2]agozie.eneh@unn.edu.ng, [3]olumide.longe@aun.edu.ng
Tel: +2348066532557, +2348076756975, +233595479930

Abstract

Domain Name System is a hierarchical naming system built on a distributed database for resources connected to the internet. DNS provides a scalable naming system for the Internet and it provides a good mapping between human understandable mnemonics and machine-readable IP addresses (Internet Protocol addresses). This work covers the concept of DNS, review of related literature, domain name system security threats and their solutions.

Keywords: Domain Name System, Cache poisoning, DNSSEC

Introduction

With the advent of Internet and with wide-area distributed systems, it becomes important to have a naming system, which must be standard, structured and scalable. The system should also contain information in human readable form that allows users to navigate through the vast library along with addressing formats to the name server to know where to start searching. Domain Name System is one such Naming Service. DNS was invented to provide a scalable naming system for the Internet and it provides a good mapping between human understandable mnemonics and machine-readable IP addresses (Internet Protocol addresses). The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols [1]. The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. The Internet maintains two principal namespaces, the domain name hierarchy [2] and the Internet Protocol (IP) address spaces [3]

Citation: Arinze, U.C., Eneh, A.H. & Longe, O.B. (2022). Performance Evaluation of Domain Name System (DNS) Security
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address spaces. Internet name servers and a communication protocol implement the Domain Name System [4]. DNS forms an entity of WWW architecture that also includes the client using a browser and the server [5]. The accuracy of the information contained within the DNS is vital to many aspects of IP based communications. DNS has no authentication mechanisms included by default and so, increases the risk of falsified DNS information being stored on your DNS resolver by hosts without permission [6]. This lack of authentication and integrity checking of the information within the DNS threaten the proper functionality of the DNS.

Statement of the Problem

Domain Name System resolves host names to IP addresses and IP addresses back into host names over the internet. Information stored in DNS database is public; it tends to be less secure and vulnerable to attacks such as cache poisoning. If DNS is not secure, the information passing through it is prone to attack.

Aim and Objectives

The aim of this work is to develop a reliable security strategy that will protect domain name system (DNS) server. The objectives include:

- To clearly outline and describe the basic concepts of DNS security
- To outline the steps involved in managing DNS securely

Conceptual Framework

DNS is a hierarchical naming system built on a distributed database for resources connected to the internet. DNS maps domain names to their corresponding IP addresses and vice versa [6]. To connect to a system that supports IP, the host initiating the connection must know in advance the IP address of the remote system.

Fig 1: The DNS System

Source: https://medium.com/free-code-camp/an-introduction-to-http-domain-name-system-servers-b3e7060eca98

An IP address is a 32-bit number that represents the location of the system on a network. When a website is requested, it is the root server that processes that information first in order to identify the next step in the lookup process. Then, the domain name is forwarded to a Domain name resolver (DNR), which is located within an ISP, to determine the correct IP address [7].

This information is sent back to the device you requested it from. The DNS has some components: the database, the server, and the client.

The database is a distributed database and is comprised of the Domain Name Space, which is essentially the DNS tree, and the Resource Records (RRs) that define the domain names within the Domain Name Space. The server is referred to as a name server. Name servers are responsible for managing some portions of the Domain Name Space and for assisting clients in finding information within the DNS tree. Name servers are authoritative for the domains in which they are responsible. They can also serve as a delegation point to identify other name servers that have authority over sub domains within a given domain [8].The domain name system also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the internet protocol suite.

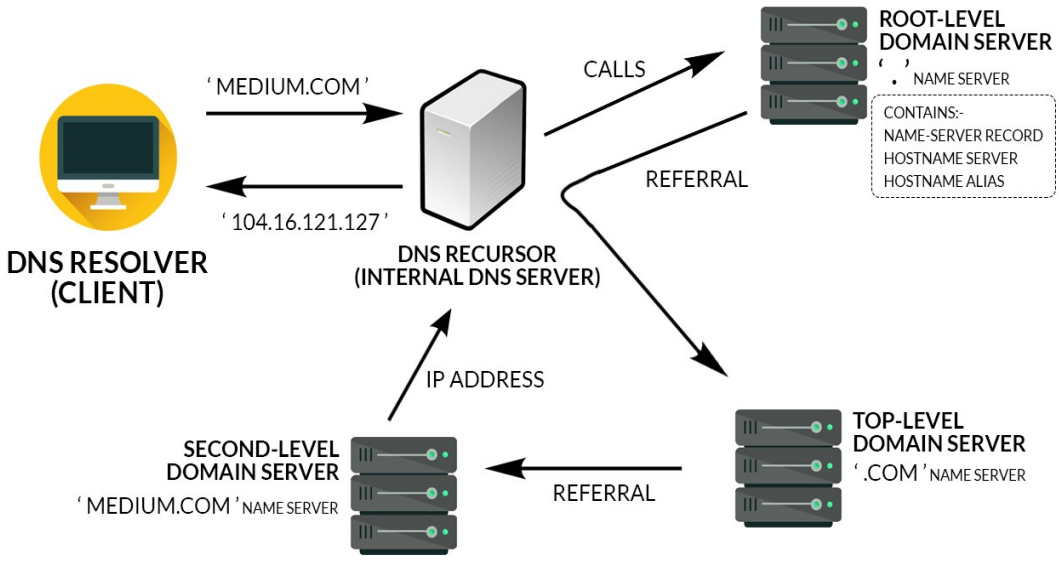

Fig 1: Flow of DNS Resolution, maintained by a distributed database system
Source: https://medium.com/free-code-camp/an-introduction-to-http-domain-name-system-servers-b3e7060eca98

Domain Name System (DNS) Threats

Domain Name Systems if not properly secured will be susceptible to the following attacks:

a. **DNS cache poisoning:** the DNS cache of a name server (or even a simple workstation client) may be poisoned with the wrong information thereby redirecting unsuspecting users to incorrect websites.

b. **Typo-squatting:** The practice of registering a domain name that is confusingly similar to an existing popular brand. It is often considered a problem for trademark attorneys, risk to the confidentiality of corporate secrets, it can also be used to steal information [18]. Distributed denial of service attacks (DDoS): DNS is vulnerable to such attacks because it represents a logical choke point on the network. If the DNS infrastructure cannot handle the number of incoming requests it receives, the performance of the site will be degraded or disabled.

c. **Illegitimate Zone Transfers:** if master and slave name servers are not secured it is possible for intruders to acquire an entire copy of your DNS information, including internal DNS information and thereby have a partial or entire picture of your internal IP structure. Search Engine Page Ranking: it is a naming threat issue as well as that of auto completers in web browsers. Page ranking can be manipulated so that key words bring up harming sites that unsuspecting users may click on assuming they are the appropriate site [12]. DNS amplification: is a tactic used in DDoS attacks that leverages DNS servers deployed in insecure recursive configurations.

d. **Registrar Hijacking:** The majority of domain names are registered through a registrar company, and these represent single points of failure (SPoF). If an attacker can compromise your account with your chosen registrar, they gain control over your domain name, allowing them to point it to the servers of their choice, including name servers, Web servers, email servers or the domain could be transferred to a new owner making domain name recovery a complex matter.

e. **DNS Tunnelling:** it encodes the data of other programs or protocols in DNS queries and responses.

f. **Client flooding:** it occurs when a client system sends out a query, but receives and accepts thousands of DNS responses from the attacker.

Solutions to Domain Name System Security Threats

DNSSEC (DNS SECurity extentions): security extensions were added to the DNS in order to address the security issues surrounding the DNS. These extensions are commonly referred to as DNSSEC extensions. These security enhancements to the protocol are designed to be interoperable with non-security aware implementations of DNS. The scope of DNSSEC can be summarized into three services: key distribution, data origin authentication, and transaction and request authentication [8]. The key distribution service not only allows for the retrieval of the public key of a DNS name to verify the authenticity of the DNS zone data, but it also provides a mechanism through which any key associated with a DNS name can be used for purposes other than DNS.

Data origin authentication is the crux of the design of DNSSEC. It mitigates such threats as cache poisoning and zone data compromise on a DNS server. The RRSets within a zone are cryptographically signed thereby giving a high level of assurance to resolvers and servers that the data just received can be trusted. DNS transaction and request authentication provides the ability to authenticate DNS requests and DNS message headers. This guarantees that the answer is in response to the original query and that the response came from the server for which the query was intended.

a. Single Purpose DNS Servers: restricting your DNS servers to performing only DNS task as well as having multiple DNS servers responsible for different name resolution tasks is another defensive as well as load-balancing and fault tolerance strategy [12]. Restricting DNS servers to being just DNS servers means that the admin can have a system with minimal services running and thus reduce its workload. If more than one machine is at your disposal, then having DNS servers that respond to different types of requests and that are potentially placed in different parts of your network structure also offers additional security.

b. Transaction Signatures (TSIG): As Householder and King and others point out, TSIG allows name servers to cryptographically authenticate and verify zone data, that is, TSIG is a mechanism that name servers can use to make sure that the data they are receiving is the data that was originally sent and that it was sent by the host they requested it from. TSIGs rely on the use of shared secret keys to authenticate and verify the data that is being transmitted.

c. Restriction on who can query your name server: by using acls, admins can restrict those users that are allowed to send queries globally or to a particular zone that the name server services. Globally queries can be controlled by a directive in the global options section of the named.conf file [12].

d. Use of response policy zones: to cut off infected devices from command-and-control servers. Response policy zones are zones that embed rules instead of records.

e. Monitoring DNS traffic: monitor traffic to your name servers, including aggregate query rate, top queriers. To reduce the risk of falling victim to a DDoS attack against your domain names, engage a managed DNS provider that uses a widely distributed, highly redundant network of Anycast servers to handle DNS traffic. Using Anycast to mirror your DNS servers can greatly improve performance as well as balance the load during a DDoS attack. Also, to reduce the risk of hijacking, choose a registrar that offers additional security precautions, such as multi-factor authentication.

DNS Server Security Recommendations

Organizations and IT Policy makers can strengthen security of their DNS servers by adopting the following strategies:

i. Audit your DNS zones
ii. Keep your DNS servers up-to-date
iii. Hide BIND version
iv. Restrict zone transfers
v. Disable DNS recursion to prevent DNS poisoning attacks
vi. Use isolated DNS servers
vii. Use a DDOS mitigation provider
viii. Use two-factor authentication

Conclusion

Hackers will always try to target your public company services, researching to find weaknesses and vulnerabilities inside your DNS. Having a solid DNS hardening policy will help to mitigate most of the cyber-attacks described above.

References

[1] Domain Name System. Retrieved February 8, 2018, from http//:www.wikipedia.com
[2] Mockapetris, P. Domain Names - Concepts and Facilities, The Internet Society.
[3] Postel, J. (Ed.) Internet Protocol - DARPA Internet Program Protocol Specification, Information Sciences Institute. The Internet Society.
[4] Mockapetris, P. Domain Names - Implementation and Specification. The Internet Society.
[5] Roberto Baldoni, Simona Bonamoneta, Carlo Marchetti. Implementing Highly-Available WWW Servers based on Passive Object Replication. Retrieved February 5, 2018, from http://crystal.uta.edu/~kumar/cse6306/papers/Charishma.pdf
[6] Domain Name System: Security strategies (2012). Retrieved February 5, 2018, from https://www.asd.gov.au/publications/protect/dns_security.pdf

[7] Fisher, T. (2017). What Is DNS (Domain Name System)? Retrieved February 7, 2018, from https://www.lifewire.com/what-is-dns-domain-name-system-2625855
[8] Davidowicz, D. Domain Name System (DNS) Security. Retrieved February 5, 2018, from http://compsec101.antibozo.net/papers/dnssec/dnssec.pdf
[9] Domain name system. Retrieved February 20, 2018, from http://www.cialfor.com/2016/02/03/domain-name-system-dns-caching/
[10] Lioy, A., Maino, F., Marian D., and Mazzocch, D. (2000), DD.DNS Security. Retrieved February 5, 2018, from http://cs.unc.edu/~fabian/course_papers/dns-_security.pdf
[11] Khan. F., Sisodia, A., & Tripathi, A. (2011). Experimental study of DNS performance. Retrieved February 5, 2018, from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1129&context=ism
[12] Drake, J. DNS Security and Threat Mitigation: An Overview of Domain Name System Threats and Strategies for Securing a BIND Name Server. Retrieved February 5, 2018, from http://www.infosecwriters.com/text_resources/pdf/JDrake_DNS_Security.pdf
[13] Householder, A., & King, B. Securing an Internet Name Server. http://www.cert.org/archive/pdf/dns.pdf
[14] Liu, C., & Albitz, P. (2006). DNS and BIND. Sebastopol, CA:O'Reilly.
[15] Ollmann, G., (2005). The Pharming Guide: Understanding & Preventing DNS-related Attacks by Phishers. http://www.ngssoftware.com/research/papers/ThePharmingGuide.pdf.
[16] Plante, N. (2004). Practical Domain Name System Security: A Survey of Common Hazards and Preventative Measures. Available at: http://www.infosecwriters.com/text_resources/pdf/dns-security-survey.pdf.
[17] Evers, J. (2005). DNS Servers: An Internet Achilles Heel. CNET News.com. http://news.com.com/2100-7349_3-5816061.html
[18] Mohan, R. (2011). Five DNS Threats You Should Protect Against. Retrieved February 7, 2018, from http://www.securityweek.com/five-dns-threats-you-should-protect-against