As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 7(12): 295-298, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0712057
Available online at: http://www.ijmtst.com/vol7issue12.html

Enhanced Security Model for Domain Name Server

Himanshu Sharma | Vibhor Sharma

[1]Department of Information Technology, Maharaja Agrasen Institute of Technology, Delhi

To Cite this Article

Himanshu Sharma and Vibhor Sharma. Enhanced Security Model for Domain Name Server. *International Journal for Modern Trends in Science and Technology* 2021, *7* pp. 295-298. https://doi.org/10.46501/IJMTST0712057

Article Info

Received: 15 November 2021; Accepted: 16 December 2021; Published: 20 December 2021

ABSTRACT

The article is based on the security related problems that is any how affecting the Domain Name Server
And its solutions that has been developed throughout the last years in order to give a remarkable, ultimate and a safer name resolution protocol for the expanding internet community of present days.
In today's world internet is the key to connect the world in easy and fast way and almost every single person accesses the internet in their day-to-day life as internet grows internet-based attack increases.
When most people use the Internet, they use domain names to specify the website that they want to visit. However, computers use IP addresses to identify different systems connected to the Internet and route traffic through the Internet. The Domain Name System (DNS) is the protocol that makes the Internet usable by allowing the use of domain names.
DNS is widely trusted by organizations, and DNS traffic is typically allowed to pass freely through network firewalls. However, it is commonly attacked and abused by cybercriminals. As a result, the security of DNS is a critical component of network security.

Web criminals doing an internet scam through phished websites that harms the user's confidentiality. Attackers spoof the data by mimicking the original websites using DNS spoofing.

INTRODUCTION

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.example.com translates to 192.0.32.10.

The Domain Name System makes it possible to assign domain names to groups of Internet users in a meaningful way, independent of each user's physical location. Because of this, World Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. Internet domain names are easier to remember than IP addresses such as 208.77.188.166 (IPv4) or 2001:db8:1f70:: 999:de8:7648:6e8 (IPv6). People take advantage of this when they recite meaningful URLs and e-mail addresses without having to know how the machine will actually locate them.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name

servers for each domain. Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed and fault tolerant and has helped avoid the need for a single central register to be continually consulted and updated.

In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

STRUCTURE OF PAPER

The paper is organized as follows: In Section 1, the introduction of the paper is provided along with the structure, important terms, objectives andoverall description.InSection 2 we have information about the platform and tools we have used. In Section 3 we have the complete information how to secure the dns. Section 4 tells us about themethodology and the process description. Section 5 tells us about the future scope and concludes the paper with acknowledgement and references.

OBJECTIVES

- Prevent Spoofing

Spoofing, or DNS cache poisoning, is a type of attack that is focused on corrupting the cached answers on DNS servers with recursion enabled, either through software exploits or protocol weakness. Software exploits can be patched with software updates, but protocol weakness can only be updated with protocol fixes or extensions. DNSSEC is the "fix" for the traditional DNS protocol.

LINUX SERVER

Linux-

From smartphones to cars, supercomputers and home appliances, home desktops to enterprise servers, the Linux operating system is everywhere.

Just like Windows, iOS, and Mac OS, Linux is an operating system. In fact, one of the most popular platforms on the planet, Android, is powered by the Linux operating system. An operating system is software that manages all of the hardware resources associated with your desktop or laptop. To put it simply, the operating system manages the communication between your software and your hardware. Without the operating system (OS), the software wouldnot function.

The Linux operating system comprises several different pieces:

1. Bootloader
2. Kernel
3. Init System
4. Daemons
5. Graphical server
6. Desktop Environment
7. Applications

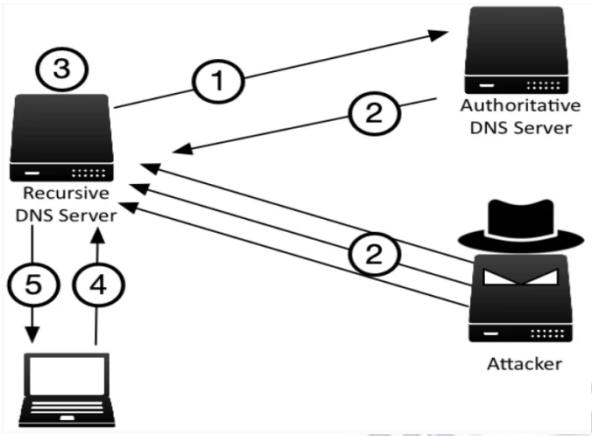
Why uses Linux?

Linux has evolved into one of the most reliable computer ecosystems on the planet.

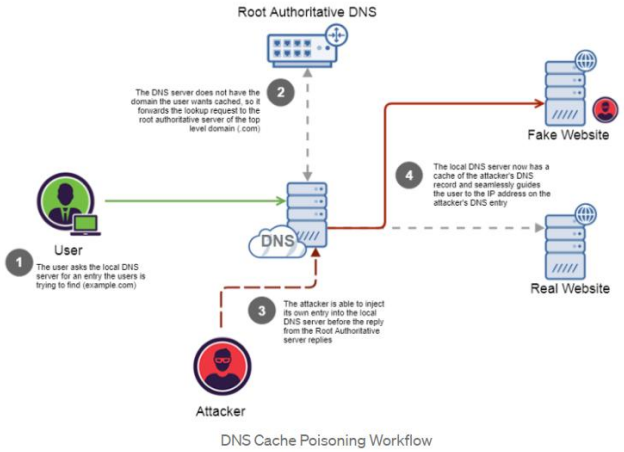
Linux server is free and easy to install and cost of operating linux machine is very low incomparison to other o.s-based machines.

DNS SECURITY

DNS SECURITY PROBLEM It is known the fact that DNS is weak in several places. By using dns we can face the problem of trusting the information which is came from the non – authenticate user or authority, problem occurs when we accepting the additional information that was not requested. Many of the classic security breaches in the history of computers and computer networking have had to do not with fundamental algorithm or protocol flaws, but with implementation errors.While we do not intend to demean the efforts of those involved in upgrading the Internet protocols to make security a more realistic goal, we have ob.-served that if BIND would just do what the DNS specifications say it should do, stop crashing, and start checking its inputs, then most of the existing security holes in DNS as practiced would go away.



1. Recursive DNS server sends a query to an authoritative server, such as querying for the MX record of example.com.
2. The attacker competes with the authoritative server by sending forged responses, through timing to arrive before the authoritative server, and often with multiple "guesses" to increase the chance of success.
3. Upon receiving the forged response, the recursive server has no mechanism to verify the validity of the response and stores the forged answer in its cache.
4. Unsuspecting client queries for the name example.com MX record.
5. The recursive server provides the answer from the now-poisoned cache with the forged answer from the attacker.



DNS Cache Poisoning Workflow

Zone transfers can even be requested from the slave's name servers

for the domains. Attackers often attempt zone transfers in order to gather information about client
local network. If they succeed then they have instantly gotten all of the information about your
internal hosts and networks with very little effort. Of course, a split horizon DNS configuration
can limit the amount of information an attacker will receive, but it is still a good idea to prevent
unauthorized hosts from downloading from zone databases.

How to stay protected? -

The first step is to provide data authentication of the resource records travelling back and forth in the internet. With authentication come also data integrity and data source authentication. The authentication is obtained by means of cryptographic digital signatures.The public key algorithms used for authentication in DNSSEC are MD5/RSA and DSA. The digital signatures generated with public key algorithms have the advantage that anyone having the pub-lic key can verify them. Each resource record in the DNS messages exchanged can be digitally signed providing data origin authentication and integrity of the message. In addition, DNSSEC defines new resource records for storage of public keys in the DNS. These RRs can be used to distribute the keys involved in the security of the DNS itself, but also to distribute keys associated with names to support other security aware protocols (e.g., IPSEC). In the following, we will examine the proposed extensions. First of all, the resource records added for authentication support are KEY and SIG. The KEY RR contains the pub-lic key for a host or for a zone. The SIG RR contains the digital signature associated with each set of records.

METHODOLOGY

Descriptive research on specific attacks that are performed on Websites have been done by me. DNS spoofing, now a days have become a critical issue to be resolved which is very common and popular in web crime. Many different approaches have been proposed against it which we discussed above. Giuseppe Ateniese from department of Computer Science of JHU Information Security Institute and Stefan Mangard from Institute for Applied Information Processing and Communications (IAIK) both proposed a new

Approach to DNS SECURITY (DNSSEC). In our paper we presented a technique to prevent DNS server from attacker. This is having a 1024 pubic key which is used by RSA encryption to encrypt the url request by user. Further more Blum BlumShub generator is used to generate 1024 binary bits and those bits are appended to the encrypted url data. Finally, this whole encrypted data will be sent to server site. At server site, RSA decryption will be done to decrypt the data received from client site. And finally resulted in an original form of request. This whole methodology will help the user from being attacked by hackers. If any attacker in middle try to eavesdrop or divert the request from original DNS server then he won't be able to judge the real request. 166 IV. RESULT RSA 1024 Encryption with Blum Blum shrub generator

FUTURE SCOPE AND CONCLUSION

DNSSEC is designed with full backward compatibility in mind. There are three (3) possible answers[1] when a validating resolver performs validation on a response. Below is a short description of each response:

- ***Secure:*** the answer passed every validation, this means DNSSEC was fully deployed for this domain and every step was configured correctly.
- ***Insecure:*** the zone has yet to deploy DNSSEC, and the validating resolver fell back to using the traditional "insecure" way of resolving this domain name.
- ***Bogus:*** the zone has deployed DNSSEC, but one of the checks has failed, indicating there might be a spoofing attempt.

As you can see, most of us are getting response #2 today, because the majority of the zones have yet to be signed; when you choose to deploy DNSSEC and have done so correctly, the rest of the world will start getting response #1 from your zone data. If someone attempts to spoof your DNS records after you have deployed DNSSEC, the validating resolvers of the world will detect that and return response #3 to the clients, preventing them from obtaining the spoofed answer.

REFERENCES

[1] A. Gulbrandsen, P. Vixie, A DNS RR for specifying the location of services (DNS SRV),October 1996

[2] BCP 20, H. Eidnes et. al. Classless IN-ADDR.ARPA delegation, March 1998. This is about CIDR, or classless subnet reverse lookups.

[3] C. Farrell, M. Schulze, S. Pleitner, D. Baldoni, DNS Encoding of Geographical Location,11/01/1994.

[4] RFC 2536 "DSA KEYs and SIGs in the Domain Name System (DNS)", Donald Eastlake, IBM, March 1999.

[5] RFC 2537 "RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)", Donald Eastlake, IBM, March 1999.

[6] RFC 2538 "Storing Certificates in the Domain Name System", Donald Eastlake, IBM, Olafur Gudmundsson, TIS Labs, March 1999