International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 07 | July - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Enhancing Cyber Defense: A Comprehensive Study of DNS Security

Vaishnavi Gulhane . Dr.R.S.Bansode

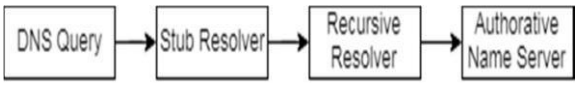
MCA Department, P.E.S. Modern College Of Engineering Pune, India

Abstract:-
As the internet continues to evolve, robust security measures are becoming increasingly vital at every stage. One crucial component, the Domain Name System (DNS), plays a pivotal role in helping users access websites. However, its lack of inherent security mechanisms makes it vulnerable to exploitation. Unsecured DNS can be manipulated, leading to threats like DNS tunneling, hijacking, and cache poisoning. To address these vulnerabilities, DNSSEC (Domain Name System Security Extension) offers a critical layer of security for a safer DNS system.

Keywords: DNS, DNSSEC, Tunneling, Cache poisoning, Hijacking

1.Introduction:

The DNS is crucial for the Internet, translating human-readable domain names like google.com into IP addresses such as 8.8.8.8, necessary for routing network traffic. Initially, security wasn't a major concern, but with the Internet's expansion, the DNS has become more vulnerable to attacks jeopardizing user data. Hence, various security mechanisms have been implemented to protect the DNS system.



2. Objective, Scope, Methodology:

2.1 Objective:

The objective of this Working Group is to enhance the security of the DNS and routing on the Internet. The DNS serves as the online version of a phone book, linking domain names to their actual IP addresses. However, its original design lacked strong security measures, making it vulnerable to mistakes or malicious attacks. The group aims to identify these flaws and recommend security-improving actions to ensure a more stable and secure DNS system.

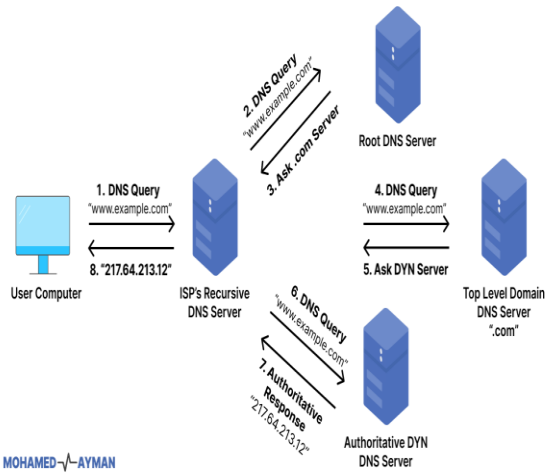
2.2 Scope:

The scope of DNS security encompasses safeguarding the Domain Name System (DNS) from threats or attacks that could hinder its functionality and ensuring its efficient and safe operation. It also involves implementing security measures to prevent unauthorized access to DNS data and addressing broader concerns related to network management and security to preserve DNS services' availability and integrity.

2.3 Methodology:

The methodology for DNS security involves identifying risks or weaknesses, implementing security measures to thwart attacks or unauthorized access, and monitoring the system for any suspicious activity. Additionally, it includes educating administrators and users on securely utilizing DNS and managing potential security incidents. The overarching goal is to ensure the reliability and security of DNS against attacks to maintain internet services' availability and integrity.

3.How Domain Name System works:



[Fig 2]

When a client inputs a domain name like "www.company.com," the client computer searches its DNS cache for the IP address. If not found, the client sends a request to the ISP's DNS server, which routes it to the Root DNS Server, eventually resolving the IP address from the top-level DNS server (.com).

3.1 Threats and Vulnerabilities in DNS:

A vulnerability refers to any flaw in a system or network that allows attackers to compromise availability, confidentiality, and integrity. Common vulnerabilities in DNS include changed DNS data and unauthorized access. Threats to DNS security encompass risks like cache poisoning, denial-of-service attacks, DNS hijacking, and DNS tunneling.

3.2.1 DNS Hijacking:

DNS hijacking is the unauthorized manipulation of data in DNS servers and domain registrar records, potentially redirecting traffic from legitimate servers to malicious ones. This exploit can stem from vulnerabilities within the domain registrar's infrastructure or through direct tampering with DNS records by malicious actors. When attackers gain control over a domain name, they often utilize it to create counterfeit websites, masquerading as trusted entities such as financial institutions or online service providers. The primary objective is typically to pilfer personal user information, such as login credentials and email addresses.

3.2.2 Cache Poisoning:

Cache poisoning represents a type of cyber attack wherein attackers tamper with the data stored in the cache memory of DNS name servers. DNS translates domain names into corresponding IP addresses to enable communication across networks and the internet. In a cache poisoning attack, perpetrators manipulate the cache to serve incorrect IP addresses for domain names, leading unsuspecting users to malicious websites. This tactic can give rise to various forms of exploitation, including denial-of-service (DoS) attacks and man-in-the-middle (MITM) attacks, which redirect users to fraudulent websites surreptitiously.

3.2.3 Denial of Service (DoS):

A denial-of-service attack aims to disrupt legitimate users' access to a network or website by inundating it with an overwhelming volume of traffic until it becomes unreachable. Perpetrators orchestrate DoS attacks by flooding the target with an excessive number of requests, causing the network to become congested and unresponsive. Distributed denial-of-service (DDoS) attacks, orchestrated from multiple sources simultaneously, are frequently employed to amplify the impact of such assaults. The term "denial-of-service" denotes the scenario in which genuine users are unable to access network resources due to the inundation of malicious traffic.

3.2.4 DNS Tunneling:-

DNS tunneling exploits the DNS protocol to transmit data between a source and a DNS resolver. It establishes a covert communication channel between the user and the resolver, enabling data transfer. Malicious actors often exploit this technique by embedding malware within the tunnel to intercept communications between end users. Since users perceive the connection as established with the DNS server, they may overlook the attack. Given the

critical role of DNS in internet functionality, DNS security is essential. Various techniques, including VPNs, DNSSEC, encryption, and other security measures, are employed to safeguard DNS.

4.IMPLEMENTATION AND RESULTS:-

Securing the Domain Name System (DNS) requires addressing numerous inherent vulnerabilities and threats. To effectively mitigate these risks, we have implemented a variety of security measures, including DNSSEC, BIND9, OpenDNS, Certificate Verification, and Encryption. A comprehensive overview of the parameters addressed by these security techniques is provided in Table 1 at the end of this section.

4.1 DNSSEC

Domain Name System Security Extensions (DNSSEC) signify a significant advancement in DNS security. DNSSEC consists of extensions to DNS aimed at enhancing its security by providing authentication and integrity verification mechanisms. Widely acknowledged as a highly effective tool, DNSSEC mitigates vulnerabilities such as DNS hijacking, DNS tunneling, Denial of Service (DoS) attacks, and cache poisoning. Given the inherent weaknesses in the DNS system and the potential exploitation of DNS data by malicious actors, DNSSEC stands as a crucial defense against these threats.

4.2 THE IMPORTANCE OF DNSSEC:-

The recent discovery of vulnerabilities within the DNS system highlights the critical need to reinforce its security. These vulnerabilities have exposed the risk of session hijacking and compromise of authentication credentials, posing significant threats to the confidentiality and integrity of online communications. Unauthorized alterations to IP addresses in DNS databases can result in traffic redirection and manipulation, exacerbating security risks. In response to these challenges, the adoption of DNS Security Extensions (DNSSEC) has become increasingly essential. DNSSEC aims to strengthen the internet's infrastructure by introducing authentication mechanisms to DNS, thereby enhancing overall security. By addressing vulnerabilities within the DNS system, DNSSEC plays a pivotal role in defending against various DNS-based attacks and preserving the integrity of online communication channels.

4.3 Implementation of DNSSEC:

The primary goal of DNSSEC is to verify the data's origin, or to confirm that the information a genuine user receive from the DNS resolver is unaltered by attackers. A small tweak to the DNS protocol is all that DNSSEC needs to keep it backwards compatible. Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS), and Next Secure (NSEC) are the four record types that DNSSEC adds to DNS.

4.3.1 Working of DNSSEC:

Public Key Infrastructure (PKI) authentication, which involves both public and private cryptographic keys, serves as the cornerstone of DNSSEC's security validation method. Here's a detailed explanation of how DNSSEC works:--

An authoritative zone server begins by generating a hash value for the resource record (RR set) using a one-way hash method. Next, the authoritative server encrypts this hash value using its private key, resulting in the creation of an RRSIG (Resource Record Signature), which serves as the digital signature for the RR set. Upon receiving a query from the DNS resolver, the authoritative server sends back the RR set along with the accompanying RRSIG. Subsequently, the DNS resolver utilizes the public DNSKEY to decrypt the RRSIG and computes the hash value using the aforementioned method. It's important to note that the parent zone's private key functions as the DS (Delegation Signer) record and must sign the public DNSKEY to obtain certification. The final step involves the DNS resolver verifying whether the hash value it computed matches the hash value extracted from the RRSIG. Successful

validation of DNSSEC occurs when these two values align otherwise, validation fails.

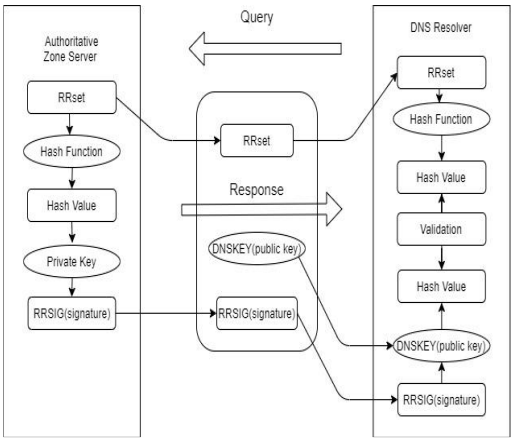


Fig:- 3

A. Using Open DNS and BIND9:

To defend against various attacks such as DNS spoofing, DNS hijacking, and man-in-the-middle attacks, we manage our private DNS server employing services like OpenDNS, Cloudflare, and BIND9. User queries are automatically directed to DNS servers by ISPs, posing a risk of traffic redirection to malicious servers and potential attacks. Since ISPs cannot guarantee user security, we employ our private servers like BIND9 and OpenDNS to mitigate this risk.

B. Certificate Verification:

Ensuring a secure connection between users and DNS servers is paramount in the contemporary digital landscape. HTTP does not encrypt communication initiated by a client and terminated by the server, leaving it susceptible to interception by third parties, potentially compromising data confidentiality and important online credentials. To prevent this, we utilize HTTPS web servers, each equipped with a unique certificate for authentication purposes.

C. Encryption:
Data transmitted between the user and the DNS resolver is often unencrypted, posing a risk to confidentiality. To address this concern, implementing robust encryption mechanisms is essential for maintaining security. We employ two methods to achieve encryption:

1)DNSCrypt:

DNSCrypt is a process that authenticates communications between a user and a DNS resolver, aiming to prevent Man-in-the-Middle attacks, DNS spoofing, and similar threats. It operates similarly to SSL, transforming regular DNS traffic into encrypted and authenticated data, akin to how SSL converts HTTP to HTTPS for web traffic. DNSCrypt effectively safeguards against various attacks, including eavesdropping and Man-in-the-Middle attacks, by securely encrypting communication between the user and the DNS resolver. However, it should be noted that while DNSCrypt ensures secure communication, it does not guarantee the confidentiality of DNS data or the security of DNS services.

2) Use of VPN:
To get their query resolved, the user sends a request to the relevant DNS server. This query is typically sent through the user's ISP in an unencrypted format. However, there is a possibility that the user's ISP might redirect the request to a malicious server, increasing the risk of an attack such as a Man-in-the-Middle (MITM) or DNS Hijacking. This user may utilize a VPN to circumvent. A VPN encrypts user queries so that the corresponding ISP cannot see them. Users' queries may be answered based on the VPN they choose to use. Rather than utilizing open or free DNS, some premium VPNs offer private DNS servers to prevent DNS Hijacking.

Challenges	DNS	DNSSEC	Encryption	Open DNS	Certificate Verification
Authentic	—	✓*	—	—	✓

ation					
Confidentiality	—	—	✓	✓	—
Integrity	—	—	✓	✓	—
Availability	—	✓	—	—	✓

Table:-

The table provided above outlines the security mechanisms employed to safeguard DNS and the key objectives they address, including Confidentiality, Integrity, Availability, and Authentication, as discussed earlier.

5.Discussion and Future Work:

Our primary focus will center on implementing robust security measures such as DNSSEC (Domain Name System Security Extensions), which integrates cryptographic signatures into DNS records to validate their integrity and authenticity. While we recognize that our depiction of DNS is not flawless, we are aware that malicious actors could exploit vulnerabilities to manipulate or intercept DNS data, potentially resulting in security breaches and unauthorized access to sensitive information. Additionally, we plan to explore emerging technologies such as DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH), which encrypt DNS connections to enhance privacy and mitigate eavesdropping risks.

We are dedicated to enhancing authentication mechanisms, encryption protocols, and proactive threat detection to fortify DNS security and enrich users' online experiences. Sustaining a more secure online environment for all users and remaining proactive against emerging threats will necessitate ongoing research and collaboration with domain experts.

6.Conclusion:

As evident from our exploration, the security of the DNS system is of paramount importance. However, its availability, integrity, and authentication are often compromised. Transmitting queries in an unencrypted manner poses significant risks to data security, leaving user information vulnerable to interception by ISPs or malicious actors. To mitigate these risks, we have implemented our DNS server utilizing Open DNS, which efficiently responds to user queries without redirecting them to potentially unsafe servers. The fundamental concept underpinning this approach is the centralization of name bindings within the DNS system. Furthermore, we propose the adoption of DNSSEC as a solution to enhance security. When implemented correctly, DNSSEC offers the highest level of security and reduces network traffic. By safeguarding the integrity and authenticity of DNS records, DNSSEC addresses critical vulnerabilities within the DNS system, thereby bolstering overall security. In conclusion, prioritizing the security of the DNS system is essential to safeguarding user data and ensuring a secure online environment. Implementation of measures like DNSSEC and utilization of secure DNS servers are crucial steps toward achieving this goal.

7. REFERENCES

[1] "NVD - Control - SC-20 - SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)", Nvd.nist.gov, 2020. [Online]. Available: https://nvd.nist.gov/800-53/Rev4/control/SC-20. [Accessed: 06- Jan- 2020].

[2] M. Dooley and T. Rooney, *DNS Security Management*. John Wiley and Sons, Incorporated, 2017, 2017, pp. 57–83.

[3] F. Zou, S. Zhang, B. Pei, L. Pan, L. Li and J. Li, "Survey on Domain Name System Security", 2016 First International Conference on Data Science in Cyberspace (DSC), pp. 603-606, 2016. Available:. [Accessed 10 January 2020].

[4] "SecurityTrails | The Most Popular Types of DNS Attacks", Securitytrails.com, 2018. [Online]. Available: https://securitytrails.com/blog/most-

popular-types-dns-attacks. [Accessed: 11- Jan-2020].[5] S. Bocetta, "What is DNS Cache Poisoning (and How To Prevent It)", GlobalSign Blog, 2018.[6] M. Sammour, B. Hussin, M. Othman, M. Doheir, B. AlShaikhdeeb and M. Saad Talib, "DNS Tunneling: a Review on Features", International Journal of Engineering & Technology, vol. 7, no. 320, 2018.