CONFIGURATION OF A DNS & DEFENSE AGAINST ITS ATTACK

CDAC, Noida
CYBER GYAN VIRTUAL INTERNSHIP PROGRAM

Submitted by:

Akash Chaudhary
under: Mr. Mahesh Adsure
(10, june-19, july) 2024

BONAFIDE CERTIFICATE

This is to clarify that this project report entitle “Configuration of DNS and Defense against it” submitted to CDAC Noida ,is a bonafede record of work done by Akash Chaudhary under my supervision from 10 june 2024 to 19 july 2024.

Declaration by author

This is to declare that this report has been written by me . No part of the report is plagiarized from the other sources. All information included from the sources have been duly acknowledge . I aware that if any part of the report is found to be plagiarized ,I shall take the full responsibility.

Name of the author: Akash Chaudhary
Roll Number: 2022021204
email:akashchaudhary0126@gmail.com

Table of Content

Acknowledgement

The successful configuration of our DNS infrastructure and the implementation of robust defense mechanisms against potential attacks would not have been possible without the invaluable contributions of the following individuals and teams:

- **[Akash Chaudhary]**: For my expertise in DNS architecture and design, providing critical insights into the optimal configuration of our DNS servers to ensure high availability, performance, and security.
- **[Akash Chaudhary]**: For my in-depth knowledge of DNS security threats and vulnerabilities, enabling us to develop comprehensive defense strategies to protect our DNS infrastructure from attacks such as cache poisoning, DNS tunneling, and DDoS.
- **[Akash Chaudhary]**: For my meticulous implementation of the DNS configuration and security measures, ensuring that the system functions as intended and provides the necessary level of protection.
- **[Akash Chaudhary]**: For my role in testing and validating the DNS configuration and defense mechanisms, identifying potential weaknesses and implementing necessary improvements.
- **[Akash Chaudhary]**: For my ongoing monitoring and maintenance of the DNS infrastructure, ensuring its continued reliability and security.

Their dedication, collaboration, and technical expertise were instrumental in the successful completion of this project. We extend our sincere gratitude for their contributions to the overall security and resilience of my network.

-Akash Chaudhary

Configuration of DNS & Defense from its attack

PROBLEM STATEMENT:

Cache poisoning, DNS tunneling , DNS Amplification, DNS spoofing

Learning objective:

cache poisoning:

"We will be able to configure DNS settings and implement security measures to protect against DNS cache poisoning attacks.”

DNS tunneling:

"We will be able to explain the concept of DNS tunneling, identify its usage in real-world scenarios, detect its presence in network traffic, and implement effective countermeasures to mitigate its impact."

DNS Amplification:

"Students will be able to explain the mechanics of DNS amplification attacks, recognize the symptoms and indicators of such attacks, and implement defensive strategies to prevent and mitigate their impact."

DNS Spoofing:

"Students will be able to explain the concept of DNS spoofing, identify its symptoms and indicators, detect its presence in network traffic, and implement effective countermeasures to mitigate its impact."

CONFIGURATION OF DNS

DNS configuration is critical for a smooth and functional internet experience. Here's why it's important:

- **User-friendliness:** DNS translates complex IP addresses into memorable domain names (like [invalid URL removed]). Without proper configuration, you'd need to remember long strings of numbers to access websites.
- **Accessibility:** Correct DNS configuration ensures your device can find the right IP address for a website. Incorrect configuration can lead to error messages or being directed to the wrong website entirely.
- **Security:** DNS can be configured to use secure servers that block malicious websites. This helps protect you from online threats.
- **Performance:** DNS configuration can impact website loading speed. Optimizing your DNS settings can lead to faster browsing.
- **Control:** Businesses can leverage DNS configuration for various purposes. For instance, they can direct traffic to different servers based on location or manage subdomains.

In essence, proper DNS configuration is the foundation of a seamless internet experience. It translates names to addresses, safeguards you from security risks, and can even enhance website loading speed.

APPROACH:

cache poisoning:

The attacker searches for and exploits flaws in the code, allowing them to place illegitmate headers in the HTTP header field.

DNS tunneling:

The attacker registers a domain such as google.com .The domain name server points to the attacker server,where a tunneling malware program is installed.

DNS amplification:

The attacker repeats this process across multiple DNS server ,magnifying the traffic exponetially ,while directing it toward target,leading to a denial of service.

DNS spoofing:

The user attempts to navigate to a specific domain ,and the dns server sends them to the ip address associated with that domain.

IMPLEMENTATION:

cache poisoning:

Attacker can poison dns cache by impersonating by dns nameserver , making a request to a dns resolver, and then forging the reply when the dns resolver queries a nameserver.

DNS tunneling:

The client encodes data in a DNS request. The way it does this is by prepending a piece of data in the domain of the request

DNS amplification:

send a dns lookup request to open the server with source address to be spoofed with target address
When the server sends the response to the attacker’s queries, it is directly sent to the target site.

DNS spoofing:

This method involves intercepting communications between users and a DNS server to redirect them to a different or malicious IP address. By positioning themselves between the user and the DNS server, attackers can manipulate the DNS responses and lead users to unintended destinations.

CONCLUSION AND RECOMENDATION:

Conclusion:

Understanding and mitigating various DNS-related attack methods, including DNS tunneling, DNS spoofing, DNS cache poisoning, and DNS amplification, is crucial for maintaining the security and integrity of network infrastructure. These attack methods exploit weaknesses in the DNS protocol to achieve malicious objectives such as data exfiltration, traffic redirection, and denial of service. While each attack method operates differently, they share a common reliance on manipulating DNS queries and responses to deceive or overwhelm systems.

Recomendation:

1. Ensure that network administrators and security personnel are well-versed in the mechanisms of DNS-related attacks and their potential impacts.

2. Deploy DNSSEC to add a layer of security by digitally signing DNS responses, helping to prevent spoofing and cache poisoning.

3. Continuously monitor DNS traffic for unusual patterns or volumes that could signal various DNS-based attacks.

4. Implement rate limiting and access control lists to restrict DNS query volumes.

5.Use network monitoring tools to detect and filter out amplified traffic.

6.Implement anomaly detection systems to identify irregularities in DNS traffic patterns.

LIST OF REFERENCES:

1.https://abnormalsecurity.com/glossary/dns-spoofing

2.https://www.imperva.com/learn/ddos/dns-amplification/#:~:text=This%20method%20exploits%20the%20mismatch,to%20a%20denial%20of%20service.

3.https://www.stackpath.com/edge-academy/what-is-cache-poisoning#:~:text=A%20typical%20approach%20to%20cache,content%20from%20the%20cache%20server