Internet Society
India Bengaluru
Chapter

DNS AND

DNS SECURITY

2025

BENGALURU

7 JAN 2025

isocindiabengaluru.org

Introduction

The Domain Name System (DNS) is one of the most essential components of the Internet. It enables users to access websites using easy-to-remember domain names instead of complex numerical IP addresses. DNS acts as a translator between human-readable domain names and machine-readable IP addresses, making internet usage simple and efficient.

The first day of the workshop was dedicated to understanding the fundamentals of DNS and exploring its security aspects. The session aimed to build a strong conceptual foundation by explaining DNS architecture, the query resolution process, and common security challenges. The importance of protecting DNS infrastructure in today's digital world was strongly emphasized throughout the session.

DNS Architecture

DNS follows a hierarchical and distributed architecture to ensure scalability, reliability, and global accessibility. It consists of Root Servers, TLD Servers, Authoritative Name Servers, and Recursive Resolvers. Root servers direct queries to TLD servers, which then guide them to authoritative servers containing domain records. Recursive resolvers coordinate this process to provide the correct IP address and ensure efficient domain resolution across the internet.

DNS Query Resolution Process

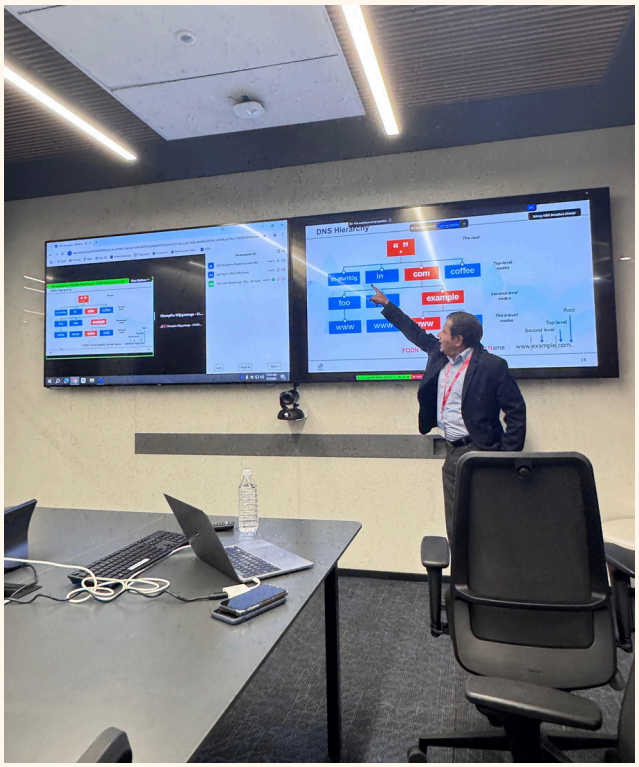
The DNS query resolution process was explained step-by-step to give participants a clear understanding of how websites are accessed.

When a user enters a domain name in a browser, the request is first sent to a recursive resolver. The resolver then contacts the root server, which directs it to the relevant TLD server. The TLD server provides the address of the authoritative name server, which finally responds with the correct IP address of the requested domain.

This structured process ensures accurate and reliable communication between users and web servers.

Common DNS Attacks

DNS is a critical part of internet infrastructure and is frequently targeted by cyber attackers. The session discussed several common DNS-based attacks and their serious impacts. DNS Spoofing (Cache Poisoning) involves inserting false information into a resolver's cache to redirect users to malicious websites. Distributed Denial of Service (DDoS) attacks overload DNS servers with excessive traffic, disrupting services. Man-in-the-Middle attacks intercept and manipulate DNS responses, while DNS Amplification attacks exploit servers to generate massive traffic against a target. These attacks can cause data theft, service disruption, and financial losses, emphasizing the need for strong DNS security mechanisms.



DNSSEC – Enhancing DNS Security

To address DNS vulnerabilities, the concept of DNS Security Extensions (DNSSEC) was introduced. DNSSEC enhances security by adding cryptographic signatures to DNS records, ensuring data authenticity and integrity.

DNSSEC works by digitally signing DNS data so that users can verify whether the response they receive is genuine and has not been tampered with. It establishes a chain of trust from root servers to authoritative servers, protecting users from spoofing and cache poisoning attacks.

Practical explanations were provided to demonstrate how DNSSEC validates domain authenticity and strengthens the overall security of internet infrastructure.

Conclusion

The day of the workshop provided a comprehensive understanding of DNS fundamentals and security mechanisms. Participants gained valuable insights into DNS architecture, query resolution, common attack vectors, and the implementation of DNSSEC.

The session successfully highlighted the critical role of DNS in maintaining a secure, reliable, and resilient internet ecosystem. By combining theoretical concepts with practical demonstrations, the workshop enhanced participants' awareness of DNS security challenges and solutions.