A DNS Spoofing Tool Used to Manipulate DNS Records, Directing Users to Malicious Websites Instead of the Intended Ones

D. Kalyan Kumar [1], Mancham Srilekha [2], Shaik Khaja Masthan [3], Vupputuri Tharun Kumar Reddy [4],
[1,2,3,4,5] **Chalapathi Institute Of Technology**, **A.R.Nagar, Mothadaka**, Guntur -522016,A.P, India.

ABSTRACT:

Domain Name System (DNS) spoofing, also known as DNS cache poisoning, is a critical cyber attack that exploits vulnerabilities in the DNS protocol to redirect traffic from legitimate websites to malicious sites [12]. This attack manipulates the DNS cache to insert false address mappings, compromising the integrity of the DNS resolution process. The primary objective of this project is to demonstrate the mechanics of DNS spoofing, analyze its potential impacts on network security, and explore mitigation techniques [1]. The project will showcase practical demonstrations of DNS spoofing in a controlled environment, highlighting the consequences of such attacks on web traffic and user data. Additionally, the research will delve into defensive measures like DNSSEC (Domain Name System Security Extensions), which help mitigate these types of threats. By understanding DNS spoofing and its countermeasures, this project aims to raise awareness about the importance of securing DNS infrastructure to protect against emerging cyber security risks [2].

KEYWORDS: Domain Name System, Unauthorized access, malicious activities, Security Extensions and DNS infrastructure.

1] INTRODUCTION:

The DNS Spoofing Demonstration project is designed to showcase the potential risks and implications of DNS spoofing (also known as DNS cache poisoning) in real-world network environments [4]. This project simulates a DNS spoofing attack to demonstrate how malicious actors can redirect user traffic to unauthorized websites by poisoning the DNS cache. The project highlights the techniques used to carry out the attack, the vulnerability in the DNS protocol, and explores mitigation strategies to prevent such attacks [3]. Project Features: DNS Spoofing Simulation: The project demonstrates how attackers manipulate the DNS resolution process to inject false address mappings into the DNS cache, leading to redirected traffic [2]. Real-Time Demonstration: Users can witness how DNS cache poisoning works in real-time by observing the impact on network traffic and website accessibility [9]. Vulnerability Analysis: The project explains the weaknesses in the DNS protocol that make it susceptible to spoofing, focusing on the lack of

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

authentication in DNS responses [10].

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

Mitigation Strategies: The project also covers countermeasures like DNSSEC (Domain Name System Security Extensions) to protect against DNS spoofing attacks and ensure the integrity of DNS records [5].Technologies Used: Python: Python is used to build the DNS spoofing attack tool and simulate the DNS resolution process. It handles network traffic interception and manipulation during the attack. Scapy: Scapy is a powerful Python library for network packet manipulation [7]. It is used to craft and inject malicious DNS responses into the DNS cache. DNSSEC: DNSSEC is a suite of extensions that add an additional layer of security to the DNS protocol. The project explores how DNSSEC can prevent DNS spoofing by ensuring that DNS responses are authentic. Wireshark: Wireshark is used for packet sniffing to capture and analyze DNS traffic, providing insight into how the spoofing attack works [8].

Project Components: DNS Spoofing Tool (Python/Scapy): The tool that simulates the attack by sending forged DNS responses to target systems, poisoning their DNS cache. Network Traffic Analyzer (Wireshark): Captures and displays DNS queries and responses during the attack, allowing users to observe the manipulation in action. DNS Server Configuration: The DNS server setup that interacts with the victim client, allowing the demonstration of a successful attack and the potential risks. Usage: Running the Attack: The DNS spoofing demonstration can be started by executing the script on the attacker's machine [7]. This initiates the attack by sending spoofed DNS responses to the target client. Observing the Impact: Users can see how the victim machine's DNS cache is poisoned, redirecting traffic to a malicious site instead of the intended legitimate website. Testing Mitigations: Users can also test how DNSSEC and other security measures can prevent the attack, allowing them to compare the effectiveness of different defenses. Future Improvements: Enhanced Attack Variants: Expand the attack to target more sophisticated DNS configurations and explore additional techniques like DNS tunneling or cache exhaustion [10]. User Authentication for DNS Servers: Implement authentication mechanisms for DNS queries to ensure only legitimate servers can resolve domain names. Real-World Case Studies: Include real-world DNS spoofing attacks and their impact on organizations, providing a more comprehensive understanding of the risks. UI for Demonstration: Develop a user-friendly interface to control and visualize the attack in a more interactive manner, allowing users to trigger and monitor the

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

spoofing in a graphical environment [11].

2] LITERATURE SURVEY:

.Chien, A. S., & Cheng, L. (2008). DNS Spoofing and Mitigation Techniques. IEEE Security & Privacy This paper discusses various methods of DNS spoofing attacks and introduces techniques to

mitigate these attacks, such as DNSSEC (Domain Name System Security Extensions), which helps prevent cache poisoning by ensuring the authenticity of DNS data.

2. Mankin, A., & Atkins, D. (2005). DNSSEC:

Domain Name System Security Extensions. IETF RFC 4033, RFC 4034, RFC 4035.This is the foundational document on DNSSEC, which provides cryptographic protection to prevent DNS spoofing. It describes the implementation of DNSSEC and its role in enhancing DNS security against poisoning attacks

3. RFC 5452: DNS Security Threats.

IETFRFCRFC 5452 outlines different DNS security threats, including DNS spoofing and cache poisoning, and provides detailed discussions of how these threats can be mitigated through secure DNS practices.

4. Bertino, E., Sandhu, R., & Bharadwaj, N. (2009).

Securing DNS Against Attacks.

IEEE Transactions on Dependable and Secure Computing This paper provides a comprehensive review of DNS security, focusing on DNS spoofing, its potential impact, and the defense mechanisms available to prevent it, such as DNSSEC and randomizing source ports.

5.Sullivan, M., & Thompson, S. (2004).

Techniques for Defeating DNS Spoofing. Black Hat Briefings This paper discusses real-world scenarios of DNS spoofing and details various methods employed by attackers, while also explaining how administrators can protect their DNS infrastructure through proper configuration and tools.

6.Sweeney, T. (2006). Detecting DNS Spoofing Attacks. Journal of Computer Security

This research proposes techniques for detecting DNS spoofing attempts using anomaly-based methods to identify mismatches between the expected and actual DNS responses.

7.Yang, X., & Liu, Z. (2010). Detection of DNS Spoofing Attacks with Cross-Checking.

International Journal of Computer Science and Network Security This study explores the use of cross-checking mechanisms to detect DNS spoofing, where DNS queries are validated by querying multiple DNS servers to ensure the

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

accuracy of responses.

8. National Institute of Standards and Technology (NIST). (2008). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. NIST This publication includes recommendations for DNS security controls to prevent spoofing,

among other security measures for federal information systems, which can be adopted by organizations to secure their DNS infrastructure.

9. OWASP: DNS Spoofing and Man-in-the-Middle Attacks. OWASP the Open Web Application Security Project (OWASP) provides a guide to web security, including a section on DNS spoofing and other domain-related attacks. It includes best practices for defending against DNS attacks in the context of web applications.

10.CVEDatabase: Common Vulnerabilities and Exposures (CVE). CVE Database. The CVE database tracks known DNS spoofing vulnerabilities across different systems, including detailed descriptions of affected software and corresponding patches. This resource is essential for identifying DNS spoofing vulnerabilities and staying up to date with new exploits.

11.CERT Coordination Center (CERT/CC). CERT/CC, CERT provides advisories and incident reports related to DNS spoofing, including real-world examples of attacks and detailed analysis of how they were carried out. This can help understand the impact and nature of DNS spoofing on a practical level.

3. PROBLEM DEFINTION:

Currently, several tools and techniques are available to demonstrate and analyze DNS spoofing attacks. These systems typically

focus on exploiting vulnerabilities within the Domain Name System (DNS) to manipulate DNS records or inject malicious data into DNS caches. Here are a few examples of existing systems and tools used in DNS spoofing attacks or for detecting and mitigating such attacks:

Ettercap: Ettercap is a widely-used network security tool that can perform man-in-the-middle attacks, including DNS spoofing. It allows attackers to intercept and modify network traffic, including DNS queries, to redirect users to malicious websites.

Scapy: Scapy is a Python-based network manipulation tool that is often used to perform DNS spoofing. It enables attackers to craft custom DNS responses and inject them into the DNS cache of targeted systems. Scapy is highly

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

customizable and can be used for both learning purposes and real-world attacks.

Kali Linux Tools: Kali Linux, a popular penetration testing distribution, includes various tools for executing DNS spoofing attacks. It leverages existing tools like Ettercap and Scapy but offers an integrated environment for attackers and security professionals to test DNS vulnerabilities in different network configurations.

Dsniff: Dsniff is a suite of network tools designed for sniffing and injecting traffic. It includes DNS spoofing capabilities that can be

used to poison DNS caches and redirect users to malicious sites without their knowledge. Wireshark: Wireshark is a powerful network protocol analyzer that can be used to capture DNS traffic and analyze attacks such as DNS spoofing. It allows users to observe how DNS responses are tampered with and provides useful insights into identifying vulnerabilities within the DNS protocol. DNSSEC (Domain Name System Security Extensions): DNSSEC is a security protocol designed to prevent DNS spoofing by adding cryptographic signatures to DNS records. While not a tool for spoofing, DNSSEC is a key mitigation technology used to secure DNS against cache poisoning attacks and ensure the authenticity of DNS data.

4. PROPOSED APPROACH: The proposed DNS spoofing demonstration system is designed to simulate and showcase the mechanics of DNS cache poisoning, identify potential vulnerabilities in DNS implementations, and explore countermeasures to mitigate the risks associated with DNS spoofing attacks. It offers a range of features that enhance the learning experience and provide practical insights into DNS spoofing and its impact on network security [3].

Key Features: Real-Time Attack Simulation: The system allows users to

conduct real-time DNS spoofing attacks by poisoning DNS caches and redirecting web traffic to malicious websites. Users can observe the impact of the attack in real-time as DNS queries are manipulated. Comprehensive Attack Techniques: It supports various DNS spoofing techniques, such as cache poisoning, DNS redirection, and DNS spoofing with custom response injection. Users can experiment with different scenarios to understand how attackers exploit DNS vulnerabilities. DNS Vulnerability Discovery: The system helps identify DNS vulnerabilities such as missing or improperly

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

configured DNSSEC, lack of response validation, and insufficient security measures against spoofing attempts. Impact Analysis and Reporting: After performing the attack, the system generates detailed reports outlining the steps taken, affected systems, and the severity of the impact. Reports also include recommendations for remediation and securing DNS configurations [5]. Countermeasure Integration: The system incorporates security measures like DNSSEC to demonstrate how these countermeasures can prevent DNS spoofing. Users can toggle between configurations with and without DNSSEC to observe its effectiveness in mitigating attacks [8]. User-Friendly Interface: The system features an intuitive interface that allows users to configure and initiate DNS spoofing attacks,

observe results, and understand the attack's behavior with minimal technical knowledge required. Integration with External Security Tools: The system can be integrated with network monitoring and intrusion detection systems (IDS), such as Snort or Suricata, to demonstrate real-time detection of DNS spoofing and related attacks.

Architecture: Attack Engine: The core of the system, the attack engine, performs the DNS spoofing by injecting malicious DNS responses into the target's DNS cache. The engine is powered by tools like Scapy or Ettercap to craft custom DNS responses [9]. User Interface: The user interface provides a dashboard for configuring the attack, viewing live results, and generating attack logs. It allows users to initiate and control the attack, observe its effects, and analyze captured network traffic [2]. DNS Server Simulation: The system simulates both legitimate and malicious DNS servers. Users can configure the server settings to replicate real-world attack scenarios and observe how the DNS cache is poisoned. Reporting Module: Once the attack is completed, the reporting module generates detailed reports on the attack's success, affected systems, and suggested actions to mitigate the attack.

Security Measure Integration: The system supports integrating security measures, such as DNSSEC and DNS filtering, to showcase how these techniques prevent DNS spoofing attacks.

Benefits: Educational Tool: The system is an ideal educational tool for understanding DNS spoofing and its implications. It enables students, network administrators, and cyber

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

security professionals to gain hands-on experience with real-world attacks and defenses.

Proactive Security Testing: By simulating DNS spoofing attacks, users can proactively test their DNS infrastructure and identify potential vulnerabilities before they are exploited in a real-world scenario. Enhanced Awareness: The system raises awareness of DNS security risks, helping organizations understand the importance of securing their DNS infrastructure to prevent attacks such as DNS spoofing. Real-Time Attack Simulation: The ability to perform and observe attacks in real-time allows users to better grasp the dynamics of DNS vulnerabilities and responses, improving their understanding of network security.

Future Enhancements: Integration with Advanced Security Tools: Future versions of the system could include integration with advanced security tools such as SIEM platforms, intrusion prevention systems (IPS), and network firewalls to provide a more comprehensive demonstration of DNS spoofing detection and prevention. Automated Vulnerability Detection:

Implement automated DNS vulnerability detection algorithms that can scan DNS configurations for weaknesses, such as missing DNSSEC or weak response validation, and provide actionable recommendations for hardening DNS security. Cloud Infrastructure Support: Extend support to simulate DNS spoofing attacks in cloud environments, addressing emerging threats related to cloud DNS services and hybrid infrastructure. AI-Driven Attack Simulation: Leverage artificial intelligence to develop adaptive attack simulation techniques that evolve in response to new DNS vulnerabilities and emerging attack strategies [10]. User Authentication and Logging: Implement user authentication and detailed logging to enable the system to track different users' activities and attack scenarios for better accountability and auditing [6].

5. System Design

The system development for the Socket.IO Chat Application involves several key steps to create a real-time messaging platform. Initially, requirements are gathered to understand the stakeholders' needs and expectations [15]. With this information, the system architecture is designed, considering both server-side (Flask, Socket.IO) and client-side (HTML, python) components, as well as the communication protocol

(Web Socket) and data storage requirements. Once the environment is set up, development begins with the creation of the Flask server to

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

handle HTTP requests and Web Socket connections using Socket.IO, alongside the client-side interface development [10]. Integration and testing follow to ensure proper functionality, security measures are implemented to protect against common web vulnerabilities, and the application is deployed to a production environment. Ongoing maintenance, user authentication and authorization implementation, scaling, optimization, documentation, and continuous improvement complete the system development process, ensuring a robust, secure, and scalable real-time messaging platform. Identify the stakeholders and gather requirements for the chat application.

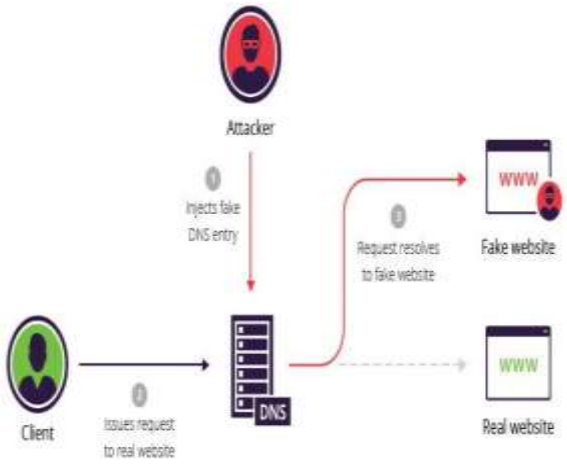

Fig 1: SYSTEM DESIGN

5.1 Implementation

During this activity, the off-the-shelf components relevant to the DNS Spoofing Demonstration Tool are identified and analyzed. These components are crucial in understanding how DNS operates, how spoofing attacks exploit vulnerabilities, and how security measures can be implemented.

The key components include DNS software, such as BIND (Berkeley Internet Name Domain), Unbound, or other custom DNS implementations [12]. These software solutions are responsible for handling domain name resolutions and caching DNS responses. Attackers often target these components to manipulate DNS responses and redirect traffic. Another critical component is the DNS cache, which is present in routers, operating system components, and web browsers. Since DNS caching is used to store previously resolved domain names for faster access, it becomes a prime target for cache poisoning attacks [13].

Additionally, network components, including firewalls, routers, load balancers, and DNS resolvers, play a crucial role in handling DNS traffic. These components can be exploited to intercept and modify DNS responses. By thoroughly identifying and documenting these off-the-shelf components within the system model, security researchers can better understand how they interact with DNS

ISSN: 2278-4632
Vol-15, Issue-04, No.01, April: 2025

spoofing

techniques and assess their impact on the overall security posture of the system. This information becomes essential for architecture analysis, as it helps in identifying security weaknesses and evaluating safeguards that can be implemented to prevent DNS spoofing attacks [11].

6. CONCLUSION:

In conclusion, the development of the vulnerability scanner represents a significant milestone in enhancing cyber security measures for both organizations and individuals. The project aimed to address the critical need for proactive identification and mitigation of potential vulnerabilities within computer systems, thereby bolstering their resilience against malicious threats and attacks. Through meticulous planning, design, and implementation, the vulnerability scanner has emerged as a robust and indispensable tool for fortifying the security posture of target systems.

REFERENCES:

[1] Dr .K. Sujatha, Dr.Kalyankumar Dasari , S. N. V. J. Devi Kosuru , Nagireddi Surya Kala , Dr. Maithili K , Dr.N.Krishnaveni, " Anomaly Detection In Next-Gen Iot:Giant Trevally Optimized Lightweight Fortified Attentional Convolutional Network," Journal of Theoretical and Applied Information Technology, 15th January 2025. Vol.103. No.1, pages: 22-39.

[2] Kalyan Kumar Dasari & Dr, K Venkatesh Sharma, "A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework", JASRAE, vol: 11, Pages: 209-214, 2016.

[3] Kalyankumar Dasari, Mohmad Ahmed Ali, NB Shankara, K Deepthi Reddy, M Bhavsingh, K Samunnisa, "A Novel IoT-Driven Model for Real-Time Urban Wildlife Health and Safety Monitoring in Smart Cities" 2024 8th International Conference on I-SMAC, Pages 122-129.

[4] Kalyankumar Dasari, Dr. K. Venkatesh Sharma, "Analyzing the Role of Mobile Agent in Intrusion Detection System", JASRAE, vol : 15, Pages: 566-573,2018.

[5] Kalyan Kumar Dasari&amp, M Prabhakar, "Professionally Resolve the Password Security knowledge in the Contexts of Technology", IJCCIT, Vol: 3, Issue:1, 2015.

[6] S Deepajothi, Kalyankumar Dasari, N Krishnaveni, R Juliana, Neeraj Shrivastava, Kireet Muppavaram, "Predicting Software Energy Consumption Using Time Series-Based Recurrent Neural Network with Natural Language Processing on Stack Overflow Data", 2024 Asian Conference on Communication and Networks (ASIANComNet), Pages:1-6, Publisher: IEEE.

[7] S Neelima, Kalyankumar Dasari, A Lakshmanarao, Peluru Janardhana Rao, Madhan Kumar Jetty, "An Efficient Deep Learning framework with CNN and RBM for Native Speech to Text Translation", 2024 3rd International Conference for Advancement in Technology (ICONAT), Pages: 1-6,Publisher :IEEE.

[8] A Lakshmanarao, P Bhagya Madhuri, Kalyankumar Dasari, Kakumanu Ashok Babu, Shaik Ruhi Sulthana, "An Efficient Android

Malware Detection Model using Convnets and Resnet Models",2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Pages :1-6, Publisher : IEEE

[9] Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao, GanugapantaVenkata Pavan Reddy, "Build a Tool for Digital Forensics to Analyze and Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.

[10] Dr.D.Kalyankumar, Kota Nanisai Krishna, Gorantla Nagarjuna, PuvvadaVenkata Naga Sai Jagadesh Kumar, Modepalli Yeswanth Chowdary, "Email Phishing Simulations Serve as a Valuable Tool in Fostering a Culture of Cyber security Awareness", IJMTST, Vol: 10, Issue: 02, Pages:151-157, 2024.

[11] Dr.D.Kalyankumar, Muhammad Shaguftha, Putti Venkata Sujinth, Mudraboyina Naga Praveen Kumar, Namburi Karthikeya, "Implementing a Chatbot with End-To-End Encryption for Secure and Private Conversations", IJMTST, Vol: 10, Issue: 02, Pages:130-136, 2024.

[12] Dr.D.Kalyankumar, Panyam Bhanu Latha, Y. Manikanta Kalyan, Kancheti Deepu Prabhunadh, Siddi Pavan Kumar, "A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System", IJMTST, Vol: 10, Issue: 02, Pages:110-116, 2024.

[13] Kalyan Kumar Dasari, K Dr , "Mobile Agent Applications in Intrusion Detection System (IDS)'-JASC, Vol: 4, Issue : 5, Pages: 97-103, 2017.

[14] V.Monica, D. Kalyan Kumar, "BACKGROUND SUBTRACTION BY USING DECOLOR ALGORITHM", IJATCSE, Vol. 3, No.1, Pages: 273 – 277 (2014).

[15]GanugapantaVenkata Pavan Reddy Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao "Build a Tool for Digital Forensics to Analyze and Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.