International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04061
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Zapper: Vulnerability and Port Scanner Tool

Yahaiya Faiz Mulla
Department of MCA, Trinity Academy of Engineering, Pune, India Email: yahaiyamulla123@gmail.com

Under the Guidance of: Prof. Vaishali Hatkar Assistant Professor
Department of MCA, Trinity Academy of Engineering, Pune, India

Abstract

Zapper is a multi-functional port and vulnerability scanner tool designed to identify security weaknesses and potential vulnerabilities in networks and web applications. This paper outlines the architecture, methodology, and implementation of Zapper, emphasizing its significance in penetration testing and cybersecurity. By integrating features like firewall detection, port scanning, and vulnerability analysis, Zapper provides a robust solution for enhancing system security. Developed by Crypto26, Zapper addresses limitations of traditional tools through efficiency, adaptability, and ease of use.

I. Introduction

With the increasing frequency of cyberattacks, ensuring the security of networks and applications has become a priority for organizations. Cybercriminals exploit vulnerabilities to breach systems, steal data, and disrupt operations. Tools like Zapper serve as essential allies in identifying and mitigating such risks.

Existing tools like Nmap, Nessus, and OpenVAS, while effective, often require significant expertise and computational resources, making them inaccessible to smaller organizations or beginners. Zapper addresses these challenges by offering a user-friendly and lightweight alternative that combines multiple functionalities, including port scanning, firewall detection, and vulnerability analysis.

II. Literature Review

A. *Existing Tools and Limitations*

- **Nmap**: Focuses on port discovery and service identification but lacks comprehensive vulnerability analysis.
- **Nessus and OpenVAS**: Provide advanced vulnerability scanning but demand high computational resources and expertise.

B. *Emerging Needs in Cybersecurity*

Research highlights the need for tools that integrate real-time scanning with vulnerability detection in a unified interface. Zapper fulfills this need by combining lightweight methodologies with advanced scanning capabilities.

III. Block Diagram

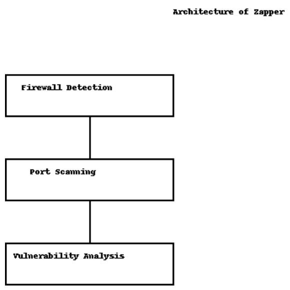

Fig. 1. Architecture of Zapper

A. *Explanation of Stages*

- **Firewall and IDS Detection**: Evaluates responses to detect security systems like firewalls or intrusion detection systems.
- **Port Scanning**: Identifies open ports and their associated services using multi-threaded socket programming.
- **Vulnerability Analysis**: Inspects HTTP responses and headers for common vulnerabilities, such as XSS, SQL injection, and CSRF.
-

IV. Methodology

A. *Stages of Scanning*

1) **Firewall Detection**: Identifies firewalls or IDS based on response behaviors.
2) **Port Scanning**: Uses multi-threaded connections to scan a range of ports.
3) **Vulnerability Assessment**: Matches responses to known vulnerability signatures.

B. *Algorithmic Details*

- **Port Scanning**: Employs optimized multi-threading to minimize delays.
- **Dynamic Analysis**: Real-time probing for runtime vulnerabilities.

V. Components Used

- **Python**: Core programming language for socket and HTTP functionalities.
- **ThreadPoolExecutor**: Enables multi-threaded operations.
- **Libraries**: Includes Scapy, BeautifulSoup, and SQLite for extended capabilities.
-

VI. Conclusion

Zapper provides an efficient, user-friendly, and lightweight solution for port and vulnerability scanning. By addressing the limitations of existing tools, it simplifies penetration testing while ensuring robust security assessments. Future enhancements will focus on integrating machine learning and distributed scanning to expand its capabilities.

References

[1] Fyodor, *Nmap Network Scanning*, Insecure.Org, 2008.
[2] OWASP Foundation, *OWASP Top 10 Vulnerabilities*, 2021.
[3] Tenable, *Nessus Vulnerability Scanner*, Tenable Inc., 2023.
[4] Greenbone Networks, *OpenVAS Vulnerability Scanner*, 2023.
[5] Yahaiya Faiz Mulla, *Zapper: Port and Vulnerability Scanner Implementation Notes*, Trinity Academy of Engineering, 2025.