iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80108

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

A Review of Vulnerability Scanner Tools for Network Security

Karan Das[1], Ganesh Bhoir[2], Piyush Utekar[3], Bhumika More[4], Prof. Supriya Pawar[5]
Department of Computer Engineering, Bharat College of Engineering, Badlapur

Abstract: ***The rapid growth of digital systems and internet-based services has significantly increased the risk of cyber threats, making vulnerability assessment a crucial aspect of cybersecurity. This review paper examines various vulnerability scanner tools and techniques used to identify security weaknesses in networks and applications. It analyzes widely used tools such as Nessus, OpenVAS, and Nikto, focusing on their working mechanisms, features, advantages, and limitations. The paper also discusses different types of scanning approaches, including network-based, host-based, and web application scanning. Furthermore, key challenges such as false positives, performance overhead, and limited vulnerability coverage are highlighted. Based on the analysis of existing studies, the paper provides insights into current trends and suggests future improvements, including the integration of artificial intelligence and automated security solutions. This review aims to assist researchers and practitioners in understanding and selecting appropriate vulnerability scanning tools for enhancing system security.***

I. INTRODUCTION

In the modern digital era, the widespread use of computer networks, cloud platforms, and web-based applications has significantly increased the exposure to cyber threats. Organizations and individuals rely heavily on interconnected systems for data storage, communication, and business operations, making security a critical concern. Cyberattacks such as unauthorized access, data breaches, and malware infections exploit weaknesses present in systems, which are commonly referred to as vulnerabilities. Identifying and addressing these vulnerabilities at an early stage is essential to maintain system integrity and confidentiality.

Vulnerability scanning is an important process in cybersecurity that involves detecting, analyzing, and reporting security flaws in networks, hosts, and applications. It is widely used by security professionals as a preventive measure to reduce risks and strengthen defenses. Various automated tools have been developed to simplify this process, enabling faster and more efficient identification of potential threats. This review paper focuses on analyzing different vulnerability scanner tools and techniques used in network security. It examines the working principles, features, advantages, and limitations of commonly used tools such as Nessus, OpenVAS, and Nikto. In addition, the paper highlights key challenges associated with vulnerability scanning, including false positives, performance issues, and incomplete detection capabilities. The aim of this study is to provide a clear understanding of existing solutions and assist in selecting suitable tools for effective vulnerability assessment.

II. LITERATURE SURVEY

Authors	Paper Title	Year	Focus Area	Advantages	Limitations
A. Kumar et al.	"A Study on Network Vulnerability Scanning Techniques and Tools"	2022	Network Scanning	Detects open ports and network weaknesses, improves security	Limited detection of advanced/zero-day threats
R. Sharma et al.	"Analysis of Web Application Vulnerability Scanners for Security Enhancement"	2023	Web Scanners	Identifies SQL injection, XSS, easy to use	Limited to web applications, misses network-level issues
S. Singh et al.	"Comparative Analysis of Vulnerability Scanning Tools: Nessus vs OpenVAS"	2024	Tool Comparison	High accuracy, detailed reporting, effective comparison	Open-source tools complex to configure
B. Barchuk et al.	"Limitations of Modern Vulnerability Scanners and CVE	2024	Scanner Limitations	Highlights weaknesses, improves understanding of	No implementation solution provided

Authors	Paper Title	Year	Focus Area	Advantages	Limitations
	Systems"			gaps	
Y. Churakova et al.	"Consistency Evaluation of Container Vulnerability Scanners"	2025	Container Security	Scalable, useful for cloud environments	Inconsistent detection results
P. Devadiga et al.	"AI-Based Web Vulnerability Scanner: A Comprehensive Review"	2025	AI-Based Scanning	Reduces false positives, improves detection accuracy	High computational requirements
J. Smith et al.	"Advanced Techniques in Vulnerability Scanning for Modern Cybersecurity Systems"	2026	Advanced Scanning	Faster scanning, real-time detection improvements	Still struggles with zero-day vulnerabilities

III. COMPARATIVE ANALYSIS OF VULNERABILITY SCANNER TOOLS

Vulnerability scanning tools play a crucial role in identifying security weaknesses in systems and networks. Various tools are available, each offering different features, capabilities, and performance levels. This section provides a comparative analysis of some widely used vulnerability scanning tools based on their functionality, advantages, and limitations.

Table: Comparison of Tools

Tool	Type	Features	Advantages	Limitations
Nessus	Commercial	Comprehensive scanning	High accuracy	Paid
OpenVAS	Open-source	Regular updates	Free	Complex setup
Nikto	Web scanner	Fast scanning	Lightweight	Limited scope
Qualys	Cloud-based	Remote scanning	Scalable	Subscription

A. Discussion

The comparison shows that commercial tools such as Nessus provide higher accuracy and better user support, making them suitable for enterprise environments. Open-source tools like OpenVAS are cost-effective and flexible but may require technical expertise for configuration. Lightweight tools such as Nikto are useful for quick web vulnerability assessments but have limited capabilities. Cloud-based solutions like Qualys offer scalability and ease of access but involve recurring costs.

Overall, no single tool is sufficient to detect all types of vulnerabilities, and a combination of tools is often recommended for comprehensive security assessment.

IV. CHALLENGES IN VULNERABILITY SCANNING

Vulnerability scanning tools are essential for identifying security weaknesses; however, they are not without limitations. Several challenges affect the accuracy, efficiency, and reliability of these tools.

One of the major challenges is the occurrence of false positives and false negatives. False positives arise when a tool reports a vulnerability that does not actually exist, leading to unnecessary efforts in verification. On the other hand, false negatives occur when real vulnerabilities are not detected, which can pose serious security risks.

Another significant issue is performance overhead. Comprehensive scanning processes can consume considerable system and network resources, potentially affecting system performance and causing delays in operations. This becomes more critical in large-scale networks where multiple systems are scanned simultaneously.

Limited vulnerability databases also present a challenge. Many tools rely on predefined databases of known vulnerabilities, which may not always be updated with the latest threats. As a result, newly discovered or zero-day vulnerabilities may go undetected.

Additionally, complex configuration and usability issues can make certain tools difficult to operate, especially for beginners. Open-source tools, while flexible, often require technical expertise for proper setup and usage.

Finally, lack of real-time detection is another limitation. Traditional vulnerability scanners operate periodically rather than continuously, which may delay the identification of newly introduced vulnerabilities.
These challenges highlight the need for more advanced, efficient, and intelligent vulnerability scanning solutions.

V. FUTURE SCOPE AND TRENDS

With the rapid evolution of cybersecurity threats, vulnerability scanning tools are continuously improving to address existing limitations. Several emerging trends are shaping the future of vulnerability assessment.
One of the key advancements is the integration of **Artificial Intelligence (AI) and Machine Learning (ML)**. These technologies can enhance vulnerability detection by identifying patterns, reducing false positives, and enabling predictive analysis of potential threats.
Another important trend is the adoption of **cloud-based vulnerability scanning**. Cloud solutions provide scalability, flexibility, and remote accessibility, making them suitable for modern distributed systems and organizations.
The concept of **continuous and real-time monitoring** is also gaining importance. Unlike traditional periodic scans, real-time scanning helps detect vulnerabilities as soon as they appear, reducing the risk of exploitation.
Furthermore, **automation in patch management** is being integrated with vulnerability scanners to automatically fix identified issues, improving efficiency and reducing manual effort.
The use of **threat intelligence integration** is also increasing, allowing scanners to stay updated with the latest cyber threats and vulnerabilities.
These advancements are expected to make vulnerability scanning tools more accurate, efficient, and proactive in ensuring system security.

VI. CONCLUSION

This review paper examined various vulnerability scanner tools and techniques used to identify security weaknesses in networks and applications. Through the analysis, it is evident that vulnerability scanning plays a vital role in strengthening cybersecurity by enabling early detection of potential threats. Different tools offer distinct capabilities; for instance, commercial solutions generally provide higher accuracy and better support, while open-source tools offer flexibility and cost advantages. Similarly, specialized tools such as web scanners are efficient in their specific domains but may lack broader coverage.
The comparative study highlights that no single tool is sufficient to detect all types of vulnerabilities. Each tool has its own strengths and limitations in terms of detection accuracy, performance, usability, and scope. Therefore, a combination of multiple tools and techniques is often required to achieve comprehensive security assessment.
Despite their importance, vulnerability scanners face challenges such as false positives, resource consumption, and limited ability to detect emerging threats. Addressing these issues is essential to improve their reliability and effectiveness. Future advancements, particularly the integration of artificial intelligence, real-time monitoring, and cloud-based solutions, are expected to enhance the overall capability of vulnerability scanning systems.
In conclusion, vulnerability scanning remains a fundamental component of modern cybersecurity practices. Continuous improvements and the adoption of advanced technologies will further strengthen its role in protecting systems against evolving cyber threats.

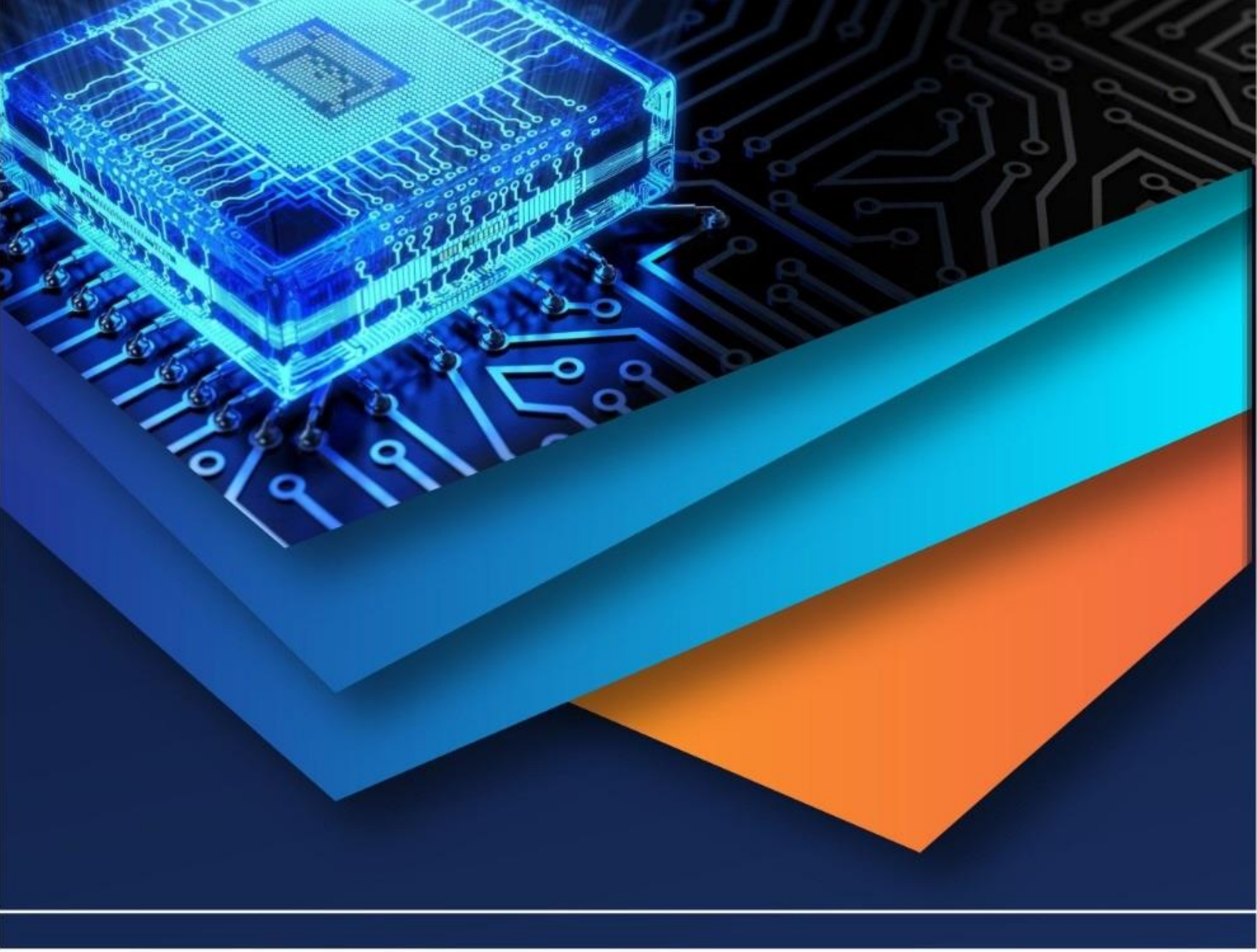
VII. ACKNOWLEDGEMENT

The author would like to express sincere gratitude to Prof. Supriya Pawar for their valuable guidance, continuous support, and constructive suggestions throughout the preparation of this review paper. Their insights and encouragement played a significant role in improving the quality of this work.
The author also extends thanks to the faculty members of the Department of Computer Engineering, Bharat College of Engineering, for providing the necessary academic environment and resources. Appreciation is also given to peers and friends for their support and helpful discussions during the course of this study.

REFERENCES

[1] P. Devadiga, S. Varankar, S. Kumari, and N. Mishra, “AI-Based Web Vulnerability Scanner: A Comprehensive Review,” *Proc. ICICC*, 2025.
[2] B. Barchuk and K. Volkov, “Limitations of Modern Vulnerability Scanners and CVE Systems,” *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 2, pp. 973–989, 2024.
[3] Y. Churakova and M. Ekstedt, “Consistency Evaluation of Container Vulnerability Scanners,” *arXiv preprint arXiv:2503.14388*, 2025.

[4] S. Shimmi, H. Okhravi, and M. Rahimi, "AI-Based Software Vulnerability Detection: A Systematic Literature Review," *arXiv preprint arXiv:2506.10280*, 2025.
[5] Z. Sheng *et al.*, "LLMs in Software Security: A Survey of Vulnerability Detection Techniques and Insights," *arXiv preprint arXiv:2502.07049*, 2025.
[6] B. Steenhoek *et al*., "AI-Powered Vulnerability Detection and Repair in IDE," *arXiv preprint arXiv:2412.14306*, 2024.
[7] H. Singh, "Vulnerability Scanning Tools Review and Industry Insights," Cyphere Security Blog, 2025.
[8] D. Bechenea, "Benchmarking Network Vulnerability Scanners," Pentest-Tools, 2024.
[9] Pentest-Tools, "Year in Review: Vulnerability Scanning Trends," 2024.
[10] L. Derczynski, "Garak: Vulnerability Scanner for Large Language Models," 2024.
[11] Anchore Inc., "Grype: Open Source Vulnerability Scanner for Containers," 2024.
[12] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2023–2025 (updated).
[13] NIST, "National Vulnerability Database (NVD)," 2024.
[14] MITRE, "Common Vulnerabilities and Exposures (CVE) List," 2024–2025.
[15] IEEE, "Recent Advances in Vulnerability Detection Techniques," IEEE Xplore Digital Library, 2024–2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY