Akash Sharma, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Security Vulnerability Assessment and Risk Analysis

[1]Akash Sharma, [2]Arslaan, [3]Shikha Sharma

[1 2] Undergraduate, Department of Computer Science & Engineering, SDCET, MZN
[3]Assistant Professor, Department of Computer Science & Engineering, SDCET, MZN

Abstract- This study presents a systematic approach to vulnerability assessment and risk analysis within a controlled laboratory environment. A virtual network infrastructure was deployed, comprising Kali Linux as the scanning platform and Metasploitable 2 as the target system, to emulate a small-scale enterprise network. Network reconnaissance was conducted using Nmap, followed by vulnerability assessment using Nessus. Identified vulnerabilities were evaluated and classified based on severity using the Common Vulnerability Scoring System (CVSS), and subsequently mapped to corresponding risk levels. The analysis revealed multiple high-severity vulnerabilities, including the presence of default credentials and outdated services, which pose significant security risks and necessitate immediate remediation. Furthermore, the results underscore the effectiveness and extensive coverage of Nessus, supported by its comprehensive plugin database exceeding 80,000 entries. The proposed methodology provides a practical and reproducible framework applicable to both academic research and real-world cybersecurity assessments.

Keywords: Vulnerability Assessment, Risk Analysis, Nessus, CVSS, Network Security

I. INTRODUCTION

In today's interconnected digital environment, organizations increasingly depend on computer networks and information systems to support critical operations. While this advancement enhances efficiency and accessibility, it also introduces significant security challenges. Systems are often exposed to various vulnerabilities arising from misconfigurations, outdated software, and weak authentication mechanisms. If exploited, these vulnerabilities can lead to unauthorized access, data breaches, and disruption of services. Therefore, ensuring the security of networked systems has become a critical concern in both academic and industry domains [1].

Vulnerability assessment plays a vital role in identifying and managing these security weaknesses. It is a systematic process that involves detecting, analyzing, and prioritizing vulnerabilities within an information system [1],[6]. By evaluating known flaws and assigning severity levels, vulnerability assessment helps organizations understand their security posture and take appropriate corrective actions. When combined with risk analysis, it further enables prioritization based on the potential impact and likelihood of exploitation, ensuring that critical vulnerabilities are addressed promptly.

With the advancement of automated security tools, the process of vulnerability assessment has become more efficient and scalable. Tools such as Nmap and Nessus are widely used for network scanning and vulnerability detection. Nmap is primarily utilized for network reconnaissance, allowing the identification of active hosts, open ports, and running services. Nessus, on the other hand, provides comprehensive vulnerability scanning capabilities through its extensive plugin database, enabling the detection of a wide range of known security issues [2],[3].

In this study, a controlled laboratory environment is established to simulate a real-world enterprise network. A virtual setup is created using Kali Linux as the scanning system and Metasploitable 2 as the target machine. This setup provides a safe and controlled platform for conducting experiments and analyzing vulnerabilities without affecting real

systems. The use of Metasploitable 2, which is intentionally designed with known vulnerabilities, allows for consistent and reproducible testing.

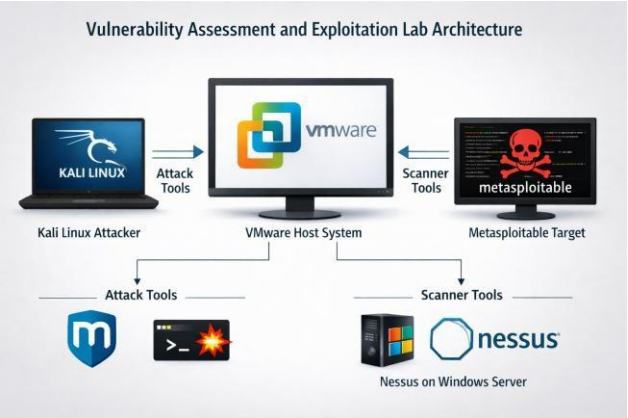
The primary objective of this research is to demonstrate a structured approach to vulnerability assessment and risk analysis using industry-standard tools. The study involves performing network and vulnerability scans, identifying security weaknesses, and classifying them based on severity using the Common Vulnerability Scoring System (CVSS) [4]. The findings aim to provide practical insights into identifying critical risks and prioritizing remediation efforts. Additionally, this work serves as a useful reference for students and professionals seeking to understand the practical implementation of cybersecurity assessment techniques.

II. SYSTEM ARCHITECTURE

The proposed system architecture is designed to simulate a realistic enterprise network within a controlled virtualized environment. The architecture leverages virtualization technology to deploy multiple interconnected systems, enabling safe and isolated security testing. This approach ensures that vulnerability assessment activities can be performed without affecting real-world infrastructure.

The architecture consists of three primary components: a scanning system, a vulnerability assessment server, and a target system. Kali Linux is configured as the primary scanning machine due to its extensive suite of penetration testing and network analysis tools. A Windows-based system is used to host the Nessus vulnerability scanner, which performs comprehensive vulnerability detection using its extensive plugin database [2]. The target system is implemented using Metasploitable 2, an intentionally vulnerable platform designed for security testing and research purposes.

All systems are connected through an isolated virtual network, ensuring controlled communication between components. The scanning system initiates reconnaissance and interacts with the target, while the Nessus server performs in-depth analysis based on detected services and configurations. This layered architecture enables both surface-level and deep vulnerability analysis, closely resembling real-world security assessment workflows. Furthermore, the design supports repeatability and scalability, making it suitable for both academic research and practical cybersecurity experimentation.



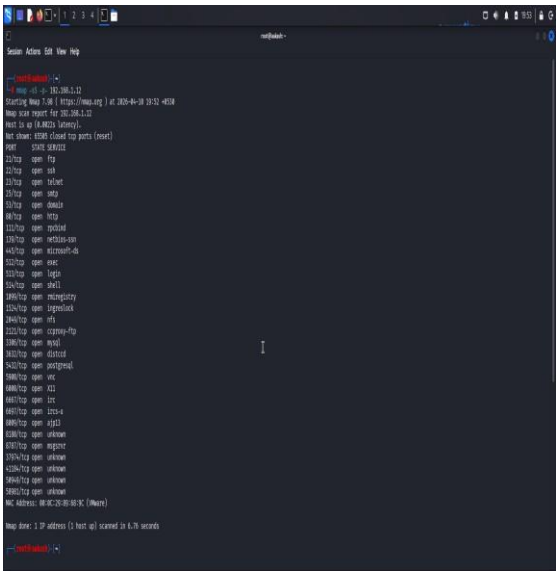
III. METHODOLOGY

A. Experimental Environment Setup

A controlled experimental environment was established using virtualization technology to replicate a small-scale enterprise network. Multiple virtual machines were deployed; each assigned a specific role within the assessment framework. Kali Linux functioned as the attacker system, while Metasploitable 2 served as the vulnerable target. A dedicated system hosting Nessus was configured to perform automated vulnerability scanning. All machines were connected within an isolated network to ensure safe execution of security testing procedures.

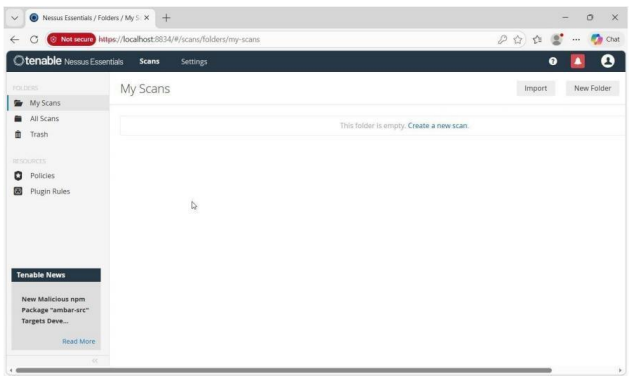
B. Network Reconnaissance and Scanning

The initial phase of the methodology involved network reconnaissance using Nmap. Advanced scanning techniques, including service version detection and operating system fingerprinting, were employed to identify active hosts, open ports, and running services. This step is critical in defining the attack surface and understanding how the target system is exposed to potential threats. The scanning results provided detailed insights into accessible services, forming the basis for further vulnerability analysis [3].



C. Vulnerability Identification

Following reconnaissance, vulnerability scanning was conducted using Nessus. The tool analyses detected services by comparing them against a continuously updated database of known vulnerabilities and security misconfigurations [2]. This process enabled the identification of critical issues such as outdated software, weak authentication mechanisms, and exposed services. Nessus also assigns severity ratings to each vulnerability, allowing structured classification and prioritization.



D. Data Analysis and Interpretation

The results obtained from Nmap and Nessus were systematically analyzed to identify patterns and critical weaknesses. Vulnerabilities were examined in terms of their potential impact on system security, including unauthorized access, data exposure, and service disruption. This phase bridges the gap between raw scan data and meaningful security insights, enabling informed decision-making for risk assessment and mitigation.

IV. EXPLOITATION ANALYSIS

The exploitation analysis phase focuses on understanding how identified vulnerabilities can be leveraged by attackers to compromise system security. While this study does not perform active exploitation, it evaluates the potential consequences of vulnerabilities based on their characteristics and known attack vectors.

Several identified vulnerabilities indicate the possibility of unauthorized access and remote code execution. For instance, services with weak authentication mechanisms can be targeted through brute-force attacks, while outdated software components may contain publicly known exploits [7]. One of the critical observations includes vulnerabilities that allow remote command execution, which can lead to complete system compromise if exploited.

The presence of such vulnerabilities significantly increases the attack surface of the system. Attackers can exploit these weaknesses to gain initial access, escalate privileges, and maintain persistent control over the system. This highlights the importance of timely patch management, secure configurations, and continuous monitoring.

Overall, the exploitation analysis emphasizes the real-world impact of unaddressed vulnerabilities and reinforces the need for proactive security measures to prevent potential attacks.

V. RISK ASSESSMENT

Risk assessment is a critical phase in vulnerability analysis that evaluates the potential impact and likelihood of exploitation of identified security weaknesses.[6] While vulnerability scanning tools provide raw findings, risk assessment transforms these findings into actionable intelligence by prioritizing threats based on their severity and potential consequences.

In this study, the Common Vulnerability Scoring System (CVSS) was used as the primary framework for evaluating vulnerability severity. CVSS provides a standardized scoring mechanism [4] ranging from 0 to 10, considering multiple factors such as exploitability, attack complexity, required privileges, and impact on confidentiality, integrity, and availability. This standardized approach ensures consistency in assessing and comparing vulnerabilities across different systems.

The identified vulnerabilities were categorized into three primary risk levels: high, medium, and low. High-risk vulnerabilities (CVSS score ≥ 7.0) represent critical security issues that can be easily exploited and may lead to severe consequences such as remote code execution, unauthorized system access, or complete system compromise. Medium-risk vulnerabilities (CVSS score between 4.0 and 6.9) indicate moderate threats that may require specific conditions or partial access to exploit but still pose significant risks if ignored. Low-risk vulnerabilities (CVSS score < 4.0) generally represent minor issues or informational findings with limited immediate impact.

The assessment revealed that several vulnerabilities fall into the high-risk category, primarily due to the presence of outdated services, weak authentication mechanisms, and exposed network services. For example, vulnerabilities associated with backdoor services and default credentials significantly increase the likelihood of exploitation, as they require minimal effort for attackers to gain unauthorized access. Similarly, exposed database services and unsecured communication channels contribute to increased attack surface and data exposure risks.

In addition to severity scoring, risk prioritization was performed by considering both the potential impact and the likelihood of exploitation. Vulnerabilities with high impact and high exploitability were given the highest priority for remediation. This approach ensures that critical security issues are addressed first, thereby reducing the overall risk to the system.

Overall, the risk assessment highlights the importance of a structured approach to vulnerability management. By leveraging CVSS scoring and prioritization techniques, organizations can efficiently allocate resources, focus on critical threats, and enhance their overall security posture.

Risk Assessment of Identified Vulnerabilities

Vulnerability	Port	CVSS Score	Risk Level	Likelihood	Impact
UnrealIRCd Backdoor	6667	10.0	High	High	Full system compromise
FTP Anonymous Access	21	7.5	High	High	Unauthorized data access
MySQL Exposure	3306	6.5	Medium	Medium	Data leakage
Open SSH Service	22	4.0	Low	Low	Brute-force attempts

VI. MITIGATION STRATEGIES

To address the identified vulnerabilities, a set of mitigation strategies is proposed to enhance system security and reduce potential risks. These strategies focus on strengthening system configurations, minimizing exposure, and ensuring continuous monitoring.

One of the primary recommendations is to disable unnecessary services and restrict access to critical components. For example, anonymous access to file transfer services should be disabled to prevent unauthorized data access. Similarly, database services should be protected using firewall rules and access controls to limit exposure to trusted systems only.

Regular software updates and patch management are essential to eliminate vulnerabilities associated with outdated components. Implementing strong authentication mechanisms, including complex passwords and multi-factor authentication, can further reduce the risk of unauthorized access.

In addition to these measures, organizations should deploy firewalls and intrusion detection systems to monitor network activity and detect potential threats [8]. Continuous vulnerability scanning and periodic security assessments are also recommended to identify new vulnerabilities and ensure ongoing protection.

VII. RESULTS AND DISCUSSION

The results of the vulnerability assessment provide a comprehensive overview of the security posture of the target system within the simulated environment. By combining network scanning (Nmap) and vulnerability scanning (Nessus), both surface-level exposure and deep security weaknesses were effectively identified and analyzed.

The Nmap scan results revealed multiple open ports and active services, including FTP (21), SSH (22), HTTP (80), and MySQL (3306). These exposed services represent potential entry points for attackers and significantly contribute to the overall attack surface of the system. Service version detection further indicated that several of these services were outdated, increasing their susceptibility to known exploits.

Subsequent analysis using Nessus identified a wide range of vulnerabilities categorized into critical, high, medium, and low severity levels. A notable observation from the results is the dominance of high-severity vulnerabilities, particularly those associated with weak authentication mechanisms, default credentials, and outdated software components. These vulnerabilities are especially dangerous because they can often be exploited with minimal effort, making them attractive targets for attackers [7].

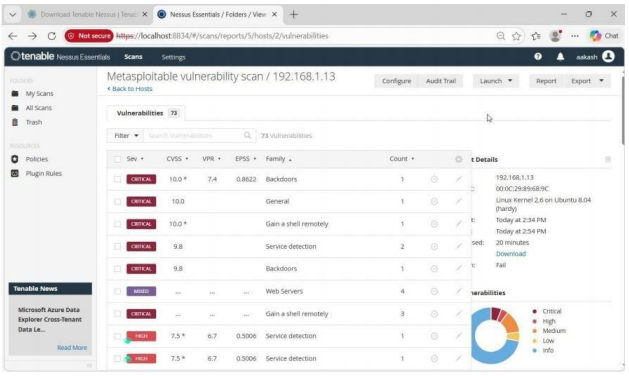
One of the most critical findings includes vulnerabilities that enable remote command execution, which can result in complete system compromise. Such vulnerabilities pose a severe threat to system confidentiality, integrity, and availability. Additionally, the presence of misconfigured services and unnecessary open ports further increases the risk by expanding the attack surface.

The combined use of Nmap and Nessus proved to be highly effective in identifying both network-level and application-level vulnerabilities. While Nmap provided valuable insights into exposed services and system structure, Nessus offered detailed vulnerability analysis, including CVSS-based severity ratings. This complementary approach enhances the accuracy and depth of the assessment.

Another important observation is the relationship between service exposure and vulnerability severity. Services that are publicly accessible and poorly configured tend to have higher associated risks. This highlights the importance of minimizing exposed services and enforcing secure configurations.

Although the tools provided extensive vulnerability data, careful analysis was required to interpret the results and filter potential false positives. This emphasizes that automated tools should be used in conjunction with expert analysis to achieve reliable outcomes.

Overall, the results demonstrate that even a small network setup can contain multiple critical vulnerabilities if not properly secured. The findings reinforce the importance of regular vulnerability assessments, proper configuration management, and timely patching. The study also validates the effectiveness of automated scanning tools in identifying and prioritizing security risks in a structured manner.



VIII. CONCLUSION

This study presented a structured and systematic approach to vulnerability assessment and risk analysis within a controlled virtual laboratory environment. By integrating network reconnaissance and automated vulnerability scanning techniques, the research successfully identified and evaluated multiple security weaknesses present in a simulated enterprise network. The use of Nmap enabled effective discovery of open ports, active hosts, and running services, while Nessus provided detailed insights into known vulnerabilities, misconfigurations, and outdated software components.

The analysis revealed that a significant portion of the identified vulnerabilities falls into the high-risk category, primarily due to factors such as weak authentication mechanisms, default credentials, and exposure of critical services. These findings highlight the potential risks associated with improperly secured systems and emphasize the importance of proactive security measures. The application of the Common Vulnerability Scoring System (CVSS) further enabled systematic classification and prioritization of vulnerabilities, facilitating a more effective risk management process.

One of the key contributions of this research is the development of a practical and reproducible framework that combines multiple security tools to achieve comprehensive vulnerability assessment. The study demonstrates that the integration of network scanning and vulnerability detection tools provides deeper visibility into system security and enhances the accuracy of risk identification [5]. Additionally, the research underscores the importance of interpreting scan results carefully to distinguish between critical vulnerabilities and less significant findings.

The results reinforce the need for continuous security monitoring, regular vulnerability assessments, and timely patch management to maintain a strong security posture. Organizations must adopt a proactive approach to cybersecurity by minimizing exposed services, enforcing strong authentication policies, and implementing robust network security controls.

While this study was conducted in a controlled lab environment, the methodology and findings are applicable to real-world scenarios. Future work may involve expanding the test environment to include more complex network infrastructures, integrating additional security tools, and exploring automated remediation techniques. Furthermore, incorporating machine learning-based risk prediction models could enhance the efficiency and accuracy of vulnerability prioritization.

In conclusion, this research highlights the critical role of vulnerability assessment and risk analysis in modern cybersecurity practices and provides a solid foundation for both academic research and practical implementation in securing networked systems.

IX. REFERENCES

[1] UpGuard, "What Is a Vulnerability Assessment and How to Conduct One," 2025. [Online]. Available: https://www.upguard.com/blog/vulnerability-assessment

[2] Tenable Inc., "Nessus Vulnerability Scanner User Guide," 2024. [Online]. Available: https://www.tenable.com/products/nessus

[3] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. USA: Insecure.Com LLC, 2009.

[4] FIRST.org, "Common Vulnerability Scoring System (CVSS v3.1 Specification Document)," 2019. [Online]. Available: https://www.first.org/cvss

[5] A. E. Malaka, "Benchmarking Vulnerability Scanners: Nessus and Burp Suite," M.S. thesis, University of Arizona, 2013.

[6] P. Mell, K. Scarfone, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," *National Institute of Standards and Technology (NIST)*, 2007.

[7] S. Frei, M. May, U. Fiedler, and B. Plattner, "Large-scale Vulnerability Analysis," in *Proc. ACM SIGCOMM Workshop on Rapid Malcode*, 2006, pp. 131–138.

[8] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST Special Publication 800-94*, 2007.