International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Literature Survey on System Security and Network Vulnerability Assessment

Dr. R. Raju
Professor
Department of Information Technology
Sri Manakula Vinayagar Engineering College
Puducherry,India
hodit@smvec.ac.in

Anamika Ananda Krishnan
Department of Information Technology
Sri Manakula Vinayagar Engineering College
akanamika9@gmail.com

Dhivya Bharathy M
Department Of Information Technology
Sri Manakula Vinayagar Engineering College
dhivyabharathy0507@gmail.com

Dhivyadhesrni K
Department Of Information Technology
Sri Manakula Vinayagar Engineering College
divyadhershni03@gmail.com

Abstract:- This abstract outlines a detailed study on improving network security through vulnerability assessment and penetration testing, using tools like Nessus, Nmap, Metasploit, on the Kali Linux OS. The methodology involves identifying vulnerabilities, conducting simulated attacks, and developing a bash script to address false positives from Nessus scans. The research aims to enhance network security, provide practical recommendations, and contribute to cybersecurity practices, with a focus on both internal and external network security.

Keywords: Vulnerability Assessment, Pentest, Nessus, Metasploit, Kali Linux

INTRODUCTION

In the ever-evolving landscape of cybersecurity, the proactive identification and mitigation of vulnerabilities stand as paramount pillars in safeguarding digital assets and organizational integrity. As organizations navigate complex networks and intricate systems, the need for robust vulnerability assessment and penetration testing methodologies becomes increasingly imperative. The Steps in the vulnerability assessment process are to Define Scope and Objectives, Gather Information, Identify and Prioritize Vulnerabilities, Assess Risks, Develop a Remediation Plan, Implement Remediation Measures, Reassess and creating the Reports.

Our project embarks on a journey to fortify cybersecurity defenses through a comprehensive approach that integrates cutting-edge tools and techniques. Leveraging industry-standard tools such as Nessus, Nmap, bash scripting, and the Metasploit framework, we aim to conduct a thorough examination of potential vulnerabilities within our organization's IT infrastructure.

Central to our endeavor is the utilization of Kali Linux, a purpose-built operating system renowned for its rich set of pre-installed tools specifically designed for cybersecurity professionals. With its Debian-based distribution, extensive toolset of over 600 penetration testing tools, and custom kernel optimized for performance and security testing, Kali Linux serves as the cornerstone of our cybersecurity toolkit.

By harnessing the power of Kali Linux alongside specialized tools like Nessus, Nmap, bash scripting, and Metasploit, we seek not only to identify weaknesses but also to fortify our digital fortresses, in still confidence in our stakeholders, and uphold the integrity of our organization's cybersecurity posture.

Advantages of Cyber Security: Early Threat Detection, Reduced False Positives, Comprehensive Testing, Prioritized Remediation, Enhanced Security Resilience, Cost Savings.

LITERATURE SURVEY

The main goal was to fully comprehend and evaluate the research that various researchers in this sector had done. The review sought to examine the many facets that are essential to PEN testing and to investigate its importance in assessing the functional elements of systems.

[1] This paper presents a systematic literature review of 39 studies related to network penetration testing. It analyses different types of network penetration testing approaches, tools, methodologies, vulnerabilities, attacks, and mitigation techniques. Wireless local area networks (WLANs) were identified as facing vulnerabilities in encryption protocols like WEP2 and WEP3, with possible attacks being KRACK and downgrade attacks. Common tools for detecting open ports discussed were Nmap, Metasploit, Wireshark, etc. DoS attacks were found to be a frequent threat exploiting open ports. Deep reinforcement learning was identified as the most proposed technique for protecting vulnerable ports. Automated network penetration testing based on machine learning was recommended for future research.

[2] This paper presents internet security is a major concern because practically all interactions take place online. Penetration testing identifies security flaws and assesses the security of networks and systems. Piercing testing is done to make sure the system or network is secure and doesn't have any vulnerabilities that could allow unauthorised access. Pen testing, also referred to as penetration testing, is a group of procedures used to identify potential openings for an attacker to exploit in a system, network, or online application. It helps to verify the efficacy and efficiency of the various security measures implemented. This paper provides a clear explanation of the principles of penetration testing and shows when, how, and how to use various tools and techniques for penetration testing with Kali Linux for detecting system vulnerabilities and give an overview of networking protocols, firewalls, and fundamental security issues that need to be resolved for the system to be better protected, concluding with an analysis of the finding.

[3] The paper discusses penetration testing, a method to identify vulnerabilities in a system by simulating attacks. It involves five phases: reconnaissance, scanning, gaining access, maintaining access, and reporting. Tools such as Nmap, netcat, and metasploit are used to execute these phases on the Kali Linux forensic platform. The aim is to uncover weaknesses and provide recommendations for improvement.

[4] This paper discusses penetration testing techniques and tools that can be used to identify vulnerabilities within a system. It describes the different phases of a penetration test like information gathering, vulnerability analysis, exploitation, and reporting. It provides information on tools used for tasks like packet sniffing, wireless hacking, password cracking, and gaining unauthorized access. The goal is to simulate real-world attacks to help organizations identify security issues before hackers can exploit them.The overall goal of conducting penetration testing, as per the document, is to simulate real-world attacks in order to identify security vulnerabilities within a system. This helps organizations to proactively address and mitigate potential security issues before malicious attackers can exploit them. The penetration testing process aims to assess the risk of potential security lapses, identify vulnerabilities that attackers might use, and point out potential points of access. Additionally, it involves documenting the methods used to gain access to valued assets and conveying findings to the customer in a meaningful and clear way. Ultimately, the goal is to protect organizations from major attacks, financial losses, and reputational damage by eliminating risks proactively.

[5] The paper discusses how Vulnerability Assessment and Penetration Testing (VAPT) can prevent cyber attacks effectively. It covers the life cycle of VAPT and techniques like static analysis, manual testing, automated testing, and fuzz testing. Top VAPT tools are listed, emphasizing the importance of regularly conducting VAPT to proactively identify vulnerabilities before attackers exploit them. Resolving these vulnerabilities hardens systems against cyber attacks. Key steps in the VAPT life cycle include scope definition, reconnaissance, vulnerability

assessment, penetration testing, result analysis, and documentation. Regular VAPT helps find vulnerabilities before they're exploited, reducing the risk of cyber attacks. Top VAPT tools include Nessus, OpenVAS, Burp Suite, Acunetix, Nmap, Wireshark, Metasploit, and zaproxy. Proactively addressing vulnerabilities via VAPT ensures systems remain secure by eliminating known vulnerabilities for attackers to exploit.

[6] The paper explores the use of penetration testing techniques to enhance network security management and control. It introduces a management control model, detailing elements such as control targets, standards, and corrective measures. The model involves simulating networks of varying security levels to detect and block suspicious information flows. Tools like Hydra are suggested for website vulnerability testing, while deep learning methods are proposed for intrusion detection. Frameworks for access control and adaptive authorization are discussed for securely managing distributed authorization infrastructures. The article emphasizes the potential benefits of deep learning methods in improving intrusion detection accuracy, particularly in dealing with big data and resisting deformation attacks.

[7] The paper addresses security verification challenges in system-on-chip (SoC) designs and suggests using techniques like fuzz testing, penetration testing, and AI testing to tackle them. It outlines the steps for SoC security verification, including identifying vulnerabilities, defining security assets and policies, formalizing security policies, and implementing and testing the design. The paper explores applying fuzz testing, penetration testing, and AI testing to SoC security verification by converting hardware to a software model and using metrics like cost functions for guidance. It discusses vulnerabilities such as inadvertent designer mistakes, insider threats, and untrusted third-party IP vendors, which could lead to insecure boot modes, illegal accesses, information breaches, and malfunctioning security operations.

[8] The article explores network security concerns and suggests solutions using penetration testing. It introduces a management control model for accurate identification and detection of vulnerabilities. Penetration testing technology is highlighted as crucial for optimizing the risk index model for effective network security management. It details different types of penetration tests: black box, white box, and covert testing, each offering unique approaches based on knowledge and access levels.

[9] The paper highlights the growing concern over network security due to the internet's development and network globalization. A management control platform addressed over 600 network security vulnerabilities and dozens of incidents during its trial, significantly improving network security standards. With the rise of denial-of-service attacks, network security has become a top priority for administrators, who often rely on penetration testing to ensure system security. As information technology advances, the need for secure information systems grows, making penetration testing essential for accurately locating and addressing security flaws. By integrating penetration testing into management and control systems, the risk index model can effectively enhance network security management and efficiency.

[10] The article explores using penetration testing techniques to enhance network security management and control. It introduces a management control model and discusses elements like control targets, standards, and corrective measures. Penetration testing is defined and classified. The article then delves into building a simulation model with networks of varying security levels to detect and block suspicious information flows. It also covers the use of tools like Hydra for website vulnerability testing and deep learning methods for intrusion detection. Frameworks for access control and adaptive authorization are presented for securely managing distributed authorization infrastructures. The article emphasizes the potential benefits of deep learning methods in improving intrusion detection accuracy, particularly in dealing with big data and resisting deformation attacks.

[11] Cybersecurity is increasingly crucial as society relies more on technology, prompting heightened concern about system safety against cyber-attacks. Advanced Persistent Threats (APTs) pose significant challenges, involving unauthorized network access and prolonged evasion of detection. While penetration testing (PT) is common for assessing security, it only addresses current vulnerabilities, overlooking potential

future risks, particularly those associated with APTs. Limited datasets hinder research into using machine learning (ML) for APT detection. This thesis aims to demonstrate Threat Led APT PT, an enhanced approach, to assess network security against known vulnerabilities and uncover hidden risks using APT tactics. It also involves gathering and testing a new dataset related to APT attacks with an ML model.

[12] The necessity for confidentiality has grown with Internet usage, emphasizing secure infrastructure for user data protection. Cyber threats like phishing, hacking, and theft are on the rise, costing trillions annually. Ethical Hacking helps evaluate vulnerabilities and secure networks, demonstrated through practical experiments using the Metasploit framework on Kali Linux. Recommendations for security enhancements are provided to fend off hacking attempts.

[13] In this paper, through PEN testing, a system's functional features can be verified, as well as the system's defenses against intrusion and network security attacks, as well as how vulnerable the system is to these threats. We have reviewed the literature on the work that has been done by different researchers in the field of penetration testing (PEN) in this research article. We have made an effort to go over all the different PEN test-related features. The several PEN testing tools have also been examined in terms of their functionality, technical details, release date, platform compatibility, etc.

[14] Information security is often overlooked without proper awareness strategies, leaving sensitive data vulnerable. Vulnerability assessment and penetration testing (VAPT) are vital for evaluating system strengths and weaknesses. SQL plays a crucial role in RDBMS and website functionality. Goal-oriented penetration tests are

This study focuses on government websites in Indonesia, identifying serious and moderate vulnerabilities such as directory listing and PHP info disclosure.

[15] This paper highlights the vulnerability of higher education institutions to cyberattacks due to scientific advancements. Tools like Nessus and Burp identify vulnerabilities but overwhelm with information. Lack of expertise hampers cybersecurity defense. Vulnerability screening is crucial for effective cybersecurity education. The study reviews open-source vulnerability scanning technologies and literature on cybersecurity. It offers a comprehensive analysis and suggests future directions. Detailed descriptions of open-source network vulnerability scanning tools are provided, along with a study design for interactive labs to enhance cybersecurity curriculum.

[16] The paper addresses the significant risks posed by cyberattacks on IT infrastructure, particularly with the increasing digitization of enterprises. Data privacy laws have been enacted to protect companies and clients, mandating the creation of information and cybersecurity policies, standards, and controls. Cybersecurity budgeting is a top priority for small and medium-sized businesses, with open-source technology seen as a valuable resource for meeting regulatory standards and technical control requirements. Using a case study of the Sorosoro Ibaba Development Cooperative (SIDC), researchers developed implementation guidelines for network security assessment using Open-Source Vulnerability Assessment and Penetration Testing with Security Information and Event Management. Strategic tools like PEST were employed to oversee comprehensive documentation creation, while thematic analysis was used to present the study's findings. Various frameworks were developed based on survey, interview, and document review results, including the Open-Source Stage Model of Implementation and the SIDC MINI SOC Implementation Framework. Test results of the tools indicate the organization's capability to utilize open-source cybersecurity tools effectively, enhancing infrastructure visibility and threat assessment.

SL. NO	TITLE	AUTHOR AND YEAR	TECHNIQUES	PROS & CONS
1.	A Systematic Literature Review on Penetration Testing in Networks"	M Mariam Alhamed and M. M. Hafizur Rahman,2023	Deep Reinforcement Learning, Automated Network Penetration Testing using ML	Pros: Adaptive, Efficient Cons: High cost, risk of false positives
2.	Kali Linux based Empirical Investigation on Vulnerability Evaluation using Pen-Testing tools	Biresh Kumar, Sahil Prasad Bijo, Riya kedia, Pallab Banerjee, Pooja Jha, Mohan Kumar Dahury, 2023	Penetration Testing	Pros:Identifying Vulnerabilities, Risk Mitigation Cons: Resource Intensive, Disruption
3.	A Process of Penetration Testing Using Various Tools	Deepika kongara, Shivani krishnama, 2023	Reconnaissance, Scanning, Gaining Access, Maintaining Access, Reporting	Pros: Identifies vulnerabilities proactively Cons: Disruptions
4.	Penetration Testing And Security Measures To Identify Vulnerability Inside The System	Shivani Singh1, Garima Srivastava2, Sachin Kumar3, Shikha Singh4, 2023	Ethical hacking Or White Hat Hacking	Pros: Real-world Simulation, Risk Assessment Cons: Limited Scope, Disruptions
5.	VAPT & Exploits, along with Classification of Exploits	Sheetakshi Shukla1, Tasneem Bano Rehman2,2022	Vulnerability testing.	Pros: Advanced techniques, Comprehensive approach. Cons: Complexity.
6.	A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs	Abeneesh Kejiou,Girish Bekaaroo,2022	Management control model, Simulated network environments.	Pros:Identifying Vulnerabilities using tools. Cons: Time issue.
7.	Auto Vulnerability Assessment and Penetration 42 Testing Tools	Vishal Kumar and Abhay Singh,2021	Penetration testing, Intrusion detection.	Pros: Comprehensive exploration Cons: Lack specificity on implementation
8.	Vulnerability Assessment and Penetration Testing (VAPT) Framework	Ahmad Almaarif, Muharman Lubis, 2020	Vulnerability assessment, penetration testing (VAPT), SQL analysis	Pros: Securing sensitive data. Cons: Impact of vulnerabilities in Indonesian government websites

CONCLUSION

In conclusion, vulnerability assessment and penetration testing, alongside tools like Nessus, Nmap, bash scripting, and Metasploit, offer crucial advantages for modern cybersecurity. Proactively identifying weaknesses, minimizing false positives, and simulating real-world attacks enhance security posture, prioritize remediation efforts, and ensure regulatory compliance. This approach not only mitigates risks but also saves costs and fosters stakeholder trust in an organization's commitment to cybersecurity, serving as cornerstones for resilient cybersecurity strategies in today's digital landscape.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the anonymous referees whose incisive critiques and helpful suggestions made this article much better. Their insightful advice has been crucial in improving the content's caliber and readability. Additionally, I would like to sincerely thank my guide, for their continuous support, knowledgeable advice, and encouragement during the research process. The direction and thoroughness of this paper have been greatly influenced by their knowledge and mentoring.

REFERENCES

[1] M Mariam Alhamed and M. M. Hafizur Rahman,2023,"A Systematic Literature Review on Penetration Testing in Networks"

[2] Biresh Kumar, Sahil Prasad Bijo, Riya kedia, Pallab Banerjee, Pooja Jha, Mohan Kumar Dahury, 2023," Kali Linux based Empirical Investigation on Vulnerability Evaluation using Pen-Testing tools"

[3] Deepika kongara, Shivani krishnama, 2023," A Process of Penetration Testing Using Various Tools"

[4] Shivani Singh1, Garima Srivastava2, Sachin Kumar3, Shikha Singh4, 2023, “Penetration Testing And Security Measures To Identify Vulnerability Inside The System”

[5] Vinod Varma Vegesna,2022, ”Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing)” as a Method for Actively Preventing Cyberattacks.

[6] Sheetakshi Shukla1, Tasneem Bano Rehman2 ,2022,”VAPT & Exploits, along with Classification of Exploits”

[7] Kimia Zamiri Azar, Muhammad Monir Hossain, Arash Vafaei, Hasan Al Shaikh, Nurun N. Mondol, Fahim Rahman, Mark Tehranipoor, and Farimah Farahmandi,2022, "Fuzz, Penetration, and AI Testing for SoC Security Verification"

[8] Abeneesh Kejiou,Girish Bekaaroo,2022, ”A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs”

[9] Liwei Wang , Robert Abbas , Fahad M. Almansour , Gurjot Singh Gaba , Roobaea Alroobaea and Mehedi Masud,2021,”An empirical study on vulnerability assessment and penetration detection for highly sensitive networks”

[10] Vishal Kumar and Abhay Singh, 2021, "Auto Vulnerability Assessment and Penetration 42 Testing Tools"

[11] Masarweh, Ala’ Ahmad, 2021, "Enhancing the Penetration Testing Approach and Detecting Advanced Persistent Threat Using Machine Learning"

[12] Mujahid Tabassum, Tripti Sharma, Saju Mohanan,2021," Ethical Hacking and
Penetrate Testing using Kali and Metasploit Framework"

[13]Prashant vats, Manju mandot, Anjana gosain, 2020 "A Comprehensive Literature Review of Penetration Testing & Its Applications"

[14] Ahmad Almaarif, Muharman Lubis, 2020,"Vulnerability Assessment and Penetration Testing (VAPT) Framework"

[15] Prajakta Subhash Jagtapm, 2020" Vulnerability Scanning"

[16] Mr Abdur Rahman, Mahfida Amjad, Mr Saieed Siddik, Byzeid Ahmed,2020,"Network security assessment using open-source vulnerability assessment and penetration testing (VAPT) with security information and event management (SIEM)"