DS Journal of Cyber Security
Volume 2 Issue 4, 1-9, Oct - Dec 2024
ISSN: 2584-0665/ https://doi.org/10.59232/CYS-V2I4P101

Original Article

Agentless Vulnerability Detection for Windows System and Network

R. Karthiban[1], S. Christ Michael Jeniston[2], S. Divya Sree[3], N.U. Haripriya[4], M. Harish[5], J. Lalith Kumar[6], S. Manikandan[7]

[1,2,3,4,5,6,7]*Department of Computer Science and Engineering (Cyber Security), Sri Shakthi Institute of Engineering and Technology, Tamil Nadu, India.*

[3]divyasreesureshkumar23cys@srishakthi.ac.in

Received: 02 October 2024; Revised: 08 November 2024; Accepted: 26 November 2024; Published: 21 December 2024

Abstract - The current outcomes generated by various network scanning and vulnerability assessment tools exhibit considerable divergence. These discrepancies result in inconsistent data formats and varying levels of detail, complicating the integration of results from different instruments. Furthermore, network and system scanners often operate as standalone tools, exacerbating the challenges associated with the evaluation process. This paper introduces a cohesive strategy that bridges the divide between network and system scanning, providing a unified report on the overall security posture of the network and system within the targeted machine. By harmonizing data from multiple scanning mechanisms, this approach facilitates a thorough and streamlined evaluation, offering a clearer perspective on potential vulnerabilities. Operating without agents, this solution reduces the impact on the target system, mitigating performance issues and security threats linked to agent-based approaches.

Keywords - Audit policies, Defender settings, Firewall rules, Installed hotfixes, Scheduled tasks.

1. Introduction

In the current rapidly evolving technology landscape, many individuals either hastily update their Windows Operating System without thoroughly evaluating potential vulnerabilities or entirely overlook updates, leaving their systems susceptible to various cyber threats. A scanner that can swiftly and effectively pinpoint these vulnerabilities would be invaluable, offering critical security advantages for both individuals and organizations by assisting them in maintaining protection and ensuring they remain current. Regular system scanning is essential for the stability and security of any computer network or individual device. By routinely scanning, users can uncover malware, configuration issues, and vulnerabilities that may jeopardize sensitive information, degrade system performance or facilitate unauthorized access. Similarly, a computer application known as network scanning or enumeration is utilized to retrieve usernames, hostnames, shares, and services from computers connected to a network. It comprises a comprehensive suite of networking utilities encompassing a wide array of tools for vulnerability auditing, network security assessments, network monitoring, and more, as elaborated in Section 2.

This research centres on the development of an Agentless Windows System and Vulnerability Scanner—a tool crafted to enhance the identification of security vulnerabilities within Windows-based networks without necessitating agent software on each device. Contrasting with traditional vulnerability scanners that mandate agent installations on individual machines, as discussed in Section 3, an agentless scanner functions by remotely

evaluating systems, thereby minimizing deployment complexities and maintenance challenges. The proposed approach, detailed in Section 5, simplifies the scanning process and mitigates the performance issues on client devices that are often linked with agents. The results and demonstration of the system are presented in Section 6, followed by the Conclusion in Section 7. Planned future advancements are highlighted in Section 8.

2. Literature Survey

With the rapid advancements in technology, web services, and browser-based applications, many businesses rely on online platforms for their communications and transactions. Nonetheless, it is important to recognize that these websites and applications are not entirely secure. System and network scanning are crucial in identifying vulnerabilities, ensuring adherence to compliance standards, and maintaining operational efficiency. By conducting regular scans, organizations can proactively identify and rectify security gaps, thereby preventing unauthorized access and potential data breaches [1]. This practice not only aids in fulfilling regulatory requirements but also optimizes resources and keeps an accurate inventory of devices and software. In summary, system and network scanning is an essential strategy for protecting an organization's infrastructure, significantly enhancing both security and reliability.

2.1. Vulnerability Assessment

Vulnerability assessment entails the identification of weaknesses within a system before malicious actors can exploit them. This proactive strategy ensures that vulnerabilities are promptly detected and mitigated, thereby safeguarding the network from potential harm [13]. While firewall protection is often prioritized, the internal operations of the network are equally essential for maintaining security [2]. Vulnerability assessments extend beyond individual applications to encompass the platforms they operate on, including middleware and the underlying operating systems [10]. This comprehensive approach considers all factors contributing to accurately evaluating the system's vulnerability and security posture. Consequently, vulnerability scanners are employed to assess the network system and/or the software applications [3].

A Common Vulnerabilities and Exposures (CVE) represents a standardized identifier for publicly recognized cybersecurity vulnerabilities and exposures. Each CVE is assigned a distinct identifier, facilitating security professionals in referencing and exchanging information on specific vulnerabilities across varying platforms and tools. The CVE framework streamlines the processes of identifying, tracking, and managing vulnerabilities, thereby enabling more rapid and effective responses to security threats. Typically, CVE entries encompass comprehensive details about the vulnerability, including a description, affected systems, and potential risks [5].

Threat intelligence integration is a critical component in bolstering the effectiveness of security tools [11]. The CVE Scanner class utilizes external threat intelligence by querying the National Vulnerability Database (NVD) for known vulnerabilities related to the services detected in the network [7]. By incorporating threat intelligence resources such as the NVD, the scanner can deliver real-time, actionable insights regarding the vulnerabilities associated with specific software versions running on the network [12]. This integration enables the scanner not only to identify devices and services but also to cross-reference them against a recognized database of vulnerabilities, yielding a more thorough assessment of potential security risks [4].

2.2. Network Scanning

Network scanners scan the organization's network in an effort to locate any loopholes in the network's configuration or operation that can be exploited by attackers [6]. Scanners assist in locating vulnerabilities like open ports, out-of-date software, and incorrectly configured settings by evaluating devices, ports, services, and protocols throughout the network. They also shed light on possible weaknesses that might allow unwanted access, such as unencrypted data transfers or missing patches. The best practices to be followed while Network Vulnerability scanning is illustrated in Figure 1.

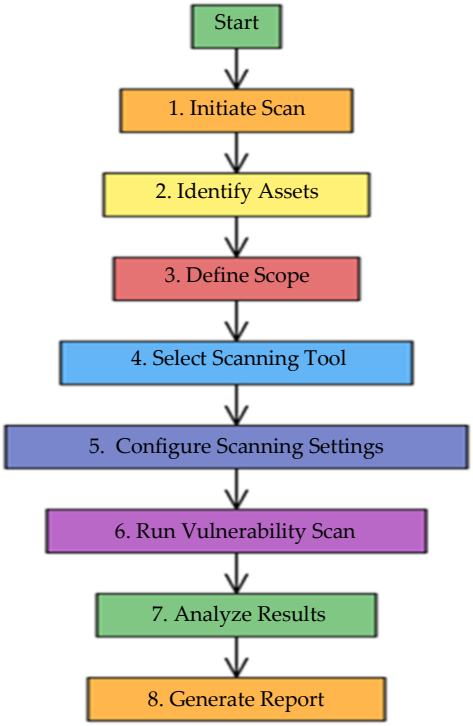

Fig. 1 Network vulnerability scanning

Utilizing tools such as *nmap*, network mapping delivers an in-depth perspective of the network's architecture, identifying potential security vulnerabilities, troubleshooting challenges, and planning infrastructure. It facilitates the discovery of open ports, obsolete services, and susceptible devices, attractive targets for exploiters [14]. Furthermore, network mapping promotes efficient network segmentation, enhancing security and optimizing performance through a thorough understanding of device interconnectivity and data flow. Additionally, it supports planning network expansions, ensures compliance with regulations, and contributes to maintaining a well-organized, scalable infrastructure.

2.3. IP Addressing and Subnetting

IP addressing and subnetting are essential elements in networking that play a pivotal role in structuring and safeguarding network infrastructures.

IP addressing refers to the method of allocating unique identifiers (IP addresses) to devices on a network. These addresses enable devices to communicate with one another effectively. IP addresses are generally classified into five categories (A, B, C, D, and E), with Classes A, B, and C being the most prevalent for both public and private networks.

Conversely, subnetting involves dividing a large network into smaller, more manageable sub-networks (subnets). This process is done by modifying the subnet mask, which defines the boundary between the network and host portions of an IP address. Subnetting helps improve network performance, optimize IP address usage, and enhance security by isolating network traffic within smaller segments. It allows administrators to control traffic flow and limit the scope of potential attacks, as each subnet can be treated as a separate security zone. Figure 2 gives a deeper understanding of both subjects.

Overall, subnetting and proper IP addressing are essential for managing modern networks, ensuring both performance and security [10].

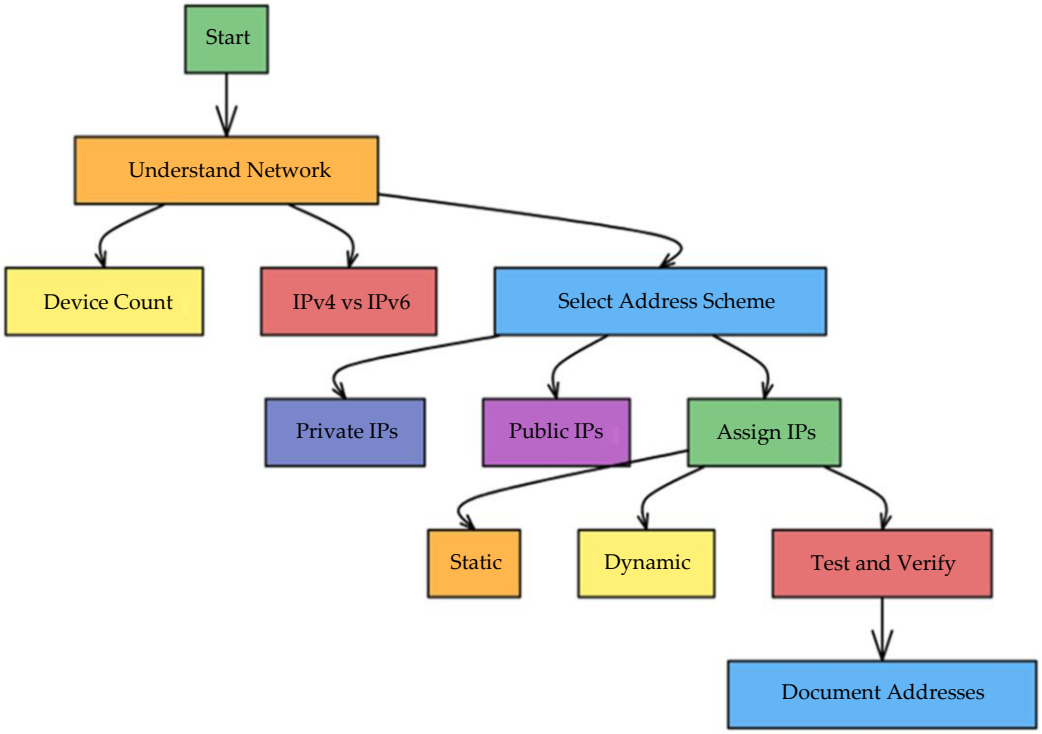

Fig. 2 IP Addressing and subnetting

2.4. System Scanner

A vulnerability assessment system scanner is an essential tool for identifying potential security weaknesses within an organization's systems and applications [11]. It evaluates the operating system, software, configurations, and internal settings to detect vulnerabilities such as unpatched software, weak passwords, misconfigurations, and outdated software versions. By generating comprehensive reports on these vulnerabilities, the scanner empowers security teams to prioritize and address risks before they can be exploited. This proactive measure is crucial for enhancing the overall security posture and ensuring adherence to security policies and standards.

2.5. Report Generation

The report generated through scanning is available for download in PDF format and is created automatically. Utilizing FPDF for PDF generation facilitates the development of professional, customizable documents with meticulous control over layout, fonts, and formatting. This method supports various elements such as text, images, and tables, making it particularly suitable for reports, assessments, and summaries. Automating this process guarantees that the produced documents are consistent, clearly readable, and prepared for sharing or printing while maintaining content integrity across diverse devices and platforms.

3. Related Works

3.1. Open Vulnerability Assessment System (OpenVAS)

OpenVAS is capable of conducting comprehensive network scans across a variety of systems, including servers, workstations, and Internet of Things (IoT) devices. It evaluates for prevalent vulnerabilities such as outdated software versions, unpatched security issues, misconfigured settings, and insecure open ports. The tool employs Network Vulnerability Tests (NVTs), predefined assessments designed to uncover known vulnerabilities. These assessments are routinely updated to incorporate newly identified vulnerabilities found in various software packages and operating systems [8].

3.1.1. CVE Integration

OpenVAS seamlessly integrates with publicly accessible vulnerability databases, such as the Common Vulnerabilities and Exposures (CVE) database, which catalogues recognized security vulnerabilities found across various software and hardware platforms. OpenVAS employs CVEs to effectively identify and document vulnerabilities, often providing in-depth information pertaining to each CVE, including its severity, assessed by CVSS scores and recommended mitigation strategies. The following Figure 3 demonstrates the operational framework of OpenVAS.

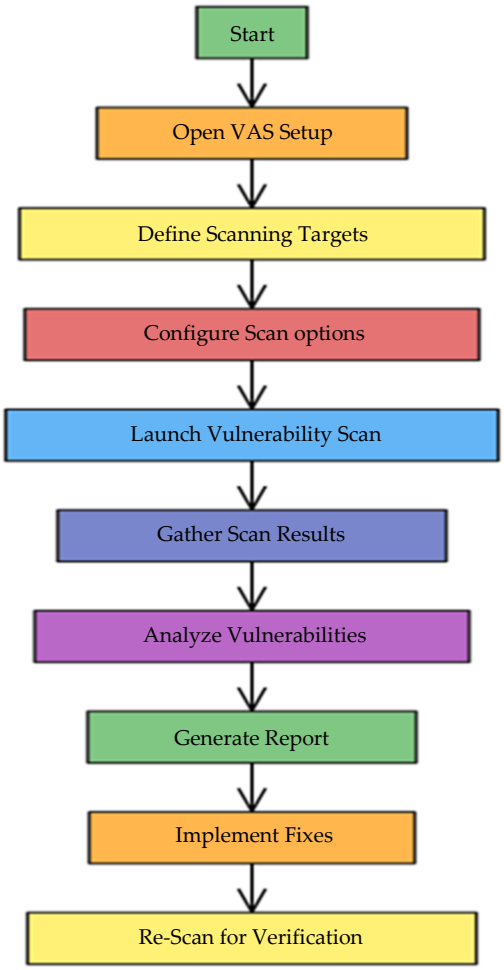

Fig. 3 Working of OpenVAS

3.1.2. Limitations of OpenVAS

OpenVAS installation and configuration can be more complex than commercial alternatives, particularly when deployed for extensive enterprise applications. Conducting large scans may demand substantial resources; OpenVAS may experience challenges when scanning expansive networks or systems with constrained capabilities [15].

3.2. Nessus

Nessus is a comprehensive remote security scanning tool that assesses computers and notifies users of any detected vulnerabilities that may be exploited by malicious hackers seeking access to connected networks. It achieves this by conducting over 1200 checks on a specified computer, evaluating the potential for various attacks to compromise the system or cause harm [9].

3.2.1. Scanning Types

Nessus offers several types of vulnerability scans, including:

1. Network Scanning: This entails scanning entire networks or specific IP ranges to identify vulnerabilities in networked devices such as routers, firewalls, servers, and switches.
2. Host Scanning: This involves scanning individual hosts or devices for vulnerabilities within their operating systems, installed software, or services.
3. Web Application Scanning: Nessus can identify vulnerabilities within web applications, including issues such as SQL injection and Cross-Site Scripting (XSS).
4. Configuration Scanning: Nessus evaluates systems and applications for misconfigurations that could expose vulnerabilities, such as open ports or weak security settings.

3.2.2. Limitations of Nessus

Nessus can be resource-intensive when scanning large networks or multiple systems simultaneously. Extensive scans may impact network and system performance if not properly scheduled [15]. Although Nessus provides a free version (Nessus Essentials) for non-commercial use, the comprehensive version, Nessus Professional, requires a subscription, which may be cost-prohibitive for smaller organizations.

3.3. Distinguishing Characteristics of the Proposed Idea of Scanner

The proposed scanner solution is designed to operate without requiring any agent installation on target systems, simplifying deployment and reducing maintenance efforts. In contrast to conventional scanners, which are often categorized as either network or system scanners, this project combines both functionalities. This integrated approach enables seamless scanning of both the network and individual systems without necessitating further configurations. By merging these capabilities into a singular solution, the scanner effectively decreases overall system load, thereby optimizing performance and enhancing efficiency relative to traditional scanners that typically require separate setups for different scanning tasks.

4. Agentless Windows System Vulnerability and Network Scanner

The proposed solution is an agentless vulnerability scanner tailored for Windows environments, utilizing Python for the backend and PySide6 to provide an intuitive user interface. It harnesses the National Vulnerability Database (NVD) to deliver current information on known vulnerabilities and exploits, facilitating effective vulnerability assessment and reporting. This approach reduces operational strain on system resources and streamlines maintenance, as administrators are relieved from the need to update and manage software agents on each individual device. By cross-referencing system data with the most recent vulnerability entries in the NVD, the system can detect security weaknesses and provide actionable recommendations for remediation, thereby assisting organizations in sustaining a robust security posture.

4.1. Agentless Vulnerability Scanning

Agentless vulnerability scanning is the process of evaluating the security of devices, systems, or networks without necessitating the installation of software agents on the target devices. This methodology is especially advantageous in scenarios where installing and managing agents on each system is unfeasible, such as in extensive networks, cloud environments, or rapidly evolving infrastructures. This solution utilizes remote scanning techniques with *nmap* in conjunction with the National Vulnerability Database (NVD) to detect vulnerabilities in services and configurations without the requirement of installing any software agents on the target devices.

4.2. Automated Vulnerability Assessment

By employing Nmap for network discovery and service scanning while integrating with the National Vulnerability Database (NVD) for real-time vulnerability information, the system conducts automated

vulnerability assessments. It autonomously identifies active devices within the network, examines the operational services, and cross-references their versions with known vulnerabilities in the NVD. Automating these processes mitigates the need for manual intervention, facilitating faster and more dependable vulnerability assessments across extensive networks. Integrating with the NVD ensures that the vulnerability data remains up-to-date, thereby reducing the administrative burden and identifying vulnerabilities promptly.

4.3. PySide6

PySide6, the official Python bindings for Qt 6, has been selected for the system's user interface to deliver a modern, responsive, and cross-platform graphical interface. It enables the creation of intuitive and visually engaging applications with extensive functionality. PySide6 facilitates seamless integration with the backend Python code, providing users with a user-friendly interface for managing network scans, reviewing vulnerability reports, and interacting with system data.

5. Architecture Design

The architecture of the agentless Windows system vulnerability scanner is outlined below:

1. User Initiates a Scan: Through the PySide6 interface, the user selects specific Windows devices or network ranges for scanning. The interface offers flexibility, providing options for both scheduled and on-demand scans.
2. Data Collection (Agentless): The backend connects to each target system by employing WMI, SMB, or PowerShell protocols to gather data regarding system configurations, software versions, and open network ports. This data is collected without installing any software on the target machine, thus minimizing system impact.
3. NVD Integration and Vulnerability Matching: Following data collection, the backend retrieves updated entries from the NVD and cross-references the acquired system details with known vulnerabilities. The matching logic identifies vulnerabilities based on software version, patch status, and security configurations.
4. Report Generation and Display: The identified vulnerabilities are processed into a comprehensive report displayed within the PySide6 interface. The report includes each vulnerability, its CVSS score, and a succinct description in a PDF format.

Figures 4 and 5, illustrated below, visually represent the architectural design and workflow.

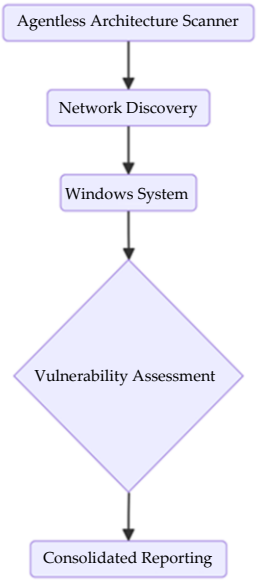

Fig. 4 Design of the agentless architecture windows system vulnerability and network scanner

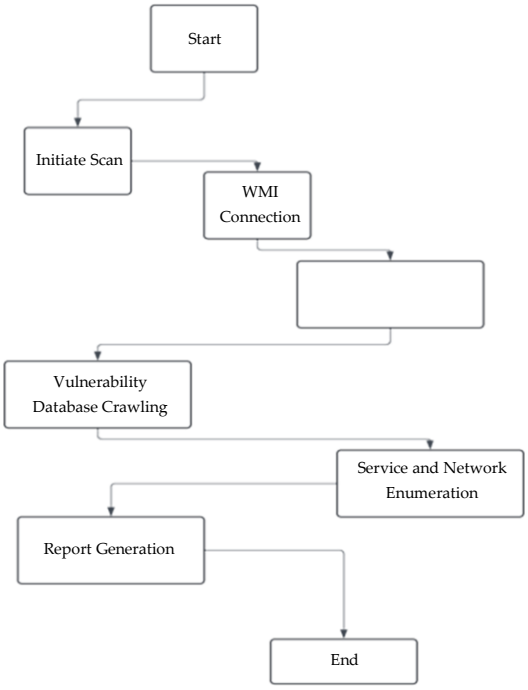

Fig. 5 Workflow of the agentless windows system vulnerability and network scanner

6. Results and Discussion

The agentless Windows vulnerability scanner proficiently detected vulnerabilities across a range of systems by leveraging current NVD data to ensure precise outcomes. The PySide6 interface facilitated the straightforward initiation of scans and comprehensive report examination, enabling users to prioritize critical issues, as illustrated in Figure 6. The demonstration of the scanning process and report generation is depicted in Figure 7.

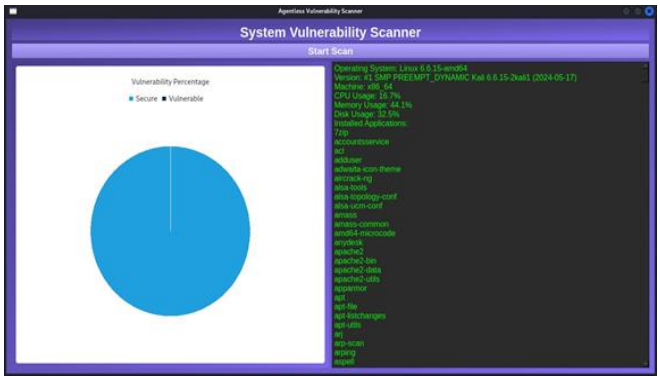

Fig. 6 UI with PySide6

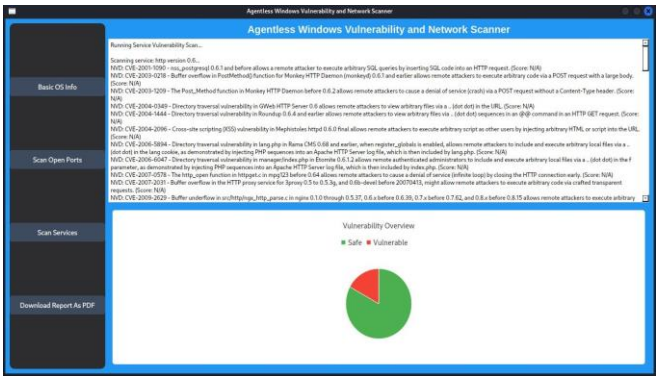

Fig. 7 Running of vulnerability scan

7. Conclusion and Future Enhancements

The agentless Windows vulnerability scanner has proven highly effective in detecting and managing vulnerabilities across extensive networks while exerting minimal impact on system resources. This method presents a scalable and resource-efficient solution, which is particularly suitable for environments with demanding performance requirements. Overall, the system is a pragmatic and effective choice for organizations aiming for scalable and minimally intrusive vulnerability management, enabling security teams to address emerging threats proactively.

To further advance the system in the future, enhancements such as cloud scanning capabilities and AI-driven vulnerability prioritization will be developed. With the growing reliance on cloud infrastructure, extending vulnerability scanning beyond conventional on-premises systems is critical to ensure that cloud environments are also thoroughly secured. By integrating AI and machine learning algorithms, the system will evaluate historical attack patterns, gauge the significance of vulnerabilities, and deliver actionable insights based on the potential risks posed to the organization.

References

[1] Bing Zhang et al., "Efficiency and Effectiveness of Web Application Vulnerability Detection Approaches: A Review," *ACM Computing Surveys*, vol. 54, no. 9, pp. 1-35, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ömer Aslan et al., "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Asem Ghaleb, "*Agentless Endpoint Security Monitoring Framework*," Electronic Theses and Dissertations (ETD), University of Victoria, 2019. [Google Scholar] [Publisher Link]

[4] João Pedro Seara, and Carlos Serrão, "Automation of System Security Vulnerabilities Detection Using Open-Source Software," *Electronics*, vol. 13, no. 5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Santiago Figueroa-Lorenzo, Javier Añorga, and Saioa Arrizabalaga, "A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS," *ACM Computing Surveys*, vol. 53, no. 2, pp. 1-53, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Kismat Chhillar, and Saurabh Shrivastava, "Vulnerability Assessment of University Computer Network Using Scanning Tool Nexpose," *Recent Trends in Communication and Intelligent Systems*, pp. 207-214, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Francisco R.P. da Ponte, Emanuel B. Rodrigues, and César L.C. Mattos, "CVEjoin: An Information Security Vulnerability and Threat Intelligence Dataset," *Advanced Information Networking and Applications*, pp. 380-392, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sagar Rahalkar, *Quick Start Guide to Penetration Testing with NMAP, OpenVAS and Metasploit*, 1st ed., Apress, Berkeley, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Pooja D. Pandit, "Nessus: Study of a Tool to Assess Network Vulnerabilities," 2021. [Google Scholar]

[10] U. Kumaran et al., "Web Vulnerability Scanner," *Advances in Information Communication Technology and Computing*, pp. 193-207, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Rabaya Sultana Mim, Toukir Ahammed, and Kazi Sakib, "Automated Software Vulnerability Detection in Statement Level Using Vulnerability Reports," *Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering*, pp. 454-455, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Xigao Li et al., "Scan Me If You Can: Understanding and Detecting Unwanted Vulnerability Scanning," *Proceedings of the ACM Web Conference*, pp. 2284-2294, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Michał Walkowski, Jacek Oko, and Sławomir Sujecki, "Vulnerability Management Models Using a Common Vulnerability Scoring System," *Applied Sciences*, vol. 11, no. 18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Dipali N. Railkar, and Shubhalaxmi Joshi, "A Study on Vulnerability Scanning Tools for Network Security," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 8, no. 6, pp. 340-350, 2022. [Google Scholar] [Publisher Link]

[15] A. Sowmyashree, and H.S. Guruprasad, "Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS," *International Research Journal of Engineering and Technology*, vol. 7, no. 5, pp. 2068-2073, 2020. [Google Scholar] [Publisher Link]