Journal of Computer Science & Computational Mathematics, *Volume 14, Issue 04, December 2024*
DOI: 10.20967/jcscm.2024.04.001

A Comparative Analysis of Network Enumeration Tools

Fatimah Alghamdi

Department of Computer Science and Artificial Intelligence, University of Jeddah, Jeddah, Saudi Arabia

falghamdi0534.stu@uj.edu.sa

***Abstract*:** Network enumeration is a critical phase in ethical hacking and cybersecurity, enabling the identification of vulnerabilities and weaknesses in network security. This review paper provides an overview and analysis of existing research related to network enumeration tools and techniques. It emphasizes the significance of network enumeration in ethical hacking, compliance with security standards, and proactive vulnerability assessment. The paper discusses the importance of selecting appropriate tools and adhering to legal and ethical considerations in network enumeration activities. The literature review section examines five research papers that evaluate the effectiveness and usability of network enumeration tools, which include Wireshark, Zenmap, Nessus, Nmap, and OpenVAS. Each paper is reviewed, and its strengths and weaknesses are explored, revealing information about the tools' capabilities, implementation, and potential limitations. The review highlights the importance of practical experimentation, comparative analysis, and consideration of user experience in evaluating network enumeration tools. By analyzing their findings, it provides guidance for practitioners, researchers, and beginners in the field of network security.

***Keywords*:** Network enumeration, network enumeration tools, network cybersecurity, Wireshark, OpenVAS, Zenmap, Nmap, Nessus.

1. Introduction

The network enumeration phase is a critical step in cybersecurity and ethical hacking because it helps to identify weaknesses in a network's security defences [1]. By probing the network for data, ethical hackers can get information about its architecture, operating systems, applications, and services [2]. Using this information, potential flaws and configuration errors that could be used by malicious parties to their advantage can be found. In the context of ethical hacking, enumeration refers to the process of gathering detailed information about a target network, including user accounts, system configurations, network topology, services, security measures, and other relevant data [3]. Enumeration also assists ethical hackers in understanding a network's architecture and locating the most effective attack opportunities. They can prioritize the vulnerabilities that pose the greatest risk to the organization and develop a more effective attack strategy using this information. The enumeration phase is also a crucial step in adhering to various security standards and laws like PCI-DSS and HIPAA [4]. By carrying out a thorough network enumeration, organizations can show that they are dedicated to maintaining a secure and compliant network environment. Conducting a study to compare network enumeration tools is significant for several reasons. Firstly, it enhances knowledge and awareness among ethical hackers and cybersecurity professionals by providing insights into the strengths and weaknesses of different tools. This enables them to make informed decisions and improve their efficiency and effectiveness. Secondly, it improves security by helping organizations proactively identify vulnerabilities and address them before they can be exploited. Additionally, utilizing the best network enumeration tools ensures compliance with industry regulations, avoiding penalties for non-compliance. The enumeration phase in ethical hacking builds upon the preliminary foot-printing and scanning phases, which provide basic information about the target's infrastructure, open ports, and services, by extracting more detailed and specific data about the target's systems and applications. During the enumeration phase, an ethical hacker gathers a variety of critical information. This includes usernames and passwords, which when enumerated, can uncover weak credentials that can be exploited for unauthorized access [5]. Additionally, enumeration reveals system information such as operating systems, software versions, and patch levels, providing valuable insights for planning an attack. Network topology can be determined by enumerating network devices, routers, and switches, offering a better understanding of the target's infrastructure. Enumerating open ports, services, and applications exposes potential attack vectors and vulnerabilities. Enumeration also uncovers user and group policies, shedding light on user accounts, groups, and access control permissions that may be exploitable. Furthermore, by enumerating security measures like firewalls, intrusion detection systems, and antivirus software, ethical hackers can identify potential obstacles or opportunities for evasion. The enumeration phase plays a crucial role in gathering detailed information that assists in formulating effective strategies for subsequent stages of the ethical hacking process. Overall, the enumeration phase is a critical component of the ethical hacking process, because it provides detailed insights and intelligence that can be used to identify vulnerabilities and plan attacks.

2. Background

2.1 Network Enumeration

Network enumeration is the process of discovering hosts, services, and other network resources [5]. Learning about the target network is an important part of penetration testing. The goal of network enumeration is to find any potential attack points and security gaps in the network. It employs a number of techniques, including port scanning, service identification, user enumeration, and network mapping. A network vulnerability is a flaw that allows unauthorized access to a network or jeopardizes its integrity. System configuration errors, out-of-date software, weak passwords, and other issues can lead to network vulnerabilities [6]. Penetration testing assists in locating and addressing network vulnerabilities.

Penetration testing is a technique used to check for vulnerabilities that an attacker could exploit against a network, system, or application. It involves simulating an attack on the target system to identify weaknesses and assess the security posture of the network [6]. The goal of penetration testing is to find weak points in the network's security and offer suggestions for strengthening it. In a controlled environment, a network or system is tested for security flaws and vulnerabilities using the ethical hacking process [7]. Network enumeration is an essential phase of ethical hacking, which involves gathering information about the target network. It helps to identify potential attack vectors and vulnerabilities in the network.

2.2 Legal and Ethical Considerations for the Use of Network Enumeration Tools

The legality and ethics of network enumeration depend on the context in which it is carried out. In general, network enumeration can be ethical and legal if it is carried out for proper reasons, such as identifying weaknesses in a system or network, evaluating the effectiveness of security measures, or performing a penetration test with the organization's consent. Network enumeration, however, can be illegal and unethical if it is carried out without the organization's consent [3], or is done for malicious purposes, such as gaining unauthorized access to a network or stealing confidential data. Enumeration in these situations may lead to both civil and criminal penalties. Therefore, it is important for ethical hackers to get explicit permission from the organization before conducting any network enumeration activities and to adhere to established ethical guidelines for penetration testing and vulnerability assessments. This includes getting written permission, limiting the scope of the testing to only those systems and networks that have been authorized, and ensuring that all activities are conducted in a manner that minimizes the risk of disruption or damage to the target network.

3. Literature Review

This section aims to provide a comprehensive overview and analysis of the existing research related to network enumeration tools and techniques.

In the paper titled "Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic", Nawal A. L. Mabsali et al. explore the capabilities of Wireshark, a well-known packet analyzing tool, in detecting and analyzing network attacks and vulnerabilities [8]. The paper begins with an overview of network security and the need for network traffic monitoring. It emphasizes Wireshark's role in capturing and analyzing packets, identifying various types of attacks, and generating detailed reports. The paper presents a penetration test scenario involving a syn flood attack and three different scenarios to assess the tool's effectiveness. The overall objective is to investigate Wireshark's capabilities for vulnerability detection and syn flood attack detection. The paper has several strengths, such as its thorough explanation of Wireshark and its features and the actual experimentation used to gauge the tool's usefulness. The paper provides a clear research methodology/experimental setup and relevant background information on network security and the significance of monitoring network traffic. It also goes over Wireshark's features, which make it a useful tool for network administrators and security analysts. The inclusion of a penetration test scenario adds practicality to the research, allowing for a real-world evaluation of Wireshark's performance in detecting syn flood attacks and vulnerabilities. The paper does, however, have a few flaws. To begin, the paper's organization and structure could be improved to make it easier to follow. Furthermore, the paper lacks a discussion of the research's limitations.

Next, the paper titled "Implementation of Network Security Tool Zenmap on University Computer Network" by Kismat Chhillar and Saurabh Shrivastava focuses on the implementation of Zenmap, a GUI interface for Nmap, in university computer networks [9]. It emphasizes the importance of timely vulnerability assessment in university networks to protect critical data. The paper describes the implementation process and showcases different scan profiles, such as ping scan, quick scan, and intense scan, to gather detailed information about hosts and their security status. The scan results obtained from Zenmap are analyzed, and various sections of the output window are explained. The paper highlights Zenmap's user-friendly nature, interactive result viewing, and the ability to close open ports. It suggests further work involving the implementation of additional vulnerability scanning tools to enhance network security. This paper addresses the importance of network security in university computer networks and provides a detailed overview of Zenmap as a tool for vulnerability assessment. It effectively describes the implementation of Zenmap on a university network and discusses different scan profiles and their outcomes. The paper's emphasis on network security in an educational setting adds practical value to the research. One weakness of this paper is the lack of comparative analysis with other vulnerability scanning tools. Including such comparisons would have provided a broader perspective on Zenmap's strengths and weaknesses. Additionally, the paper could have discussed potential limitations or challenges associated with the implementation of Zenmap in a university environment.

Anudeepa Gon wrote the paper titled "Study Of Network Security, Use Of Network Simulators And Security Tools," which provides an overview of network security, network simulators, and security tools [10]. It highlights the significance of network security in today's digital landscape, where various threats threaten network integrity and confidentiality. The paper discusses various types of attackers, such as white hat hackers, black hat hackers, gray hat hackers, script kiddies, hacktivists, and academic hackers. It also discusses different categories of network attacks, including passive attacks and active attacks. The paper further explores network simulation and highlights some popular network simulators like NS2, NS3, NetSim, OMNeT++, and QualNet. It also contains information on network security tools such as Wireshark, Nmap, and Nessus. This paper's strength lies in its comprehensive coverage of various aspects of network security, network simulation, and security tools. It gives a good overview of network security and its significance in protecting networks from both external and internal threats. The inclusion of different types of attackers and attack categories adds depth to the understanding of network vulnerabilities. The paper also introduces readers to popular network simulators and security tools, giving them an overview of the available options for network analysis and protection. One of this paper's flaws is the lack of in-depth analysis or evaluation of the topics discussed. It provides a general overview without delving into specific details or offering critical insights. Additionally, the paper could benefit from more recent examples and references. Furthermore, the paper could have provided more information about the limitations or drawbacks of the network simulators and security tools mentioned, enabling readers to make more informed decisions regarding their selection and usage.

The paper "A First Look at the Usability of OpenVAS Vulnerability Scanner" [11] presents the findings of a study that evaluated the usability of OpenVAS, a vulnerability scanner, conducted by M. Ugur Aksu, et al. The evaluation was conducted using two methodologies: expert-based (cognitive walkthrough and heuristic analysis) and user-based testing. The cognitive walkthrough identified several issues related to the user interface and functionality of OpenVAS, such as default login credentials, lack of customization options for scan settings, and difficulties in defining credentials for scanning multiple hosts. The heuristic analysis revealed additional issues, including the lack of critical error log display, network performance impact, and limitations in the plugins (NVT) database. The user-based testing showed mixed results, with users being able to complete some tasks successfully but facing challenges in configuring scan tasks. One of the strong points of the paper is its comprehensive evaluation approach. By employing both expert-based and user-based testing, the study provides a well-rounded assessment of OpenVAS usability. The cognitive walkthrough and heuristic analysis allow for an in-depth examination of the software's interface and functionality, uncovering specific issues that may affect user experience. The user-based testing provides real-world insights by involving actual users and measuring their ability to complete tasks. This methodological combination helps strengthen the study's findings and increases its credibility. While the evaluation objectives are mentioned, there is no systematic analysis of the implications of the issues on the overall usability and security of OpenVAS. This limits the practical insights that can be drawn from the study.

Finally, the paper "Learning of Penetration Testing Using Open Source Tools for Beginners" by Kajal Kashyap et al. addresses the relevant topic of learning penetration testing using open source tools [12]. It provides an overview of different tools available in Kali Linux and discusses their step-by-step usage. The inclusion of a comprehensive literature review and the citation of previous studies enhance the credibility of the research, although almost half of the references need to be more up to date. One weakness of this paper is the lack of empirical evidence or case studies demonstrating the effectiveness of the discussed tools. Additionally, the paper could have discussed potential limitations or challenges associated with the learning process using open source tools. It would have been beneficial to address the complexity or potential difficulties beginners might face when utilizing these tools and provide guidance or recommendations to overcome such challenges. Furthermore, for beginners in the field of penetration testing, the paper could have included a comparative analysis of various open- source tools to highlight their respective strengths and weaknesses. Overall, these literature reviews provide useful information about the usability, implementation, capabilities, and effectiveness of key network security research tools such as OpenVAS, Zenmap, Nmap, Nessus, and Wireshark.

4. Methodology

The methodology used in this study involved a comprehensive review of relevant literature from various academic databases. The papers selected for review underwent an analysis to extract relevant information about the enumeration tools that were chosen. This involved a careful reading of the papers to identify key points related to the tools, such as their features, limitations, and applications. The information gathered was then organized to provide a comprehensive understanding of the selected enumeration tools. The selection of tools was an important part of this paper. First, Nmap is a widely used and popular network exploration tool with a wide range of features. Its relevance in network enumeration and penetration testing is well-established [13]. The graphical user interface (GUI) version of Nmap is called Zenmap, and it gives users a simpler and more simplified way to access Nmap's robust features. Its ease of use makes it a popular choice for network enumeration and penetration testing [14]. Nessus is a risk and vulnerability scanning tool for identifying potential network vulnerabilities. It is popular for penetration testing and vulnerability assessments due to its high level of accuracy [15]. Similar to Nessus, OpenVAS is an open-source vulnerability scanner. It is renowned for its precision in locating potential network vulnerabilities

[16, 17]. Finally, Wireshark is a well-known network protocol analyzer that is used for network exploration and penetration testing. It is known for its ability to identify potential vulnerabilities and network issues [18, 19]. The selection of the criteria for evaluating network enumeration tools, including usage, strengths, limitations, and operating system availability, is justified by the need to comprehensively assess these tools from multiple perspectives. By considering usage, we can understand the tool's practicality and compatibility with various network environments. Examining strengths allows us to identify the tool's standout features and capabilities, highlighting its effectiveness in detecting vulnerabilities. Assessing limitations helps us understand any drawbacks, constraints, or potential risks associated with using the tool. Lastly, considering operating system availability ensures that the chosen tools can be effectively utilized across different platforms, providing a wider range of options for network security professionals. The comparison of prices for the network enumeration tools was not conducted as all the tools included in the study are freely available as open-source software, eliminating the need for price evaluation.

5. Results

The results of the analysis are shown in this section. Table 1 provides a brief overview of various network scanning and analysis tools, including their functions, features, limitations, and supported operating systems.

Nmap, a powerful network scanner, detects operating systems and performs port scanning, but generates substantial network traffic. Zenmap offers a user-friendly interface and the ability to compare and save scan results in a database. Nessus excels in providing fewer false positives and supports plug-ins, while OpenV AS offers advanced scanning capabilities but requires manual configuration and may produce false results. Finally, Wireshark captures real-time network traffic and visualizes packets, but its difficulty should be noted. All tools support Linux, Windows, and Mac platforms, except OpenVAS, which doesn't support MacOS [20].

Table 1. Comparison of Network Enumeration Tools

Tool	**Function**	**Features**	**Limitations**	**Supported Platforms**
Nmap	Network and port scanning, OS Detection	Powerful, Flexible	Generates a lot of traffic	Linux, Windows, MAC
Zenmap	Network and port scanning, OS Detection, GUI for Nmap	User-friendly interface, Compare and save scan results in a database, Can display network system topology in a graphical way	Takes longer to scan than Nmap, Learning Curve	Linux, Windows, MAC
Nessus	Vulnerability scanning	Fewer false positives compared to other scanners, Plug-ins	Slow	Linux, Windows, MAC
OpenVAS	Vulnerability scanning	Advanced vulnerability scan and can analyze the results	Need for manual configuration, May produce false positives and false negatives	Linux, Windows
Wireshark	Network packet analyzing, Real-time network traffic capture	Powerful, Visualize Network Packets	Complex	Linux, Windows, MAC

6. Discussion

Nmap is highly configurable and can provide detailed information on every active IP on a network. It supports many advanced techniques for mapping out networks, such as port scanning mechanisms, OS detection, version detection, and ping sweeps [**?**]. However, Nmap can generate a lot of traffic and noise on the network, which can be detected and blocked [21]. Nmap is still a useful tool for auditing network systems and finding new vulnerabilities, despite these drawbacks. Zenmap is a network mapping and enumeration tool that has advantages over plain Nmap, such as a more user-friendly interface and the ability to compare and save scan results in a database for future use. It can also display network system topology in a graphical way [14]. However, sometimes scanning can take more time than usual even when using the same commands. For network scanning, vulnerability scanning, and auditing purposes, Zenmap is a helpful tool. It should be noted that Zenmap is not a replacement for Nmap, but rather a graphical user interface for Nmap. Zenmap is intended to make Nmap more useful, and it provides advantages over ordinary Nmap. Zenmap's main drawback is that, even when using the same commands, scanning can occasionally take longer than usual. Zenmap also has a small learning curve that needs to be overcome before becoming proficient [9]. OpenVAS is a free and open-source application that provides a variety of vulnerability assessment services and tools. It can perform an advanced vulnerability scan and analyze the results. It is a useful tool for detecting system vulnerabilities and can be used for single-feature testing [16]. However, there are some limitations to OpenVAS, such as the possibility of producing false positives and false negatives, which can lead to inaccurate results [11]. Nessus is a vulnerability scanner that is best at performing vulnerability scans and providing accurate findings of the assessments. It uses quick and precise scanning to find vulnerabilities that need to be fixed and emphasizes those that should be fixed immediately. Nessus is excellent for operating system vulnerability detection and provides fewer false positives compared to other scanners [22]. Additionally, it features plug-ins that go beyond what other products provide in terms of customization and extensibility. It also has plug- ins that allow for extensibility and customization beyond what other products offer [15, 23]. However, Nessus isn't designed to perform penetration tests, but it is a tool that should be used in conjunction with pen testing tools. In addition, Nessus has the slowest scanner in the list [22]. Even with these drawbacks, Nessus is a powerful tool for detecting system vulnerabilities and can be used for vulnerability scanning and assessment. Wireshark is a network packet analyzer that displays captured packet data as precisely as possible. It has effective features like protocol dissection, real-time network traffic capture, and packet analysis. Wireshark can be used by network administrators to troubleshoot network issues, and security engineers to investigate security issues. It also allows users to sort, group, and filter packets, as well as identify the protocols that are responsible for their creation. Wireshark is a useful tool for network analysis and troubleshooting because it allows users to dive into the middle of a network packet and visualize it [18]. Wireshark, on the other hand, can be difficult to use and requires a thorough understanding of network protocols and packet analysis. Furthermore, Wireshark can generate a lot of data, which can be overwhelming for inexperienced users.

7. Conclusion

The purpose of this research was to compare and evaluate various network enumeration tools in order to determine their functions, strengths, limitations, and operating system compatibility . Nmap, Zenmap, Nessus, OpenV AS, and Wireshark were the tools that were reviewed. We gained valuable insights into the strengths and weaknesses of these tools through an in-depth analysis of the selected papers, allowing ethical hacking and cybersecurity beginners to make informed decisions in their network security assessments. The comparative analysis revealed that each tool possesses unique features and functionalities. OpenV AS is highly regarded for its comprehensive vulnerability scanning capabilities, while Zenmap and Nmap excel in network mapping and port scanning. Nessus stands out for its extensive vulnerability database and robust reporting capabilities, while Wireshark offers powerful packet analysis and network troubleshooting capabilities. It is essential to keep in mind that no single tool can provide a comprehensive solution for network enumeration because their effectiveness is dependent on a variety of factors such as the target environment, scope of assessment, and specific objectives. Therefore, it is advised to use a combination of these tools based on the needs of each assessment. This review paper has also highlighted the significance of conducting studies comparing network enumeration tools. These studies help to increase cybersecurity knowledge and awareness, which leads to improved security and adherence to industry regulations.

8. Future Work

Future work could expand on this study by conducting experimental evaluations of the network enumeration tools discussed in this paper. We can gain firsthand experience with the performance, accuracy, and usability of these tools by conducting practical tests and comparisons. This would entail creating controlled environments and simulating various network scenarios to assess each tool's effectiveness in identifying vulnerabilities, extracting system information, mapping network topology, and assessing their strengths and weaknesses in various contexts, such as large-scale networks or specific industries. Furthermore, future research should concentrate on developing comprehensive network security guidelines and best practices, empowering individuals, and organizations to proactively protect their networks from potential attacks. These guidelines should cover aspects such as implementing robust authentication mechanisms, regular patching and updates, intrusion detection systems, and secure network configurations. It is important to ensure that these guidelines are accessible and practical for users with varying levels of technical expertise, enabling them to enhance their network security knowledge and minimize the risks associated with network vulnerabilities. By conducting hands-on evaluations and providing practical guidelines, future research can contribute to the continual improvement of network enumeration tools, enhance cybersecurity practices, and strengthen defense against malicious actors.

References

[1] H. Burhan, U. Haq, M. Z. Hassan, M. Z. Hussain, R. A. Khan, S. Nawaz, H. R. Khokhar, and M. Arshad, "The impacts of ethical hacking and its security mechanisms," *hpej.net*, 2022. [Online]. Available: https://www.hpej.net/journals/pakjet/article/view/2226

[2] K. Salman, "Assessing work from home security packages vulnerabilities," 2022. [Online]. Available: https://openrepository.aut.ac.nz/handle/10292/15289

[3] M. R. Ibrahim and K. H. Thanoon, "Quasar remote access trojan feature extraction depending on ethical hacking," 2022. [Online]. Available: https://techniumscience.com/index.php/technium/article/view/5831

[4] S. W. A. Hamdani, H. Abbas, A. R. Janjua, W. B. Shahid, M. F. Amjad, J. Malik, M. H. Murtaza, M. Atiquzzaman, and A. W. Khan, "Cybersecurity standards in the context of operating system," *ACM Computing Surveys (CSUR)*, vol. 54, 5 2021. [Online]. Available: https://dl.acm.org/doi/10.1145/3442480

[5] C. Hines, M. C. C. on Electro Information ,Ä¶, and undefined 2022, "Uncover security weakness before the attacker through penetra-

tion testing," *ieeexplore.ieee.org*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9813950/

[6] J. Softi$f$á, Z. V. . 22nd International Symposium, and undefined 2023, "Impact of vulnerability assesment and penetration testing (vapt) on operating system security," *ieeexplore.ieee.org*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10094095/

[7] P. Cisar, R. P. J. of Applied Technical, Educational, and undefined 2019, "Some ethical hacking possibilities in kali linux environment," *real.mtak.hu*, 2020. [Online]. Available: http://real.mtak.hu/105347/1/139.pdf

[8] N. Mabsali, H. Jassim, J. M. 1st International Conference on, and undefined 2023, "Effectiveness of wireshark tool for detecting attacks and vulnerabilities in network traffic," *atlantis-press.com*, 2022. [Online]. Available: https://www.atlantis-press.com/proceedings/iciitb-22/125984173

[9] K. Chhillar and S. Shrivastava, "Implementation of network security tool zenmap on university computer network," *sageuniversity.in*. [Online]. Available: https://sageuniversity.in/journal/admin/upload/ETRCS-404.pdf

[10] A. Gon, "Study of network security, use of network simulators and security tools," *International Journal of Current Science*, vol. 13, pp. 2250–1770, 2023. [Online]. Available: www.ijcspub.org

[11] M. U. Aksu, E. Altuncu, and K. Bicakci, "A first look at the usability of openvas vulnerability scanner," 2019. [Online]. Available: https://dx.doi.org/10.14722/usec.2019.23026

[12] A. Noor, K. Kashyap, R. Saraswat, and V. K. Sharma, "Learning of penetration testing using open source tools for beginner," *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 3, p. 1287, 2021. [Online]. Available: https://www.researchgate.net/publication/359815702

[13] "Nmap: the network mapper - free security scanner." [Online]. Available: https://nmap.org/

[14] "Chapter 12. zenmap gui users' guide | nmap network scanning." [Online]. Available: https://nmap.org/book/zenmap.html

[15] "Nessus vulnerability scanner: Network security solution | tenable®." [Online]. Available: https://www.tenable.com/products/nessus

[16] "Openvas - open vulnerability assessment scanner." [Online]. Available: https://openvas.org/

[17] S. Rahalkar, "Openvas," *Quick Start Guide to Penetration Testing*, pp. 47–71, 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4842-4270-4_2

[18] "Wireshark ¬ go deep." [Online]. Available: https://www.wireshark.org/

[19] H. Iqbal and S. Naaz, "Wireshark as a tool for detection of various lan attacks big data in healthcare sector view project investigating dhcp and dns protocols using wireshark view project wireshark as a tool for detection of various lan attacks," *Article in INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*, 2019.

[20] A. Kejiou, G. B. . 3rd International Conference on, and undefined 2022, "A review and comparative analysis of vulnerability scanning tools for wireless lans," *ieeexplore.ieee.org*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9932245/

[21] S. Rahalkar, "Introduction to nmap," *Quick Start Guide to Penetration Testing*, pp. 1–45, 2019.

[22] L. Urbano, G. Perrone, and S. P. Romano, "Reinforced wavsep: a benchmarking platform for web application vulnerability scanners," in *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. IEEE, 2022, pp. 1–6.

[23] P. Pandit and P. D. Pandit, "Nessus: Study of a tool to assess network vulnerabilities," 2021. [Online]. Available: https://www.researchgate.net/publication/355040185