Borneo International Journal eISSN 2636-9826; Vol.8 (2); 2025; 69-80
Published by *Majmuah Enterprise*
www.majmuah.com

A Comparative Analysis of Penetration Testing Tools for Network Vulnerability Assessment

MUHD AMIRUL NAJHAN SHAMSUDIN, MOHAMAD FADLI ZOLKIPLI
School of Computing, Awang Had Salleh Graduate School, College of Arts and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: amirul_najhan@ahsgs.uum.edu.my, m.fadli.zolkipli@uum.edu.my

Received: June 27, 2025
Accepted: June 30, 2025
Online Published: July 02, 2025

Abstract

Network enumeration constitutes a vital phase in ethical hacking and cybersecurity, enabling the proactive identification of vulnerabilities and weaknesses within network defenses. This paper presents a comparative analysis of prominent network enumeration and penetration testing tools, including Wireshark, Zenmap, Nessus, Nmap, and OpenVAS, by synthesizing insights from existing research. We highlight the significance of network enumeration in ethical hacking, its role in ensuring compliance with security standards, and its contribution to proactive vulnerability assessment. The review explores each tool's unique capabilities, implementation nuances, and identified limitations, offering a nuanced understanding of their practical utility. A particular emphasis is placed on the importance of tool selection, usability considerations, and adherence to legal and ethical frameworks in cybersecurity activities. By distilling key findings, this analysis aims to guide network security professionals and beginners in making informed decisions for their assessments, recognizing that a combination of these tools often provides the most comprehensive solution.

Keywords: Penetration Testing; Vulnerability Assessment; Network Security; Cybersecurity Tools; Ethical Hacking;

1. Introduction

The digital landscape has profoundly reshaped human interaction, commerce, and governance, with an unprecedented reliance on interconnected systems and online platforms. This pervasive digital transformation, significantly accelerated by recent global shifts, has simultaneously ushered in a new era of complex cybersecurity challenges. As individuals and organizations increasingly conduct their daily activities within cyberspace, the imperative to protect digital assets from exploitation and misuse by malicious entities has become a top global concern. The threat sphere continues to expand rapidly, with cyber-attacks evolving in sophistication, leveraging emerging technologies, and even being offered as a service. In this dynamic environment, traditional protective measures often prove insufficient against new-generation attacks and evasion techniques. In response to this escalating threat, cybersecurity professionals employ a range of proactive strategies to bolster defenses. Among the most crucial is network enumeration, a meticulous process of gathering detailed intelligence about a target network's architecture, operating systems, applications, and services. This phase is foundational to ethical hacking, which involves authorized, simulated cyber-attacks conducted by trained security experts to identify and address vulnerabilities before they can be exploited by actual adversaries. The insights derived from enumeration enable the detection of potential flaws and misconfigurations, allowing organizations to prioritize risks and develop robust security measures. Furthermore, adhering to a thorough enumeration process is essential for compliance with various industry security standards and regulations, such as PCI-DSS and HIPAA, reinforcing an organization's commitment to data protection.

The effectiveness of network enumeration and subsequent penetration testing hinges significantly on the tools employed. This paper provides a focused, comparative analysis of five prominent tools widely recognized in the cybersecurity community: Wireshark, Zenmap, Nessus, Nmap, and OpenVAS. Each tool offers distinct functionalities and capabilities, yet also comes with its own set of limitations. By critically reviewing existing literature that evaluates the effectiveness and usability of these tools, we aim to offer practical insights into their strengths, weaknesses, and optimal application scenarios. Our goal is to provide a guide that transcends mere technical specifications, offering a "humanized" perspective on how these tools integrate into the broader practice of network security, assisting practitioners, researchers, and particularly beginners in making informed decisions for their network security assessments. Ultimately, this work reaffirms the notion that a multi-tool approach, tailored to specific assessment needs, is often the most effective strategy for achieving comprehensive network security

2. Background

In our increasingly interconnected world, the underlying principles and practices of cybersecurity have become indispensable. To fully appreciate the role of network enumeration tools, it is crucial to understand the foundational concepts that underpin their application within the broader cybersecurity domain. This section outlines these essential background elements.

2.1 Cybersecurity: A Growing Imperative

Cybersecurity, fundamentally, is the discipline of protecting digital assets, systems, and networks from unauthorized access, damage, or disruption. Its significance has grown exponentially as societies become more reliant on computational devices for virtually all aspects of daily life, from personal communications to critical national infrastructure. The coronavirus (COVID-19) pandemic, in particular, accelerated this digital shift, pushing more transactions and interactions into the online realm and, consequently, broadening the attack surface for cybercriminals.
The core objective of cybersecurity is often encapsulated by the "CIA triad": ensuring the Confidentiality, Integrity, and Availability of information. However, modern frameworks extend this to include additional aspects like Possession/Control, Authenticity, and Utility, forming the "Parkerian Hexad". The threats to these principles are diverse, ranging from traditional viruses and worms to sophisticated phishing campaigns, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). Emerging technologies such as cloud computing, the Internet of Things (IoT), and wireless communication further introduce new vulnerabilities and expand the landscape for potential exploitation

2.2 Network Enumeration

At its heart, network enumeration is a critical phase in the reconnaissance and information-gathering stages of a security assessment. It involves systematically querying and probing a network to identify detailed information about its hosts, services, and configurations. This process is not a superficial scan; rather, it aims to uncover as much granular data as possible, including:

- Network Architecture and Topology: Understanding how devices are interconnected.
- Operating Systems (OS) and Versions: Identifying the OS running on hosts and their specific versions.
- Applications and Services: Discovering active applications and services, along with their versions, running on exposed ports.
- User Accounts and Groups: Gaining insight into valid user accounts and security groups.
- Security Measures: Identifying deployed firewalls, intrusion detection systems (IDS), and other security controls.
- Potential Flaws and Misconfigurations: Pinpointing vulnerabilities that could be leveraged by attackers.

The detailed information gathered through enumeration is invaluable. For an ethical hacker, it forms the blueprint for understanding a network's weaknesses and formulating targeted attack strategies. For network administrators, it serves as an essential component of proactive vulnerability assessment, enabling them to identify and remediate security gaps before they are discovered and exploited by malicious parties.

2.3 Ethical Hacking and Penetration Testing

Ethical hacking, often synonymous with penetration testing (or "pen testing"), is a legally authorized and simulated cyber-attack conducted against a system or network. The purpose is to mimic the tactics and techniques of real-world attackers to discover exploitable vulnerabilities. Unlike malicious hacking, ethical hacking operates with explicit permission from the target organization, with the ultimate goal of improving security. Ethical hackers, also known as "white hat hackers" or "penetration testers," employ the same tools and methods as "black hat" (malicious) or "grey hat" hackers, but their intent is purely protective and constructive.
The process of ethical hacking typically follows a structured methodology, which can be broadly categorized into several key phases:

1. Planning and Preparation (Pre-Engagement Scoping): Defining the scope, objectives, legal agreements, and rules of engagement.
2. Reconnaissance (Information Gathering): Collecting as much information about the target as possible, using both passive (e.g., public sources) and active (e.g., scanning) techniques. Network enumeration falls heavily into this phase.

3. Vulnerability Identification/Assessment (Discovery & Threat Modeling): Identifying potential weaknesses in the target system, often through automated scanning tools.
4. Exploitation: Attempting to gain access to the system or achieve specific objectives by leveraging identified vulnerabilities.
5. Post-Exploitation: Documenting the impact of the exploitation, maintaining access for further testing, and identifying deeper system compromises.
6. Reporting: Documenting all findings, exploited vulnerabilities, associated risks, and providing actionable recommendations for remediation.
7. Resolution/Re-Testing (Clean-up): Ensuring that identified vulnerabilities are patched and verifying the effectiveness of remedial actions, often involving a clean-up of any temporary files or tools left on the system.

Figure 1: Illustration of Ethical Hacking Phases.

2.4 Vulnerability Assessment vs. Penetration Testing

While often used interchangeably, **vulnerability assessment (VA)** and **penetration testing (PT)** are distinct yet complementary cybersecurity practices.

- **Vulnerability Assessment**: This process focuses on identifying, quantifying, and prioritizing vulnerabilities within a system, network, or application. It typically involves automated scanning tools that check for known weaknesses, missing patches, misconfigurations, and other security flaws. The outcome is a report detailing identified vulnerabilities, their severity, and potential impact, without actively exploiting them.
- **Penetration Testing**: This takes the process a step further by actively simulating an attack to exploit identified (or undiscovered) vulnerabilities. The goal is to determine if a vulnerability is indeed exploitable, assess the potential depth of a breach, and understand the real-world impact of a successful attack. It demonstrates the risk posed by vulnerabilities rather than just listing them.

Both VA and PT are crucial for a robust security posture. VA provides a broad overview of potential weaknesses, while PT offers a deeper, more realistic validation of exploitable paths and their business impact. The tools discussed in this paper often serve both functions, sometimes with an emphasis on one over the other.

3. Literature Review

The landscape of network enumeration and penetration testing tools is rich and continuously evolving. This section reviews key research papers that evaluate the effectiveness and usability of five prominent tools: Wireshark, Zenmap, Nessus, Nmap, and OpenVAS. By examining these studies, we gain valuable insights into each tool's capabilities, typical applications, and identified limitation

3.1 Wireshark

Nawal A. L. Mabsali et al. (2023) thoroughly explore the capabilities of Wireshark as a packet analyzing tool for detecting and analyzing network attacks and vulnerabilities. Their paper underscores the importance of network traffic monitoring and highlights Wireshark's role in capturing and analyzing packets, identifying various attack types, and generating detailed reports. The researchers conducted a penetration test scenario involving a SYN flood attack across Windows 8.1, Windows 10, and Metasploitable virtual machines, assessing Wireshark's effectiveness in detecting both vulnerabilities and the SYN flood itself. Strengths: Mabsali et al. provide a comprehensive explanation of Wireshark and its features, complemented by actual experimentation to gauge the tool's utility. The research methodology and experimental setup are clearly defined, with relevant background on network security and traffic monitoring. Wireshark's features, such as its ability to filter protocols, use color-coding to distinguish traffic, and provide a graphical user interface (GUI) for packet display, make it valuable for administrators and analysts. It is particularly

effective in detecting SYN flood attacks, ARP poisoning, and DNS attacks. Wireshark is also recognized for its role in network forensics, assisting investigators in gathering digital evidence and tracking threat sources.

Weaknesses: Despite its strengths, the paper by Mabsali et al. could benefit from improved organization and structure for easier readability. A notable omission is a discussion of the research's limitations, which would provide a more balanced perspective on Wireshark's performance. Additionally, while powerful, Wireshark can be difficult to master, and its effectiveness in capturing real-time traffic comes with a steep learning curve.

3.2 Zenmap

Penetration Kismat Chhillar and Saurabh Shrivastava's paper, "Implementation of Network Security Tool Zenmap on University Computer Network" (2023), focuses on the practical deployment of Zenmap, which serves as the graphical user interface (GUI) for Nmap. The study emphasizes the critical need for timely vulnerability assessment within university networks to safeguard sensitive data.

Strengths: The paper effectively describes the implementation process of Zenmap within a university network environment and showcases various scan profiles—such as ping scan, quick scan, and intense scan—used to gather detailed information about hosts and their security status. Zenmap's user-friendly interface, interactive result viewing capabilities, and the ability to close open ports are highlighted as significant advantages. Its ease of use makes it a popular choice for network enumeration and penetration testing. An "intense scan" in Zenmap is noted as a common profile that quickly detects TCP ports and identifies operating system types, services, and versions.

Weaknesses: A key limitation identified in this paper is the absence of a comparative analysis with other vulnerability scanning tools. Such comparisons would have provided a broader context for understanding Zenmap's unique strengths and weaknesses relative to its counterparts. Furthermore, the paper could have benefited from a discussion of potential limitations or challenges associated with Zenmap's implementation and usage.

3.3 Nessus

Anudeepa Gon's paper, "Study Of Network Security, Use Of Network Simulators And Security Tools" (2023), offers a broad overview of network security, including various security tools. Within this comprehensive discussion, Nessus is mentioned as one of the significant network security tools. Alghamdi (2024) and others also categorize Nessus as a core tool for network enumeration and vulnerability assessments.

Strengths: Nessus is highly regarded as a risk and vulnerability scanning tool known for its high level of accuracy in identifying potential network vulnerabilities. It stands out for providing fewer false positives compared to some other tools and supports an extensive range of plugins, enhancing its scanning capabilities. Nessus is particularly popular for its robust reporting capabilities and extensive vulnerability database.

Weaknesses: Gon's paper, while comprehensive in its overview, lacks an in-depth analysis or evaluation of the individual tools it discusses, including Nessus. It provides a general introduction without delving into specific details or offering critical insights into its performance or limitations.

3.4 Nmap

Similar to Nessus, Nmap (Network Mapper) is also briefly mentioned in Anudeepa Gon's overview of network security tools. However, its prominence in the cybersecurity community is well-established, making it a frequent subject of discussion in more focused studies.

Strengths: Nmap is widely recognized as a powerful and popular network exploration tool, boasting a wide array of features crucial for network enumeration and penetration testing. Its capabilities include robust operating system (OS) detection and versatile port scanning. Nmap can identify open ports, determine service versions, and even infer the OS running on a target machine. It is highly valued by ethical hackers for its ease of use and extensive scanning options, including TCP, UDP, SYN, ACK, FIN, NULL, and XMAS scans. Nmap is designed to scan large networks but is equally effective for single hosts.

Weaknesses: While powerful, Nmap can generate substantial network traffic during scans, which might be a concern in certain network environments. Some studies indicate that aggressive Nmap scans can be easily detected, potentially alerting defenders.

3.5 OpenVAS

M. Ugur Aksu et al. (2019) specifically conducted a study titled "A First Look at the Usability of OpenVAS Vulnerability Scanner". Their research aimed to evaluate the usability of OpenVAS, an open-source vulnerability scanner, employing both expert-based (cognitive walkthrough and heuristic analysis) and user-based testing methodologies.

Strengths: The paper's comprehensive evaluation approach, combining expert and user-based testing, provides a well-rounded assessment of OpenVAS's usability. This methodological combination strengthens the study's findings and enhances its credibility. The cognitive walkthrough and heuristic analysis identified specific issues affecting user experience, such as problematic default login credentials, a lack of customization options for scan settings, and difficulties in defining credentials for scanning multiple hosts. OpenVAS is highlighted as a highly regarded open-source vulnerability scanner with comprehensive capabilities. The rarity of usability studies conducted with cybersecurity specialists, as noted by the authors, makes their work significant.

Weaknesses: Aksu et al. identified several usability flaws that could lead to insecurity or a "false sense of security". These include:

- Default login credentials that are not forced to be changed upon first use.
- Unclear information about default scan configurations and the advantages/disadvantages of different scan features in the "Advanced Task Wizard".
- Lack of indication regarding network traffic overhead before starting a scan.
- Unclear syntax for defining multiple IP addresses.
- Issues with defining credentials for credentialed scans at the task wizard page.
- No clear information on when to choose authenticated vs. unauthenticated scans.
- Lack of critical error log display.
- Network performance impact not explicitly stated.
- Limitations in the plugins (NVT) database and a lack of information on its update status, leading to potential false negatives or an outdated sense of security.
- Users often focused on simply starting scan tasks rather than properly configuring them to detect as many vulnerabilities as possible.

The paper also noted a lack of systematic analysis regarding the implications of these usability issues on the overall security provided by OpenVAS, limiting practical insights. OpenVAS does not support MacOS.

3.6 Synthesis and Gaps in Literature

The reviewed literature collectively underscores the critical role of network enumeration and penetration testing tools in maintaining cybersecurity. However, several common themes and gaps emerge:

- Need for Comparative Analysis: Many individual tool-focused studies, like the one on Zenmap, lacked comparative analysis with other tools, which would provide a broader perspective on their strengths and weaknesses.
- Depth vs. Breadth: While some papers offer comprehensive overviews of various tools (e.g., Gon's paper), they often sacrifice in-depth analysis for breadth, limiting critical insights into specific tool performance and limitations.
- Empirical Evidence and Case Studies: There is a general need for more empirical evidence and real-world case studies demonstrating the effectiveness of these tools, especially in the context of learning for beginners.
- Usability Focus: The OpenVAS study uniquely highlights the crucial, yet often overlooked, aspect of tool usability in cybersecurity. Poor usability can directly translate into security deficiencies or a false sense of security, emphasizing that functional effectiveness alone is insufficient.
- Real-world Data Challenges: The broader literature on network intrusion detection frequently points to the challenges of collecting and labeling real-world network traffic for effective model training and evaluation.

Many studies still rely on outdated or synthetically generated datasets, which may not accurately represent current attack patterns.

These observations collectively highlight the ongoing need for rigorous, user-centric research in evaluating cybersecurity tools to ensure they not only function effectively but also empower practitioners to leverage their full potential securely and efficiently.

4. Methodology

This section outlines the methodological approach undertaken for this paper, focusing on the comprehensive review of existing literature, the rationale behind the selection of the primary network enumeration tools, and the analytical framework applied to synthesize the findings. Our goal is to provide a clear, transparent, and academically rigorous process for generating the insights presented herein.

4.1 Research Approach

The core of this study is a comprehensive literature review. We systematically identified, collected, and analyzed relevant research papers from various academic databases. This approach allowed us to consolidate existing knowledge, identify key findings, and pinpoint common themes, strengths, and weaknesses associated with the selected network enumeration tools.

4.2 Selection of Network Enumeration Tools

The selection of Wireshark, Zenmap, Nessus, Nmap, and OpenVAS for this comparative analysis was based on their widespread recognition, popularity, and distinct functionalities within the cybersecurity and ethical hacking communities. The rationale for including each tool is as follows:

- Nmap: As a widely used and popular network exploration tool, Nmap possesses a broad range of features crucial for network enumeration and penetration testing. Its relevance in discovering hosts, operating systems, and open ports is well-established.
- Zenmap: Zenmap was included as the graphical user interface (GUI) version of Nmap. Its selection emphasizes the importance of user-friendliness and simplified access to Nmap's robust features, making it a preferred choice for many network enumeration and penetration testing activities due to its ease of use.
- Nessus: Nessus is a leading commercial risk and vulnerability scanning tool. Its inclusion is due to its high level of accuracy in identifying potential network vulnerabilities, its plugin support, and its extensive vulnerability database, making it popular for comprehensive vulnerability assessments.
- OpenVAS: OpenVAS was chosen as a prominent open-source alternative to commercial vulnerability scanners like Nessus. It is renowned for its comprehensive vulnerability scanning capabilities and is a vital tool for organizations seeking robust security solutions without proprietary software constraints.
- Wireshark: Wireshark, a well-known packet analysis tool, is indispensable for deep network traffic inspection. Its ability to capture and visualize real-time network traffic, identify anomalous activities, and analyze various protocols makes it critical for detailed forensic analysis and attack detection beyond just scanning.

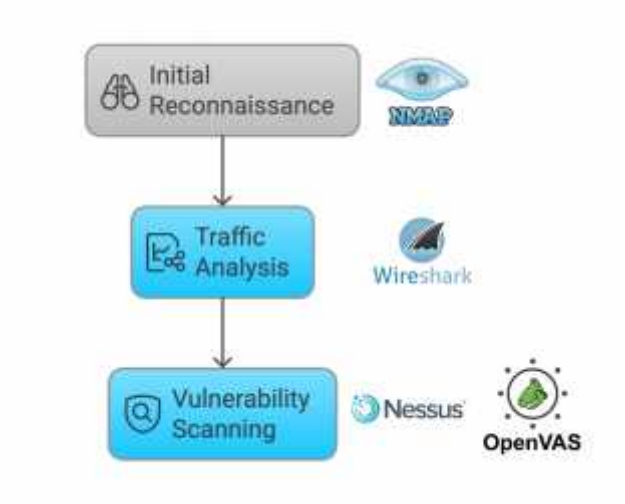

Figure 2: Conceptual Diagram illustrating the interconnectedness of chosen tools in a typical penetration testing workflow.

4.3 Data Collection and Analysis

The methodology involved a meticulous process of extracting relevant information from the selected research papers. This included:

i. Careful Reading: Each paper was read thoroughly to identify key points related to the chosen tools.

ii. Information Extraction: Data pertinent to features, capabilities, implementation details, strengths, limitations, and operating system compatibility of each tool were extracted.

iii. Thematic Organization: The gathered information was then organized thematically to facilitate a comprehensive understanding and comparative analysis of the selected enumeration tools. This involved structuring the findings based on common attributes across the tools, such as their primary function (e.g., port scanning, vulnerability assessment, packet analysis), their key features (e.g., GUI, plugin support, reporting), and their identified limitations (e.g., traffic generation, usability issues, OS support).

By systematically applying this methodology, we aimed to provide a structured and insightful overview that enables ethical hacking and cybersecurity beginners to make informed decisions regarding their network security assessments.

5. Results

The comprehensive analysis of the selected literature yielded distinct profiles for each of the network enumeration and penetration testing tools, highlighting their primary functions, notable features, specific limitations, and operating system compatibility. These findings are synthesized below to provide a comparative overview.

5.1 Comparative Overview of Tools

Table 1: A comparative overview of network enumeration and penetration testing tools.

Tool Name	Primary Functions	Key Features	Limitations & Challenges	Supported OS
Nmap	Network mapping, OS detection, Port scanning	Powerful, versatile scan options (TCP, UDP, SYN, ACK, FIN, NULL, XMAS); Scriptable Interaction	Generates substantial network traffic; can be easily detected	Linux, Windows, Mac

Zenmap	Network mapping, OS detection, Port scanning (GUI for Nmap)	User-friendly GUI; interactive result viewing; compare and save scan results in a database; visual topology mapping	Lacks comparative analysis in studies; potential for unaddressed limitations	Linux, Windows, Mac
Nessus	Risk and vulnerability scanning	Fewer false positives; supports extensive plugins; comprehensive vulnerability database; robust reporting	General overview in some studies, lacks in-depth evaluation; commercial licensing	Linux, Windows, Mac
OpenVAS	Comprehensive vulnerability scanning	Advanced scanning capabilities; open-source; extensible via NVTs	Requires manual configuration; may produce false results; significant usability issues (e.g., default credentials, unclear scan options, limited error logs, NVT database visibility); No MacOS support	Linux, Windows
Wireshark	Packet analysis, Real-time traffic capture	Visualizes packets; extensive filtering capabilities; color-coding for traffic types; identifies malicious activity; protocol analysis	Can be difficult to master; organization issues in some reviews; lack of limitations discussion in some studies	Linux, Windows, Mac

5.2 Detailed Findings per Tool

1. Nmap: This tool stands out for its raw power in network discovery and operating system identification. It is highly effective in probing networks to identify active hosts, their open ports, and the services running on them, including detailed version information. Ethical hackers widely use it for its comprehensive scanning options and its ability to work across large or single networks. However, its verbosity can lead to significant network traffic, which might be a detection risk in monitored environments.

2. Zenmap: As the graphical front-end for Nmap, Zenmap significantly enhances user accessibility. It simplifies the execution of complex Nmap commands and provides an intuitive interface for visualizing scan results, comparing different scans, and managing scan profiles. Its user-friendly nature makes Nmap's powerful features more approachable for beginners and those who prefer a GUI. The ability to save scan results in a database is a practical feature for ongoing assessments.

3. Nessus: Nessus is positioned as a sophisticated vulnerability assessment solution. Its core strength lies in its ability to accurately identify vulnerabilities with a low rate of false positives. The tool's extensibility through plugins allows it to adapt to new threats and maintain a comprehensive vulnerability database, which is crucial for robust reporting on identified risks. Its accuracy makes it a favored choice for in-depth vulnerability assessments.

4. OpenVAS: As an open-source counterpart to Nessus, OpenVAS offers advanced and comprehensive vulnerability scanning capabilities. It is a powerful option for organizations seeking cost-effective, yet robust, security assessments. However, usability emerges as a significant challenge for OpenVAS. Studies indicate that it often requires extensive manual configuration, which can be demanding for new users. Critical usability issues identified include a default login that is not forced to change, a lack of clear

explanations for scan configurations, and difficulties in setting up credentialed scans for multiple hosts. The tool's interface sometimes hides crucial information, such as the status of its vulnerability test (NVT) database, potentially leading to a false sense of security or inaccurate scan results. Notably, OpenVAS does not support MacOS, which is a significant limitation for users on that platform.

5. Wireshark: This tool excels in deep packet inspection and real-time network traffic analysis. It provides a granular view of network communications, enabling security analysts to identify suspicious behaviors, analyze attack patterns, and pinpoint the origin of malicious traffic. Wireshark's capabilities extend to detecting specific attack types like SYN floods, ARP poisoning, and DNS attacks, making it invaluable for both proactive monitoring and post-incident forensic analysis. However, mastering Wireshark's full potential, particularly its filtering and analysis functionalities, requires considerable expertise and can be challenging for beginners.

5.3 Overall Operating System Compatibility

A common observation across most of these tools is their broad compatibility with popular operating systems. Nmap, Zenmap, Nessus, and Wireshark generally support Linux, Windows, and Mac platforms. OpenVAS, while supporting Linux and Windows, is noted for its lack of support for MacOS. This broad compatibility ensures that these tools can be integrated into diverse IT environments for security assessments.

6. Discussion

The detailed analysis of Wireshark, Zenmap, Nessus, Nmap, and OpenVAS reveals a landscape of specialized and complementary tools, each bringing unique strengths and confronting distinct limitations in the realm of network enumeration and penetration testing. Our findings reinforce several critical insights for practitioners and researchers in cybersecurity.

6.1 The Inherent Complementarity of Tools

A recurring theme across the literature is that no single tool can provide a comprehensive solution for all network enumeration needs. The effectiveness of any given tool is profoundly dependent on the specific context of the assessment, the network environment, and the particular security objectives. For instance, Nmap and Zenmap excel in network mapping and port scanning, providing the foundational reconnaissance layer by identifying active hosts and open services. Wireshark then takes on the role of deep-dive packet analysis, crucial for understanding communication patterns, detecting anomalous traffic, and performing forensic investigations. Meanwhile, Nessus and OpenVAS are designed for extensive vulnerability scanning, identifying known weaknesses and misconfigurations across various systems and applications.

Therefore, for truly robust and comprehensive security assessments, it is not merely advisable but essential to employ a combination of these tools. An ethical hacker might start with Nmap/Zenmap for initial network discovery, then use Nessus or OpenVAS to pinpoint specific vulnerabilities, and finally leverage Wireshark to analyze attack traffic or confirm successful exploitation during a penetration test. This multi-tool approach allows for a layered assessment, ensuring that different aspects of network security are thoroughly examined from various perspectives.

6.2 The Overlooked Importance of Usability

One of the most striking insights, particularly highlighted by the study on OpenVAS, is the critical role of usability in security tools. While IT security software is often developed with functionality as the primary concern, overlooking usability can directly lead to security deficiencies or foster a dangerous "false sense of security". The OpenVAS evaluation revealed that despite its advanced capabilities, issues such as non-forced default login credential changes, unclear explanations for scan configurations, and opaque NVT (Network Vulnerability Test) database status actively hinder users from making informed security decisions. Users, especially novices, tend to focus on initiating tasks rather than ensuring optimal and secure configurations, inadvertently leaving gaps in their assessments. This underscores that a tool, no matter how powerful its underlying algorithms or features, is only as effective as its users can make it. Recommendations for improving usability include:

- Forcing initial credential changes.
- Providing clear, intuitive explanations for complex scan configurations and their implications (e.g., network traffic load).

- Elucidating acceptable syntax for inputs (e.g., multiple IP addresses).
- Transparently displaying critical system statuses, like the update freshness of the NVT database, with appropriate warnings.

Addressing usability is not merely about convenience; it is a fundamental security imperative that ensures practitioners can correctly and comprehensively utilize these sophisticated tools to enhance network defenses.

6.3 Challenges in Data Realism and Reproducibility

Beyond tool-specific discussions, the broader field of network intrusion detection and security assessment faces persistent challenges related to data realism and reproducibility. Many seminal works and ongoing research still rely on publicly available datasets like KDD Cup 1999, which, despite their historical significance, are synthetically generated and outdated, potentially introducing bias that does not reflect real-world traffic patterns or modern attack behaviors. While newer datasets like LITNET-2020 aim to provide real-world, long-term network traffic data, the availability of such high-quality, labelled datasets remains a significant gap. Furthermore, the reproducibility of research findings, particularly concerning the implementation of machine learning models for intrusion detection, is often hampered by a lack of accessible and well-documented code repositories. This makes it difficult for other researchers to validate results, build upon existing work, and transition theoretical models into practical applications. Future research must prioritize not only the collection of diverse, real-world network data but also the open sharing of thoroughly documented and reproducible code to foster collaborative advancement in the field.

6.4 The Rise of Automation and Intelligent Solutions

An exciting development in the field is the growing integration of machine learning (ML) and deep reinforcement learning (DRL) in automating aspects of network security, particularly penetration testing and cyber-attack path prediction. Researchers are exploring how DRL agents can learn optimal strategies for exploiting vulnerabilities, predicting attack paths, and even designing intelligent, automated penetration testing frameworks. Tools like Microsoft's CyberBattleSim are emerging to provide environments for training such agents. This trend signifies a shift towards more proactive and adaptive defense mechanisms, where systems can learn to identify and respond to threats with minimal human intervention. While still in nascent stages for real-world deployment due to complexities like handling large, dynamic datasets and ensuring model explainability, the potential for intelligent automation to enhance cybersecurity is immense. This represents a promising direction for future work, focusing on developing more realistic reward functions, expanding vulnerability sets, and integrating real-world data into these intelligent systems. In conclusion, the discourse surrounding network enumeration tools highlights their foundational role in cybersecurity. However, their true value is unlocked through strategic combination, user-centric design, and continuous adaptation to the evolving threat landscape and advancements in intelligent automation.

7. Conclusion

In this comprehensive review, we embarked on a journey to compare and evaluate five pivotal network enumeration and penetration testing tools: Nmap, Zenmap, Nessus, OpenVAS, and Wireshark. Our endeavor was driven by the recognition that network enumeration is not merely a technical step but a critical phase in the proactive identification of vulnerabilities, essential for ethical hacking and compliance with stringent security standards. Through an in-depth analysis of existing research, we gained invaluable insights into the distinct strengths, functionalities, and limitations of each tool. We observed that Nmap and its graphical counterpart, Zenmap, excel in network mapping and port scanning, providing the essential groundwork for understanding network topology and exposed services. Nessus emerged as a leader in comprehensive vulnerability scanning, lauded for its accuracy, plugin support, and robust reporting capabilities. OpenVAS, while a powerful open-source alternative, demonstrated significant usability challenges, emphasizing that functional prowess must be matched with intuitive design to prevent misconfiguration and a false sense of security. Lastly, Wireshark proved indispensable for deep packet analysis, crucial for real-time traffic inspection and the forensic identification of malicious activities. A fundamental takeaway from this comparative analysis is the recognition that no single tool offers a panacea for all network enumeration needs. Their individual effectiveness is highly contingent upon the specific assessment objectives, the characteristics of the network environment, and the expertise of the user. Consequently, we strongly advocate for the strategic utilization of a combination of these tools to achieve truly comprehensive and resilient security assessments. For instance, combining Nmap's discovery capabilities with Nessus or OpenVAS's vulnerability detection, and then using Wireshark for granular traffic analysis and attack verification, creates a formidable layered approach to network security.

This review also underscored the broader challenges and future directions within cybersecurity, particularly the imperative for improved tool usability, the need for more realistic and reproducible real-world datasets for training and evaluation, and the exciting potential of integrating advanced artificial intelligence techniques like deep reinforcement learning for automated penetration testing. Such advancements promise to further enhance cybersecurity knowledge and awareness, leading to improved security postures and stricter adherence to industry regulations. In closing, our research contributes to the continuous improvement of network enumeration practices by providing practical guidance for current practitioners and laying a foundation for future research. By embracing a holistic view of tool application and continually refining methodologies, we can collectively strengthen our defenses against the ever-evolving landscape of cyber threats.

8. Acknowledgement

The authors extend their gratitude to all members of the School of Computing for their invaluable contributions to this study. This research was conducted under the Hacking and Penetration Testing Project and supported by Universiti Utara Malaysia.

9. References

M. U. Aksu, E. Altuncu, and K. Bicakci, "A First Look at the Usability of OpenVAS Vulnerability Scanner," 2019, doi: 10.14722/usec.2019.23026.

F. Alghamdi, "A Comparative Analysis of Network Enumeration Tools," *Journal of Computer Science and Communication*, 2024, doi: 10.20967/jcscm.2024.04.001.

M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," *Appl. Sci.*, vol. 13, no. 6986, 2023, doi: 10.3390/app13126986.

Anon., "Fundamentals of Ethical Hacking and Penetration Testing," in *SIGITE '19*, Tacoma, WA, USA, October 3–5, 2019, doi: 10.1145/3349266.3351391.

Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 1333, 2023, doi: 10.3390/electronics12061333.

G. Bagyalakshmi *et al.*, "Network Vulnerability Analysis on Brain Signal/Image Databases Using Nmap and Wireshark Tools," *IEEE Access*, vol. 6, pp. 57144–57151, 2018, doi: 10.1109/ACCESS.2018.2872775.

M. Chen, "Evolving Network Security in the Era of Network Programmability," in *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*, Salt Lake City, UT, USA, October 14–18, 2024, pp. 3 pages, doi: 10.1145/3658644.3690859.

D. Chou and M. Jiang, "A Survey on Data-driven Network Intrusion Detection," *ACM Comput. Surv.*, vol. 54, no. 9, Art. no. 182, October 2021, doi: 10.1145/3472753.

P. Cisar and R. Pinter, "Some ethical hacking possibilities in Kali Linux environment," *Journal of Applied Technical and Educational Sciences (jATES)*, vol. 9, no. 4, pp. 129–149, 2019, doi: 10.24368/jates.v9i4.139.

R. H. Dolon, M. Ridowan, and I. J. Mouri, "The Resilience of Digital Bangladesh: A Case Study on Web Vulnerabilities in the Private Sector of Bangladesh," in *ICCA 2024*, Dhaka, Bangladesh, October 17–18, 2024, doi: 10.1145/3723178.3723203.

L. Erdődi, Å. Å. Sommervoll, and F. M. Zennaro, "Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents," *Journal of Information Security and Applications*, vol. 61, no. 102903, 2021, doi: 10.1016/j.jisa.2021.102903.

A. Gupta and L. S. Sharma, "Mitigation of DoS and Port Scan Attacks Using Snort," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 248–258, April 2019, doi: 10.26438/ijcse/v7i4.248258.

S. W. A. Hamdani *et al.*, "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons," *ACM Comput. Surv.*, vol. 54, no. 3, Art. no. 57, May 2021, doi: 10.1145/3442480.

M. R. Ibrahim and K. H. Thanoon, "Quasar Remote Access Trojan feature extraction depending on Ethical Hacking," *Technium Science Journal*, 2022. [Online]. Available: https://techniumscience.com/index.php/technium/article/view/5831.

K. R. R. Daniel and L. Nayak, "Wireless Network Penetration Testing," *International Journal of Latest Trends in Engineering, Management and Agricultural Sciences*, vol. XIV, no. IV, pp. 56, April 2025, doi: 10.51583/IJLTEMAS.2025.140400056.

P. Lachkov *et al.*, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," *Journal of Web Engineering*, vol. 21, no. 7, pp. 2187–2208, 2022, doi: 10.13052/jwe1540-9589.2178.

N. A. L. Mabsali, H. Jassim, and J. Mani, "Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic," in *ICIITB 2022, ACSR 104*, 2023, pp. 114–135, doi: 10.2991/978-94-6463-110-4_10.

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, no. 12, pp. 1287–1305, Dec. 2021, doi: 10.35629/5252-031212871305.

K. A. G. Quilantang *et al.*, "Exploiting Windows 7 Vulnerabilities using Penetration Testing Tools: A Case Study about Windows 7 Vulnerabilities," in *The 2021 9th International Conference on Computer and Communications Management (ICCCM '21)*, Singapore, Singapore, July 16–18, 2021, pp. 6 pages, doi: 10.1145/3479162.3479181.

A. Saktiansyah and M. Muharrom, "Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas," *IJECSA*, vol. 2, no. 2, pp. 51–58, Sep. 2023, doi: 10.30812/IJECSA.v2i2.3297.

Z. Tashenova, Z. Abdugulova, S. Amanzholova, and E. Nurlybaeva, "PENETRATION TESTING APPROACHES EMPLOYING THE OPENVAS VULNERABILITY MANAGEMENT UTILITY," *News of the National Academy of Sciences of the Republic of Kazakhstan. Physico-Mathematical Series*, vol. 4, no. 352, pp. 218–230, 2024, doi: 10.32014/2024.2518-1726.319.

F. Terranova, A. Lahmadi, and I. Chrisment, "Leveraging Deep Reinforcement Learning for Cyber-Attack Paths Prediction- Formulation, Generalization, and Evaluation," in *The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024)*, Padua, Italy, September 30–October 02, 2024, pp. 16 pages, doi: 10.1145/3678890.3678902.