Comparative Study of Open Source Network Security Tools: Nmap and New Candidates in Network Scanning

Laura Carvalho de Barros
Colégio Técnico Industrial de Santa Maria - CTISM/UFSM
Santa Maria, Brasil
e-mail: laura.barros@redes.ufsm.br

Gabriel Denarde
Colégio Técnico Industrial de Santa Maria - CTISM/UFSM
Santa Maria, Brasil
e-mail: gabriel.denarde@redes.ufsm.br

Guilherme de Mello Pasa
Colégio Técnico Industrial de Santa Maria - CTISM/UFSM
Santa Maria, Brasil
e-mail: guilherme.pasa@redes.ufsm.br

Pedro Henrique Salvador
Colégio Técnico Industrial de Santa Maria - CTISM/UFSM
Santa Maria, Brasil
e-mail: pedro.salvador@redes.ufsm.br

Walter Priesnitz Filho
Colégio Técnico Industrial de Santa Maria - CTISM/UFSM
Santa Maria, Brasil
e-mail: walter@redes.ufsm.br

***Abstract*—This article analyzes the benefits and limitations of using alternative tools to Nmap in network scanning and vulnerability detection activities. While Nmap is widely recognized for its depth of analysis, versatility, and scripting support, tools like Masscan, ZMap, RustScan, Angry IP Scanner, and OpenVAS offer specific advantages such as increased speed, simplicity, or a focus on automated tasks. However, these alternatives may sacrifice accuracy, detail, or flexibility. The choice between them depends on the necessary balance between speed, depth, and context of the application. In conclusion, using multiple tools together works best. Fast tools like Masscan and ZMap are good for the first scan. Nmap or RustScan can then give more details. And OpenVAS should be used for in-depth security checks.**

***Keywords*—Security Tools; Network scanning; Nmap Alternatives; Vulnerability assessment; Port scanning.**

I. Introduction

The way networks work and how information systems have become more complex has made cybersecurity a key concern for companies of all sizes. One important method for keeping digital resources safe is network scanning, which helps find open ports, services that are running, and potential weaknesses. Because of its wide range of features, in-depth analysis, and support for advanced scripts, Nmap has become the most commonly used tool among professionals [1]. But as the need for quicker, simpler, or more targeted scans has grown, other tools have come into play.

This paper is divided into six main parts. The first part, the Introduction, explains the background of the research and what the study is trying to achieve. The next section, Methodology, explains the rules and steps used to pick and study the tools. The Proposal section talks about how the proposed network scanners were compared. Then the Results section that shows all the data gathered. After that, the Discussion of Results looks closely at the findings and explains what they mean. Finally, the Conclusions wrap up the study's main points and give ideas for future research.

Some popular alternatives include Masscan, ZMap, RustScan, Angry IP Scanner, and OpenVAS. Masscan is known for its speed in scanning ports, but it doesn't check what services are running [2]. ZMap is designed mainly for academic use, allowing fast scans of large IP ranges, though it has limited support for different protocols [3]. RustScan is special because it combines fast scanning with Nmap for service detection, offering both speed and depth [4]. Angry IP Scanner is user-friendly and has a simple graphical interface, making it a good choice for new users [5]. OpenVAS is a strong tool for businesses, offering in-depth vulnerability checks based on known issues, authenticated scans, and detailed reports [6].

This article compares these tools, explaining their best uses, advantages, and drawbacks when compared to Nmap. The goal is to give a balanced view that helps experts and researchers pick the right tool depending on the time, depth of scan, and specific needs of their scenarios.

II. Methodology

This paper is a qualitative, exploratory, and document-based study. The goal was to compare different tools used for network scanning and finding security weaknesses, looking at their features, drawbacks, and how they are used. To do this, the research relied only on official technical guides, developer repositories like GitHub, and the official websites of the tools being studied. Six tools were chosen for the study: Nmap, Masscan, ZMap, RustScan, Angry IP Scanner, and OpenVAS.

These were selected because they are widely used in the security field, have plenty of public information available, and each has different ways of working, which allowed for a broad comparison. Nmap was used as the main reference because it is commonly used and has a wide range of functions for checking ports and services [1].

The comparison was based on information from the official sites, project pages like GitHub and GitLab, and up-to-date user guides as of 2024. Key factors looked at included how fast the tools scan, how well they detect services, whether they have a user-friendly interface or require command-line use, if they can be automated, if they generate reports, and if they work with standards like CVE or CVSS. Also considered was what kind of use case they are best suited for, such as academic, business, or personal use. All the information was gathered and organized in a descriptive way, without actually testing the tools in a real or simulated environment.

Using the collected data, a review was created that highlights the main advantages and disadvantages of each tool. The analysis focused on balancing speed, depth of analysis, and how complex the tool is to use. The study aims to identify, based on the available documentation, which tools are best for specific scenarios, helping professionals and researchers make informed choices.

III. Proposal

This paper suggests a thorough review of existing research to look at how various network scanning and vulnerability checking tools stack up against Nmap.

Nmap is well-known for being accurate, having advanced features, and being very flexible. Even though Nmap is powerful, it isn't always the best choice when quick results, simplicity, or automation over a large network are needed [1]. Because of this, other tools like Masscan, ZMap, RustScan, Angry IP Scanner, and OpenVAS are becoming more popular. Each of these tools has its own strengths and is suited for different purposes, such as speed, user-friendliness, or use in corporate environments.

The goal of this review is to collect, sort, and examine the technical details and research already available about these alternatives. It will highlight how each tool is used, what it does well, and what limitations it has. The focus isn't just on comparing the tools themselves, but also on figuring out which tool is most appropriate for different scenarios. Additionally, the paper aims to identify areas that haven't been widely studied and to suggest where future research or improvements might be useful. Ultimately, the goal is to provide a strong reference that helps people working or studying in this field make better, more informed choices about which tool to use based on their specific needs and goals.

IV. Results

By looking at the tools selected - Nmap, Masscan, ZMap, RustScan, Angry IP Scanner, and OpenVAS - we got comparisons on how fast they are, how deep their analysis goes, and how well they work in different security scenarios.

Nmap, which started in 1997 by Gordon Lyon (also known as Fyodor), is the most popular network scanning tool among security experts. It's open source and helps find open ports, running services, software versions, and operating systems on local networks or the internet [1]. It does more than just check ports; it also has a scripting engine called NSE that lets you run automated scripts for tasks like finding vulnerabilities, checking security, and doing custom tests. Because of its strong features and clear documentation, it's a standard tool used in security tests and audits in both schools and businesses. It has features like identifying system details, checking versions, supporting different scan types like TCP SYN or UDP, and has detailed documentation. However, it's slower when scanning large groups of IP addresses.

Masscan, made by Robert David Graham, is very fast for scanning many IP addresses at once. It can send up to 10 million TCP SYN packets every second, so it can scan whole IP ranges in minutes. This makes it great for quickly finding which ports are open on big networks, especially the public internet [2]. But unlike Nmap, it doesn't find out what services are running or gather detailed information, only which ports are open. You can export its results in a format that works with Nmap for more detailed checks. It needs some technical skills to use, and it's often used by offensive security teams and researchers.

ZMap was created at the University of Michigan, mainly for use in academic settings and large-scale internet research. It stands out because it can efficiently perform statistical scans on IPv4 networks. It sends TCP SYN packets either randomly or in a planned way to avoid being detected and to prevent overloading target networks [3]. Like Masscan, ZMap is limited to basic port scanning, but it has a modular system that allows for adding new features. It's often used in internet security studies, mapping how protocols are used, and measuring global vulnerabilities. ZMap needs a more advanced technical setup. Its efficient design enables the use of sampling methods that make sure there's enough statistical coverage when scanning large IP blocks.

Masscan and ZMap are known for their high performance in scanning [1], [2]. Masscan is especially fast, handling up to 10 million packets per second. However, it only detects open ports and doesn't check for specific services [2]. It does TCP scanning and gives results that match Nmap standards. ZMap is also very fast in TCP scans and is used for academic research, though it needs some technical setup [3].

RustScan is a newer tool built using the Rust programming language, which focuses on safety and performance. It's designed for fast detection of open ports using modern multi-threading methods. After initial detection, it can automatically run Nmap to do a more detailed analysis [4]. This combination of speed and depth makes it a powerful tool. It has a simple command-line interface and is aimed at technical users who want to quickly discover services on a network. RustScan has become popular among professionals who want modern, fast, and well-integrated tools.

RustScan combines fast port detection with automatic Nmap use for deeper analysis. It uses multithreading and has a modern interface, making it effective in environments that need quick results without losing detail [4]. This hybrid approach makes RustScan a strong choice when speed and in-depth scanning are required.

Angry IP Scanner was first made in 2001. It stands out because it has a simple and easy-to-use graphical interface. It is one of the few tools that work on multiple operating systems like Windows, Linux, and macOS. This makes it useful for both network administrators and people who are just starting out. Its main features include scanning for IP addresses and checking which ports are open. It can also save the results in formats like CSV, TXT, and XML. While it doesn't have advanced features for scanning ports, its simplicity makes it a good choice for everyday tasks on local networks, such as finding which devices are connected. Its main strengths are how easy it is to use and how simple it is, which is different from more complex tools like Nmap and Masscan. Angry IP Scanner is better suited for basic scenarios. It's easy to use because of its graphical interface, but it can only do simple port scans, which makes it accessible to people without much technical knowledge [5].

OpenVAS, which stands for Open Vulnerability Assessment System, was developed by Greenbone Networks. It is a powerful platform used for finding and classifying security weaknesses. It started as a fork of the Nessus project after Nessus became a commercial product. Now, it is a strong open-source solution. OpenVAS uses up-to-date databases for CVEs (Common Vulnerabilities and Exposures) and CVSS (Common Vulnerability Scoring System) to check for vulnerabilities. It does this by performing authenticated scans through methods like SSH or SMB and creates detailed technical reports. Its graphical interface, called Greenbone Security Assistant, helps users to see and to track the results. OpenVAS is often used in corporate settings for audits, compliance checks, and formal security evaluations. However, setting it up, configuring it, and the resources it uses are more involved than tools that only do port scanning [7]. A comparison of the different tools is shown in Table I.

TABLE I
General Comparison of Tools

Tool	GUI	Depth of Analysis
Nmap 1	Yes	Complete
Masscan	No	Low (Ports)
ZMap	No	Low (Ports)
RustScan	No	Medium (w/ Nmap)
Angry IP	Yes	Low
OpenVAS	Yes	Very High

In this context, the depth of analysis varies across tools, depending on their scope and capabilities. The Complete level includes the detection of ports, services, versions, and operating systems, as well as automation capabilities that enhance flexibility and detail during network assessments. The Very High level encompasses the detection of ports and services, while also performing authenticated scans, known vulnerability assessments based on CVE databases, and the generation of comprehensive security reports. At the Medium level, tools are limited to identifying open ports but may integrate with other solutions or provide additional modules for a more detailed analysis. Finally, the Low level of analysis refers to tools that solely identify open ports without offering deeper insights into services or existing vulnerabilities.

The technical characteristics of the analyzed tools highlight their different approaches and intended purposes. Nmap stands out for its detailed fingerprinting capabilities, execution of NSE scripts, and comprehensive service and operating system analysis. Masscan, in contrast, performs pure TCP scans focused on performance and allows exporting results in a format compatible with Nmap. ZMap adopts a statistical methodology for TCP scanning, primarily aimed at academic applications and large-scale internet research. RustScan combines multi-threading implemented in Rust with direct integration into Nmap, offering both speed and analytical depth. Angry IP Scanner prioritizes simplicity, featuring an intuitive graphical interface and support for exporting results in CSV and TXT formats. Finally, OpenVAS provides the most complete feature set, including authenticated scans, CVE-based vulnerability analysis, and the generation of detailed security reports.

V. Results Discussion

When comparing the tools, there isn't one tool that can do everything well at the same time. No single tool can be fast, detailed, and easy to use for network scanning and checking for weaknesses. Each tool has its own strengths and is better suited for certain scenarios.

Nmap is the most popular and flexible tool, especially for experienced users. It can check ports, services, operating systems, and run custom scripts, making it a key tool for complete technical checks. However, for big networks, tools like Masscan and ZMap perform better. These tools can quickly scan large groups of IP addresses, but they only check ports, so other tools are needed to get more detailed information.

RustScan is a good choice for teams that want both speed and detailed analysis. It can be used with Nmap for more in-depth checks after the initial scan, making it a smart combination for regular network scans in companies.

Angry IP Scanner, while not as powerful, works well for small networks and for people who aren't experts. Its simple interface makes it easy to use, but it's not good for complex tasks.

OpenVAS is great for professional use. It can do deep scans, check for known vulnerabilities, and help with security and compliance. But it takes longer to run and needs more computational resources. It's also tricky to set up, so it's best used for planned audits or as part of a bigger security plan.

This study's findings support these ideas, indicating that choosing the best tool depends on the specific technical scenario, the amount of time you have, and how detailed the scan needs to be. It's also important to think about things like how easy the tool is to learn, how well it works with other systems, and how much technical skill the team has when deciding on the most effective set of tools. A table suggesting possible uses for the tools is presented in Table II.

VI. Conclusions

The study made it possible to analyze and compare six network scanning and vulnerability detection tools: Nmap, Masscan, ZMap, RustScan, Angry IP Scanner, and OpenVAS. Each of them presented distinct characteristics regarding speed, depth of analysis, complexity of use, and practical applicability.

TABLE II
Practical Applications

Scenario	Recommended tool
Rapid mapping of large networks	Masscan or ZMap
Detailed service detection	Nmap or RustScan
Use by beginners with graphical interface	Angry IP Scanner.
Compliance and vulnerability audits	OpenVAS

Nmap has confirmed its position as the industry standard solution for detailed network inspections, benefiting from NSE script support and the broad user base and documentation [1]. However, its speed limitation in extensive networks reinforces the need for complementary tools.

In this sense, Masscan and ZMap stood out as ultra-fast solutions for scanning open ports, being suitable for the initial recognition of large networks [2], [3]. However, the absence of service detection limits their isolated application.

RustScan, by combining high performance with Nmap integration, represents a modern and efficient option for rapid inspections followed by in-depth analysis [4]. Tools such as Angry IP Scanner, in turn, are recommended only for novice users and small networks due to their limited functionality [5].

Finally, OpenVAS proved essential in formalized security audits, with the ability to detect CVE-based vulnerabilities and CVSS classification, authenticated scanning, and technical reporting [6], [7].

Therefore, the combined use of these solutions is recommended, adapting their application according to the objectives of the security assessment. Specialized performance tools should be used in the initial recognition, while solutions such as Nmap and OpenVAS should compose the most analytical and documentary stages of the process.

The results corroborate the methodological guidelines of [8], emphasizing the importance of systematizing technical knowledge for strategic decision-making in information security.

As future work, it is suggested to expand the practical analysis in productive environments and investigate the impact of the constant updating of vulnerability databases (CVEs) on the effectiveness of the evaluated tools.

References

[1] G. Lyon. (2024) The network mapper. [Online]. Available: https://nmap.org/

[2] R. D. Graham. (2024) (masscan: Mass ip port scanner. [Online]. Available: https://github.com/robertdavidgraham/masscan

[3] J. A. Durumeric Z. Wustrow, E. Halderman. (2024) The zmap project. [Online]. Available: https://zmap.io/

[4] A. Skerritt. (2024) The modern port scanner. [Online]. Available: https://github.com/bee-san/RustScan

[5] A. Keks. (2024) Angry ip scanner fast and friendly network scanner. [Online]. Available: https://angryip.org/

[6] G. Group. (2024) Openvas scan — vulnerability management for enterprises public sector organizations - greenbone. [Online]. Available: https://www.greenbone.net/en/openvas-scan/

[7] H. Poston. (2024) A brief introduction to the openvas vulnerability scanner. [Online]. Available: https://www.infosecinstitute.com/resources/penetration-testing/a-brief-introduction-to-the-openvas-vulnerability-scanner/

[8] M. C. B. Galvão and I. L. M. Ricarte, “Revisão sistemática da literatura: conceituação, produção e publicação,” *Logeion: Filosofia da informação*, vol. 6, no. 1, pp. 57–73, 2019.