NETWORK MONITORING TOOLS: A COMPREHENSIVE STUDY

VARSHA V.G[1] , DR. PRINCY ANN THOMAS[2]

[1] *Student, Computer Science and Engineering, Government Engineering College Thrissur, Kerala, India*
[2] *Assistant Professor, Computer Science and Engineering, Government Engineering College Thrissur, Kerala, India*

ABSTRACT

In today's dynamic and interconnected digital environment, effective network monitoring is critical for maintaining cybersecurity and optimizing network performance. As organizations face increasingly sophisticated threats and ever-growing volumes of network traffic, selecting the right network monitoring tool becomes paramount. This comparative analysis aims to provide an in-depth assessment of prominent network monitoring tools:Wireshark,Tshark,Snort, and Suricata. By evaluating these tools across key metrics such as functionalities, ease of use, scalability, and customization options, the study offers valuable insights to help network administrators and organizations make informed decisions regarding their network monitoring strategies. Leveraging existing literature, user feedback, and real-world case studies, this project presents a comprehensive overview of each tool's strengths, weaknesses, and suitability for different network monitoring scenarios.

Keyword : - *Network monitoring tools , Security capabilities, Network security enhancement*

1. INTRODUCTION

In an era marked by the relentless growth of digital connectivity and the proliferation of network-enabled devices, the importance of robust network monitoring cannot be overstated. From safeguarding sensitive data to ensuring uninterrupted service delivery, effective network monitoring forms the backbone of modern cybersecurity and operational resilience efforts.However, amidst the vast array of network monitoring tools available in the market, selecting the most suitable solution for a particular organizational context can be a daunting task. Recognizing this challenge, this report embarks on a comprehensive comparative analysis of four leading network monitoring tools: Wireshark,Tshark,Snort,andSuricata.

The rationale behind this comparative analysis lies in the need to provide network administrators and organizations with actionable insights into the strengths and limitations of each tool, thereby facilitating informed decision-making in tool selection. By meticulously evaluating Wireshark, Tshark, Snort, and Suricata across a range of critical metrics including functionalities, ease of use, scalability, and customization options this study aims to shed light on which tool best aligns with specific network monitoring requirements.

Drawing upon a diverse range of sources, including academic research, industry reports, user reviews, and real-world case studies, this study endeavors to offer a nuanced understanding of each tool's performance and applicability in varied network monitoring scenarios. Through this endeavor, we seek to empower network administrators and organizations with the knowledge needed to navigate the complex landscape of network monitoring tools effectively, ultimately enhancing their ability to safeguard their networks and achieve operational excellence in an ever-evolving digital landscape.

2. PROPOSED SYSTEM DESIGN: A FRAMEWORK FOR ENHANCED NETWORK SECURITY

Amidst the rapid evolution of network threats and the increasing complexity of modern network infrastructures,there exists a need to enhance security measures and adaptability in safeguarding against cyber threats. Recognizing the existing research gaps in addressing these challenges, this study proposes a comparative analysis of leading network monitoring tools. Focusing on two critical aspects of security for modern networks and adaptability to changing threat landscapes, the study aims to provide valuable insights into the effectiveness of these tools in mitigating network security risks.

Within this context, the study will delve into an exhaustive examination of prominent network monitoring tools, including Wireshark, Snort, Tshark, and Suricata. By scrutinizing these tools against key metrics such as functionality, scalability, ease of use, and customization,tailored specific threat scenarios,the study seeks to identify the optimal solution for strengthening network security defenses.

Through meticulous analysis and comparison, the study endeavors to fill existing research gaps and provide actionable recommendations for network administrators and organizations seeking to fortify their cyber security posture.By shedding light on the strengths and weaknesses of each tool in addressing diverse network security challenges, this research aims to empower stakeholders with the knowledge needed to navigate the complex landscape of network security tools effectively.

2.1 The Proposed Model

In the ever-evolving landscape of cybersecurity, effective network monitoring plays a pivotal role in safeguarding digital assets against a myriad of threats. However, the selection of an appropriate network monitoring tool poses a significant challenge for organizations, given the multitude of options available in the market. To address this challenge and bridge existing research gaps, this project proposes a comprehensive comparative analysis of leading network monitoring tools. By systematically evaluating these tools across key metrics and criteria, the study aims to provide actionable insights for network administrators and organizations striving to strengthen their cybersecurity defense.

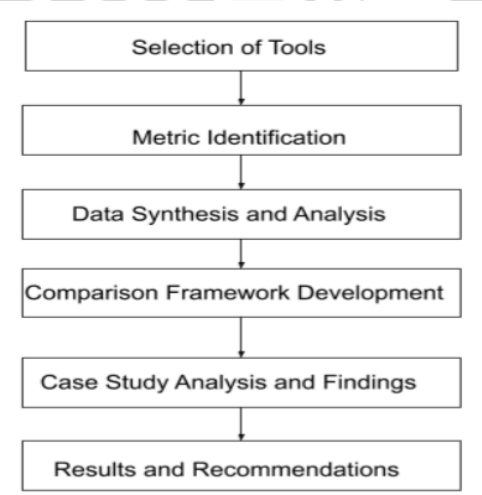

Fig -1: Proposed Model Architecture

2.2 Selection of Network Monitoring Tools

The first step in the proposed model involves the careful selection of network monitoring tools to be evaluated. Notable tools such as Wireshark, Snort,Tshark, and Suricata are chosen based on their prevalence, popularity, and significance in the field of network security. These tools represent a diverse range of functionalities and capabilities, ensuring a comprehensive evaluation of the network monitoring landscape.

- Wireshark
  Wireshark is a widely-used network protocol analyzer known for its comprehensive packet capturing capabilities and extensive protocol support. Its user-friendly interface and rich feature set make it a popular choice among network administrators for network traffic analysis.
- Tshark
  Tshark is the command-line version of Wireshark, offering similar packet capturing and analysis capabilities in a command-line interface. It provides flexibility for advanced users and automation of network monitoring tasks through scripting and command-line usage.
- Snort
  Snort is an open-source intrusion detection system renowned for its signature-based detection, protocol analysis, and rule-based alerts. It offers robust security capabilities and customizable rule sets, making it suitable for detecting and mitigating various security threats real-time.
- Suricata
  Suricata is an open-source intrusion detection and prevention system known for its high performance, scalability, and multi-threaded rule matching capabilities. It offers extensive protocol support, file extraction, and flow logging features, making it suitable for large-scale network environments.

2.3 Metric Identification

Following the selection of tools, the study proceeds to identify key metrics and criteria for evaluation. Metrics such as functionality, scalability, ease of use, and customization options are identified as pivotal factors in assessing the effectiveness of network monitoring tools. These metrics serve as the foundation for comparing the performance of each tool and determining their suitability for different security scenarios.

2.4 Data Synthesis and Analysis

With the metrics identified, the study gathers data from various sources, including research papers, articles, user reviews, and case studies. This data is synthesized and analyzed to gain insights into the performance of each tool across the defined metrics. By examining real-world use cases and scenarios, the study supplements its analysis with practical insights into the effectiveness of each tool in addressing specific security challenges

2.5 Comparison Framework Development

Based on the analysis of gathered data, a structured framework for comparative analysis is developed. This framework delineates the methodology for evaluating each tool and serves as a guide for comparing their performance against the identified metrics.

- Functionality Comparison: The functionality of each tool is compared based on its packet capturing capabilities, protocol support, analysis features, and reporting functionalities. Insights are drawn regarding the tool's effectiveness in monitoring and analyzing network traffic, detecting security threats, and generating actionable insights.
- Scalability Assessment: The scalability of each tool is assessed by evaluating its capacity to handle increasing network traffic and data volume without compromising performance. Factors such as resource utilization, support for distributed deployment, and scalability options are compared to determine the tool's suitability for deployment in large-scale network environments.
- Ease of Use Analysis: Usability is compared by examining the user interface, navigation, documentation, and learning curve of each tool. A user-friendly interface, intuitive navigation, comprehensive documentation, and minimal learning curve are considered indicative of the tool's ease of use and accessibility to network administrators.
- Customization Review: Customization options are compared based on each tool's support for custom rules, plugin architecture,and integration with third-party systems. The flexibility to tailor the tool to specific

security requirements and operational needs is compared to assess its adaptability to changing security landscapes and unique network monitoring challenges.

2.5 Case Study Analysis and Findings

Real-world case studies and scenarios are analyzed to supplement the comparative analysis. The findings from case studies provide practical insights into the effectiveness of each tool in addressing specific security challenges and use cases.

2.5 Results and Recommendations

The results of the comparative analysis represented, highlighting the strengths and weaknesses of each tool across the defined metrics. Based on these results, actionable recommendations are provided for network administrators and organizations seeking to enhance their cybersecurity defenses.

3. COMPARATIVE ANALYSIS OF NETWORK MONITORING TOOLS AND RESULTS

This comparative study delves into four prominent network monitoring tools: Wireshark, Snort, Suricata, and Tshark. By evaluating their functionalities,ease of use, scalability, and real-world case studies, the project aims to offer valuable insights to network professionals. Through an analysis of user reviews, it provides first hand perspectives on these tools. The results aim to guide organizations in optimizing network monitoring and enhancing cybersecurity defenses.

3.1 Wireshark

Wireshark's extensive documentation and active user community significantly contribute to its usability, providing valuable resources and support for users of all proficiency levels. However, it's worth noting that while highly effective for analyzing network traffic in smaller or medium-sized environments, Wireshark's scalability may encounter limitations in larger networks or high-traffic scenarios due to resource constraints like memory and processing power. Nevertheless, Wireshark does offer customization options through scripting and filtering features, enabling users to automate tasks and tailor analysis workflows. User reviews on TrustRadius.com generally express a positive sentiment towards Wireshark, highlighting its comprehensive features for network analysis and troubleshooting, which solidifies its position as a preferred choice among network administrators and security professionals.

3.2 Tshark

Tshark serves as the command-line counterpart to Wireshark, offering comparable packet capturing and analysis capabilities within a terminal environment. Its functionality extends to capturing, dissecting, and analyzing network traffic directly from the command line, rendering it suitable for automated or scripted analysis tasks. Despite lacking the graphical interface of Wireshark, Tshark provides robust command-line capabilities adept for experienced users or automated workflows. However, transitioning from graphical interfaces to Tshark's text-based output may entail a learning curve for users unaccustomed to command-line interfaces. In terms of scalability, Tshark demonstrates high scalability owing to its command-line interface and efficient packet processing, making it proficient in handling large volumes of network traffic effectively. Its lightweight footprint and minimal resource requirements ensure optimal performance, even in high-traffic environments, thus catering to both small-scale troubleshooting tasks and enterprise-level network analysis. Furthermore, Tshark offers extensive customization options through command-line parameters and scripting capabilities, enabling users to specify filters, output formats, and analysis options directly from the command line. This feature facilitates tailored packet analysis workflows, augmented by Tshark's integration with scripting languages like Python for advanced automation and customization of analysis tasks. User reviews of Tshark underscore its functionality for packet analysis and troubleshooting, with its efficiency, scalability, and customization options contributing to positive user experiences, particularly among those comfortable with command-line interfaces.

3.3 Snort

Snort is primarily engineered for intrusion detection and prevention, emphasizing signature-based detection and rule-based alerts. It conducts real-time analysis of network traffic by scrutinizing packet contents against predefined rules to pinpoint potentially malicious activity. Supporting a wide spectrum of protocols, Snort furnishes detailed logging and alerting features to promptly notify administrators of detected threats. Despite its proficiency, Snort's command-line interface and configuration-based setup may pose a learning curve for users unaccustomed to network security

tools. However, once configured, Snort demonstrates efficient intrusion detection capabilities, furnishing effective protection against network threats. Concerning scalability, while Snort manages moderate network traffic volumes capably, limitations arise in high-speed or heavy traffic conditions due to its single-threaded operation and resource requirements. Efforts to improve scalability through distributed analysis may alleviate these constraints partially. Moreover, Snort offers extensive customization avenues through rule management and configuration settings, empowering users to tailor custom rule sets aligned with their organization's specific security requirements. Additionally, Snort's support for plugins and extensions facilitates further customization and integration with other security tools and systems. User reviews typically convey positive sentiments toward Snort, commending its effectiveness in network intrusion prevention and detection. The active community support and availability of rule sets garner appreciation, fostering effective threat detection and response strategies among users.

3.4 Suricata

Suricata offers advanced packet capturing and analysis capabilities than Wireshark, with a primary focus on intrusion detection and prevention. Utilizing multi-threaded rule matching and flow logging, it efficiently scrutinizes network traffic in real-time. Suricata's support for protocol decoding, file extraction, and signature-based detection renders it a comprehensive solution for network security. Similar to Snort, Suricata's setup and configuration demand technical expertise, necessitating users to grasp the tool's configuration options and rule management for effective intrusion detection deployment. Nonetheless, extensive documentation and community support provided by Suricata assist users in setting up and optimizing their security policies. Designed to be highly scalable, Suricata can adeptly manage large volumes of network traffic. Its multi-threaded architecture and optimized processing algorithms allow it to horizontally scale across multiple CPU cores, making it suitable for environments with high-speed or heavy traffic conditions. Suricata's scalability ensures effective threat detection and response across diverse network environments. Offering extensive customization capabilities through various management and configuration options, Suricata empowers users to create custom rule sets tailored to their organization's security requirements. Additionally, its support for plugins and extensions facilitates seamless integration with other security tools and systems, augmenting its flexibility and functionality. User sentiment towards Suricata, akin to comparable tools like Snort, suggests appreciation for its effectiveness and scalability in network security. Suricata's advanced features and community support likely contribute to positive user experiences, positioning it as a preferred choice for organizations seeking robust intrusion detection capabilities.

4. STRATEGIES FOR ENHANCED PERFORMANCE

The strategies provided aim to enhance the performance, usability, and effectiveness of Wireshark, Snort, Suricata, and Tshark in network analysis and security. Informed by an assessment of each tool's current capabilities and user feedback, these recommendations prioritize scalability enhancements, simplification of rule management, strengthening integration capabilities, and optimizing performance. Wireshark would benefit from scalability improvements and integration with cloud environments, alongside advanced filtering options and analysis features. Tshark could improve through expanded documentation, integration with other tools, and a graphical interface option. For Snort, scalability improvements and enhanced integration with SIEM solutions are crucial, along with simplified rule management. Suricata could enhance usability, performance, and integration with threat intelligence feeds. These recommendations aim to empower users in conducting efficient and comprehensive network analysis, thereby strengthening network security posture.

5. CONCLUSIONS

In the realm of network monitoring tools, conducting a comparative study of Wireshark, Snort, Suricata, and Tshark Has Provided Valuable Insights into their respective capabilities, strengths, and areas for improvement. The objective was to evaluate these tools comprehensively to evaluate security capabilities, assess adaptability, identify best practices, and thus enhance network security. Wireshark, renowned for its versatility and feature-rich interface, stands as a reliable tool in the field of network protocol analysis. Despite its widespread adoption, the study highlights the need for enhancements in scalability and integration with cloud environments to accommodate the evolving landscape of network architectures. Tshark, with its formidable command-line interface and advanced packet analysis capabilities, offers a compelling option for network analysts. Nonetheless, improvements in documentation and

usability are imperative to broaden its adoption and facilitate seamless integration with other analysis tools. Snort, recognized for its expertness in intrusion prevention and detection, enjoys a robust user community and real-world success stories. However, the analysis underscores the importance of scalability enhancements and streamlined rule management processes to support its effectiveness in enterprise settings. Suricata, applauded for its detection capabilities and community engagement, exhibits promise as a formidable network monitoring tool. Yet, opportunities for usability improvements and stronger integration with threat intelligence feeds can further enhance its efficacy in mitigating emerging threats.

It is evident that each tool has its unique strengths and areas for improvement. By incorporating the recommendations outlined in this study, organizations can optimize their network monitoring and security operations, improving their defenses against evolving cyber threats. Continuous collaboration, training, and engagement with the user community will help in maximizing the full potential of these tools and staying ahead in the dynamic landscape of network security.

6. REFERENCES

[1].M.Fuentes-García,J.Camacho,andG.Maciá Fernández,"Present And Future Of network security monitoring,"IEEEAccess,vol.9,pp.112744–112760,2021

[2]. I. Ghafir, V . Prenosil, J. Svoboda, and M. Hammoudeh, "A survey on network security monitoring systems," in 2016 IEEE 4th International Conference on Future Internet of ThingsandCloudWorkshops(FiCloudW), pp.77–82,IEEE,2016.

[3]. D. Goli, H. Al-Mohannadi, and M. Shah, "Plan, prepare and respond: A holistic cybersecurity risk management platform,"in202310thInternational Conference on Future Internet of Things and Cloud (FiCloud),pp.367–374, IEEE,2023

[4]. J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L.Galletta,andR.DeNicola, "Framework, tools and good practices for cybersecurity curricula," IEEE Access,vol.9,pp.94723–94747,2021

[5]. N. Tatipatri and S. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis,detection and cybersecurity,"IEEEAccess, 2024.

[6]. H. Li and S. Yoo, "Information systems sourcing strategies and organizational cybersecurity breaches," IEEE Transactions on Engineering Management,vol.71,pp.481–490,2021.

[7].M. V . Chester and B. R. Allenby, "Perspective: the cyber frontier and infrastructure,"IEEEAccess,vol.8,pp.28301–28310,2020.

[8].D. Ghelani, "Cyber security, cyber threats, implications and future perspectives:A Review,"AuthoreaPreprints,2022.

[9]. H. Alamro, W. Mtouaa, S. Aljameel, A. S. Salama, M. A. Hamza,andA.Y . Othman, "Automated android malware detection using optimal ensemble learning approach for cybersecurity,"IEEEAccess,2023.

[10]. R. Pasupuleti, R. Vadapalli, and C. Mader, "Cyber security issues and challenges related to generative ai and chatgpt," in 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS),pp.1–5,IEEE,2023.

[11]. Y . Li and Q. Liu, "Acomprehensivereviewstudyofcyber-attacksandcyber security; emerging trends and recent developments," Energy Reports,vol.7, pp.8176–8186,2021.

[12]. M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S.Mahmood,"Cyber security threats and vulnerabilities: a systematic mapping study," Arabian JournalforScienceandEngineering,vol.45,pp.3171–3189,2020

[13]. P. Saxena and S. K. Sharma, "Analysis of network traffic by using packet sniffing tool: Wireshark," International Journal of Advance Research, Ideas and Innovations inTechnology,vol.3,no.6,pp.804–808,2017.

[14]. G. Kurundkar, N. Naik, and S. Khamitkar, "Network intrusion detection using snort," International Journal of Engineering Research and Applications,vol.2,no.2,pp.1288–1296,2012.

[15]. I. Karim, Q.-T. Vien, T. A. Le, and G. Mapp, "A comparative experimental design and performance analysis snort-based intrusion detection system in practical computer networks,"Computers,vol.6,no.1,p.6,2017.

[16]. B. R. Murphy, Comparing the performance of intrusion detection systems: Snort and Suricata.PhDthesis,ColoradoTechnicalUniversity,2019.

[17]. N.Granberg,"Evaluating The Effectiveness Of Free Rulesets For Snort,"2022.

[18]. E. Albin and N. C. Rowe, "A realistic experimental comparison of the suricata and snort intrusion detection systems," in 2012 26th International Conference on Advanced Information Networking and Applications Workshops,pp.122–127,IEEE,2012.

[19]. R. Bonnerji, An approach to enhance low-interaction honeypots by enabling them to detect spoofing attacks via network analysis. PhD thesis, Dublin, NationalCollegeofIreland,2020.
[20]. A. Shah, "Evaluating network forensics applying advanced tools," International Journal of Advanced Engineering, Management and Science, vol.9,p.4,2023.
[21]. U.Banerjee,A.Vashishtha,andM.Saxena,"Evaluation Of Withcapabilities wireshark as a tool for intrusion detection,"InternationalJournalofcomputer applications,vol.6,no.7,pp.1–5,2010.
[22]. https://www.researchgate.net/publication/347554046_An_IDS_Rule_Redund ancy_Verification
[23]. https://www.trustradius.com/products/wireshark/reviews?qs=product-usage# overview
[24]. https://www.packetsafari.com/blog/2022/11/10/wifi-traffic-analysis-wireshar k/
[25]. https://www.wireshark.org/docs/man-pages/tshark.html
[26]. https://www.g2.com/products/snort/reviews
[27].https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/suricata/product/suricata-open-source