Global Scientific JOURNALS

GSJ: Volume 11, Issue 8, August 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

An In-Depth Comparative Analysis and Evaluation of Snort and Suricata IDS/IPS Functionality in pfSense

Shah Zaib

Department of Computer Science & Information Technology, University of Engineering & Technology Peshawar, Pakistan
E-mail: kingxaib@gmail.com

ABSTRACT

As cyber-attacks become more frequent and complicated, having strong network security solutions is essential. The main components of good security are firewalls and intrusion detection systems (IDS). Firewalls protect the network by acting as barriers between internal and external connections. IDS systems closely monitor network traffic and promptly alert administrators if they detect anything suspicious. This study examines two widely used open-source IDS systems, Suricata and Snort, in conjunction with the pfSense firewall. We aim to understand their accuracy, speed, and memory requirements. The results show that Suricata is better at handling large amounts of network traffic while maintaining accuracy. Additionally, the research helps us comprehend how Suricata and Snort function, leading to potential improvements in network security. With this research, network administrators can compare Suricata and Snort to select the best IDS system for their security needs. The study also proposes a cost-effective approach to enhance enterprise network security, reducing the risk of cyber-attacks. In conclusion, this evaluation equips organizations with the knowledge and tools they need to safeguard their networks from security breaches. It promotes a safer cyber environment and protects critical data from cybercriminals.

Keywords: Cyber-attacks, Network security, Firewalls, Intrusion Detection Systems (IDS), Suricata, Snort, pfSense firewall.

INTRODUCTION

In today's interconnected digital landscape, computer security faces an ever-increasing and concerning threat - unauthorized access to computer systems. As the use of network applications continues to grow exponentially, new and sophisticated network attacks emerge, posing serious risks to organizations and individuals alike. In this context, safeguarding information, which serves as the backbone of any organization, becomes paramount [1]. The protection of computer systems, operating procedures, and internal controls is crucial to preserve the integrity and confidentiality of sensitive data.

The realm of information security extends beyond mere data protection; it encompasses ensuring the secure operation of applications, responsible data collection and usage, safeguarding technology assets, and ensuring the seamless functioning of organizations. As information becomes more valuable than ever, the installation of suitable application software, including robust antivirus programs, becomes indispensable to protect data assets and fortify the supporting computers.

The importance of safeguarding organizational data cannot be overstated, as leaving it unprotected can lead to severe consequences if it falls into the wrong hands. Effective information security measures, therefore, serve as a critical defense against data breaches, privacy violations, and identity theft, especially in businesses where information serves as a crucial driver of operations and growth.

The ever-expanding interconnectivity of business environments brings with it a wide range of threats, from computer hacking to Distributed Denial of Service (DDoS) attacks and the execution of malicious codes. In response, organizations must adopt robust information security systems to protect their valuable technology assets.

Establishing information security is a collaborative effort, involving both general management and IT personnel. Preserving the confidentiality of information stands as a fundamental pillar for the seamless operation of any organization. As a result, organizations must prioritize secure data storage and management to ensure their success.

The significance of information security awareness rose significantly following the infamous Morris Worm attack in 1988 [2]. This incident highlighted the pressing need for proactive measures to defend against viruses, worms, and other malicious software, reinforcing the importance of a strong information security framework.

As per the report [3][4] the year 2022 was marked by a surge in major cyber-attacks and data breaches, affecting countries, corporations, and individuals globally. These incidents served as wake-up calls for many organizations, underscoring the necessity for heightened protection measures and robust incident response strategies. The escalating threat landscape has led to an increase in demand for cyber security insurance and intensified the focus on strengthening information security measures.

To establish a comprehensive defense-in-depth

approach to network security monitoring, intrusion detection and prevention technologies play a pivotal role. Intrusion Detection Systems (IDS) emerge as a critical element, continuously monitoring network data to detect and alert on suspicious or malicious activities. Given the mounting security incidents, the role and significance of IDS have grown exponentially in recent years. As a result, many organizations have developed their own security applications, both free and paid, to enhance the effectiveness of IDS. Open-source IDS applications have become particularly popular due to their adaptability and customizability, offering organizations greater flexibility for integration with other security tools, such as firewalls and access controls. The seamless integration of IDS with additional security measures empowers organizations to promptly detect and respond to security incidents, bolstering overall incident response readiness.

Amid the rapid advancement of technology and cyber threats, ensuring robust information security remains an ongoing endeavor, calling for continual improvements and adaptations. This research aims to contribute to the broader field of information security by evaluating two well-known open-source IDS/IPS, Snort and Suricata, within the pfSense firewall environment. By assessing their performance, memory requirements, and detection capabilities, we aim to provide insights into the most effective intrusion detection system and explore the potential of PFSense as a cost-effective alternative to paid firewalls. Through this research, we seek to contribute to the fortification of enterprise network security and promote a safer digital landscape for organizations worldwide.

BACKGROUND

Intrusion Detection/Prevention System (IDS/IPS):

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can be categorized into signature-based and anomaly-based detection methods. Signature-based systems rely on predefined patterns or signatures to identify known threats, while anomaly-based systems detect deviations from established network behavior, signaling potential security breaches. As cyber threats continue to evolve, attackers employ increasingly sophisticated techniques to breach network security. The dynamic nature of these threats necessitates a comprehensive and adaptable approach to intrusion detection and prevention.

pfSense:

pfSense [5] is an open-source network firewall and router solution based on the FreeBSD operating system. Its open-source nature allows for continual development, community contributions, and frequent updates, making it a reliable and cost-effective security solution. pfSense offers Unified Threat Management capabilities, which consolidate various security features, such as firewall, VPN, antivirus, and web filtering, into a single platform. This integration streamlines network security management and enhances overall protection.

The flexibility and customizability of pfSense enable organizations to tailor the system to their specific security needs. With support for third-party packages, pfSense can be extended to include additional security tools and features.

Suricata:

Suricata [6], developed by the Open Information Security Foundation (OISF), is touted as a next-generation IDS/IPS. It is designed to address the evolving threat landscape and provide advanced features to combat sophisticated attacks effectively. Suricata's integration with a Hyper Text Transfer Protocol (HTTP) normalizer enhances its security-awareness capabilities. By analyzing HTTP traffic and detecting evasion techniques used by attackers, Suricata strengthens its ability to protect against web-based threats.

Snort:

Snort [7], introduced by Sourcefire in 1998, is one of the pioneering signature-based Network Intrusion Detection Systems (NIDS). Its ability to monitor network data at the application layer and detect a wide range of attacks has solidified its position as a respected security solution. Snort's modular design allows security professionals to customize and extend its intrusion detection capabilities. This adaptability has contributed to its continued popularity and relevance in the ever-changing threat landscape.

LITERATURE REVIEW

PFSense is a widely recognized open-source network firewall distribution built on the FreeBSD Operating System. It offers the flexibility of installation as a standalone firewall or in a Virtual Machine, with the added benefit of supporting 3rd party packages like Intrusion Detection Systems (IDS), monitoring tools, and VPNs, expanding its functionalities [7].

Studies comparing Snort and Suricata have evaluated their performance and detection capabilities.

Shimel's work [8] highlights Suricata's multi-threaded engine, providing better signature detection and fragmented processing decisions, crucial for handling the increasing network bandwidth predicted by Nielsen's Law [9]. Moore's Law [10], predicting computational speed improvements, favors multi-threading, which Suricata leverages to enhance performance [11].

The authors in [12] conducted a comprehensive literature review on Next-Generation Firewalls (NGFWs) effectiveness in mitigating internal network attacks. Focusing on PFSense NGFW, the review identified gaps and limitations, which led to the current study. Smith tested various attack scenarios on a company network, revealing PFSense NGFW's significant capabilities in improving network security beyond traditional firewalls.

Another review [13] explored the efficiency of IDS, firewalls, and packet analysis in network security. Introducing an innovative open-source model integrating security monitoring, intrusion detection and prevention, firewall services, and packet analysis, the model demonstrated robust attack detection and visualization capabilities. Snort emerged as the preferred IDS software choice due to its reliability and compatibility.

Studies comparing Snort and Suricata's performance [14], [15], [16], [17], [18] identified their strengths and weaknesses. Snort was found to be more resource-efficient in single-core environments, while Suricata excelled in multi-CPU setups and handling larger network data flows.

Suricata's performance was enhanced by enabling hyper-threading and running in specific modes [16]. However, both systems showed similar numbers of False-Positives and False-Negatives [17].

Boštjan [19] evaluated Snort and Suricata's security and performance on Windows and Linux. Suricata showed higher resource utilization but performed well in handling packet drops during simulated attacks. Both systems displayed an equal number of False-Positives and False-Negatives. Linux-based systems were deemed more suitable for deployment due to their efficient handling of resource-intensive tasks.

These literature reviews provide valuable insights into the capabilities and limitations of PFSense, Snort, and Suricata, highlighting their significance in enhancing network security and their performance under different scenarios.

RESEARCH METHODOLOGY

Literature Review

This step involves conducting a comprehensive review and analysis of existing literature, scholarly articles, books, and relevant sources related to the research topic. The goal is to understand the current state of knowledge, identify key concepts, methodologies, and research gaps in the field of IDS/IPS within the context of the research.

Analysis of IDS/IPS

In this step, the focus is on analyzing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The analysis includes studying various types of IDS/IPS, their underlying principles, architectures, detection algorithms, and their effectiveness in different scenarios. The aim is to assess the strengths and weaknesses of these security mechanisms and understand how they contribute to network protection.

Execution of Experiments

This phase involves designing and conducting controlled experiments to evaluate the performance, effectiveness, and efficiency of the IDS/IPS systems under different conditions. A test environment is set up, various network configurations are created, and attack scenarios are simulated. The behavior and response of the IDS/IPS systems are closely monitored, and data is collected to assess their performance.

Analysis of Results

After conducting the experiments, the collected data and results are analyzed to draw meaningful conclusions. The goal is to examine the experimental findings, validate or challenge hypotheses, and gain insights into the effectiveness of the IDS/IPS systems. Statistical analysis techniques may be used to identify patterns and significant findings in the data. The analysis of results aims to provide valuable insights and contribute to the overall understanding of the research topic.

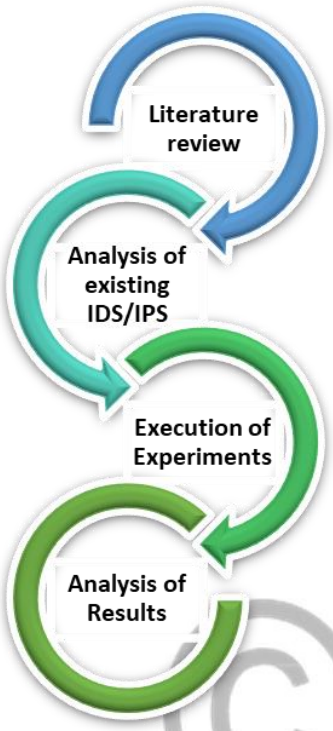

Figure 1: Research Methodology Flow

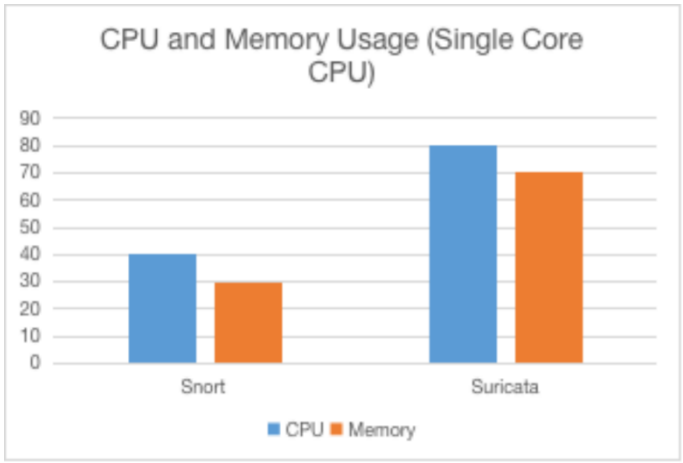

Figure 2: CPU and Memory Comparison (Single Core)

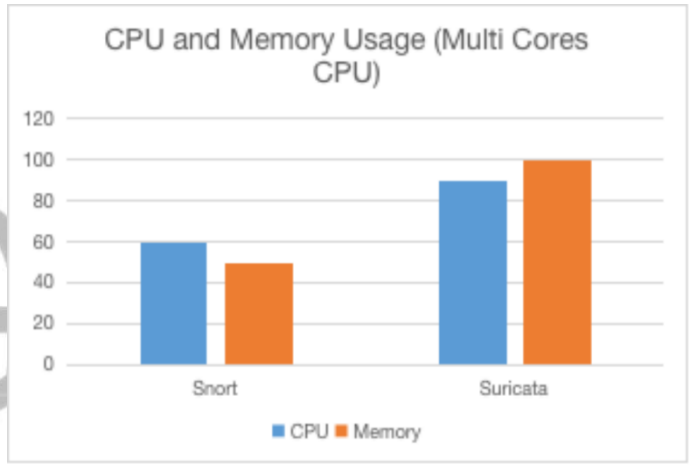

Figure 3: CPU and Memory Comparison (Multi-Cores)

RESULTS

The evaluation of CPU and Memory usage revealed that Snort reached its full potential but lacked support for multi-threaded CPUs, whereas Suricata adapted effectively to a multi-core environment, optimally utilizing available resources.

Figure 7.1 depicts the CPU and Memory comparison for both IDSs in a single-core CPU environment, while Figure 7.2 shows the comparison in a multi-core CPU environment

CONCLUSION

In this in-depth analysis, we evaluated the performance of two widely used open-source Intrusion Detection Systems (IDS), Suricata and Snort, within the pfSense firewall environment. Suricata stood out for its efficient handling of large network traffic volumes while maintaining high precision, due to its multi-threaded processing capabilities. However, it came with higher memory usage and network overheads. On the other hand, Snort proved lightweight with low CPU utilization and low packet loss..

Both systems showed instances of false positives and false negatives, but Snort performed better in detection

due to its efficient algorithm. Suricata demonstrated scalability in handling high network traffic, making it suitable for demanding scenarios. The findings from this analysis offer valuable guidance to network administrators, empowering them to make well-informed decisions when choosing an IDS system that suits their specific security requirements. These insights significantly contribute to enhancing the effectiveness of defense mechanisms against ever-evolving cyber threats.

REFERENCES

[1] Aumreesh Ku. Saxena et al., (2017). General study of intrusion detection system and survey of "agent-based intrusion detection system"

[2] Cara Giamo. (2015) from https://www.atlasobscura.com/articles/in-1988-one-rogue-worm-shut-down-10-percent-of-the-internet

[3] 2022 In Review: An Eventful Cybersecurity Year Link: https://www.forbes.com/sites/emilsayegh/2022/12/13/2022-in-review-an-eventful-cybersecurity-year/?sh=22ffa0dc352f

[4] The biggest data breaches and leaks of 2022. Article Link: https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022

[5] PFSense download Link: https://www.PFSense.org/

[6] Suricata: https://suricata.io/download/

[7] Snort: https://www.snort.org/downloads

[8] Shimel, A. (2010). Is this town big enough for two IDS? Message posted to www.networkworld.com/community/node/67435

[9] Nielsen, J. (2010). Nielsen's Law of Internet bandwidth. Retrieved 18/10/2020, from www.useit.com/alertbox/980405.html

[10] Moore, G. (1965). Cramming more components onto integrated circuits. Electronics, 38(8).

[11] Open Information Security Foundation (OISF). (2010). Suricata IDS (1.1 Beta2 ed.) Link https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Runmodes

[12] Alhasan, A.J. and Surantha, N., 2021. Evaluation of Data Center Network Security based on Next-Generation Firewall. International Journal of Advanced Computer Science and Applications, 12(9).

[13] Al-Qassim, M.A. and Al-Hemiary, E.H., 2018. Network Perimeter Defenses Using Open-Source Software. Iraqi Journal of Information and Communication Technology, 1(2), pp.41-51.

[14] Open Information Security Foundation (OISF). (2011a). Open information security foundation (OISF) from www.openinfosecfoundation.org

[15] Day, D., & Burns, B. (2011). Performance analysis of Snort and Suricata network intrusion detection and prevention engines. IDCS 2011, the Fifth International Conference on Digital Society, Gosier, Guadeloupe, France. 187–192.

[16] Damaye, S. (2011b). Suricata-vs-snort. URL: www.aldeid.com/wiki/Suricata-vs-snort

[17] Leblond, E. (2011). Optimizing Linux on multicore CPUs. Message posted to home.regit.org/2011/01/optimizing-suricata-on-a-multicore-cpu

[18] Eugene Albin and Neil C. Rowe (2012). A Realistic Experimental Comparison of the Suricata and Snort Intrusion-Detection Systems.

[19] Boštjan Brumen and Jernej Legvart (2016). Performance analysis of two open-source intrusion detection systems.