## Literature Review

IDS has been embedded in the common defense mechanisms of a network since time immemorial and has played vital roles in furnishing the much needed information on malicious activities and unauthorized access to a network. The current solutions used to protect against infections and attacks using IDS are usually divided into two major categories Host-Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS) that have developed over the last 20 years. Whereas Host-Based systems search individual hosts or devices to detect intrusion, Network-Based systems like the Snort detect possible threats by searching the network traffic (Scarfone & Mell, 2007; Garcia-Teodoro et al., 2009).

**Snort: IDS modular network-based**

Snort is a well-known network intrusion detection and prevention system within an open-source network-based IDS tool used to stay safe. Snort uses rule-based detection engine, where both the packet header and payload are used to determine patterns pointing to malicious activity. It is this signature-based detection which forms the base functionality of Snort with pre set rules constantly updated by user community to match known attack signatures. But the strength of Snort is that it is flexible by its modular design having the packet decoder, preprocessors, detection engine, logging facility and output module. This modularity supports massive customization, which gives its users the option to develop specialist rules to suit the specific nature of their networks and threats experienced.

One of the strongest characteristics of Snort is the possibility to set the detection capabilities and fine-tune the revolution tool to various environments adopted by organizations. As an example, we can use distinct preprocessor modules to support the usage of different protocols including HTTP, FTP and DNS, in this way it will make sure that Snort can be able to inspect traffic on a number of network protocols. Also, Snort uses a logging facility that will generate a lot of information on the attack, and its out put modules can be configured to provide a way of informing or reporting on the out come like alerting the security departments as the threats are detected in time.

**Effectiveness and Challenges of Snort**

Snort signature based detection model is very effective in detecting known attack signatures. According to the research conducted by Ahmed and Habib (2021) and Ali and Al-Yasiri (2020), Snort can be used to protect against known exploits and attacks since the program is efficient in identifying existing patterns of attacks. This trustworthiness has made Snort to be a choice of convenience among various organizations that are in need to use an IDS that is very reliable.

Nevertheless, similar to any other signature-based IDS, Snort suffers shortcomings when it comes to identifying something new or zero-day attacks that do not have known signatures. According to Sommer and Paxson (2010) and Zhang and Lee (2000), protection against the encrypted or obfuscated attacks is one of the major drawbacks of Snort. This decreases the effectiveness of Snort to examine the payload of such traffic, and in a world where more and more communications are being secured (HTTPS, SSL/TLS, and/or VPN), the effectiveness of Snort is reduced.

To meet that challenge, the research and practice have proposed to integrate Snort with the algorithms of anomaly detection which are not based on the premade signatures but rather work to sense the abnormalities in the system and network behavior. This set up contributes greatly to the detection abilities of Snort as it now has the capacity to detect the attack methods that may not have been known or elusive in the past. What is more is the possibility of incorporating Snort into Security Information and Event Management (SIEM) systems so as to facilitate centralized logging and more advanced analysis of these Snort alerts and hence the overall effectiveness of analyzing the threats (Sommer & Paxson, 2010; Zhang & Lee, 2000).

**Advancements and Alternatives to Snort**

Different graphical interfaces have been evolved over the decades to provide Snort alert in a more user-friendly format. Snort analyses tools like BASE (Basic Analysis and Security Engine) and Snorby also offer user friendly interfaces to view, search and analyze Snort alerts as well. Such interfaces enhance usage of Snort, particularly in big scale implementation by facilitating the collection and display of alerts in order to recognize possible danger easily.

Besides the recent gains in improvements in the interface and functionality of Snort, recent literature has discussed the comparisons between Snort and other solutions of IDS including Suricata and Zeek (formerly Bro). Although Snort is still very popular having the advantages of a simple installation process, extensive documentation and an active user community, others such as Suricata have started providing features like multi-threading which makes all the difference in high throughput systems. The ability of Suricata to handle a large amount of data at the same time and the advantage that Snort has over Suricata is its performance time and scales very well in network settings issues. Nonetheless, the persistence of Snort has been supported by its unswerving ease of use and support offered by thousands of admirers as well as its proficiency (Kumar & Singh, 2022).

# References

1. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94. National Institute of Standards and Technology.
2. Beale, J., Baker, A., Posluns, J., Northcutt, S., & Poor, M. (2007). *Snort Intrusion Detection and Prevention Toolkit*. Syngress Publishing.
3. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE.
4. Kumar, A., & Singh, H. (2022). Comparative Study of Snort, Suricata and Zeek Intrusion Detection Systems. *International Journal of Network Security & Its Applications*, 14(1).
5. Ahmed, H., & Habib, A. (2021). Lightweight IDS for IoT Networks Using Snort. *Procedia Computer Science*, 184, 674–681.
6. Ali, M., & Al-Yasiri, A. (2020). Custom Rule Optimization for Snort to Reduce False Positives. *Journal of Cyber Security Technology*, 4(3), 145–160.
7. Garcia-Teodoro, A., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges. *Computers & Security*, 28(1-2), 18–28.
8. Iqbal, M., Shah, M. A., & Khan, M. A. (2019). Performance Evaluation of Open Source Intrusion Detection Systems on Encrypted Network Traffic. *IEEE Access*, 7, 115104–115116.
9. Axelsson, S. (2000). The Base-Rate Fallacy and the Difficulty of Intrusion Detection. *ACM Transactions on Information and System Security*, 3(3), 186–205.
10. Zhang, Y., & Lee, W. (2000). Intrusion Detection in Wireless Ad-Hoc Networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (pp. 275–283). ACM.