ISSN: **3107-6513**

Metagaurd- A Privacy Preserving Network Intrusion Detection

Sriyaash J, Karan R
III B.Sc Information Technology, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India . Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India
sriyaashjeyakrishnan@gmail.com , karanrajas2000@gmail.com

ABSTRACT - *Network-based attacks continue to pose a significant and evolving threat in modern cybersecurity, exploiting both system vulnerabilities and behavioral weaknesses in network communication. This paper presents MetaGuard, a behavior-driven network detection framework designed to identify suspicious activities through structured analysis of network logs. The system integrates rule-based detection techniques with statistical and pattern-based analysis for effective threat identification in near real-time. MetaGuard leverages structured feature extraction from DNS and connection logs, including entropy calculation, timing patterns, and communication frequency, to detect malicious behavior with high accuracy.*

A multi-layered detection pipeline is implemented to optimize performance while maintaining detection reliability across various attack scenarios. Experimental observations indicate that the system effectively identifies threats such as command-and-control communication, domain generation activity, data exfiltration, and abnormal scanning behavior. The framework is lightweight, scalable, and adaptable, making it suitable for deployment in academic, research, and real-world network monitoring environments..

Keywords: *Network Threat Detection, Behavioral Analysis, Cybersecurity, DNS Log Analysis, Traffic Monitoring, Rule-Based Detection, Real-Time Network Analysis*

1.INTRODUCTION

The rapid advancement of digital technologies and the widespread adoption of interconnected systems have significantly increased concerns regarding network security and data protection. In modern computing environments, organizations and individuals rely heavily on network communication for data exchange, cloud services, and real-time applications. However, this growing dependence has also expanded the attack surface, making networks more vulnerable to sophisticated cyber threats. Malicious actors increasingly exploit network communication channels to perform activities such as command-and-control communication, data exfiltration, and stealthy intrusion, often blending their actions with legitimate traffic to avoid detection.

Network-based threats are primarily influenced by communication behavior, traffic patterns, and the lack of effective monitoring mechanisms. Attackers often use advanced techniques such as Domain Generation Algorithms (DGA), encrypted communication channels, and periodic beaconing to maintain persistence within a network. These activities are difficult to detect using traditional methods, as they do not always match known attack signatures. By analyzing network logs, including DNS queries and connection records, along with timing patterns and communication frequency, it becomes possible to identify anomalies and detect suspicious behavior. This behavior-driven approach enhances the ability to detect both known and unknown threats.

Traditional security solutions mainly focus on signature-based intrusion detection, firewall rules, and predefined attack patterns. While effective against previously identified threats, these approaches often fail to detect zero-day attacks and evolving attack techniques. Moreover, they lack the capability to analyze deeper behavioral patterns within network traffic. With the increasing use of cloud environments, remote access systems, and distributed networks, the need for advanced

monitoring solutions that can analyze network behavior in real time has become critical. This highlights the importance of developing systems that go beyond static detection and incorporate dynamic analysis of network activity.

To address these challenges, this work proposes MetaGuard, a network detection framework designed to monitor and analyze network activity through structured log analysis. The system processes network metadata logs such as DNS logs and connection logs to extract relevant information about communication patterns. It applies rule-based and statistical analysis techniques to identify suspicious behavior, including high entropy domains, abnormal DNS query patterns, periodic communication indicative of command-and-control activity, excessive connection attempts, and unusual data transfer volumes.

Furthermore, MetaGuard maintains structured records of analyzed network activity, enabling detailed investigation and supporting digital forensic analysis. The system operates as a lightweight and standalone tool, ensuring minimal impact on system performance while providing efficient detection capabilities. Its modular design allows multiple detection components to function independently while contributing to a comprehensive threat detection process. By combining real-time analysis, behavioral detection, and structured reporting, MetaGuard provides an effective solution for identifying and mitigating network-based threats.

Overall, MetaGuard contributes to enhancing network security by addressing the limitations of traditional detection systems and emphasizing behavior-based analysis. It provides a practical and scalable approach for detecting suspicious activities, improving network monitoring practices, and supporting forensic investigations in modern cybersecurity environments.

2.LITERATURE REVIEW

Network threat detection has become a significant area of research due to the rapid expansion of digital networks and the increasing exchange of data across interconnected systems. As organizations and individuals rely heavily on network communication for critical operations, there is a growing need to monitor and analyze network-level activities to prevent unauthorized access and malicious behavior. Traditional security approaches primarily focus on predefined attack signatures and system-level vulnerabilities, while recent studies emphasize the importance of analyzing network behavior through logs such as DNS queries and connection records.

Various techniques have been proposed for detecting network threats, with rule-based detection and statistical analysis being among the most widely used methods. Rule-based techniques are effective in identifying known attack patterns by applying predefined conditions such as abnormal connection frequency, suspicious domain queries, and unusual data transfer volumes. Statistical methods further enhance detection by analyzing metrics such as domain entropy, traffic distribution, and communication intervals to identify anomalies within network activity. These approaches are efficient, lightweight, and suitable for real-time or near real-time monitoring systems.

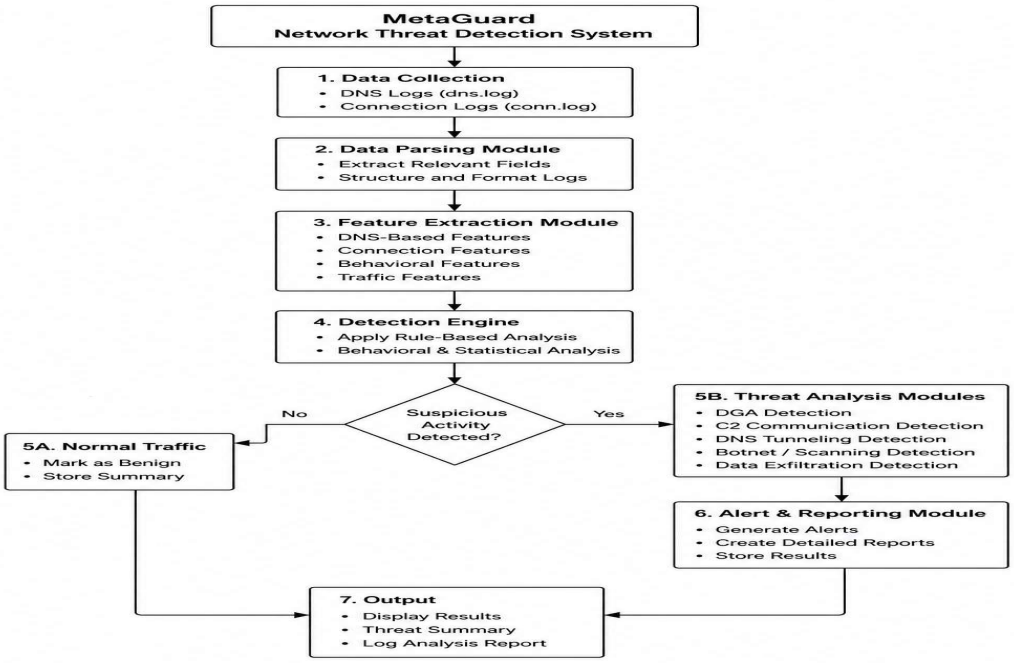
Recent advancements in this field highlight the use of behavioral analysis to improve detection accuracy. These systems analyze network communication patterns, timing intervals, and interaction frequency to identify abnormal or malicious behavior. By understanding how systems and hosts communicate within a network, it becomes possible to detect threats such as command-and-control communication, domain generation activity, and botnet behavior more effectively. Behavioral analysis also helps reduce false positives by distinguishing between normal traffic patterns and suspicious anomalies.

In addition, multi-layered detection approaches that combine rule-based and behavior-driven techniques have been explored to enhance reliability and performance. These methods integrate log

analysis, pattern recognition, and anomaly detection to provide more accurate and consistent results. Continuous monitoring of DNS and connection logs enables early detection of suspicious activities, allowing timely response and improved network security management.

Overall, existing research highlights the importance of combining rule-based detection, behavioral analysis, and structured logging to address network security challenges. These approaches contribute to building efficient systems capable of detecting and preventing network-based threats in modern cybersecurity environments.

3.METHODOLOGY



3.1 Data Collection

Data collection is a critical step in the MetaGuard system, as it forms the foundation for detecting network-based threats and suspicious activities. The system gathers network metadata logs from monitoring tools such as Zeek or tcpdump in a non-intrusive manner. It continuously processes log files such as DNS logs (dns.log) and connection logs (conn.log) without interfering with normal network operations. Each log entry contains detailed information about network communication, including source and destination IP addresses, domain queries, ports, timestamps, connection duration, and data transfer size.

The collected data consists of various types of network activity information, including DNS queries, connection sessions, and traffic patterns that may indicate malicious behavior. By collecting this data in near real-time, MetaGuard can observe network behavior and identify potential indicators of threats

All collected data is stored in a structured format, enabling efficient access and processing by the detection modules. This structured dataset serves as the primary input for feature extraction and behavioral analysis, supporting both real-time threat detection and detailed forensic investigation.

3.2 Data Pre-processing and Exploration

The collected network log data undergoes a preprocessing stage to ensure accuracy, consistency, and suitability for analysis. This process involves removing duplicate log entries, filtering irrelevant or noisy records, and handling missing or incomplete values. These steps help maintain a clean and structured dataset, which is essential for reliable detection of network anomalies

and suspicious activities.

Following preprocessing, data exploration is performed to understand the characteristics and patterns of network activity. Key attributes such as communication frequency, DNS query patterns, connection duration, and data transfer volume are analyzed to identify trends within the network. This exploration helps in recognizing normal traffic behavior, detecting unusual patterns, and identifying potential indicators of threats such as periodic communication, abnormal query spikes, or irregular traffic flow.

Statistical observations and pattern analysis further support the identification of relationships between different network variables, such as the frequency of DNS queries, connection attempts, and data transfer patterns. These insights help in understanding how network entities communicate over time and assist in identifying abnormal behavior. For example, a high frequency of DNS queries or repeated connection attempts to specific destinations may indicate suspicious activities such as scanning, command-and-control communication, or automated traffic generation.

Overall, the preprocessing and exploration stage plays a crucial role in improving data quality and supporting accurate threat detection. It ensures that MetaGuard operates efficiently while providing reliable results for identifying network anomalies, detecting suspicious activities, and analyzing communication behavior within modern network environments.

3.3 Data Splitting

The processed network log data is organized into structured records to support efficient analysis and validation of the detection system. The dataset is arranged based on key attributes such as timestamps, source and destination IP addresses, DNS queries, connection details, and traffic patterns, ensuring consistency in data handling. This structured organization allows MetaGuard to systematically process network logs during monitoring and analysis.

To evaluate the effectiveness of the detection techniques, the dataset is logically divided into subsets for validation and continuous monitoring. A portion of the log data is used to verify the accuracy of rule-based and behavioral detection methods, while the remaining data supports real-time analysis and system operation. This approach ensures that the detection mechanisms perform reliably across different network conditions and traffic patterns.

The data segmentation strategy also helps in assessing system performance by enabling comparison between detected anomalies and expected normal behavior. By validating detection accuracy on a subset of data, the system can be refined to improve reliability and minimize false positives. This structured approach ensures consistent performance and enhances MetaGuard's ability to identify potential network threats effectively.

3.4 Algorithm Selection

The selection of appropriate techniques is essential for accurately detecting suspicious activities within network log data. The proposed MetaGuard system utilizes rule-based analysis as a primary method to identify known patterns of malicious behavior such as abnormal DNS queries, high-frequency connections, and unusual data transfer activity. This technique compares network attributes against predefined conditions, enabling efficient and reliable detection of threats in near real time.

In addition to rule-based analysis, behavioral detection is employed to analyze network activity based on communication patterns. These techniques evaluate factors such as domain entropy, timing intervals, and frequency of interactions to identify anomalies.

Data processing techniques are also integrated into the system to support filtering, validation, and organization of network logs. These techniques ensure that only relevant and

properly structured data is analyzed, improving the efficiency of the detection process.

The combination of rule-based detection, behavioral analysis, and data processing techniques provides a reliable and efficient framework for identifying network threats. This integrated approach enhances detection accuracy, supports near real-time monitoring, and ensures consistent system performance across different network environments.

4.RESULTS

The experimental results demonstrate the effectiveness of the proposed MetaGuard system in detecting network-based threats through log analysis. The system was tested on various network scenarios using DNS logs and connection logs containing both normal and suspicious activities to evaluate its detection capability. The results show that the system successfully identifies anomalies such as high entropy domains, abnormal DNS query patterns, periodic communication indicative of command-and-control activity, and unusual data transfer behavior using rule-based and behavioral analysis techniques.

The detected activities are clearly classified as normal or suspicious, providing a comprehensive understanding of potential threats within the network. The system generates structured outputs that include relevant details such as source and destination IP addresses, timestamps, query patterns, and detected threat indicators. This enables users and administrators to effectively analyze network activity and identify potential security risks.

The evaluation also indicates that the integration of data processing and behavioral analysis techniques improves detection accuracy by filtering irrelevant log data and reducing false positives.

Overall, the results confirm that the proposed approach is efficient, accurate, and suitable for identifying network anomalies and malicious activities. MetaGuard provides a practical solution for enhancing network security and supports forensic analysis through structured logging and detailed reporting of detected events.

(DGA) Detection:

MetaGuard analyzes domain names using entropy calculation and pattern analysis to identify randomly generated domains commonly used by malware for communication.

Command-and-Control (C2) Detection:

The system detects periodic communication patterns by analyzing timing intervals between repeated DNS queries or connections, which indicates potential C2 beaconing behavior.

DNS Tunneling Detection:

MetaGuard identifies abnormal DNS query patterns, such as unusually long domain names or high query frequency, which may indicate hidden data transfer through DNS channels.

Botnet and Scanning Detection:

The system monitors connection patterns to detect high-frequency requests, multiple destination targeting, and rapid connection attempts that are typical of botnet activity or network scanning.

Data Exfiltration Detection:

MetaGuard analyzes data transfer volumes and outbound traffic patterns to identify unusually large or repeated data transfers that may indicate unauthorized data leakage.

Anomaly Detection:

The system evaluates overall network behavior, including frequency, timing, and communication patterns, to detect deviations from normal activity.

5.CONCLUSION

This paper presents MetaGuard, a network threat detection system designed to identify suspicious activities through continuous monitoring and analysis of network logs. The system effectively processes DNS and connection data using rule-based and

behavioral detection techniques to identify potential threats such as command-and-control communication, domain generation activity, abnormal DNS patterns, and data exfiltration. The detected activities are clearly classified as normal or suspicious, providing a comprehensive understanding of potential risks within the network.

6.REFERENCES

[1] Paxson V*: A System for Detecting Network Intruders in Real-Time*, Lawrence Berkeley National Laboratory, 1998.

[2] Zeek Project, *Zeek Network Security Monitor Documentation*, 2024.

[3] Mahdavifar S., et al., *Lightweight Hybrid Detection of Data Exfiltration using DNS*, ACM, 2021.

[4] Moomtaheen F., et al., *Extended Isolation Forest for Intrusion Detection in Zeek Data*, MDPI, 2024.

[5] Zhang W., et al., *Malicious DNS Detection using Network Traffic Analysis*, Springer, 2025.

[6] Okolie S. A., *Anomaly Detection in Cybersecurity Data*, ScienceDirect, 2025.

[7] Pinto D., *A Review on Intrusion Detection Datasets and Network Traffic Analysis*, Elsevier, 2025.

[8] Behl A., et al., *A Review of Network Intrusion Detection Systems*, IEEE Access,

[9] Sommer R., & Paxson V., *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*, IEEE Symposium on Security and Privacy, 2010.

[10] Sommer R., & Paxson V., *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*, IEEE Symposium on Security and Privacy, 2010.

[11] Roesch M., *Snort: Lightweight Intrusion Detection for Networks*, Proceedings of the 13th USENIX Conference on System Administration (LISA), 1999.