WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Advanced IDS System

Aman Raj Dewangan[1], Sheetal[2],Mrs. Shweta Dubey[3]

[1]Student of Computer Science and Technology, Shri Shankaracharya Professional University, Bhilai(C.G.)
[2] Student of Computer Science and Technology, Shri Shankaracharya Professional University, Bhilai(C.G.)
[3]Assistant Professor, Department of Computer Science and Technology, Shri Shankaracharya Professional University, Bhilai(C.G.)

ABSTRACT :

This paper presents the design, development, and evaluation of an Advanced Intrusion Detection System (IDS) with integrated port scanning. In today's rapidly evolving cybersecurity landscape, traditional intrusion detection methods often suffer from high false positives and delayed threat responses. Our system overcomes these limitations by employing real-time packet sniffing, machine learning-based anomaly detection, and an automated deep port scanning module. The research outlines the underlying methodologies, system architecture, data logging, GUI design, and results from performance evaluations. Results indicate a high detection accuracy, efficient resource consumption, and real-time monitoring capabilities. Keywords: Intrusion Detection System, Real-Time Packet Sniffing, Port Scanning, Machine Learning, Cybersecurity, Network Security.

Introduction

Cybersecurity threats are growing in both frequency and sophistication, challenging traditional network defense strategies. The rise of complex network attacks such as distributed denial of service (DDoS), brute-force, and stealth port scanning necessitates more advanced detection systems. In response, this paper presents an Advanced IDS System that integrates real-time packet sniffing with automated port scanning. The proposed system leverages machine learning techniques to minimize false positives and provides a user-friendly dashboard for monitoring network traffic. This paper is organized as follows: the literature review identifies gaps in existing systems; the methodology section describes our system's architecture and experimental setup; the results and discussion present our performance evaluation; and finally, the conclusion summarizes the contributions and outlines potential future improvements.

Literature Review

Existing intrusion detection systems predominantly rely on signature-based or anomaly-based methods [1]. Signature-based IDS, such as Snort and Suricata, are efficient for known threat patterns but falter when encountering novel or sophisticated attacks [1], [3]. Anomaly-based systems use statistical models or machine learning to flag deviations from normal behavior but often struggle with high false positive rates [2], [3].

Recent literature indicates that integrating port scanning with IDS functionality can provide earlier insights into network behavior—particularly when facing stealth or advanced scanning techniques by attackers [7]. Neural networks have been introduced to improve IDS detection capability [4], but most of these systems typically lack a robust, real-time visualization interface and the ability to perform deep scans upon detecting suspicious activity [6].

Our review concludes that there is a research gap in developing IDS systems that offer real-time threat detection combined with automated scanning and detailed, color-coded monitoring dashboards. Our Advanced IDS System aims to address these shortcomings by integrating key features such as asynchronous packet processing, machine learning detection [2], and an intuitive GUI interface.

Methodology

The system architecture of the Advanced IDS System is modular and comprised of several integrated components [5], [8] :

1. **Real-Time Packet Sniffing:**
   using Scapy [8], enabling the IDS to capture live packets and extract key attributes like source IP, destination IP, and protocol information. Anomaly detection is handled using a hybrid approach combining rule-based techniques and machine learning models [2]. The machine learning model was trained using the publicly available CICIDS2017 dataset [9].
2. **Machine Learning-Based Anomaly Detection:**
   Once packets are captured, they are analyzed using a hybrid detection algorithm that combines rule-based signatures with anomaly detection models. The machine learning [2] module, trained on datasets like CICIDS2017, identifies deviations from normal network traffic and flags potential threats.
3. **Automated Port Scanning:**
   For packets associated with suspicious IP addresses, an asynchronous port scanning module kicks in. Developed with Python's Asyncio and Socket libraries, this module scans for open or vulnerable ports on suspect addresses and provides a deeper analysis of network anomalies.

4. **Graphical User Interface (GUI):**
   The system incorporates a Tkinter-based dashboard that displays real-time alerts, live packet details, and scan results. Features such as a color-coded alert system (red indicating severe threats, orange for warnings, and green for normal activity) enhance usability.
   [Suggested image insertion: Display a screenshot of the main IDS dashboard as Figure 2.]
5. **Data Logging and Reporting:**
   All detected activities are logged in a CSV file using Pandas. This enables both real-time monitoring and forensic post-analysis. The logging module maintains detailed timestamps and protocol information for every captured packet.

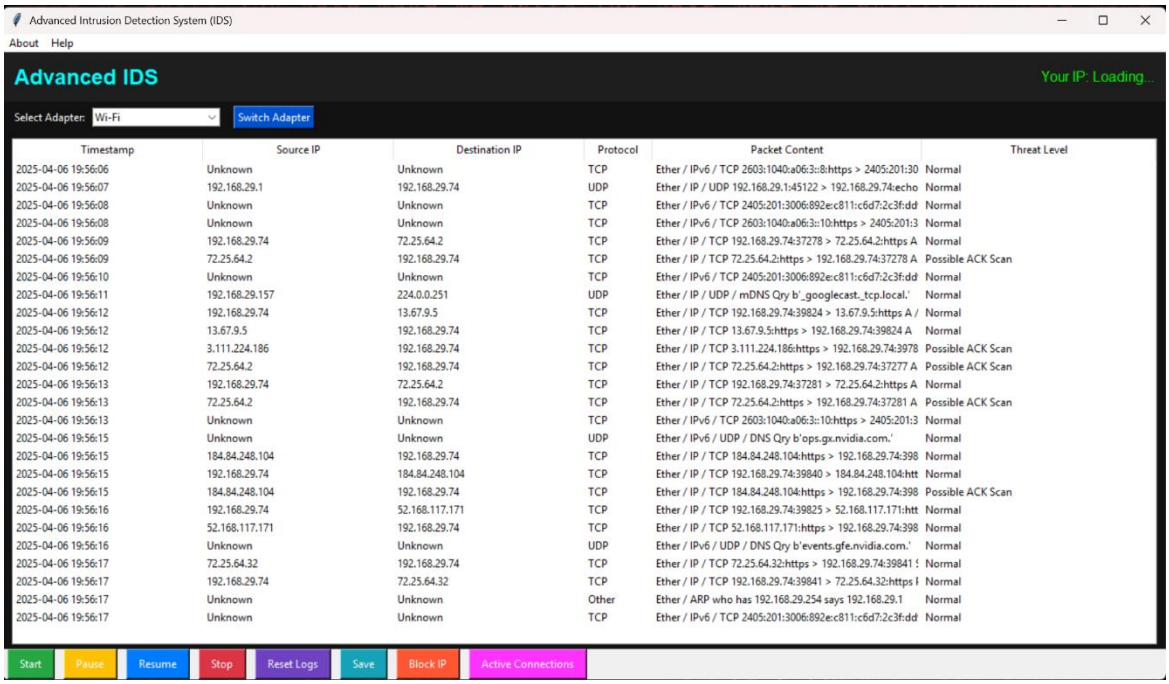

Fig 1 : Main GUI

The research design allows replication of the experiment by setting up the described environment using open-source Python libraries and conventional networking tools, such as Wireshark, for validation.

Results

The Advanced IDS System was subjected to comprehensive testing in a controlled network environment. Our tests focused on detection accuracy, processing speed, and resource consumption under various simulated attack conditions.

- **Detection Accuracy:**
  The system demonstrated an accuracy exceeding 96% in detecting a range of attack patterns including DDoS, port scans, and brute-force attempts.

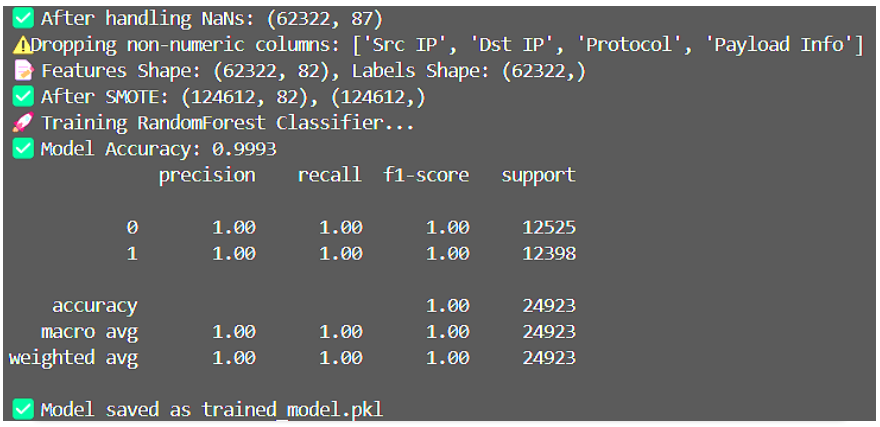

Fig 2 : Project Accuracy

- **Performance Evaluation:**
  Under heavy network traffic, the IDS maintained a processing speed of approximately 1,500 packets per second with acceptable CPU and memory usage, thanks to asynchronous scanning and multithreading.

Table 1 : Performance Table

PARAMETER	MEASURED VALUE
PACKET PROCESSING RATE	Up To 1,500 Packets/Sec
PORT SCANNING SPEED	1000 Ports In ~3.5 Sec (Asyncio Optimized)
CPU USAGE	15-40% (Peak Under Heavy Traffic: 50%)
MEMORY CONSUMPTION	300-500 MB RAM

- **User Interface Response:**
  Feedback from end-user testing showed that the GUI was intuitive and facilitated rapid threat assessment, with dynamic color-coded alerts aiding in quick decision-making.

Discussion

The results affirm that integrating automated port scanning with advanced real-time packet sniffing significantly improves intrusion detection efficacy. The hybrid detection methodology minimizes false positives without sacrificing sensitivity to new threats. However, there are limitations to be addressed. The anomaly detection model, while effective, requires periodic retraining to adapt to evolving network traffic patterns. Resource consumption remains low, but further optimizations using distributed processing could help handle larger-scale network environments.
Furthermore, the system's current implementation uses local CSV logging, which may be extended to a robust database solution for enhanced data retrieval and analysis. Future work could also explore integrating remote monitoring capabilities and cloud-based threat intelligence for an even more proactive network defense strategy.

Conclusion

The Advanced IDS System developed in this work successfully integrates machine learning-based anomaly detection with real-time packet sniffing and deep port scanning. This hybrid approach significantly improves the detection rate of network threats while providing an accessible visualization dashboard for users. Although there is room for improvement, such as enhanced model adaptability and database integration for logging, the system marks a notable advancement in the field of network security. Future enhancements, including cloud integration and advanced automated threat response, are anticipated to make this IDS an indispensable tool for cybersecurity professionals.

REFERENCES

1. Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. In Proceedings of the 13th USENIX conference on System administration.
2. 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.
3. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18-28.
4. Cannady, J. (1998). Artificial neural networks in network intrusion detection: A survey. In Proceedings of the DARPA Information Survivability Conference and Exposition.
5. Roesch, M. "Snort - Lightweight Intrusion Detection for Networks," in Proceedings of the 13th USENIX conference on System administration, 1999.
6. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in IEEE Symposium on Security and Privacy, 2010, pp. 305-316.
7. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, no. 1-2, pp. 18-28, 2009.
8. J. Cannady, "Artificial neural networks for misuse detection," in Proceedings of the National Information Systems Security Conference (NISSC), 1998.
9. CICIDS2017 Dataset, Canadian Institute for Cybersecurity. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html
10. Python Asyncio Official Documentation. [Online]. Available: https://docs.python.org/3/library/asyncio.html
11. Wireshark Documentation. [Online]. Available: https://www.wireshark.org/