INCIDENT RESPONSE AUTOMATION

[1]MOHAMMAD AARIF, [2]Y SRINIVAS RAJU

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor, Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

With the rapid growth of digital technologies, cyber-attacks have become increasingly frequent and sophisticated, posing serious threats to organizational networks and data security. Traditional manual incident response methods are time-consuming and often ineffective in handling large-scale and real-time attacks. To address these challenges, this project proposes an automated Incident Response System that can efficiently detect, analyze, and mitigate cyber threats using network log data. The proposed system utilizes network traffic analysis through the Wireshark API to monitor and identify suspicious activities in real-time. It processes uploaded network log data to detect various types of cyber-attacks such as Distributed Denial of Service (DDoS) and abnormal traffic patterns. Once an attack is identified, the system generates detailed reports and visualizations, highlighting attack sources such as IP addresses and port numbers. Additionally, the system supports automated response actions, including isolating compromised systems to prevent further damage and spread within the network. The application is designed with multiple modules including user registration, login, data collection, incident detection, and alert analysis. Graphical representations provide better insights into attack patterns and frequency, enabling users to make informed decisions. By automating the incident response process, the system significantly reduces response time, minimizes damage, and enhances overall network security. This solution is highly beneficial for cybersecurity operations, offering scalability, efficiency, and real-time monitoring capabilities for modern network environments.

Keywords : Cybersecurity, Incident Response Automation, Network Security, Wireshark, DDoS Detection, Log Analysis, Intrusion Detection, Threat Detection, Network Monitoring, Data Security

I. INTRODUCTION

The increasing dependence on digital systems and network infrastructures has led to a significant rise in cyber threats and security breaches. Organizations today face various types of attacks such as Distributed Denial of Service (DDoS), malware injections, and unauthorized access, which can disrupt operations and compromise sensitive data. Traditional incident response methods often

rely on manual monitoring and analysis, making them slow and inefficient in handling large volumes of network traffic. As cyber-attacks become more advanced and frequent, there is a growing need for automated solutions that can quickly detect and respond to such threats. This project focuses on developing an Incident Response Automation system that enhances the efficiency and speed of detecting and mitigating cyber-attacks using network log data.

The proposed system leverages network traffic analysis using tools like Wireshark to capture and analyze packet-level data. By processing network logs, the system identifies abnormal patterns and suspicious activities that indicate potential cyber threats. The automation of incident detection reduces human intervention and enables faster identification of attacks. The system is capable of detecting multiple types of threats and provides detailed insights such as source IP addresses, port numbers, and type of attack. This helps security analysts understand the nature of the attack and take appropriate actions. The integration of visualization techniques further improves the interpretability of the detected incidents.

In addition to detection, the system also focuses on response and mitigation. Once a threat is identified, the system can isolate affected systems to prevent the spread of attacks within the network. The application is designed with user-friendly modules including registration, login, data upload, detection, and alert analysis. Graphical reports provide a clear understanding of attack frequency and patterns. Overall, this project aims to provide a comprehensive and automated solution for incident response, improving cybersecurity defense mechanisms and reducing the impact of cyber threats on modern organizations.

II SURVEY OF RESEARCH

1. Network Intrusion Detection Systems (NIDS)

Network Intrusion Detection Systems (NIDS) play a vital role in identifying unauthorized access and malicious activities in network traffic. Traditional NIDS rely on signature-based detection, where known attack patterns are matched against incoming data. While effective for known threats, these systems fail to detect new or unknown attacks. Recent research has introduced anomaly-based detection methods that identify deviations from normal network behavior. These systems use statistical and machine learning techniques to improve detection accuracy. However, they often produce false positives, making analysis difficult. This project builds upon these concepts by integrating automated log analysis and attack detection, reducing manual effort and improving response time.

2. Log-Based Threat Detection Techniques

Log analysis is a widely used method in

cybersecurity for detecting suspicious activities. Research shows that analyzing network logs can reveal patterns of attacks such as unusual traffic spikes, repeated login attempts, or abnormal packet flows. Tools like Wireshark have been extensively used for packet inspection and traffic analysis. However, manual log analysis is time-consuming and requires expertise. Automated systems have been proposed to process logs and generate alerts for potential threats. These systems improve efficiency but require robust algorithms to handle large-scale data. The proposed project automates log analysis using APIs and generates real-time alerts, enhancing detection capabilities.

3. Machine Learning in Cybersecurity

Machine learning has gained significant attention in cybersecurity for its ability to detect complex and evolving threats. Researchers have applied algorithms such as Decision Trees, Support Vector Machines, and Neural Networks to classify normal and malicious network traffic. These models learn from historical data and can identify patterns that are difficult to detect using traditional methods. Studies show that machine learning-based systems improve detection rates and reduce false positives. However, challenges such as data imbalance and model training complexity remain. This project complements these approaches by combining automated detection with structured log analysis to improve threat identification.

4. Incident Response Automation Systems

Incident Response Automation is an emerging area in cybersecurity that focuses on automating the detection, analysis, and mitigation of security incidents. Research highlights that automation reduces response time and minimizes human errors during critical situations. Automated systems can isolate affected systems, block malicious IPs, and generate alerts without manual intervention. Many organizations adopt Security Orchestration, Automation, and Response (SOAR) tools to streamline incident handling. However, implementing such systems can be complex and costly. This project provides a simplified automation approach that integrates detection and response mechanisms, making it suitable for practical deployment.

5. Visualization in Cybersecurity Analysis

Visualization techniques are widely used to represent complex network data in an understandable format. Research shows that graphical representations such as bar charts, line graphs, and heatmaps help in identifying attack trends and anomalies more effectively. Visualization tools enable security analysts to quickly interpret large datasets and make informed decisions. Many modern systems incorporate dashboards for real-time monitoring of network activities. However,

designing effective visualizations requires careful consideration of data representation. This project uses graphical analysis to display attack types, frequency, and patterns, improving user understanding and decision-making.

6. DDoS Attack Detection and Prevention

Distributed Denial of Service (DDoS) attacks are among the most common and disruptive cyber threats. Research indicates that DDoS attacks overwhelm network resources by flooding them with excessive traffic, leading to service unavailability. Various detection methods have been proposed, including traffic pattern analysis, threshold-based detection, and machine learning approaches. While these methods are effective, real-time detection remains a challenge due to the high volume of network traffic. The proposed system addresses this issue by analyzing network logs and identifying abnormal traffic patterns, enabling early detection and response to DDoS attacks, thereby reducing potential damage.

III. WORKING METHODOLOGY

The proposed system begins with user interaction through a secure web-based interface where users can register and log in to access the application. Once authenticated, the user can upload network log data for analysis. These logs contain detailed information about network packets, including source IP, destination IP, port numbers, and protocols. The system uses Wireshark-based APIs to scan and process this log data. During preprocessing, the uploaded data is cleaned, structured, and converted into a suitable format for analysis. This step ensures that irrelevant or noisy data is removed, allowing the system to focus on meaningful patterns. The processed data is then passed to the detection module, which identifies abnormal activities based on predefined attack signatures and behavioral patterns.

In the detection phase, the system analyzes network traffic to identify potential cyber threats such as DDoS attacks, unusual traffic spikes, and suspicious packet flows. The detection mechanism compares network behavior with normal patterns to identify anomalies. Once an attack is detected, the system generates detailed reports highlighting the type of attack, affected IP addresses, and port numbers involved. These reports help in understanding the nature and source of the attack. Additionally, the system classifies traffic into normal and malicious categories, enabling efficient monitoring. The detection process is designed to be automated, reducing the need for manual intervention and ensuring faster response times in critical situations.

After detection, the system performs alert analysis and visualization to provide clear insights into the identified threats. Graphical representations such as bar charts and activity

graphs are generated, where the x-axis represents different types of attacks and the y-axis indicates their frequency. This helps users quickly understand attack patterns and severity. The system can also isolate affected systems or flag suspicious activities to prevent further damage. By combining detection, reporting, and visualization, the system ensures a complete incident response process. This automated approach improves efficiency, reduces response time, and enhances overall network security, making it suitable for real-time cybersecurity applications.

IV RESULTS EXPLANATIONS

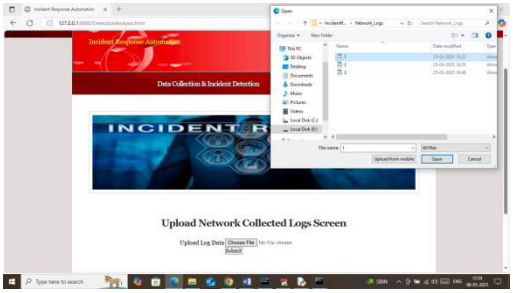
In propose work we are developing an online tool which will scan and monitor all network log data to detect all cyber-attacks and then can isolate such attacking system from the network to minimize further spread of attacks to other system. This application will detect all network attacks by employing Wireshark network attack detection API. Identifying and resolving such cyber-attack is known as Incident Response Automation.

Incident response is the process of identifying, investigating and resolving security incidents and breaches isolating the affected systems from further damage, minimize the damage and recover the systems.

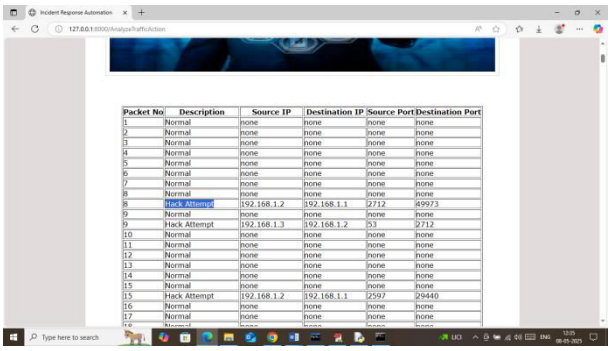
Incident response in Cyber security is a structured process an organization uses to handle a data breach or cyber-attack, aiming to minimize damage and restore systems. It involves identifying an attack, containing its spread, and recovering from the incident to reduce the risk of future attacks. This process is often guided by an Incident Response Plan (IRP) that outlines procedures for different types of cyber-attacks.

To implement cyber-attack automation process we have designed following modules

1) New User sign up: user can sign up with the application
2) User Login: user can login to system
3) Data Collection & Incident Detection: using this module user can upload network log data and then apply scanning API to detect all abnormal network activities and then generate report with different alerts
4) Alert Analysis: this module analyse all network traffic data file and then system will scan all packets to detect malicious activities and then generate detail graph on different attacks happened from different IP and PORT.

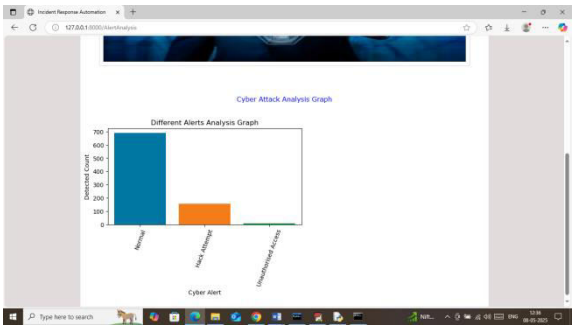


In above screen selecting and uploading network log data and then click on buttons to get below report

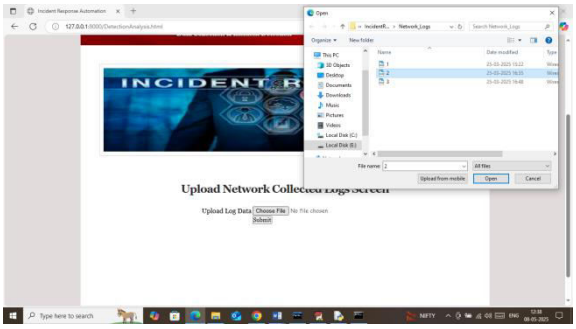


Packet No	Description	Source IP	Destination IP	Source Port	Destination Port
1	Normal	none	none	none	none
2	Normal	none	none	none	none
3	Normal	none	none	none	none
4	Normal	none	none	none	none
5	Normal	none	none	none	none
6	Normal	none	none	none	none
7	Normal	none	none	none	none
8	Normal	none	none	none	none
8	Hack Attempt	192.168.1.2	192.168.1.1	2712	49973
9	Normal	none	none	none	none
9	Hack Attempt	192.168.1.3	192.168.1.2	53	2712
10	Normal	none	none	none	none
11	Normal	none	none	none	none
12	Normal	none	none	none	none
13	Normal	none	none	none	none
14	Normal	none	none	none	none
15	Normal	none	none	none	none
15	Hack Attempt	192.168.1.2	192.168.1.1	2597	29440
16	Normal	none	none	none	none
17	Normal	none	none	none	none

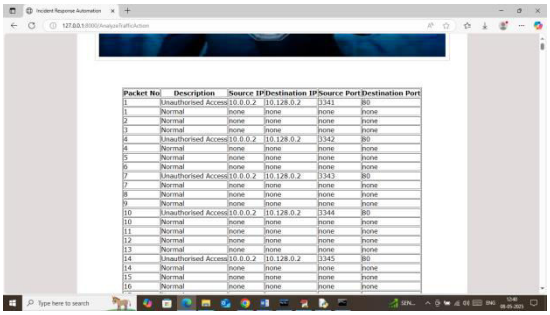
In above screen can see reports generated from log data where displaying different attack names happening from different IP and port no and now click on 'Alert Analysis' link to get below page



In above alert analysis graph where x-axis represents type of activities and y-axis represents activity count. Similarly you can upload and test any other log file and below is another log output

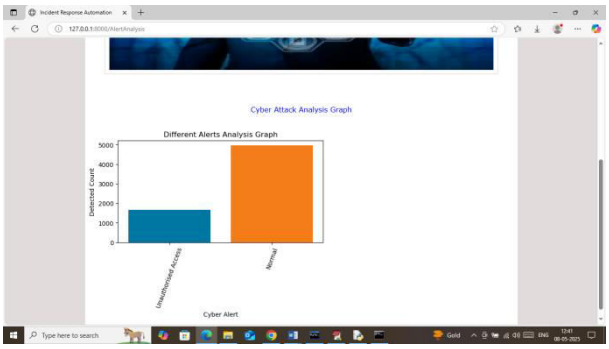


In above screen uploading another log data and then press button to get below page

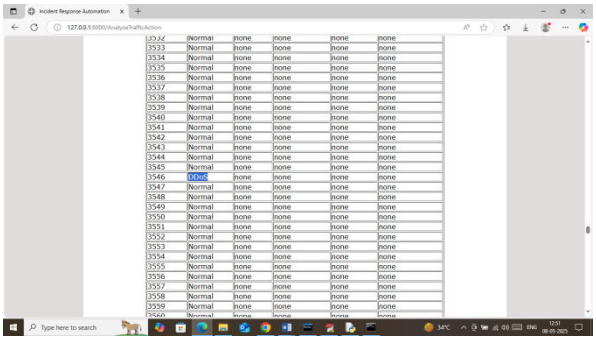


Packet No	Description	Source IP	Destination IP	Source Port	Destination Port
1	Unauthorised Access	10.0.0.2	10.128.0.2	1341	80
1	Normal	none	none	none	none
2	Normal	none	none	none	none
3	Normal	none	none	none	none
4	Unauthorised Access	10.0.0.2	10.128.0.2	1342	80
4	Normal	none	none	none	none
5	Normal	none	none	none	none
6	Normal	none	none	none	none
7	Unauthorised Access	10.0.0.2	10.128.0.2	1343	80
7	Normal	none	none	none	none
8	Normal	none	none	none	none
9	Normal	none	none	none	none
10	Unauthorised Access	10.0.0.2	10.128.0.2	1344	80
10	Normal	none	none	none	none
11	Normal	none	none	none	none
12	Normal	none	none	none	none
13	Normal	none	none	none	none
14	Unauthorised Access	10.0.0.2	10.128.0.2	1345	80
14	Normal	none	none	none	none
15	Normal	none	none	none	none
16	Normal	none	none	none	none

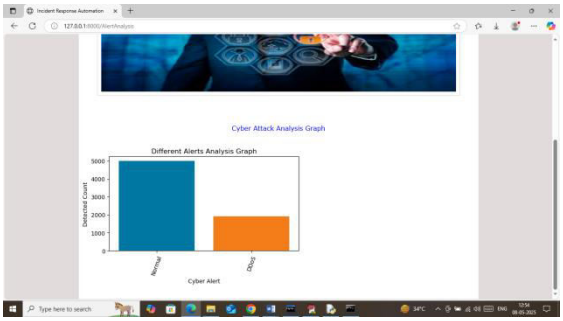
In above screen can see detected normal and attack packets and now click on Analysis Alert to get below page



In above graph can see type of detected attacks



In above screen DDOS attack detected



In above analysis graph can see number of DDOS and normal traffic detected from network log data

V. CONCLUSION

The proposed Incident Response Automation system provides an efficient and reliable solution for detecting, analyzing, and responding to cyber-attacks using network log data. By integrating automated log analysis with Wireshark-based detection techniques, the system successfully identifies malicious activities such as DDoS attacks and abnormal traffic patterns with minimal human intervention. The modular design, including user authentication, data collection, incident detection, and alert analysis, ensures a structured and user-friendly workflow. Additionally, the use of graphical visualizations enhances understanding of attack patterns and supports better decision-making. The system significantly reduces response time, minimizes potential damage, and improves overall network security. Its scalability and ability to handle multiple log files make it suitable for real-world cybersecurity applications. Overall, the project demonstrates the importance of automation in incident response and provides a practical approach to strengthening defense mechanisms against evolving cyber threats.

REFERENCES

[1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson, 2017.

[2] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 5th ed. Prentice Hall, 2015.

[3] B. B. Gupta, D. P. Agrawal, and S. Yamaguchi, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global, 2016.

[4] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[5] G. Creech and J. Hu, “A semantic approach to host-based intrusion detection systems using

contiguous and discontiguous system call patterns," *IEEE Trans. Computers*, vol. 63, no. 4, pp. 807–819, 2014.

[6] M. Roesch, "Snort: Lightweight intrusion detection for networks," in *Proc. USENIX LISA*, 1999, pp. 229–238.

[7] Wireshark Foundation, "Wireshark Network Protocol Analyzer," [Online]. Available: https://www.wireshark.org

[8] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," *Technical Report*, Chalmers University, 2000.

[9] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST Special Publication 800-94, 2007.

[10] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Syngress, 2012.

[11] R. Behl and J. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2017.

[12] S. Northcutt and J. Novak, *Network Intrusion Detection*, 3rd ed. New Riders, 2002.

[13] A. A. Ghorbani, W. Lu, and M. Tavallaee, *Network Intrusion Detection and Prevention: Concepts and Techniques*, Springer, 2010.

[14] J. McHugh, "Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations," *ACM Trans. Information and System Security*, vol. 3, no. 4, pp. 262–294, 2000.

[15] T. Holz and F. Raynal, *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, 2005.

[16] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Software Engineering*, vol. SE-13, no. 2, pp. 222–232, 1987.

[17] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 2nd ed. Syngress, 2014.

[18] P. Kazienko and P. Dorosz, "Intrusion detection systems (IDS) and their classification," *Int. J. Computer Science and Network Security*, vol. 4, no. 12, pp. 36–42, 2004.

[19] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," *ACM SIGCOMM Computer Communication Review*, vol. 19, no. 2, pp. 32–48, 1989.

[20] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.

[21] M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2003.

[22] N. Ye, *Handbook of Data Mining for Counterterrorism and Security*, Springer, 2009.

[23] R. Bace and P. Mell, "Intrusion detection systems," NIST Special Publication, 2001.

[24] S. Garfinkel and G. Spafford, *Practical UNIX and Internet Security*, O'Reilly Media, 2003.

[25] J. Behl and K. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2017.