DETECT AND MITIGATE INTRUSION DURING CYBER ATTACKS.

Lekhan H Y[1], N Pravalika[2] , N Vishal Krishna Bhat[3] , Rakshitha M[4]
Students, Dayananda Sagar Academy of Technology & Management, Bengaluru, India
Rama Abirami[5], Associate Professor , Dayananda Sagar Academy of Tech & MGMT, Bengaluru, India

lekhanyathish1812@gmail.com[1], pravalipravalika00@gmail.com[2], krishnavishal56@gmail.com[3], rakshitham.1dt19is105@gmail.com[4], ramaabirami-ise@dsatm.edu.in[5]

ABSTRACT

An intrusion detection system (IDS) is a type of security technology that tracks hostile or unauthorized activity on computer networks and systems. An IDS's main objective is to spot potential security gaps, record information about them, and notify security administrators so they may take the necessary action. There are two main types of IDS: network based IDS (NIDS) and host-based IDS (HIDS). While HIDS keeps an eye on each individual host system for odd activity, NIDS watches network traffic for suspicious behavior and spots potential dangers. IDS can be further categorized as signature based or anomaly based, depending on the detection technique used. Anomaly-based IDS employ statistical analysis to find changes from expected network behavior, while signature-based IDS compare known harmful activity patterns with observed network traffic. The employment of IDS, which is frequently used in conjunction with other security measures like firewalls and antivirus software, is essential for defending computer networks from different kinds of cyberattacks.

Malt Rail is a harmful traffic detection system that makes use of static-trails generated from various antivirus reports and user-defined custom lists, as well as publicly available (black)lists containing malicious and/or generally suspicious trails. A trail can be anything from a domain name (for example, zvpprsensinaix.com for Banjari malware), URL (for example, hXXp://109.162.38.120/harsh02.exe for known malicious executable), IP address (e.g 185.130.5.231 for known attacker) Additionally, it makes use of (optional) sophisticated heuristic methods that can aid in the discovery of new risks (like malware).

Keywords

Black lists, NIDS, HIDS, malicious, vulnerabilities, SVM's, ANN's, trails.

1. INTRODUCTION

An intrusion detection system (IDS) is an essential tool for any organization to identify potential cyber threats and mitigate the risk of cyber-attacks. The main goal of this project is to give organizations an effective way to identify and handle potential cyber risks. It gives a thorough overview of the project's architecture and design, as well as the many sensors and analyzers that were employed for data collecting and processing. We will also go through the system's reaction procedures, which can be automated or manual and include things like blocking or containing questionable traffic.

This will also emphasize the testing and evaluation procedures used for the project, which included simulating various cyber- attack scenarios to evaluate the system's efficiency and performance.

The overall goal of this implementation paper is to demonstrate how IDS may be used in real-world situations to mitigate cyberattacks and to give businesses a framework for doing so.

2. LITERETURE SURVEY

Si. No	Literature	Author	Year of publication	Description
1.	On anomalies Intrusion detection system : Techniques, Challenges and	Muhammad Usman Khan	2021	Discusses the importance of irregularity detection, various techniques, challenges, and solutions.

	future Directions			
2.	A Survey on IDS	R. Chandrasekaran and A. M. Chandrasekaran	2020	Provides an overview of signature-based, anomaly-based, and hybrid IDS techniques, their strengths, weaknesses, and the importance of combining multiple techniques.
3.	IDS: A Review of Techniques and Challenges	Aditya Singh and Rakesh Kumar	2019	Reviews signature-based, anomaly-based, and hybrid IDS techniques, their challenges, and future directions.
4.	Review of ML-Based IDS	J. A. M. Garcia, et al.	2021	Provides an overview of supervised,unsupervised, and semi-supervised machine learning-based IDS techniques, their advantages, limitations, and future directions.
5.	Hybrid IDS: A Review	M. Alazab, et al.	2017	Reviews various hybrid IDS techniques, their strengths, weaknesses, scalability, performance,and the importance of considering real-world environments.

3. PROPOSED FRAMEWORK

3.1 Algorithms & Modules

There are several algorithms that can be used in building an intrusion detection system (IDS). Here are some examples:

1. **Signature-based detection :**This method analyses the system activity or incoming network traffic with a database of recognized attack signatures. The IDS generates an alert informing the user of the existence of an attack if a match is discovered.

2. **Anomaly-based detection**: This algorithm creates a baseline of normal network or system behavior and then compares the current activity against that baseline. If the activity deviates significantly from the normal behavior, the IDS generates an alert indicating the presence of an attack.

3. **Machine learning-based detection**: This algorithm uses machine learning techniques to train the IDS to recognize patterns of network or system behavior associated with attacks. The IDS then use this information to recognize fresh assaults that it hasn't previously seen.

i) **Artificial Neural Networks (ANNs):** Machine learning algorithms known as ANNs are based somewhat on the architecture of the human brain. Based on the patterns they discover from a training dataset, they may be utilized to categorized network traffic as legitimate or malicious.

ii) **Support Vector Machines (SVMs):** Network traffic may be categorized using SVMs, a form of supervised machine learning algorithm, based on data patterns. They operate by identifying the hyperplane that best divides the various data types.

iii) **Decision Trees**: Network traffic may be categorized using decision trees, a form of supervised machine learning algorithm, according to a set of decision rules. They operate by recursively dividing the data into smaller subsets according to the characteristics that are crucial for differentiating between various classes.

iv) **Random Forests**: Multiple decision trees are combined in random forests, an ensemble learning approach, to increase the robustness and accuracy of the classification model. Each decision tree is trained by randomly picking subsets of the data and features, and the results are then combined to provide a final classification.

v) **Deep Learning**: Deep learning is a kind of machine learning that makes use of multi-layered artificial neural networks to discover intricate patterns in data. It has been used in intrusion detection systems to classify network traffic based on deep packet inspection and other advanced techniques.

4. **Hybrid detection**: This algorithm combines multiple detection techniques, such as signature-based and anomaly-based detection, to improve the accuracy of the IDS.

5. **Data mining-based detection**: This algorithm uses data mining techniques to identify patterns in large volumes of network or system data. Using this information, the IDS can then spot prospective attacks.

3.2 Architecture

The architecture for an Intrusion Detection System (IDS) typically consists of several components that work together to detect and respond to potential security threats. The architecture can vary depending on the specific requirements of the system, but typically includes the following components:

Sensors: The sensors are responsible for capturing network traffic data and analyzing it for potential security threats. The sensors can be hardware or software-based and can be deployed at various points in the network, such as at the network perimeter, between network segments, or on individual devices.

Data Aggregator: The data aggregator component collects data from multiple sensors and aggregates it into a central location for analysis. The aggregator can also normalize and correlate the data to identify potential security threats.

Analysis Engine: The analysis engine is responsible for analyzing the network traffic data and identifying potential security threats. The engine can use various techniques, such as signature-based and anomaly-based detection, to identify potential threats.

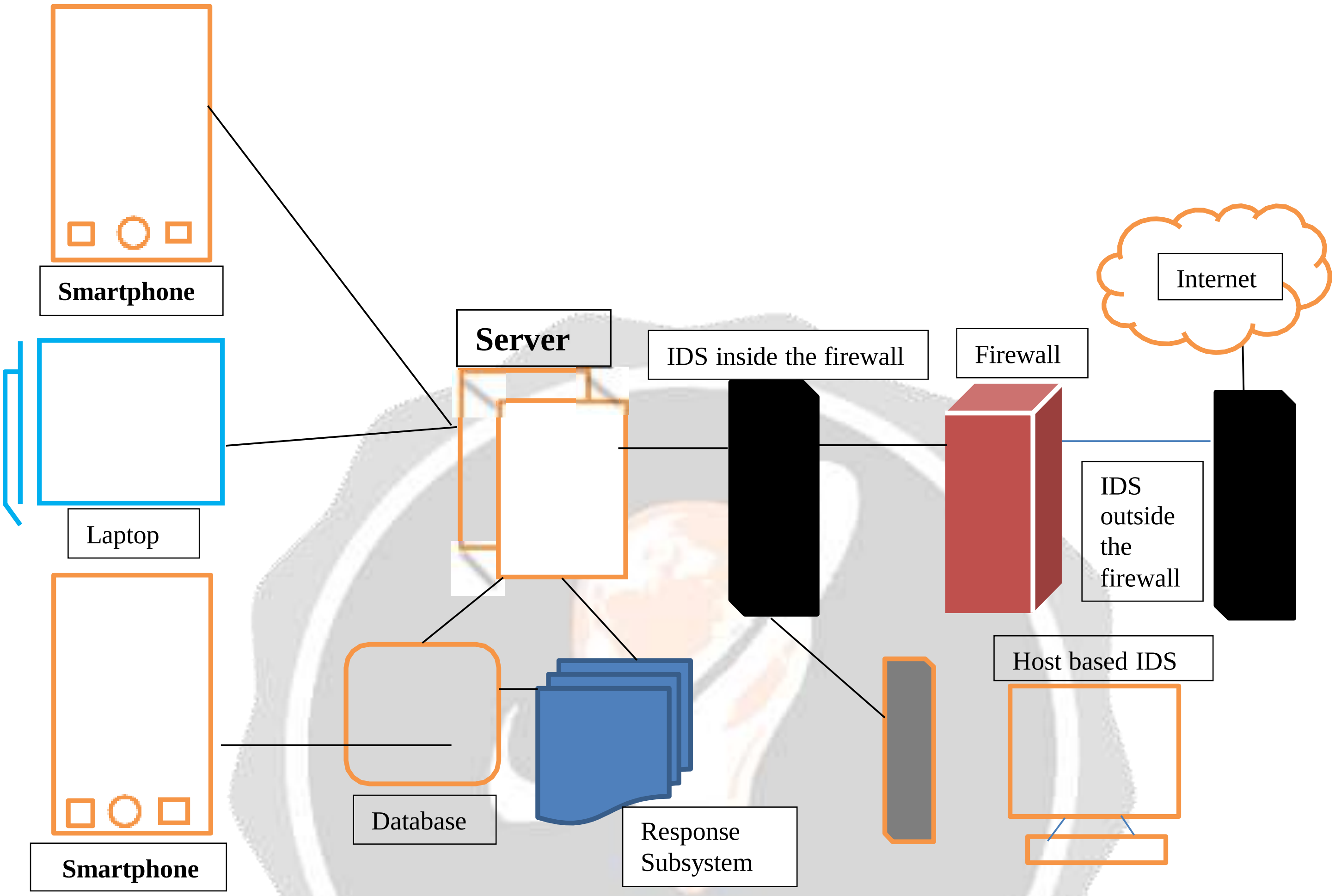
Response Mechanism: The response mechanism is responsible for responding to potential security threats detected by the IDS. The response can be automated, such as blocking or quarantining suspicious traffic, or manual, such as alerting security analysts to investigate and respond to the potential threat.

Reporting and Alerting: The reporting and component that alert is responsible for presenting the analysis results to security analysts or system administrators. The component can provide various features, such as search capabilities, filtering, and sorting of alerts, as well as the ability to take action against detected threats.

Management Console: The management console is responsible for managing the IDS system, configuring the sensors, setting up alert thresholds, and managing of the response mechanisms.

The architecture for an IDS can be distributed or centralized. In a centralized architecture, all components of the IDS are located in a single location, such as a data center The components of a distributed architecture are dispersed throughout a number of places, such as different departments or geographical regions.

Overall, the architecture of an IDS is designed to provide comprehensive protection against potential security threats. By detecting and mitigating potential cyber-attacks, an IDS can help organizations maintain the confidentiality, integrity, and availability of their networks and data.



3.3 Flowchart

A security tool called an intrusion detection system (IDS) watches network traffic for potential security threats and notifies the system administrators if it notices any unusual activity. An IDS's ability to detect and respond to possible security threats in real-time depends on the data flow that underlies its operation.

The first component in the data flow is the network traffic, which can be generated by various devices on the network, such as servers, workstations, and mobile devices. This network traffic can include various types of data, such as HTTP requests, DNS queries, and file transfers.

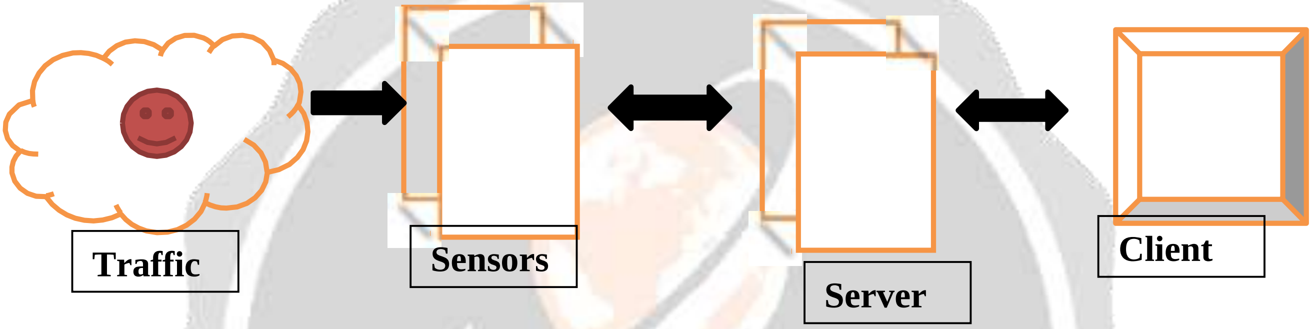
The second component in the data flow is the sensor, which captures packets of network traffic and analyzes them for potential security threats. The sensor can use various techniques, for example signature-based and anomaly-based detecting system, to look for potential threats. Once the sensor has analyzed the network traffic data, it sends the analysis results to the server.

The third component in the data flow is the server, which receives the analysis results from the sensor and correlates the data to identify potential security threats. The server can also store the data in a database for future analysis and reporting. Additionally, the server may use machine learning algorithms to analyze the data and identify new threat patterns that may not be captured by signature-based or anomaly-based detection techniques.

The fourth and final component in the data flow is the client, which presents the analysis results to security analysts or system administrators. The client can be a web-based interface or a dedicated application that displays the IDS alerts and allows theanalysts to investigate and respond to potential security threats. The client interface provides various features, such as search capabilities, filtering, and sorting of alerts, as well as the ability to take action against detected threats, such as blocking or quarantining suspicious traffic.

The data flow between traffic, server, sensor and client is a continuous and iterative process, with each component constantly exchanging data and information. The sensor continuously records and evaluates data from network traffic, sending the analysis results to the server. The server, in turn, correlates the data and identifies potential security threats, sending alerts to the client. The client presents the alerts to the analysts, who investigate and respond to the potential security threats, taking action to mitigate the risks.

In summary, the data flow in an IDS involves the collection and analysis of network traffic by sensors, the aggregation and processing of the analysis results by a server, and the presentation of the results to security analysts or system administrators via a client interface. This data flow is critical to the operation of the IDS, because it allows the system to identify and react in real-time to potential security risks. IDS can assist organization’s in maintaining the safety, integrity, and accessibility of their networks and data by spotting and thwarting prospective cyber-attacks.



4. RESULTS

Intrusion detection systems (IDS) can help lessen cyber intrusions by identifying potential threats and alerting system administrators or security personnel to take required action. The efficiency of an IDS depends on a variety of factors, includes the excellence of the system's algorithms, the dependability of the data sources it monitors, and the promptness of its notifications. When an IDS notices suspicious behavior, security experts can be informed via an alarm or alert. Depending on how serious the threat is, IDS will differentiate and present it. A strong IDS may generally help reduce the risk of cyber intrusions and protect important data and assets. It is important to keep in mind that an IDS is only a minor part of a holistic cyber safe strategy**.**

Fig 1:UI Design

Above Fig 1 describes an interface with sections for threats, dest and src ports, severity, trails, references, and flags.This interface shows the overall survey of a threat or an anomaly. Tags can be added as required by the user. The type of attack and also the information is displayed.

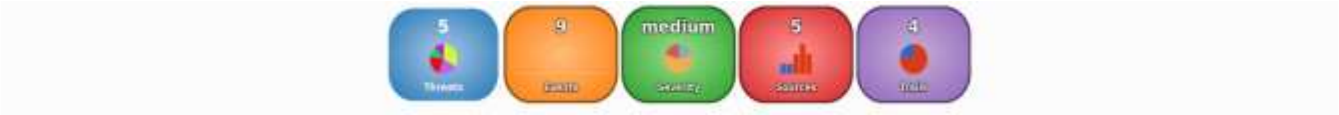


Fig 2: UI Dashboard

Above Fig 2 shows the representation of the threats, events taken place, severity, sources and also the trail chat using symbols

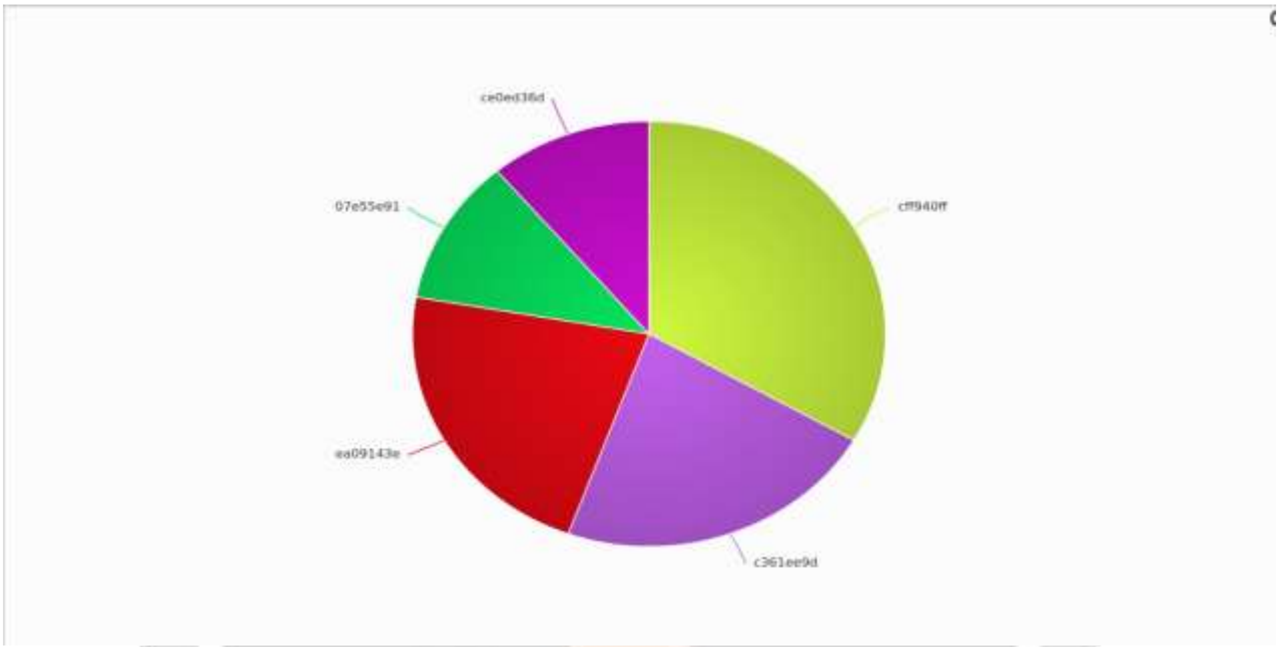


Fig 3: Pie chart

Fig 3 is a pie chart that represents the attack using different colors to segregate them.

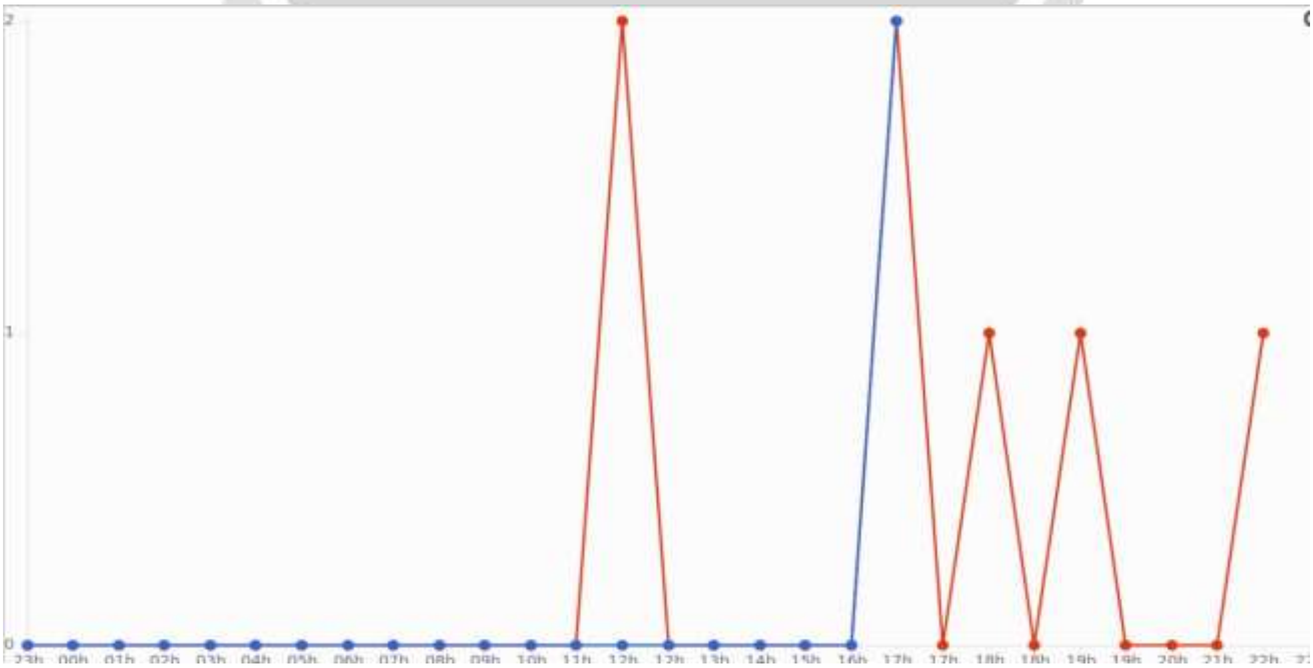


Fig 4: Graph Display

Above Fig 4, Graph represents the kind of attack i.e IP or DNS or any other kinds of attack. It also gives the time stamp for 24 hours.

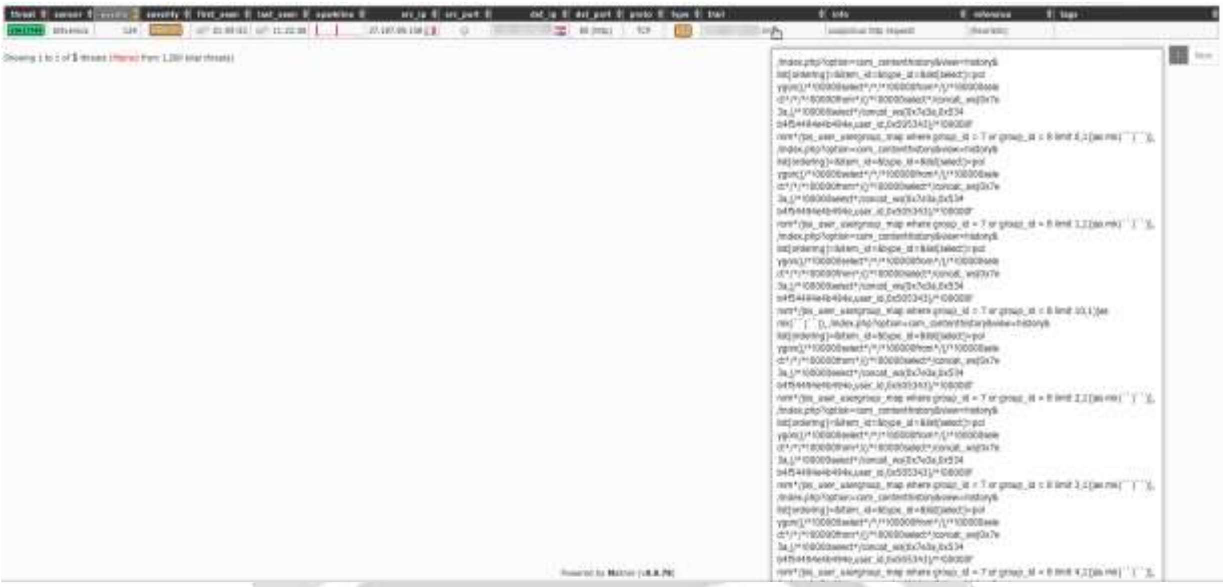


Fig 5: Threats display

The Fig 5 above represent the threats like the following could be discovered when suspicious requests from external web application security scanners (such as searching for SQLi, XSS, LFI, etc. vulnerabilities) and/or malicious internal user attempts towards unidentified web sites are made. (Real case of attackers attempting to exploit The Joomla! platform CMS CVE-2015-7297, CVE-2015-7857, and CVE-2015-7858 vulnerabilities.

5. CONCLUSION AND FUTURE WORK

In conclusion, any organization must adopt an IDS in order to reduce the danger of cyber-attack. Our research aims to offer organizations a workable solution for successfully detecting and responding to possible cyber threat.

Using both signature based and anomaly based detection techniques, we created and put into practise a hybrid IDS strategy. For data collecting and analysis, the IDS used a variety of sensors and analyzers. We also included both automated and manual response methods, such blocking or quarantining suspected traffic.

We simulated a variety of cyber-attack scenarios as part of the testing and assessment procedure to evaluate the system's efficiency. Our findings showed that the IDS was capable of quickly identifying and countering possible cyberthreat, which supported its usefulness in thwarting cyber-attack. Our implementation paper's overall goal is to demonstrate IDS's usefulness in real-world settings and to give businesses a framework for doing so. We think that by deploying an IDS, businesses can dramatically lower their risk of cyber-attacks and safeguard their valuable information and assets from potential threats.

6. REFERENCES

[1] Horng, S.-J.; Su, M.-Y.; Chen, Y.-H.; Kao, T.- W.; Chen, R.-J.; Lai, J.-L. & Perkasa, C. D.,"A novel intrusion detection system based on hierarchical clustering and support vector machines," Expert systems with Applications, Elsevier, 2011, 38, 306-313

[2] Lacroix, A. B.; Langlois, J. P.; Boyer, F.-R.; Gosselin, A. & Bois, G.,"Node configuration for the Aho-Corasick algorithm in intrusion detection systems Architectures for Networking and Communications Systems (ANCS)," 2016 ACM/IEEE Symposium on, 2016, 121-122

[3] Liao, H.-J.; Lin, C.-H. R.; Lin, Y.-C. & Tung, K. Y.,"Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, Elsevier, 2013, 36, 16-24

[4] IDS. [online]. Available: http://www.snort.org

[5] Scarfone, K. & Mell, P., "Guide to intrusion detection and prevention systems (idps)," NIST special publication,

2007, 800,94

[6] Buczak A. L. & Guven, E.,"A survey of data mining and machine learning methods for cyber security intrusion detection,"
IEEE Communications Surveys & Tutorials, IEEE, 2016, 18,1153-1176

[7] V. Gomez, C. Hernandez, and F. Martinez, "Energy policies in smart grids," Contemp. Eng. Sci., vol. 10, no. 20, pp. 987– 999, 2017.

[8] B. Li, S. Lv, and Q. Pan, "The Internet of Things and smart grid," in Proc. IOP Conf. Earth Environ. Sci., vol. 113, 2018, pp. 12–38.

[9] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, "Energy big data: A survey," IEEE Access, vol. 4, pp. 3844–3861, 2017.

[10] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal crosslayer resilient control systems," IEEE Control Syst. Mag., vol. 35, no. 1, pp. 110–127, Feb. 2015.

[11] https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

[12] https://owasp.org/www-community/controls/Intrusion_Detection.

[13] "Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID" by Rafeeq Ur Rehman Link: https://www.amazon.com/Intrusion-Detection-Systems-Snort-Techniques/dp/0131407333

[14] "Intrusion Detection and Prevention" by Carl Endorf, Eugene Schultz, and Jim Mellander Link: https://www.amazon.com/Intrusion-Detection-Prevention-Carl-Endorf/dp/0849328027

[15] "Intrusion Detection: A Machine Learning Approach" by Sunita Garhwal and Pardeep Kumar Link: https://www.springer.com/gp/book/9783030167347

[16] "Intrusion Detection Systems: A Survey and Taxonomy" by Richard A. Kemmerer and Giovanni Vigna Link: https://dl.acm.org/doi/10.1145/502059.502061

[17] "A Survey of Intrusion Detection Systems" by Ali A. Ghorbani, Wei Lu, and Mahbod Tavallaee Link: https://www.sciencedirect.com/science/article/pii/S0167404811001042

[18] "Machine Learning for Intrusion Detection: A Review" by Robin Verma and M. Hanmandlu Link: https://ieeexplore.ieee.org/abstract/document/6847129

[19] "A Review of Intrusion Detection Systems in Wireless Sensor Networks" by Mahdi H. Miraz and Cheng-Zhong Xu Link: https://ieeexplore.ieee.org/abstract/document/7428726

[20] "A Novel Intrusion Detection System for Cloud Computing Environment" by Rajendra Kumar Roul, Satchidananda Dehuri, and Sung-Bae Cho Link: https://link.springer.com/chapter/10.1007/978-3-030-19488-8_30

[21] "Anomaly-Based Intrusion Detection Systems: A Survey" by Robin Verma and M. Hanmandlu Link: https://ieeexplore.ieee.org/abstract/document/6960175

[22] "Intrusion Detection Systems: A Comprehensive Review" by M. Subramanian and D. Dharani Link: https://www.sciencedirect.com/science/article/pii/S2352914820301557