Intrusion Detection System in Network Security

Miss. Shradha P.Patil[1], Ms.Supriya S.Tambire[2] , Ms. Smita Sangewar[3]

[1]PG (Computer Science & Engineering), DKTE Society's Textile & Engineering Institute (An Empowered Autonomous Institute), Ichalkaranji
[2]Assistant Professor (Computer Science & Engineering), DKTE Society's Textile & Engineering Institute (An Empowered Autonomous Institute), Ichalkaranji
[3]Assistant Professor (Computer Science & Engineering), DKTE Society's Textile & Engineering Institute (An Empowered Autonomous Institute), Ichalkaranji

---***---

Abstract - Intrusion Detection Systems (IDS) have become a crucial part of contemporary network security, aiding organizations in identifying and addressing unauthorized access, harmful activities, and potential cyber threats in real time. As cyber-attacks grow more complex, traditional security measures like firewalls and antivirus programs are no longer adequate for comprehensive protection. IDS are generally divided into signature-based, anomaly-based, and hybrid methods. Signature-based IDS are effective at recognizing known attack patterns but struggle with zero-day threats. Anomaly-based IDS use machine learning and statistical models to spot deviations from typical network behavior, enabling them to detect unknown threats, though they often produce many false positives. Hybrid IDS strive to balance detection accuracy with false alarm rates by combining both approaches. Architecturally, IDS can be split into Host-Based IDS (HIDS), which monitor activities on individual systems, and Network-Based IDS (NIDS), which examine network traffic for potential threats. The incorporation of artificial intelligence (AI) and machine learning (ML) has greatly improved IDS capabilities, allowing for automated detection and adaptive learning to combat evolving threats. However, IDS face several challenges, such as high computational demands, scalability issues, and sophisticated evasion techniques used by attackers. To tackle these challenges, ongoing research is exploring deep learning-based IDS, blockchain-enhanced security, and cloud-based solutions for more efficient and scalable threat detection. This paper offers a comprehensive analysis of IDS methodologies, architectures, challenges, and future research directions to bolster network security in an increasingly digital world.

Keywords : Intrusion Detection System, Type, Need, Detection Methods, IDS Components, Application-Based IDS, and IDS Tools.

1.INTRODUCTION

In the modern era, ensuring internet security has become a significant challenge for organizations, particularly in protecting credential data from intruders. To safeguard this information, technologies such as Web Firewalls, encryption, authentication, and Virtual Private Networks (VPNs) have long been employed to secure network infrastructure and online communication. Intrusion detection is a relatively recent addition to the suite of security technologies. This system represents an advancement that enhances network security and protects organizational data. An Intrusion Detection System (IDS) assists network administrators in identifying malicious activities on the network, alerting them to take appropriate measures to secure the data against such attacks. An intrusion is defined as any unauthorized access or harmful use of information resources. An intruder or attacker is an entity that attempts to gain unauthorized access to information, cause damage, or engage in other malicious activities. The IDS is closely related to firewall security. While firewalls protect organizations from internet-based attacks, the IDS detects attempts to breach the firewall or any successful intrusions, alerting the system administrator to any unwanted activities within the firewall. Thus, an IDS is a security system that monitors network traffic and computer systems, analyzing this traffic for potential external attacks and internal misuse or attacks.

Types of Intrusion Detection Systems-

1. Network Based Intrusion Detection and Prevention System : An organization's network segment is monitored for ongoing attacks by a Network Based Intrusion Detection System (NIDS), which is installed on a computer or other device linked to that segment. Many different hashing algorithms, such as MD5, are used in networks to keep files secure. In the event that an attack is detected, the network-based intrusion detection system reacts by informing administrators. NIDS searches network traffic for attack patterns, such as sizable groups of related items of a particular type that might indicate that a denial-of-service attack is ongoing, or it searches for the exchange of a series of related packets in a particular pattern that might suggest that a port scan is underway. Network intrusion detection systems (NIDSs) are installed at a specific location within a network segment (a router is one example). They can be used to monitor all system traffic within a network segment or to watch over specific host computers within a network segment.

2. Host Based Intrusion Detection System A specific computer or server, referred to as the host, is equipped with a Host Based Intrusion Detection System (HIDS), which solely keeps an eye on activity on that system. The two types of host-based intrusion detection systems are anomaly-based detection methods and signature-based (also known as misuse detection) methods. Key system files are monitored by HIDS, which also detects when an intruder adds, edits, or removes the files under observation. Then, when one of the following takes place—a change in the properties of a file, the creation of a new file, or the deletion of an existing file—the HIDS raises an alarm. The primary distinction between NIDS and HIDS is that the former can access encrypted data while it is moving over the network.

2. BODY OF PAPER

Literature Review:

For many years, intrusion detection systems (IDS) have been a major focus of cybersecurity research, developing in tandem with the growing complexity of network threats.

Numerous research have investigated various IDS architectures, techniques, and improvements utilizing cutting-edge technology including deep learning, artificial intelligence (AI), and machine learning (ML). An overview of important research contributions to IDS is given in this part, together with a focus on the field's major developments and difficulties.

2.1 Evolution of Intrusion Detection Systems

Anderson (1980) first presented the idea of intrusion detection systems (IDS), and Denning (1987) expanded on it by putting out a statistical anomaly detection-based model for spotting illegal activity in computer systems. IDS have developed throughout time from basic rule-based systems to complex machine learning-powered solutions.

Conventional intrusion detection systems were mostly signature-based, detecting known threats by using predetermined attack signatures. One of the first signature-based intrusion detection systems, Snort, is frequently utilized in practical settings. Researchers are investigating anomaly-based techniques because, although signature-based IDS are successful against known threats, they are unable to identify new or zero-day assaults.

2.2 Signature-Based vs. Anomaly-Based Detection

Incoming network traffic is compared to a database of known attack signatures by signature-based intrusion detection systems (IDS), including Snort and Suricata. Numerous studies demonstrate how well signature-based intrusion detection systems (IDS) can detect particular attack patterns (Roesch, 1999; Porras & Valdes, 1998). But as Mukherjee et al. (1994) pointed out, these systems are vulnerable to zero-day threats and polymorphic malware, which are always changing to evade detection by signatures.

Denning (1987) first proposed anomaly-based intrusion detection systems (IDS), which employ statistical and machine learning models to identify departures from typical network behavior. Research like Lippmann et al. (2000) and Tavallaee et al. (2009) highlights how anomaly-based intrusion detection systems can detect unidentified attacks. According to Chandola et al. (2009), anomaly-based intrusion detection systems have a significant disadvantage in that they frequently misclassify lawful traffic as malicious due to their high false positive rates.

2.3 Machine Learning and Artificial Intelligence in IDS

Researchers have increasingly combined machine learning (ML) and artificial intelligence (AI) techniques to improve detection accuracy in order to overcome the shortcomings of conventional IDS. A number of machine learning (ML) techniques have been investigated for anomaly detection, including Decision Trees (DT), Support Vector Machines (SVM), and Neural Networks (NN). Studies by Shon & Moon (2007) and Sommer & Paxson (2010) demonstrate how well ML-based IDS work to increase detection rates .

In IDS research, deep learning methods such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have demonstrated encouraging outcomes. Deep learning models were shown by Kim et al. (2017) and Javaid et al. (2016) to be able to automatically extract pertinent features from network traffic, increasing accuracy and adaptability. However, Yin et al. (2017) point out that computational complexity is still a problem.

2.4 Hybrid IDS and Advanced Techniques

By fusing the advantages of anomaly-based and signature-based techniques, hybrid IDS have been offered as a solution to the shortcomings of separate IDS models. Research by Buczak & Guven (2016) and Bhuyan et al. (2014) demonstrates that hybrid IDS offer lower false alarm rates and improved detection accuracy. Furthermore, it has been suggested that blockchain-based IDS solutions improve the reliability and integrity of data in IDS frameworks (Singh et al., 2020).

2.5 Challenges and Future Research Directions

High false positive rates, resource-intensive processing, encrypted traffic analysis, and adversarial attacks against machine learning-based IDS are just a few of the issues that IDS currently confront in spite of major developments. To enhance IDS performance, researchers are investigating self-adaptive IDS, & federated learning.

This review emphasizes that even while IDS research has advanced significantly, ongoing innovation is required to stay ahead of changing cyberthreats. To guarantee strong network security, future studies should concentrate on improving IDS's scalability, adaptability, and real-time processing capabilities.

Methodology:

functionality of IDS-

The four primary roles of the IDS are:
1. Data collection
2. Feature selection
3. Analysis.
4. Take action.

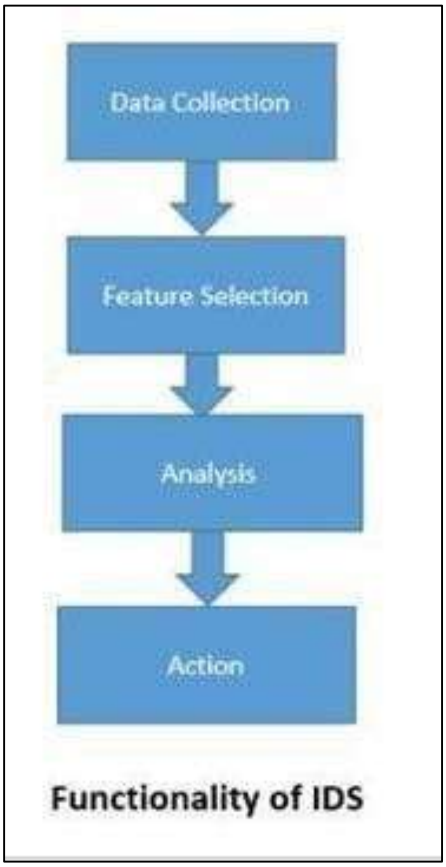

Fig.1 Functionality of IDS

1.Data Collection: This component feeds the data into the IDS. The information is logged into a file for subsequent analysis. In a network-based IDS, data packets are gathered and modified, whereas a host-based IDS gathers information such as disk usage and system processes.

2.Feature Selection: To identify specific features, extensive data is accessible within the network and is typically assessed for signs of intrusion. For instance, the Internet Protocol (IP) addresses of both the source and destination systems, the type of protocol, as well as the header length and size, can serve as crucial indicators for detecting intrusions.

3. Analysis: The data undergoes examination to verify its accuracy. In rule-based IDS, the data is scrutinized by comparing incoming traffic against established signatures or patterns. Alternatively, anomaly-based IDS involves analyzing system behavior and applying mathematical models to it.

4. Action: This term refers to the system's response and defense mechanisms. It can either notify the system administrator by sending an email or displaying alarm icons with all necessary information, or it can take a proactive role by blocking packets to prevent them from entering the system or by closing ports.

Components of an Intrusion Detection System-

There are three basic components of an IDS –
1. Sensor (Activity or packet capture engine, behavioral or signature detection engine)
2. The Backend (Event recording of database, alerting the engine)
3. The Frontend (User interface, Command & control)

The main part of an intrusion detection system (IDS) that detects network or computer intrusions is a sensor. To carry out detecting tasks, it captures a packet. It can use anomaly-based or signature-based intrusion detection methods.

The logging of events identified by the sensors is the responsibility of the IDS's backend. It also carries out the alerting function. The backend can notify the administrator in a number of methods, including by sending an email, blocking a connection, resetting a TCP connection, logging database events, and displaying the alert on the administrator’s interface.

The IDS user interface is formed by the frontend. In addition to configuring the IDS and updating the signature database and behavioral detection engine, the user can view events that the sensor has observed.

Working of IDS:-

The components of an IDS work in a structured manner to alert the administrator of an intrusion.

1. Sensor : One of the sensor's two interfaces The capture network interface comes first, followed by the management network interface. Its primary duties are to detect and report. The capture interface transfers all of the recorded data into a buffer while the sensor taps into the network to listen for network traffic. After that, the detection engine does network protocol analysis and looks over the contents of the buffer. This was also where anomaly-based and signature-based intrusion detection took place.

2. Backend : Another name for the backend is the primary purpose of an intrusion detection system. Its primary purpose is to alert and gather. The sensor's detected events are entered into the database system known as the event repository. The backend then decides how each event should be handled. Critical events are handled by blocking, emails, and displays.

3. Frontend : Command and Control the IDS can be setup, configured and updated from the frontend by the user. All events collected by the backend are presented on the frontend. Thus, the frontend provides a convenient interface through which the user can now manage these logged events. To obtain maximum benefit from an IDS, it has to be fined tune to report only significant events. Hence, the user can fine-tune the detection and response of an IDS through this console. If done with accuracy, the IDS will provides the user with adequately early warning from any intrusion.

The workflow of an intrusion detection system is roughly divided into the following steps:
(1) Information collection - The first of intrusion detection is information collection, which includes the content of network traffic, the status, and behavior of user connection activities .
(2) Signal analysis:- The information collected above is generally analyzed by three technical means: pattern matching, statistical analysis, and completeness analysis. The first two methods are used for real-time intrusion detection, while integrity analysis is used for postmortem analysis .
(3) Real-time recording, alarm, or limited counterattack :- The fundamental task of IDS is to make appropriate responses to intrusions. These responses include detailed log records, real-time alarms, and limited counterattack sources. The only technical methods to identify intrusions are user characteristics, intruder characteristics, and activity-based.

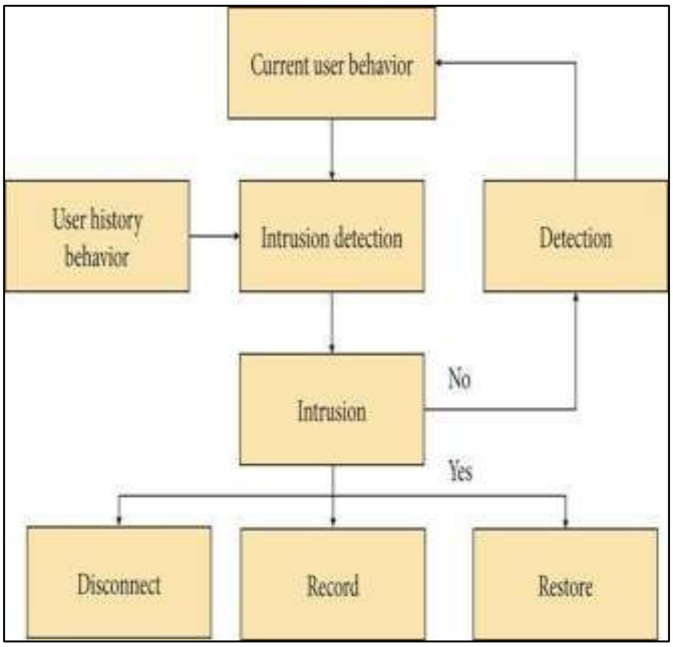

Fig.2 The structure of the intrusion detection system

Tools of Intrusion Detection

An intrusion detection product available today addresses range of organizational security goals. The security tools are as follows:-

1. **SNORT:** Snort is lightweight and open source software. Snort uses a flexible rule-based language to describe the traffic from an IP address; it records the packet in human readable form through protocol analysis, content searching, and various pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behaviour.

2. **OSSEC-HIDS:** OSSEC (open source security) is free open source software. It will run on major operating systems and uses a Client/Server based architecture. OSSEC has the ability to send OS logs to the server for analysis and storage the data. It is used in many powerful log analysis engine, ISPs, universities and data centers Authentication logs, firewalls are monitored and analyzed by HIDS.

3. **KISMET:** It is a guideline for WIDS (Wireless intrusion detection system). WIDS compromises with packet payload and happenings of WIDS. It will find the burglar access point.

IDS Example

The best example of an intrusion detection is **Suricata.**

Suricata is a free, open-source IDS/IPS cybersecurity tool that acts as both an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS). It is used by organizations all around the world to detect cyber threats and monitor networks for suspicious activity.

Suricata's strength lies in its versatility. When tuned correctly, it is a high-performance tool that can handle large volumes of network traffic and generate vast amounts of network traffic data. It is also extremely flexible, offering deep analysis of various protocols and the ability to customize rule sets to fit your organization's specific needs. Because it's an open-source IDS/IPS, Suricata benefits from a large, active community that constantly develops and refines its capabilities.

Put simply, Suricata is a powerful and adaptable tool that provides a robust layer of defense for any organization's network security strategy.

3 .CONCLUSIONS

After implementing firewall technology at the network perimeter, intrusion detection systems (IDS) are quickly taking over for many enterprises. IDS can provide defense against both internal and external intruders by preventing any traffic from passing through the firewall. Nonetheless, it is imperative to always remember the following principles. An IDS deployment and a firewall by themselves cannot provide a highly secure infrastructure if these factors are not connected.

1. Strong identification and authentication: Although intrusion detection systems (IDSs) employ excellent signature analysis techniques to identify intrusions or possible misuse, businesses still need to make sure that they have robust user identity and authentication procedures in place.

2. Not all security issues can be resolved by intrusion detection systems (IDS): IDS do a great job of making sure that intrusion attempts are tracked down and reported. To reduce the risks of invasions, businesses must also implement a process of system testing, personnel training, and the creation of a sound security strategy.

3. An effective security policy cannot be replaced by an IDS: An IDS is one component of a corporate security policy, just like any other solid security and monitoring solution. A clear policy must be adhered to in order to successfully detect intrusions and guarantee that vulnerabilities, intrusions, virus outbreaks, etc. are managed in accordance with corporate security policy directives.

REFERENCES

1. Salvatore Pontarelli, Giuseppe Bianchi, Simone Teofili. Traffic-aware Design of a High Speed FPGA Network Intrusion Detection System. Digital Object Indentifier 10.1109/TC.2012.105, IEEE TRANSACTIONS ONCOMPUTERS.
2. Przemyslaw Kazienko & Piotr Dorosz. Intrusion Detection Systems (IDS) Part I - (network intrusions; attacksymptoms; IDS tasks; and IDS architecture). www.windowsecurity.com › Articles & Tutorials
3. Sailesh Kumar, “Survey of Current Network IntrusionDetection Techniques”, available athttp://www.cse.wustl.edu/~jain/cse571-07/ftp/ids.pdf.
4. Srilatha Chebrolu, Ajith Abrahama,,*, Johnson P. Thomas,Feature deduction and ensemble design of intrusion detection systems,Elsevier Ltd.doi:10.1016/j.cose.2004.09.008
5. http://www.intechopen.com/download/get/type/pdfs/id/86 9 5.
6. Martin Roesch , “Snort – Lightweight Intrusion Detectionfor Networks”, © 1999 by The USENIX Association.
7. The Snort Project, Snort User Manual 2.9.5,May 29, 2013,Copyright 1998-2003Martin Roesch, Copyright 2001- 2003 Chris Green, Copyright 2003-2013 Sourcefire, Inc.
8. Chapter 3, Working With Snort Rules, Pearson Education Inc.
9. B. Daya ,“Network Security: History, Importance, andFuture ,”University of Florida Department of Electrical and Computer Engineering,2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf
10. Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.
11. J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library,2000.