Intrusion Detection Systems: Categories, Attack Detection and Response

By Cedric Katsaumire

***Abstract*— Cybercriminals' increasing expertise makes it very difficult to detect intrusions with any degree of precision. Any organisation that does not successfully prevent invasions may face significant repercussions. This study provides an overview of a wide variety of intrusion detection approaches, some of which are Signature-based IDS and Anomaly-based IDS. The report reviews IDS' history, the dangers of intrusions, various detection methods, the challenges associated with managing IDSs, tools and intrusion prevention systems, performance evaluation and intrusion prevention systems.**

Keywords—cyber security, attack detection, IDS response, intrusion detection system.

I. INTRODUCTION

One of the most critical challenges we face in this age of digital technology, which features an abundance of related technologies, is protecting the confidentiality, integrity, and availability of personal information and the data belonging to businesses and other organisations. Due to the rapid advancement of technology, significant security threats are now to be overcome. Cyber-attacks are not the same; identifying and stopping them before they inflict significant damage can be difficult.

An intrusion occurs when a hacker accesses a system by stealing its password, impersonating, eavesdropping, or injecting malicious code [1]. It can also be done by people inside the network who have the potential to cause damage to a system by taking advantage of security flaws in the system, which could result in the system being compromised. Intrusion detection systems (IDS) play an essential role in computer security. An intrusion detection system can be defined as software or hardware that monitors network traffic and system activities for suspicious behaviour such as penetrations, policy violations, or unauthorised access by hackers. [2] They either scan for indicators of recognised attacks or deviations from the usual activity and alerts the security administration when such action is discovered. IDSs are also capable of monitoring the functionality of critical infrastructures such as routers, servers, and firewalls, which are required to identify and prevent cyber-attacks.

II. BACKGROUND OF IDS

In 1980, James Anderson published the research "How to use accounting audit files to detect unauthorised access", which is believed to have paved the way for intrusion detection systems. In his study, he discussed techniques for enhancing computer security. This study's first task was identifying known threats before designing an IDS. It was necessary to comprehend the various types of threats and attacks that could be launched against computers and how to identify them. Between 1984 and 1986, computer scientists Dorothy Denning, Peter Neuman, and several researchers became the first people to design an Intrusion Detection Expert System (IDES). [3]. They pointed out that even though their design could not identify every single breach, it was developed to detect most intrusions and make it extremely difficult to avoid detection. [4]. By 1992, the IDES model was fully functional and could be applied to heterogeneous systems [18]. The model was divided into four main parts, Realm Interface, Statistical Anomaly Detector, Expert System Anomaly Detector, and the User Interface, each implemented independently. The objective was to deliver intrusion detection as near to real-time as feasible, which was crucial but challenging. The Realm Interface had two parts: the realm client and the actual server, responsible for gathering the target systems events, removing any real-private data, and reserving it when required. Current IDS systems use anomaly behaviour and reputation-based detection to identify threats. They may use methods of machine learning to spot risks faster.

III. RISK OF INTRUSION

Some attacks are passive, while others are active. In passive attacks, hackers gain access to networks without permission so they can scan for open ports and other weaknesses, but no change is made to the data collected or the way the system works.[5] In an active attack, the attacker takes advantage of the information acquired during a passive attack to gain control over a computer or network [19]. In addition, the attacker tries to change, destroy, or encrypt confidential data. Some other risks of intrusion are:

- Information theft- when the hacker obtains confidential information that can be used, sold, or used for other purposes.
- Identity theft- a form of information theft where information is stolen to take over someone's identity. Attackers can use this information to apply for credit or make unauthorised purchases.
- Data loss or manipulation-this is when attackers break into a system to destroy or alter records.
- Disruption of service - when legitimate users are prevented from accessing benefits they are entitled to. An example would be a Denial of Service (DoS) attack.

IV. INTRUSION DETECTION TECHNOLOGIES

The purpose of intrusion detection technologies is to detect and report potential security breaches or malicious activities

within a computer or network system. These technologies can be utilised in numerous ways, such as.

1. Network-Based Intrusion System (NIDS)- sensors are deployed at strategic points within the network level to analyse individual inbound and outbound packets from all the devices on the network for malicious activity.[6] Once a threat or attack is identified, an alert is sent to the network administrator.[7] They can be hardware or software-based and often possess two network interfaces, one for listening and the other for control and reporting. A good location where a NIDS can be placed would be the demilitarised zone or DMZ, where all traffic traverses.
2. Host-Based Intrusion Detection System (HIDS)—an application that monitors a computer or network for suspicious activity, including external invasions and internal resource or data misuse. [8] HIDS runs on all servers, endpoints, and devices in the network that have access to both the internet and the internal network. HIDS collects and analyses system data such as system calls, application logs, and other system activities to detect malicious activities [20]. Intrusions can be seen by identifying the order of anomalies in the system. They may be able to detect unusual network packets that a NIDS failed to detect because they have direct access to and control over the system processes that are targets of attacks.
3. Network Behavioural Analysis (NBA)- A network behavioural analysis system analyses network traffic or network traffic statistics to detect abnormal traffic flows, such as DDoS attacks, malware, and policy violations. NBA are like NIDS sensors; however, NIDS sensors intercept packets to monitor network activity in one or more network segments. [9] However, NBA sensors employ network flow information from routers and other devices. To detect attacks, NBA systems must collect information such as IP addresses, protocols, and TCP and UDP ports.
4. Wireless IDS- a security tool used to monitor a wireless network for potential security threats or anomalies. It cannot recognise suspicious activity occurring in the application layer or in the top layer network protocols such as TCP or UDP that network traffic traverses through. Information gathering, logging, and detection are the subheadings under which they are categorised. They begin by evaluating IEEE 802.11a and the communication protocols to detect attacks on the WLAN protocol level; nonetheless, they are vulnerable to denial-of-service attacks and other physical attacks.
5. Stateful Protocol Analysis- Analysis of stateful protocols involves comparing predefined profiles of commonly recognised expected protocol activities for each protocol state with actual events to identify deviations from the preset profiles [21]. This step must be taken to determine whether a protocol has been broken.

V. Methods of Detection

Several distinct ways might be employed while utilising an IDS. This category includes methods such as Network-Based Intrusion Detection Systems (NIDS) and Host-Based Intrusion Detection Systems, among others. Intrusion detection systems can also be classified by the sort of detection they conduct, which might be Anomaly-based, Signature-based, or Specification-based.

Signature-based IDS and patterns of normal and anomalous behaviours are developed using data from the history of attacks carried out by hackers and authorised users in the network. An example of a signature-based IDS would be SNORT.[10] SNORT is an open-source Network Intrusion Detection System that is free of cost and requires Windows, Ubuntu, or Wireshark. It analyses real-time traffic in the network and can detect different attacks with low false positives [22]. However, it can be easily fooled by simply changing the ways the attacks are made, and a more advanced IDS signature database can also require high CPU usage.

Anomaly-based detection aims to discover anomalies by comparing the acquired traffic to the typical network traffic patterns. Due to the variety of user behaviours, network traffic, and online applications and technologies, it is difficult to determine the design of network traffic. New actions that deviate from the previously established profile and are misidentified as attacks result in a high percentage of false alarms. Anomaly-based detection consists of three main phases: data collection, in which network traffic data is collected; training, in which the profile of a network is constructed; and testing and detection, in which the network model is created and compared to the traffic collected in the data collection phase.

Specification-based IDS uses system specification, which outlines the system's expected behaviour. Any deflection from the established system behaviour is recognised as a security violation. Although Specification-based IDS can be combined with Anomaly-based IDS, it is a better approach because it does not generate false alarms when unusual behaviour is detected.

Hybrid Intrusion Detection methods combine signature-based and anomaly-based systems. They feature two detection modules, one of which is responsible for identifying well-known assaults using signatures [23]. At the same time, the other can recognise and learn both normal and malicious patterns.

Heuristic-based IDS- Heuristic-based intrusion detection systems (IDS) use rules or algorithms to detect malicious network activity. Based on security experts' knowledge and experience, the algorithms highlight abnormal activities that may signal an attempted breach.[11]

Protocol-based IDS- Analyses network traffic for anomalies or deviations from standard protocol behaviour. Protocols are the rules and specifications that govern how networked devices communicate with one another. They can identify malware and other protocol-based attacks or suspicious activities that other IDS systems may miss.

Application Protocol-Based IDS- Analyses application-layer network traffic. Most network programmes, such as web browsers and email clients, run under the OSI model's

uppermost tier, the application layer. It helps detect web-based assaults and email-based phishing scams that exploit application weaknesses. The table below shows a brief comparison between Signature-based IDS and Anomaly-based IDS.

Table 1. Signature-based vs Anomaly-based

	Signature-based	Anomaly-based
Low false alarm	Yes	No
High detection rate	Yes	No
Attack anticipation	No	Yes
Ability to detect unknown attacks	No	Yes
Need a training dataset	No	Yes

VI. Challenges of Managing an IDS

In IDS, each activity under monitoring has four potential states: true positive, true negative, false positive, and false negative. [12]. A true positive state occurs when the IDS identifies an activity as an attack and the activity is, in fact, an attack. The true negative occurs when an IDS correctly identifies the activity as acceptable. Both states are sufficient since the IDS is operating as intended. However, that is not the case with false positives and false negatives. A false positive occurs when the IDS identifies specific activity as an attack even though the activity is acceptable behaviour. Identifying false positives is a significant issue as most cases, false positives are more frequent than real threats. Although an IDS can be configured to reduce the number of false positives, network engineers might still have to respond to them, and if they do not, actual attacks may slip past the detection [24]. In a false negative state, the IDS identifies activity to be normal behaviour when it is, in fact, an attack. This is a significant issue as security engineers will not know that an attack occurred until the system has suffered severe damage. Some of the challenges are:

1. Lack of visibility- There is a possibility that an IDS will only provide complete visibility into some components of a network or system. This could cause the organisation's cybersecurity weaknesses, making it easier for threats to go undetected.[13]
2. Difficulty keeping up with new threats- The threat landscape is always evolving, and new threats are constantly surfacing. Due to this, it can be difficult for an IDS to stay current, and it might not be able to detect new threats or threats that were not previously identified.
3. Limited effectiveness- IDS systems are not guaranteed against security threats and can only offer limited protection. This implies that organisations may need to deploy additional security measures, such as firewalls and access restrictions, to achieve robust cybersecurity.
4. Resource constraints- A considerable amount of time and resources, including employees, hardware, and software, may be required to manage an IDS. This can be difficult for organisations with restricted resources.
5. Managing large volumes of data- Managing an IDS's vast amounts of data is another challenge. Network traffic data from IDS systems is challenging to evaluate and interpret. This makes it harder to recognise all security concerns and increases the risk of missing important alerts.
6. Ensuring compliance- Many organisations must follow the rules and industry standards that require them to put in place and keep up IDS systems and other security controls. If you don't manage an IDS well, you might not follow the rules, which could lead to legal or regulatory penalties.

VII. Performance Evaluation

Determining how successful an intrusion detection system (IDS) is at identifying and responding to security threats is known as the performance evaluation of an IDS. This can include a variety of metrics, such as the number of attacks detected, the accuracy of the IDS in identifying intrusions, the speed with which it can respond to threats, and the overall impact of the IDS on the performance of the system or network that it is protecting.

Several metrics have been designed to measure the effectiveness of an IDS. These metrics can be divided into three classes: threshold, ranking and probability. Threshold metrics include classification rate (CR), F-measure (FM) and Cost per example (CPE). In contrast, ranking rates include False Positive Rate (FPR), Detection Rate (DR), Precision (PR), Area under ROC curve (AUC) and Intrusion Detection Capability (CID). Lastly, probability metrics include root mean square error (RMSE) [14].

An example would be the Confusion matrix. A confusion matrix is a table used to assess the performance of a classification model like IDS [25]. It is referred to as a confusion matrix because it reveals how the model is confused while making predictions. It has four quadrants, True Positives (TP), False Positives (FP), True Negatives (TN) and False Negatives). Accuracy can be calculated as (TP+TN)/(TP+TN+FP+FN), precision is calculated as TP/(TP+FP), and recall is calculated as TP/(TP+FN) [15].

VIII. Intrusion Detection Response

Reacting to an alert generated by an intrusion detection system is referred to as an "intrusion detection response." Depending on the nature of the threat that was identified and the degree of its severity, it may require a variety of different responses. Some common Intrusion Detection Responses include:

- Investigating the alarm to ascertain the reason for it and the potential consequences of the threat.
- Isolating the compromised computer system or network to stop the spread of the danger.
- Taking remedial action to reduce the severity of the threat, such as blocking malicious traffic.

- Notifying relevant parties such as the system owner, law enforcement or other security teams.
- Conducting a post-incident review to determine what actions can be taken to improve overall security.

IX. Intrusion Prevention Systems

An Intrusion Prevention System (IPS) monitors a network for potential attacks and coordinates appropriate responses to identified threats. Although, like IDSs, they can be set up in a way that eliminates the need for a system administrator to deal with potential attacks [26]. An IDS merely issues a warning when a potential threat is detected, but it does not stop the action. IPSs are often placed between a company's firewall and the rest of its network, and they may be able to prevent suspicious traffic from reaching the remainder of the network. [16]. Since they respond in real-time, IPSs can actively capture intruders that firewalls and antivirus software miss. IPSs can also be configured with organisation-specific security policies to give security controls unique to the organisation using them. An example of an IPS would be Cisco Secure Firewall by Cisco.

X. Conclusion

Protecting computer systems with advanced IDS that can identify contemporary dangers is becoming an increasingly pressing concern. This research provided an overview of IDS approaches, kinds, and technologies, along with some of the benefits and disadvantages associated with each. In conclusion, a good IDS should protect in real-time against a wide variety of security threats, with a high degree of accuracy and the ability to be customised. It should be simple to interface with other security systems. [17] The course that IDS will take in the future is difficult to foresee, but they will likely continue to develop and advance in response to the ever-shifting nature of the threats they face. It may be speculated that IDS of the future will use more advanced technologies like artificial intelligence (AI) and machine learning (ML) to provide more robust and more thorough protection against a wider variety of security risks.

XI. REFERENCES

[1] Thakkar A and Lohiya R. (2021) A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions in press.

[2] Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman (2019) Survey of intrusion detection systems: techniques, datasets and challenges.

[3] Abdulhamid, S. Kabir, I. Ghafir and C. Lei, "Dependability of the Internet of Things: Current Status and Challenges," International Conference on Electrical, Computer, Communications and Mechatronics Engineering, Maldives, Maldives, 2022.

[4] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[5] Teresa Lunt, Ann Tamaru and Ramesh Jagannathan (1992) A Real-Time Intrusion-Detection Expert System

[6] Jeffrey R. Yost (2010) The March of IDES: Early History of Intrusion-Detection Expert Systems.

[7] Bijone, M. (2016). A survey on a secure network: intrusion detection & prevention approaches. American Journal of Information Systems

[8] Merve Ozkan, Okay Refik, Samet Ömer Aslan (2021) A Comprehensive Systematic Literature Review on Intrusion Detection Systems.

[9] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[10] Nuno Oliveira, Isabel Praca, Eva Maia and Orlando Sousa (2021) Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems

[11] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018

[12] Shubham Sharma, Parma Nand and Pankaj Sharma (2022) Intrusion Detection and Prevention Systems Using Snort

[13] Yan-Jing Hu and Xu An Wang (2016) Hybrid Analysis for Mining Network Protocol's Hidden Behavior.

[14] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[15] Abdul Waleed, Abdul Fareed and Jamali Ammar Masood (2022) Which open-source IDS? Snort, Suricata or Zeek

[16] Swapnil Umbarkar and Sanyam Shukla (2018) Analysis of Heuristic-based Feature Reduction method in Intrusion Detection System.

[17] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[18] Kirsten, Wichers, Jkurucar, kingthorin (2021) Intrusion Detection.

[19] Akash Garg and Prachi Maheshwari (2016) A hybrid intrusion detection system: A review

[20] Dr Gulshan Kumar Ahuja (2015) Evaluation Metrics for Intrusion Detection Systems.

[21] M. Lefoane, I. Ghafir, S. Kabir and I. U. Awan, "Multi-stage Attack Detection: Emerging Challenges for Wireless Networks," International Conference on Smart Applications, Communications and Networking, Palapye, Botswana, 2022.

[22] Hanafi (2022) An Intrusion Detection System (IDS) using Dimensional Reduction Based on Statistical and SDAE to Enhance SVM in Classification Tasks.

[23] Asmaa Shaker Ashoor and Sharad Gore (2011) Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

[24] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[25] D. Nethra Pingala Suthishni and K. Senthil Kumar (2022) A Review on Machine Learning based Security Approaches in Intrusion Detection Systems.

[26] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.