Intrusion Detection Systems: Categories, Attack Detection and Response

Adilah Nisar
Faculty of Engineering and Informatics
Department of Computer Science
University of Bradford
Bradford, England, United Kingdom
anisar5@bradford.ac.uk

***Abstract*— In today's day and age the use of technology has risen and to make sure that data is kept safe and secure, many people and institutes across the world have implemented intrusion detection systems into their networks to help prevent cyber-attack from intercepting their computer networks resulting in data and personal information being stolen from them. However, it has been seen that cyber attackers have found ways round IDS by making changes to the packet contents to bypass these systems. This report will critically analyse intrusion detection systems, how they are used, and how they detect and respond to attacks as well as how new attacks can be used against IDSs. This paper will discuss the different methodologies available to combat intrusions to our networks as well as the changes that can be made to improve systems and techniques.**

Keywords*— *IDS, IPS, Intrusion, HIDS, NIDS, Anomaly, Heuristic, Malicious, Audit.

I. Introduction

Due to the advancements in technology and the internet, the rise in attacks have risen exponentially, causing risk to our data and personal information online. Intrusion detection systems are devices that are used to strengthen our networks by monitoring them to prevent malicious activity or policy violations. It detects such activity and reports it to management systems where they can be investigated, and appropriate action can be taken, for example, blocking the port or IP address. Another form of intrusion detection system that not only detects malicious activity but blocks it from entering the system are called Intrusion Prevention systems [20]. The growth of wireless networks has added to the increase of attacks making such devices more important than ever before in our networks because it is easier for intrusions to occur on wireless networks.

This paper will introduce the different aspects of intrusion detection systems by discussing the background and history of detection systems. Followed by the different methodologies in and classifications of IDSs and how they detect intrusions, along with some analysis of some proposed methods. Then followed by a comparison between IDS and IPSs and a summary on attack response. And finally, conclusion will sum up the paper and give some ideas of what can be done for future work.

II. Background

The importance of intrusion detection systems (IDS) in our networks is to prevent misuse of data. IDSs were invented in the 1980's, starting off with James Anderson's paper for the government insisting that it was valuable for the creation of a system that could track unauthorized access and misuse of user behaviors. This came at a time when the use of computers and data sharing across the internet was at a rise. However, there was no such security to prevent the misuse and interception of data on networks. Prior to the 1980's there was already an intrusion detection system however it was a manual system that took up a large amount of time as it consisted of huge audit logs being printed on large sheets of paper which were physically checked through to find anomalies in the data. This resulted in many attacks being let through the system as well as detecting the attacks too late. Anderson's paper was the first idea of a system that could monitor networks for misuse [1].

By 1983 SRI international and Dr. Dorothy Dennings, had already began developments on an intrusion detection system, a project given to them to check government computers and create user profiles based on their activities and behaviors. The first model was complete by 1984 named Intrusion Detection Expert System (IDES), which created the foundations of IDS technology for the future. From the report created by Dr. Dorothy Dennings, the aim of IDES was to monitor the system activity and record it into audit records [23]. It then analyzed the data from the records and created new, or updated profiles with the new data. It would also detect if an activity of a user were abnormal against their user profiles and if any abnormality were detected, it would alert a security officer of an intrusion [5].

After the initial idea of intrusion detection system was created, detecting intrusions based on anomalous results from user profiles, the development of a system that was able to detect and respond to such attacks began. This would help reduce the time and resources used to respond to an intrusion once a security officer was alerted. Intrusion prevention systems (IPS) are created in conjunction with IDS which were able to detect and respond to intrusions itself, rather than just alerting the security officer. This system was more convenient as intrusions are dealt with instantly without delay, which has also resulted in a reduction of interceptions to the network.

III. Attack Detection Methodologies

There are many categories of intrusion detection systems used daily to prevent intrusions from occurring. Two commonly used methods:

A. Signiture-based Detection (SD)

Detect attacks by looking at the patterns and signatures in network traffic. These patterns are encoded regularly into a database from the network traffic which are then used to recognize user behaviors to detect anomalies in traffic and detect an attack. False positives are low if the attacks have been detected before and this system is easy to use and generally accurate. However, there is one problem with this system, it requires the signatures or patterns of previous attacks to detect them again, indicating it does not detect new or unknown attacks [13]. This can be a problem when attackers manipulate the contents of a packet as they become undetectable by the SD model.

A study using SNORT (security tool) by Kumar and Sangwan [13], shows that when a packet is sent from one system to another, before it reaches the destination, the SD model checks the packet for any malicious content. It arranges the packet for the detection engine to check if it has been corrupted, at this stage it can also create alerts if anomalies are found. SD will check the packet against all patterns in the DARPA dataset and if detected as malicious, it will be discarded otherwise sent to the destination system. This system can analyse network traffic in real-time and was created to help new users of SNORT understand the use of it [24,25]. When using this system, the database needs to be updated regularly to include new patterns and signatures that have been used during new attacks. Due to this, when there is a build-up of traffic on the networks it can sometimes drop packets containing malicious content resulting in letting attacks through.

Uddin [22] created a signature-based Multi-layer IDS that was able to detect intrusions with high rates of success and was able to reduce the number of packets being dropped by 6.77 times. This was done by creating a mechanism that regularly updated the small databases it uses automatically.

B. Anomaly/Heuristic-based Detection (AD)

AD does not entirely rely on patterns in network traffic to detect attacks but relies on the classification of the network to normal and anomalous. It is used for detecting both computer and network intrusions and violations by monitoring the systems activity and then classifying the attack as either normal or anomalous based on if the attack matches the behavior of an authorized users and so would be classed as normal. If the attack is out of the ordinary and has not been recorded before it would be classed as an anomaly [18].

Many developers and researchers have worked on improving accuracy and reducing the number of false positive for example Dwivedi [8] created a new intelligence IDS, “Passban”. It uses a combination of feature selection and adaptive grasshopper optimization algorithms called EFSAGOA. This algorithm was evaluated on data gathered on intrusions from ISCX 2012. This proposal was presented with high detection and accuracy rates of above 99% and a reduced false detection rate of 0.067. It was used to detect intrusions from IoT systems and the internet.

With anomaly-based detection, it works great on large systems because it can effectively detect new vulnerabilities even if they are sudden [26]. However, this detection system is high in false positives resulting in some incorrect and innocent recognition of attacks to the network, meaning it prevents alerts being triggered at the right time. It is important that alarms raised by this model are accurate to determine attacks on networks.

IV. Classification Of Intrusion Detection Systems

There are three main types of Intrusion Detection Systems:

A. Host-based Intrusion Detection System (HIDS)

This type of IDS focuses on the host system only. It analyses auditing data and log from operating systems and incoming and outgoing traffic from the host. By analyzing log files, it can detect misuse for example, if logins have occurred during unusual hours, login failures, modification to critical file systems, files that are important for the functionality of the operating system, and access controls violated [7].

HIDS can create detailed and accurate signatures which can be used to detect intrusions on the host system. It also has low false positive detections due to the accuracy of the signatures it creates [27]. With the correct implementation of HIDS, it can detect malicious content within encrypted packets that cannot be detected with NIDS, this is due the ability of it being tunable to decrypt and analyse packets.

The disadvantage of HIDS is the cost of it as it must be installed on every host system and the maintenance of the system can become very costly to organizations to maintain. Apart from this, HIDS are targets of denial-of-service attacks (DoS).
According to [16], the use of more than one detection technique can improve its accuracy in detection reducing the number of false positive and negative detections. This is because each technique will monitor different aspects of the host and allow the HIDS to collect more data on the host to provide a more extensive profile of activities and host.

B. Network Intrusion Detection System (NIDS)

Analyse data from network traffic to identify malicious activity taking place [6]. Such systems are implemented as devices between the internet and the intranet of a network enterprise [14]. The use of such device in this position on a network helps in detecting intrusions to the system immediately and in many instances, this type on IDS has been missed by attackers. NIDS can collect data and create logs of hosts and common activities that take place on networks to use the different methodologies to detect

intrusions. However, with the implementation of such device on the network, it can slow the system down as well as not being able to detect packets containing malicious data if it has been encrypted [28]. Apart from this, NIDS have been seen as not very successful in detecting attacks that occur from within an organization or network. This can be critical because according to IBM in 2016, 60% of all attacks were carried out from within the organizations. This is because it cannot see traffic that does not cross it so malicious traffic in the internal network will not be detected. Another disadvantage commonly reported by NIDSs are the amount of false negative and false positive detections. False negatives are detections that have been wrongly stated as normal where indeed they posed as a threat due to being an attack. False positives are non-malicious attacks that have been detected as a threat to the network but was an innocent anomaly that was misclassified as an intrusion [10].

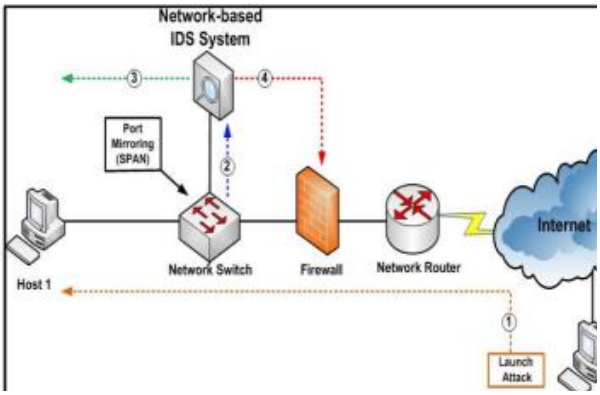

Figure 1: Network-Based Intrusion Detection [15]

C. *Hybrid-based IDS*

This type of IDS is a combination of both signature and anomaly-based IDS. It uses the advantages from both these categories to overcome the weaknesses of SIDS and AIDS and best detect intrusions on hosts and networks. For example, it used AIDS to detect the unknown attacks while it uses SIDS to detect the known attacks with the stored signatures. Hybrid-based IDS can increase the number of detections and the number of false positives it significantly decreased when SIDS is used at the first stage of detection. Apart from this, this type of IDS can monitor both hosts and the networks which can increase security on networks making data more secure and less likely to be attacked or stolen [12].

This type of IDS can be used with a reduction of false positive and negative detections of intrusions. Smys [20] proposed a Hybrid Convolutional Neural Network (HCNN) model against Recurrent Neural Network (RNN) model to compare the accuracy and rate of false positive it detected. They split the data into 70% training and 30% test set. The proposed IDS system combined both long and short-term memory processes.

From the finding it was visible that their proposed HCNN model attained better efficiency results for the accuracy than the RNN model, which can be seen in Figure 2.

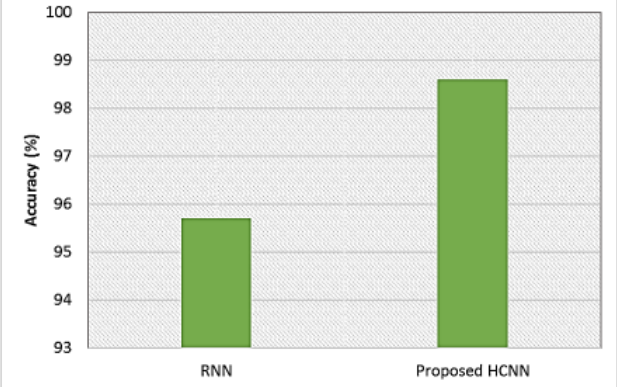

Figure 2-Accuracy comparison [20]

V. IDS vs. IPS

While IDS only detect intrusions on a network and refer it to the management team, intrusion prevention systems not only detect intrusions but take certain actions to prevent them for example block them from passing through the network [4]. IDS is a great tool that can quickly detect attacks to a network, which has been challenged with the development of IPS that can use this as well as prevent the attack making it a more commonly used security system on our networks today.

Key functionalities of an IPS [4]:

- Able to detect and prevent attacks
- Stops the attack entering a network
- Changes the security environment

The main difference between IPS and IDS is that IDS can be abused which can affect its performance. Meanwhile IPS allows the management team to create rules that it can follow to block an attack when faced with one [21].

TABLE 1. DIFFRENCE BETWEEN IDS AND IPS

Intrusion Detection System	**Intrusion Prevention System**
Visibility tool	Control tool
Only detects an intrusion	Detects and prevents an intrusion
Requires involvement from IT management teams once an attack has been detected.	Does not require any involvement from the IT teams to deal with an attack.
IDS are not directly in line with networks which only allow them to detect attacks incoming on a network.	IPS are implemented inline networks which allow them to react to intrusions directly as they pass through them.

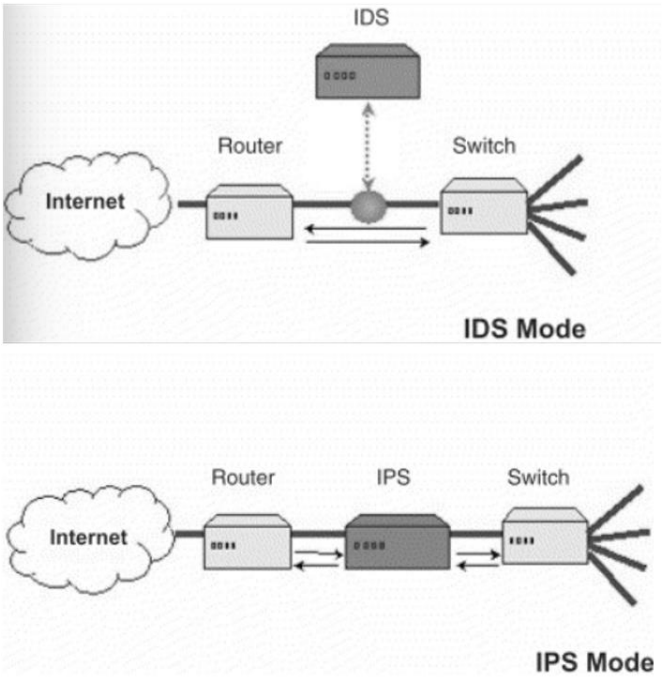

Figure 3 - Offline vs. In line placement [17].

VI. Similarities Between IDS And IPS

They are both able to detect intrusions on host and networks which is essential for network security. They also both adopt the ability to secure networks using the signature based and anomaly-based models, as well as a hybrid methodology which combines both these models to enable the best and fastest way of detecting intrusions.
Intrusion detection and prevention systems allow organizations to have an automated security system to protect their data on their network by using either hardware or software-based approaches [30]. Regulations can also be set for both these devices, which are then constantly monitored to prevent malicious activity within organizations that are recorded in logs which can be used in an instance where a policy regulation has been breached.

This system can track and prevent policy violations automatically allowing security teams more time to focus on real security aspects within an organization. For example, working in remote environments has made it more difficult for organizations to impose policies to ensure proper business operations that are legal, social, ethical, and professional. [2]. Intrusion detection and prevention systems together, can create a safer network environment within an organization as well as prevent external attacks to the network which can cause a risk to cyber security.

VII. Attack Response

Intrusion detection systems respond to attacks by reporting them to security teams that can then use the information provided by the IDS to investigate and block the intrusion on the network. The first thing after an intrusion detection system has raised an alarm, the security team will need to verify that the detection is not a false positive alarm. This is because as seen above, some methodologies raise alarms on intrusions that can be innocent [29]. An anomaly can sometimes be detected due to a spike on network activity for example an organization has had an event that has caused a spike to the number of visitors on their website. This is not malicious traffic to their network; however, it is detected by IDS raising an alarm.

VIII. Conclusion

To conclude the review of Intrusion Detection Systems, there has been a lot of work done to reduce the number of false positive and negatives detected and to find a way to stop every attack. There is more work that is needed to create a more sustainable system that can detect all intrusions and deal with them accordingly. From the research, it was found that the accuracy of IDSs are improving all the time and false alarms are being reduced considerably. This paper goes through some of the background on IDSs and has analyzed some of the methodologies that are used to detect intrusions on our systems, for example Anomaly-Based detection, which monitors computer networks to detect anomalous results. The paper also discusses how different techniques have been used to improve them, like using certain algorithms to reduce the number of false positive detections in Anomaly-Based detection. The paper has also discussed some of the similarities and differences between IDSs and IPSs.

For future work the developers should work on improving IDSs so that they can detect packets that have been manipulated. There are more benefits of the implementation of both intrusion detection and prevention systems on networks hand in hand to provide the best shield against intrusions with higher accuracy results than a system using a single methodology.

References

[1] Ashoor, A.S. and Gore, S., 2011. “Importance of intrusion detection system (IDS)”, International Journal of Scientific and Engineering Research, 2(1), pp.1-4.

[2] Ashtari, H., 2022, “Intrusion Detection System vs. Intrusion Prevention System: Key Differences and Similarities”, Spiceworks, Network Security, Technical Writer.

[3] Barracuda, 2022, “Intrusion Detection System”, “unpublished” [Online], Available at: https://www.barracuda.com/glossary/intrusion-detection-system

[4] Chakraborty, N., 2013. “Intrusion detection system and intrusion prevention system: A comparative study”. International Journal of Computing and Business Research (IJCBR), 4(2), pp.1-8.

[5] Denning, D., and Neumann, P.G., 1985. “Requirements and model for IDES-a real-time intrusion-detection expert system” (Vol. 8). Menlo Park: SRI International.

[6] I. Ghafir, M. Husak and V. Prenosil, “A Survey on Intrusion Detection and Prevention Systems,” IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[7] Dr. Abid Hussain, 2017, “Use of Firewall and Ids to Detect and Prevent Network Attacks”, International Journal of Technical Research & Science, pp. 291-292.

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

[9] Dr. Natarajan Meghanathan, “Firewalls and IDS,” Associate Professor of Computer Science Jackson State University, pp.21-34

[10] Dwivedi, S., Vardhan, M., Tripathi, S. and Shukla, A.K., 2020. Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection. Evolutionary Intelligence, 13(1), pp.103-117.

[11] I. Ghafir, J. Svoboda and V. Prenosil, “Tor-based malware and Tor connection detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[12] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung, 2013, “Intrusion detection system: A comprehensive review”, Journal of Network and Computer Applications, Volume 36, Issue 1, Pages 16-24.

[13] I. Ghafir, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, S. Lambotharan, B. Assadhan and H. Binsalleeh, "A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection," in IEEE Access, vol. 6, pp. 40008-40023, 2018

[14] J. R. Yost, Oct.-Dec. 2016, "The March of IDES: Early History of Intrusion-Detection Expert Systems," in IEEE Annals of the History of Computing, vol. 38, no. 4, pp. 42-54.

[15] I. Ghafir and V. Prenosil, “Advanced Persistent Threat Attack Detection: An Overview,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 4(4), pp. 50-54, 2014.

[16] Khraisat, Ansam & Gondal, Iqbal & Vamplew, Peter & Kamruzzaman, Joarder & Alazab, Ammar, 2020, “Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine”. Electronics. Pp:1-4

[17] Kumar, V. and Sangwan, O.P., 2012. “Signature based intrusion detection system using SNORT.” International Journal of Computer Applications & Information Technology, 1(3), pp.35-41.

[18] Liu, M., Xue, Z., Xu, X., Zhong, C. and Chen, J., 2018. “Host-based intrusion detection system with system calls: Review and future trends.” ACM Computing Surveys (CSUR), 51(5), pp.3-4.

[19] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, “Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat.” International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[20] Othman, S.M., Alsohybe, N.T., Ba-Alwi, F.M. and Zahary, A.T., 2018. “Survey on intrusion detection system types.” International Journal of Cyber-Security and Digital Forensics, 7(4), pp.446-457. (Dasgupta & González, 2001)

[21] Ozkan-Okay, M., Samet, R., Aslan, Ö. and Gupta, D., 2021. A Comprehensive Systematic Literature Review on Intrusion Detection Systems. IEEE Access.

[22] I. Ghafir and V. Prenosil, “DNS query failure and algorithmically generated domain-flux detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[23] Papadaki M, Furnell S, 2004, “IDS or IPS: what is best? Network Security”, Volume 2004, Issue 7, pp.16

[24] R. Samrin and D. Vasumathi, 2017, "Review on anomaly-based network intrusion detection system," 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), pp. 141-147.

[25] Stefan Axelsson, 2002, “Research in Intrusion-Detection Systems:”, Research publication pp. 3-5.

[26] I. Ghafir and V. Prenosil, “DNS traffic analysis for malicious domains detection,” International Conference on Signal Processing and Integrated networks. Noida, India: pp. 613 - 618, 2015.

[27] Syms, S, Basar, A and Wang, H, 2020, “Hybrid Intrusion Detection System for Internet of Things” (IoT). Journal of ISMAC, 2(04), pp.190

[28] Thurman, M (2005) “Making the ove from IDS to IPS. Coumputerworld”, 39(44), 34.

[29] Uddin, M, Rahman, A.A, Uddin, N., Memon, J., Alsaqour, R.A., and Kazi S., 2013. Signiture-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents. Int. J. Netw. Secur., 15(2), pp.97-105.

[30] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, “An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes,” International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.