A Review of Intrusion Detection Systems

Hawkar Kh. Shaikha[1], Wafaa Mustafa Abduallah[2]

[1]Department of Computer Science, Faculty of Science, Zakho University, Duhok, Kurdistan Region – Iraq
[2]Department of Computer Science and Information Technology, College of Computer Science & Information Technology, Nawroz University, Duhok, Iraq

ABSTRACT

The transformation of vast amount of information through the network channels appeared widely from one site to another and these information may be disclosed to the third party or the attackers. Thus, the protection process of transformed information is a complex process that can be established through the Intrusion Detection System (IDS). Concealment and unity of information are the most important issues achieved through the intrusion detection system. The process of intrusion detection can be used with wireless or wired networks via making use of hardware or software techniques. Consequently, this caused to have lots of new techniques for IDS in various environments and different levels of network. Unfortunately, most of these techniques do not implemented together for increasing the security of the network. This leaded us to provide a review of the recent papers including a general view of intrusion detection in various environments through the networking and using various techniques. As a result, the most important intend for this paper is to embrace the most new progressions in this region. This may help the researchers to have a general knowledge on different techniques for protection through IDS and various types of intrusion and its detection techniques.

KEYWORDS: Intrusion Detection System, Network Security, Anomaly Based Detection, Signature Based Detection.

1. INTRODUCTION

In today's word, people are addicted widely on using internet and they rely on networks for their daily issues, this makes attackers to be more dapper through using various devices and illusions to obtrusive and damage networks between various sites. This was a good factor for relying on Intrusion Detection system to distinguish and avoid the entire system and data packets from assailants and interlopers. Intrusion is a collection of spiteful actions that attempt to attack and access data sets and to damage network systems. In addition, the process of collecting and detecting intrusions that associated with knowledge through the monitoring process and then investigating and examining gathered data is called "Intrusion Detection system". Moreover, to make a decision on any system that is inquisitive or not in relation to user actions and activities [1]. Essentially, two main various kinds of intrusion detection systems can be determined which are:

Academic Journal of Nawroz University (AJNU)
Volume 6, No 3(2017), 5 pages
Received 1 May 2017; Accepted 27 August 2017
Regular research paper: Published 29 August 2017
Corresponding author's e-mail: heevy9@yahoo.com

contrast, the ABS systems depend on statistical style for illustrating the regular network traffics; it compares any new action or activity with its normal style for detecting any irregular behavior that deflects from the original style. The ABS can detect new attacks immediately after taking place in contrast to SBS. In spite of that, ABS dissimilarly to SBS; it needs a training phase of common attacks [2]. Table 1 illustrates the comparison between the two main systems. The intrusion detection system collects, scrutinizes, and monitors data in a level before analysis level. This process takes place by implementing various techniques such as: "host-based, network-based, and hybrid-based approaches". The main processes of analyzing level occur when the network sessions are in progress, compliant to the real time intrusion detection, or subsequent to the collection process of information data that compliant to the offline intrusion detection. If the intrusion detection is offline, the implementation process will be very easy in contrast to the real time intrusion detection. While, the real time one have the benefit to understand the behavior of the attacker [3].

In this paper, the main processes of IDS are presented and the location of each process regarding to the network security is indicated. As well as, a short review on around ten most resent papers is provided, that analyze different techniques of intrusion detection. Next, the IDS is

classified into its main types then, the advantages and deadlocks of each type is presented. Finally, the most common types of intrusion are described in addition to the style of their attack and the weaknesses in the network that the attackers can catch up and exploit them.

Table 1: Comparison Between Main Types Of Ids

Criteria	Anomaly-Based	Signature-Based
Update	No	Yes
Detection ability	Can detect Known and unknown attacks	Only Known attacks can be detected with extremely high-quality accuracy
Definition	Employ deviation idea from the standard usage pattern to recognize intrusions	Employ patterns of the well-known attacks to recognize intrusions
Characteristics of the system	High False Alarm	Low False Alarm
Implementation requirement	Needs fewer computation and resources	Needs extra computation and resources

2.INTRUSION DETECTION SYSTEM

In any network or any system, any type of illegal or unreliable actions is identified as intrusions. Even so, Intrusion Detection System (IDS) can be determined as an assortment of the instruments, technique, and resources that can help for recognizing, considering, and describing intrusions. In general intrusion detection is an element of the entire system of protection that is set up on any system or any device and it is not a separate protection quantifier. The intrusions are generally defined as: "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" and intrusion avoidance methods such as "encryption, authentication, access control, secure routing, etc." are offered as a shield that located to the first line of protection against intrusions. Nevertheless, as all other type of the system security, it is impossible to prevent intrusions absolutely. The intrusion and bargain of a hub prompts private data, for example, security keys being uncovered to the interlopers. This results in a consequence with disappointment of the preventive security component. In this manner, IDSs are intended to uncover intrusions, before they can unveil the secured system assets. IDSs are constantly considered as a moment mass of barrier from the security perspective. IDSs are always considered to be called the criminal cautions that are being utilized as a part of physical security systems today. As specified in [14], the normal operational necessity of IDSs is known as: "low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected". Even to all of above, the detection of attacks is only process that IDS can perform and it cannot provide any mechanism for preventing the attacks. Thus, it only employed for detecting the attacks. We can classify the common components of the IDS as: "Monitoring Component" that evaluate the traffic and maintain the track of the traffic; "Analysis and Detection" which attempts to notice the strange behaviours appear in the network; and "Alarm Component "– that raises a flag or alarm when any intimidation is detected [5]. See Fig 1.

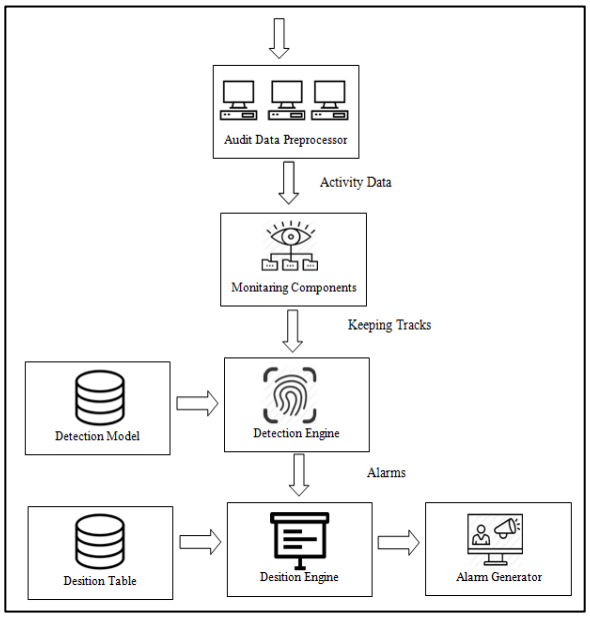

Fig. 1. Main Processes of Intrusion Detection System

3.RELATED WORKS

In this section, several of resent papers will be reviewed that they discus different issues in distributed database system.

The authors in [4] invented a network security system that depends on a new technology for intrusion detection in distributed networks. The system achieves a context that eliminates the user's doubts, additionally provides a huge degree of security defence for the computer network systems. The provided system incorporates a diversity of determining the attacker technologies, thus

the system is able to efficiently notice and establish the compound, synchronized, and complex attacks. While, in [5] the authors discussed the intrusion detections and the common attacks in Wireless Sensor Networks (WSN). They presented the main problems of security techniques in WSN, the attempting of attackers to make risks in security and they also discussed the mainly capable systems of Intrusion Detection with providing a wish that will help the investigators to perform additional investigations.

Whereas, the authors in [6] offered the consequence of study that focused on expansion the extent of IDS techniques to be encouragement for extra SCADA protocols. As a feature of the examination, they dissected multiple open source IDS frameworks and executed help in the outstanding Suricata IDS to identify digital dangers against mechanical controllers running the ENIP (EtherNet/IP) protocol that a protocol generally utilized as a part of the assembling segment. At last, through a test consider, they assessed the execution of running the ENIP-empowered form of Suricata on asset compelled equipment. This is critical on the grounds that it would enable the answer for being sent on little shape factor mechanical review equipment which could be efficiently and broadly conveyed in a substantial number of spots in a modern control arrange - hence guaranteeing higher digital security scope.

A neuromorphic subjective processing approach for Network Intrusion Detection System is presented by [7] for digital security utilizing Deep Learning (DL). The algorithmic energy of DL has been converged with quick and to a great degree control productive neuromorphic processors for digital security. In this usage, the information has been numerical encoded for training among unsupervised deep learning strategies named Auto-Encoder (AE) in the train phase. The weights that are created of AE are utilized as introductory weights for the supervised training stage utilizing neural systems. The last weights are changed over to discrete esteems utilizing Discrete Vector Factorization (DVF) for creating crossbar weight, synaptic weights, and limits for neurons. At long last, the created crossbar weights, synaptic weights, limit, and break esteems are plotted to crossbars and neurons. Additionally, in the testing stage, the converted test prototypes are transformed to spiking structure by utilizing hybrid coding methods.

On the other hand, the authors in [8] projected a technique that will be actualized through programming. The Intrusion Filtration System (IFS) will perform through the relationship of antivirus or might be with Intrusion Detection System (IDS) accessible in Operating System. The IFS will do secure correspondence and utilization of abstracted information over the intranet and the web. Their paper is also talk about how IFS will channel the uncorrupted documents. IFS will guarantee the uncorrupted records correspondence channels at the downloaded port.

A design based on fuzzy logic system is built by [9] for successfully distinguishing the intrusion exercises inside a network. The desired fuzzy logic-based system has the capacity to distinguish an intrusion conduct associated with the networks because the rule base includes a superior arrangement of standards. Here, the authors have utilized a mechanized technique for the era of fuzzy guidelines, which are gotten from the unequivocal principles utilizing successive things. The investigations and assessments of the proposed intrusion detection system are applied with datasets of intrusion detection in the KDD Cup 99. The exploratory outcomes obviously demonstrate that the proposed system accomplished higher accuracy in distinguishing whether the records are ordinary or assault one.

However, Hidden Naïve Bayes (HNB) model is considered by [10] in order to be connected to intrusion detection issues that experience the ill effects of dimensionality, exceedingly corresponded elements, and high system data stream volumes. HNB is a data mining form that unwinds the Naïve Bayes technique's contingent independency presumption. Their trial comes about demonstrate that the HNB form shows a predominant general execution as far as exactness, blunder rate and misclassification cost contrasted and the conventional Naïve Bayes demonstrate, driving expanded Naïve Bayes models and the Knowledge Discovery and Data Mining (KDD) Cup 1999 victor. Their model performed superior to anything other driving best in class models, for example, SVM, in prescient exactness. The outcomes likewise demonstrate that their model fundamentally enhances the exactness of recognizing denial-of-services (DoS) assaults.

Although, the authors in [11] depended on an introduced packet that based on selective encryption for making detection of new intrusions and attacks. Through their technique they cut down the expended energy as a consequence to distinguish the time for starting and ending of attacks. In view of the fact that energy consumption also relies on packet transmission speed, particularly throughout attacks, they also recommended to adapt it in accordance with immediate control performance. In addition they presented that Imitation results proof that the method punctually responds to attacks while energy keeping was established analytically.

Last but not least, an improper structure parameters of Artificial Neural Network (ANN) is presented by [12] to get a chance for prompting low exactness for intrusion detection of the transportation data security framework. Keeping in mind the end goal to defeat this issue, they proposed another detection technique in light of GA-Chaos streamlining and Radial Basis Function (RBF)

neural network. The GA-Chaos was initially used to upgrade the structure of the RBF and additionally, its weight esteems to acquire high learning and speculation capacity of the RBF distinguished model. At that point, the RBF display was utilized to prepare and test the intrusion data sets. They exhibited that the exploratory outcomes demonstrate the technique advances the detection rate and count speed and beat the standard GA-based strategies.

Finally, an Intrusion Detection System made in bunch head is proposed by [13]. Where, the proposed IDS is a Hybrid Intrusion Detection System (HIDS) and it comprises of anomaly and misuse detection module. The authors additionally attempted to raise the detection rate and lower the false positive rate by the upsides of misuse detection and anomaly detection.

4. INTRUSION DETECTION TECHNIQUES

The main techniques of intrusion detection can be classified as following [2]:

4.1. Signature Based Detection

Signature detection includes scanning network activity for a progression of malevolent bytes or parcel successions. The principle preferred standpoint of this system is that signatures are anything but difficult to create and comprehend on the off chance that we recognize what network conduct we are attempting to distinguish. For example, we may utilize a signature that searches for specific strings inside adventure specific cushion flood weakness. The occasions produced by signature-based IDS can impart the reason for the alarm. As example coordinating should be possible all the more effectively on present day frameworks so the measure of energy expected to play out this coordinating is insignificant for an administer set. For instance, if the framework that will be ensured just convey by means of DNS, ICMP, and SMTP, every single other signature can be overlooked.

Restrictions of these signature engines made the technique to be limited for detecting attacks, hence it can detects only these attacks whose signatures are formerly saved in database; as a result, obligate the system security to create a signature for all of the attacks; and new attacks cannot be recognized . This system mainly depends on regular expressions and the similarity of strings, thus it can be easily tricked. These procedures only try to find strings transmitted contained by packets through the wire. In addition, signature based techniques can only provide a perfect protection against the static behavioural pattern, they be unsuccessful to detect the attacks generated by human or a worms with self- altering behavioural features.

4.2. Anomaly Based Detection

The anomaly based detection is built on describing the network behaviour. The network behaviour is in conformity with the previously declared behaviour, then it is agreed to otherwise it generates the occurrence in the anomaly detection. The received network behaviour is arranged or got by the aspects of the network administrations. The real downside of anomaly detection is indicating its rule set. The productivity of the system relies upon how well it is actualized and tried on all protocols. Rule describing procedure is likewise influenced by different protocols utilized by different sellers. Aside from these, traditional protocols additionally make rule describing a troublesome occupation. For detection to happen effectively, the itemized information as regards to the accepted network behaviour should be improved by the directors. Although, once the principles are described and protocols are fabricated then anomaly detection systems perform properly.

5. MOST COMMON TYPES OF ATTACKS

There are many renowned and some of less-known security attacks that are in networks. In this area, we talk about these security attacks briefly concerning their countermeasures. All of the attacks depicted beneath concentrate on the restrictions of directing protocols in the network. In any case, some obscure attacks that are initiated considering other security limitations of the network are displayed too [15] [16].

5.1. Denial of Service (DoS) Attacks

Denial of Service (DoS) attacks can be regarded as any kind of deliberate action that is able to interrupt, be a challenge, or even can damage the network. Essentially, DoS attacks can be classified into three main kinds:

- Expenditure of scant, restricted, or unrenewable resources.
- Obliteration or modification of organization data.
- Physical damage or modification of network resources.

Alternate DoS attacks that are extremely ruinous are jamming and altering attacks. Jamming is the pondered impedance of the remote communication channel. Actually, sensor hubs are extremely helpless against this kind of physical attack. One more physical attack is meddling; this kind aims for the real hardware of the sensor hubs. While it is hard to know whether a specific DoS circumstance is caused purposefully or accidentally, there are a number of detection techniques that assist to foil each kind of DoS attack.

5.2. Black hole Attacks

In this kind, a malicious hub goes about as a black hole to attract in all traffics in the network. The attacker tunes in to the course demands and afterward answers to the objective hub illuminating that it has the most limited way to the base station. A casualty hub is lured to choose it as a forwarder for its packages. Once a malicious hub places itself among the basis station and sensor hub, it

can do anything that it needs (eliminate all packages, alter the substance, and so forth) with the packages that go through it. This sort of attack can be exceptionally destructive to sensor hubs that are sent extensively a long way from the base station.

5.3. Ser to Root Attack (U2R):

In this kind of attack the attacker begins with client level like bringing down the secret key, thesaurus attack lastly attacker accomplishes root to get to the system.

5.4. Remote to User Attack (R2U):

In this kind of attack, an attacker has the ability to send a package to a machine in excess of a network system but does not have a record on that machine, make utilization of some weakness to accomplish local entrance as a client of that machine.

6. CONCLUSION

In this paper, most of the resent papers about IDSs have been reviewed. Firstly, the IDS is defined then, detailed information about its components, the types of IDS, deadlocks for each types have been presented in addition to the environment of IDS in network security. Secondly, a short review about ten most resent papers is provided that discuss different techniques of intrusion detection. Next, the classification of IDS in to its main types is displayed and then, the advantages and deadlocks of each type is presented. Finally, the most common types of intrusion have been described, along with the style of their attack and the weaknesses in the network that the attackers can catch up and exploit them.

REFERENCES

[1] V. Singh and S. Puthran, "Intrusion Detection System Using Data Mining A Review," *IEEE*, pp. 587–592, 2016.

[2] V. Jyothsna, V. V. R. Prasad, and K. M. Prasad, "A Review of Anomaly based Intrusion Detection Systems," *Int. J. Comput. Appl.*, vol. 28, no. 7, pp. 26–35, 2011.

[3] R. Abdulhammed, M. Faezipour, and K. M. Elleithy, "Network Intrusion Detection Using Hardware Techniques : A Review," *IEEE*, pp. 1–7, 2016.

[4] H. Yi and Z. Yifei, "Research of Campus Network Security System Based on Intrusion Detection," *IEEE*, vol. 4, no. Iccda, 2010.

[5] S. Shanthi and E.G.Rajan, "Comprehensive Analysis of Security Attacks and Intrusion Detection System in Wireless Sensor Networks," *IEEE*, no. October, pp. 426–431, 2016.

[6] K. Wong, C. Dillabaugh, N. Seddigh, and B. Nandy, "Enhancing Suricata Intrusion Detection System for Cyber Security in SCADA Networks," *IEEE*, pp. 1–5, 2017.

[7] Z. Alom and T. M. Taha, "Network Intrusion Detection for Cyber Security on Neuromorphic Computing System," *IEEE*, pp. 3830–3837, 2017.

[8] M. R. Dewanjee, "Intrusion Filtration System (IFS) - mapping Network Security in new way," *IEEE*, pp. 527–531, 2016.

[9] R. Shanmugavadivu, "NETWORK INTRUSION DETECTION SYSTEM USING FUZZY LOGIC," *Indian J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 101–111, 2011.

[10] L. Koc, T. A. Mazzuchi, and S. Sarkani, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier," *Expert Syst. Appl.*, vol. 39, no. 18, pp. 13492–13500, 2012.

[11] R. Muradore and D. Quaglia, "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," *IEEE*, vol. X, no. c, pp. 1–11, 2015.

[12] Y. Shi, J. Bao, Z. Yan, and S. Jiang, "Intrusion Detection for Transportation Information Security Systems Based on Genetic Algorithm-Chaos and RBF Neural Network," *IEEE*, pp. 26–28, 2011.

[13] S. C. W. K.Q. Yan and S. S. W. and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network," *IEEE Conf.*, 2010.

[14] I. Butun, S. D. Morgera, and R. Sankar, "Wireless Sensor Networks," *IEEE*, vol. 16, no. 1, pp. 266–282, 2014.

[15] A. S. Subaira and P. G. Scholar, "Efficient Classification Mechanism for Network Intrusion Detection System Based on Data Mining Techniques : a Survey," *IEEE*, pp. 274–280, 2014.

[16] A. S. Subaira and P. G. Scholar, "Efficient Classification Mechanism for Network Intrusion Detection System Based on Data Mining Techniques : a Survey," *IEEE*, pp. 274–280, 2014.