International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

A Survey on Intrusion Detection Systems (IDS)

Swati G Kulkarni[1], Srividya M S[2]

[1]*Dept. of Computer Science & Engineering, R. V. College of Engineering, Bengaluru, India*
[2]*Asst. Professor, Dept. of Computer Science & Engineering, R. V. College of Engineering, Bengaluru, India*

Abstract - *In this digital age, billions of people have access to internet. With growth in internet users, there is subsequent increase in the number of network attacks. User device and data in the networks are under risk. The act of gaining access to a system without permission is called intrusion. Therein comes Intrusion Detection System (IDS), a technology that monitors the network to avoid any such attacks. IDS can monitor the system activities for potential breach of security policies. In this paper, we present a review on Intrusion Detection Systems.*

Key Words: Intrusion Detection System, IDS, Cyber-attacks, anomaly, network.

1. INTRODUCTION

With the rapid growth of internet users and the growth in computer technologies in the past decade, risks arise for data privacy and network security. Cyber-attacks and network attacks are showing rising continuously. Thus, efforts should be made towards improving cyber security for various fields such as medicine, finance, IT industries and suchlike. But, effectiveness of network security in encountering security threats faces some hurdles. Firstly, defence system alone cannot measure up to the security need. There is a need to monitor the behaviour of the network users and instantly detect any new intrusions that may occur at any moment. Secondly, another is that the organizations accumulate a huge amount of sensitive data about clients, employees, or it can also be intellectual property, company trade secrets, financial data or any other sensitive data. Thus, this data is not only huge in volume but also growing exponentially with time. This makes it necessary to adapt Big data technologies and practices so that this huge volume of network data can be processed in real time [1].

Detecting attacks in real-time is arduous task because the attackers use IP spoofing or they may send an overwhelming number of packets continuously to the victim device. These can bypass the preliminary forms of defence such as firewalls as they mostly rely on static techniques, they collect the packet and analyse them eventually. They lack self-adapting abilities and are thus only effective against known threats. In real-time networks, where such threats are ever increasing, Intrusion Detection System (IDS) plays a significant role in improving security of a network. It provides an auxiliary support layer after the basic authentication and authorization activities.

2. OVERVIEW OF IDS

An intrusion detection system (IDS) is a device or software application that monitors network to look for suspicious activity, threats or policy breaching, and on encountering such activities, it alerts the security personnel. IDS monitor inbound as well as outbound network flow for abnormal behavior and then alert the admin or user that a network intrusion might be occurring. It performs the task by comparing signatures of known malware against system files. It monitors the user behavior, system processes and system configurations for any unusual behavior. Security personnel are alerted on security breach with data consisting of the addresses of the source, the target and the type of attack.

2.1 IDS Detection Types

IDS can be classified into Signature-based Detection or misuse detection and Anomaly-based Detection based on analysis method or as Host based IDS and Network based IDS based on source on source of data.

Signature-based IDS: It is used to identify known threats by observing the network flow for specific patterns or string in network traffic, or malicious instruction sequences used by malwares. These patterns that are detected are called signatures. It can effectively detect known malicious threats but fail to recognize unknown threats.

Anomaly-based IDS: The need to identify new malwares which are rapidly being developed gave rise to Anomaly-based system. An anomaly is any deviation to normal or expected behaviors. Machine learning is used to create trustful activity model or a profile and the observed events are compared against this to recognize significant attacks. Though the model is successful in determining previously unknown attacks, there are possibilities of false positives.

Host-based intrusion detection system (HIDS): HIDS are installed on devices in the network to identify any unusual changes in the operating system files, abnormal client-server requests which indicate the possibility of attack or misuse. They are usually beneficial against insider attacks. It monitors and analyzes the system files and system configuration. They seek out abnormalities for instance deletion, overwriting and unauthorized port access.

Network-based intrusion detection system (NIDS): NIDS monitors and analyzes network flow for any indication of threats or suspicious behavior. It inspects the headers and contents of the packets flowing across the network. They are installed in the network at crucial points to inspect traffic incoming and outgoing from the devices. For instance, they

are placed to detect attacks trying to bypass the firewall in subnet.

3. DETECTION APPROACHES

There are a huge variety of techniques that can be adopted for IDS. The following section outlines some of the approaches.

[2] focuses on using classification approach for Intrusion Detection. The most beneficial features are captured from the data using Recursive support vector machine. KDD-CUP99 data set was used to test the model developed. Though the results were acceptable and the time taken for training and testing were reduced, it is not an ideal choice to detect irregular behavior.

A method based on unsupervised outlier detection technique called DenOD (Density Based Outlier Detection) is proposed in [3]. Outlier is any data whose characteristics deviate from the normal characteristics. Intrusion detection is usually achieved by monitoring and analyzing the log database of various devices in the network and also their service activities. Processing of such huge amount of data can give rise to higher false alarm rate which is tackled by the use of outlier detection in cloud computing environment.

The log from the various cloud nodes are collected by the IDS using the sperate connection that exists with each of the node and is mapped to the cell index. This followed by the use of density function to determine its density based on cell data value followed by Inter-quartile range (IQR) which helps detect abnormal behavior. This was easy to implement and was able to detect DDOS, Probe, R2L and U2R attacks.

In [4], an advanced machine learning approach is used for the detection of botnet traffic. Firstly, as the data being dealt with fairly complex, it reduces the dataset size by using feature ranking followed by Voronoi-based clustering thus eliminating the unnecessary features. Thus, forming the Randomized Data Partitioned Learning Model. The ISOT dataset used consists of malicious and non-malicious real-time traffic. This is also effective when the packets are encrypted as unlike most IDS that recognize the intrusion by analyzing the contents of the payload, it functions by analyzing the network traffic by its characteristics. Altogether it reduces the processing delays and effectively deals with large scale network. The model was found to have high detection accuracy.

In [5], a new ensemble clustering or NEC is developed that can be used for novel anomaly detection. Preprocessing is aimed to extract the most useful features by first transforming the records into real numbers and then clustering the feature set to get multiple subspaces. The dataset is split into normal and anomalous records. It uses a combination of classical unsupervised models for the purpose. The result is obtained by passing the classified sets to a voting model. The model is verified using NSL-KDD '09 dataset. This system succeeded in producing high detection rate and reducing false passive rate for detecting new anomalies without labelled dataset.

In [6], A Hidden Markow Model (HMM) based Intrusion Detection is proposed for Software-Defined Networking (SDN). Network intrusion system (NIDS) can utilize the HMM and with the changes in the network activities, it can make better decisions concerning the security of the network. The monitoring systems and the filters can adapt to the increasing number of devices in the network as well as the NIDS can better adapt to the ever-changing malicious threats. This proves that with refining and expansion of the feature set, the model can be a promising solution to the cybersecurity concerns.

[7] proposes the use of hybrid data mining techniques to reduce the time complexity of Collaborative Intrusion Detection System. The system is verified over KDD CUP 2009 dataset. The system used K-means followed by a Projective Adaptive Resonance Theory (PART) classifier. PART algorithm combines the divide-and-conquer and separate-and-conquer strategies by building partial decision trees over and over. The model was able to decrease the training time while maintaining the detection accuracy.

Another hybrid model was proposed in [8]. The proposes the use of Extreme Learning Machine (ELM) which has superior learning abilities along with Particle swarm optimization (PSO) as meta-heuristic to optimize ELM. Unlike the basic algorithm where the parameters are selected in random, the PSO-ELM provides the main features. The model is verified using NSL-KDD dataset. The model was successful in improving the intrusion detection accuracy with fewer neurons in the training model.

While machine learning is most popular for developing IDS, there are techniques which are used in combination with these to provide satisfactory results. [1] adopts a Multi-Agent Model. Large networks and big data complications necessitate for a model capable of detecting both known and unknown attacks. Capturing agent collects the network flow which is then filtered and categorized by Filtering/ Load Balancing Agent. Then the processed data stored in HDFS Cluster are analyzed and decision is made ultimately by Decision Maker Agent. If any intrusion is detected, it is stored in Intrusion database for future use. The multiple agents in the proposed Distributed model, each of which focus on different aspects, coordinate with each other to provide a real-time impressive detection rate.

[9] proposes a model called Genetic Programming Fuzzy Inference System for Classification which adopts multi-gene Genetic Programming, an evolutionary algorithm. Feature selection to improve the classifier accuracy and detection rate uses Modified Feature Vitality Based Reduction Method. It is tested using NSL-KDD dataset. Comparison with other classifier clearly shows that there is an improvement of 2% in average for classification accuracy.

In [10], a novel fuzzy based IDS is developed which is reinforced by hierarchical bidirectional fuzzy rule interpolation (HB-FRI) technique. The standard fuzzy interface is able to speculate the potential attack when the rule is available in the fuzzy knowledge (rule) base. To enhance the IDS to include the uncommon cases for which certain values are missing or rules from the standard classifier is unable to detect, HB-FRI is employed. It is also designed to avoid conflicting rules to reduce false positives. The system succeeded in classifying the attacks according to their threats levels and thereby reducing the frequency of false positives and false negatives.

[11] Proposed a flexible and light weighted intrusion detection approach at network-layer in cloud environment called Behavior-based Network Intrusion Detection (BNID). Behavior analysis is performed for the traffic captured at Cloud Network Node (CNN) to detect an attack or intrusion using statistical learning techniques. This eliminates the need of Intrusion Detection System in every tenant virtual machine (TVM). It is validated with Information Technology Operations Center (ITOC) attack dataset. It does not need the exhaustive monitoring of memory writes. The detection accuracy and false positives were found to be 98.8% and 1.57% respectively.

In [12], Negative Selection Algorithm (NSA), one of the popular Artificial Immune based algorithms is used. The model was validated over NSL-KDD data set. The model enhances the detectors by training it using negative selection. The radius for self-samples is calculated based on the density. The cases that could lead to false positives are taken into consideration, such as modifying expression for radius calculation to handle the samples that are close by in low density regions and for the sample that have lowest density. The model was successful in reducing the false positive rates and improve true positives by about 2%.

4. CONCLUSION

The paper describes the literature review of various technologies adapted for Intrusion Detection Systems. Each of the model developed emphasize on certain features of the network and strive to improve the detection rates in various network environments. Unfortunately, the methods that are the most effective for Intrusion Detection have not been established as they all provide comparable results. The model to be used for the purpose of intrusion detection is dependent upon the type of the network and their requirements.

ACKNOWLEDGEMENT

I would like to present my gratitude to Srividya M. S., Asst. Professor, Department of Computer Science & Engg. for her advice, guidance, and supervision. I would also like to thank R. V. College of Engineering for the support on resources.

REFERENCES

[1] Said Ouiazzane, Malika Addou, Fatimazahra Barramou, “A Multi-Agent Model for Network Intrusion Detection”, International Conference on Smart Systems and Data Science (ICSSD), 2019

[2] Gong Shang-fu, Zhao Chun-lan, “Intrusion detection system based on classification”, 2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment, 2012

[3] Manoj Kumar, Robin Mathur, “Unsupervised Outlier Detection Technique for Intrusion Detection in Cloud Computing”, International Conference for Convergence of Technology, 2014

[4] Manoj S Koli, Manik K. Chavan, “An Advanced method for detection of botnet traffic using Internal Intrusion Detection”, 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), March 10-11, 2017

[5] Weiwei Chen, Fangang Kong, Feng Mei, GuiginYuan, Bo Li, “a novel unsupervised Anamoly detection Approach for Intrusion Detection System”, 2017 IEEE 3rd International Conference on big data security on cloud, 2017

[6] Trae Hurley, Jorge E. Perdomo, Alexander Perez-pons, "HMM- Based Intrusion Detection System for software-defined networking", 2016 15th IEEE Conference on Machine Learning and Application, Dec 18-20, 2016

[7] Yi Yi Aung, Myat Myat Min, “A Collaborative Intrusion Detection Based on K-means and Projective Adaptive Resonance Theory”, 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD 2017), 2017.

[8] Mohammed Hasan Ali , Mohamad Fadlizolkipi , Ahmad Firdaus, “A hybrid Particle swarm optimization - Extreme Learning Machine approach for Intrusion Detection System”, 2018 IEEE Student Conference on Research and Development (SCOReD), 26-28 Nov. 2018

[9] Mariem Belhor, Farah Jemili, “Intrusion Detection Based on Genetic Fuzzy Classification System”, 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Nov.-Dec. 2016

[10] Shangzhu Jin, Yanling Jiang, Jun Peng, “Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation”, 2018 IEEE International Conference on Systems, Man, and Cybernetics, 2018

[11] BNID: A Behavior-based Network Intrusion Detection at Network-Layer in Cloud Environment, Kamal Kumar Ghanshala, Preeti Mishra, R. C. Joshi, Sachin Sharma, 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), 2018

[12] Fatemeh Selahshoor, Hamid Jazayeriy,Hesam Omranpour, “Intrusion Detection systems using Real-Valued Negative Selection Algorithm with Optimized Detectors”, 2019 5th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), Dec. 2019