Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 9, September 2016, pg.23 – 28

A REVIEW ON INTEGRATED INTRUSION DETECTION SYSTEM IN CYBER SECURITY

Parveen Sadotra (CEH) [1]**, Dr. Chandrakant Sharma**[2]
[1]Research Scholar, Career Point University, Kota, Rajasthan
[2]Assistant Professor, Career Point University, Kota, Rajasthan

Abstract—The fast propagation of computer networks has changed the viewpoint of network security. An easy accessibility conditions cause computer network as susceptible against several threats from hackers. Threats to networks are numerous and potentially devastating. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. Many of the technologies proposed are complementary to each other, since for different kind of environments some approaches perform better than others. This paper presents a review of intrusion detection systems that is then used to survey and classify them. The taxonomy consists of the detection principle, and second of certain operational aspects of the intrusion detection system.

Keywords—IDS, security, Network, WSN, SVM etc.

I. INTRODUCTION

Intrusion detection systems (IDSs) are an essential component of a complete defense-in-depth architecture for computer network security. IDS is an effective security technology, which can detect, prevent and possibly react to the attack [1]. It monitors target sources of activities, collects and inspects audit data looking for evidence of intrusive behaviors. When it detects suspicious or malicious attempts, an alarm is raised giving the network administrator the opportunity to react promptly.

The main objective of IDS is to detect all intrusions in an efficient manner. IDSs can be classified from different points of view. Fig. 1 shows different classifications of IDSs.

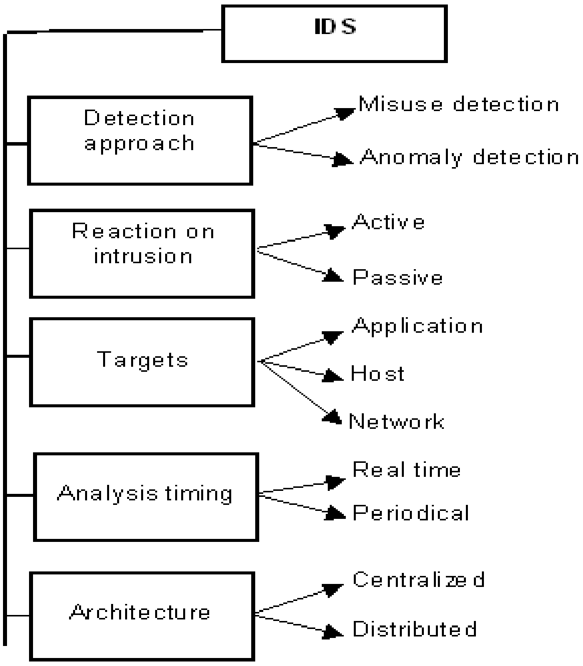

Fig. 1 Characteristics of intrusion detection systems

From the viewpoint of detection method, IDSs can be divided into two categories: anomaly and misuse (signature) based detection. Anomaly detection tries to determine whether deviation from the established normal usage patterns can be flagged as intrusions. On the other hand, misuse detection uses patterns of well-known attacks or weak spots of the system to identify intrusions [2]. As shown in Fig. 1, depending on the information source, an IDS may be either host or network-based. A host-based IDS (HIDS) analyzes events such as process identifiers and system calls, mainly related to OS information. On the other hand, a network-based IDS (NIDS) analyzes network related events: traffic volume, IP addresses, service ports, protocol usage, etc. [3]. Although IDS solutions have been used for about twenty years, an important problem is still not fully addressed: Unfortunately, these systems provide huge number of alerts which most of them are false alerts or low importance. For example, a single IDS sensor can generate tens of thousands of alerts in a day [4, 5]. Large volume of alerts is unmanageable and overwhelming to the human analyst. Inspecting thousands of alerts per day is unfeasible, especially if 99% of them are false alerts [6]. False alerts, also known as false positives occur when a legitimate activity has been mistakenly classified as malicious by the IDS. The vast imbalance between the actual and false alarms generated has undoubtedly undermined the performance of IDS [7].

Despite that anomaly-based IDSs produce more false positives rather than misuse-based IDSs, false positives are unavoidable in all types of IDS. Because of these reasons, during the last few years false positives reduction techniques have been extensively researched [4] and researches on IDSs have focused on how to handle these alerts.

II. LITRATURE SURVEY

A recent survey [10, 11] says that intrusions inside the organizations are growing exponentially. To avoid such intrusions the proposed framework has empowered with mobile agents to detect intrusions in a quick time under the given environment. In order to detect user anomalies, the normal user activity profiles are created and a similarity score range (upper and lower bound) is assigned to each user's normal pattern set. When in action, the system computes the similarity score of the current activity's patterns, and if this score is not in the similarity score range, the activity is considered as an anomaly.

Yogitha et.al. [8] Proposed intrusion detection system using Support Vector Machine (SVM). Verification is done by conducting experiments on NSL-KDD Cup'99 data set which is improver version of KDD Cup'99 data set. By using this NSL-KDD Cup'99 data set they have reduced extensive time required to build SVM model by performing proper pre-processing on data set. In this classification is done by using SVM. By doing proper kernel selection attack detection rate is increased and false positive rate (FPT) is decreased. In this proposed work author has used Gaussian Radial Basis.

Wenke Lee ET. al. [9] has first tried to mine the system audit data to study consistent use full patter of program and user behavior. They have also used the set of relevant system features presented in the patterns to compute inductively learned classifiers that can recognize anomalies and known intrusions. In order to make the classifier an effective model they should have a sufficient audit data for training and a set of predictive system features. To guide the audit data and feature selection they have proposed the association rule and frequent episodes from the audit data, which is used in classification model. They have incorporated domain knowledge into these basic algorithms using the axis and reference attributes.

Eleazar, Matthew et. al. [10] presented an adaptive model generation, a method for automatically building detection model for data mining based intrusion detection system. The data collected by intrusion detection sensor models are used to achieve this. The detection models are updated by the systems automatically as more data is collected. Adaptive model generation may significantly reduce the cost of deploying an IDS system because it removes the need for manually creating training set.

S.A. Joshi, et. al., [11] In this paper the author discuss about the data mining algorithms and Intrusion detection system to detect the unknown attacks from the dataset. There different kinds of attacks but the authors of this paper discuss the few kinds of attacks. They compares the four types of attacks are:

a) Probing attack
b) Denial of service
c) User to root
d) Remote to local

Then the author listed out the various data mining techniques and intrusion detection techniques which is used for the detecting the attacks like signature based detection, anomaly based detection, network- based intrusion detection system, host-based detection system. Comparing these types of attacks and finding the high detection rates pattern capturing algorithm has high detection rate. Finally find out the percentage for detection rate and false alarm rate.

Sushil Kumar Chaturvedi, et. al. [12]The main work of this compares the two types of algorithms C4.5 and Support Vector Machine (SVM). First the given dataset is pre-processing and then the data can be partition into training and testing. The third stage the dataset is applied in C4.5 and SVM algorithm. The author of this paper compares these two algorithms and find out the detection rate comparison and false alarm rate comparison. By using these two data mining techniques they justify the C4.5 algorithm is better than the SVM.

Omprakash Chandrakar, et. Al. [13] This paper describes about basic concepts of network intrusion detection system, components and types of attacks. The IDS contains the three types of components namely data source, analysis engine, response manager. This paper gives the overview of genetic algorithm. The genetic algorithm randomly selected the input (chromosome) and calculates the fitness value for each generated initial chromosome. The iteration has performed some specific operations namely sorting, selection, crossover, mutation and finally calculates the fitness value for chromosome.

A.R. Jakhale, et. Al [14]This paper describes an anomaly detection system and its two phases namely training and testing. The sliding window and clustering is used to monitoring the network traffic by mining the frequent patterns using algorithms. The algorithms are so effective and used in real time monitoring. The frequent multi-pattern capturing algorithm has high detection rate. Finally find the percentage for detection rate and false alarm rate.

R. Venkatesan, et al., [15] This paper describes an anomaly detection system and its two phases namely training and testing. The sliding window and clustering is used to monitoring the network traffic by mining the frequent patterns using algorithms. The algorithms are so effective and used in real time monitoring. The frequent multi-pattern capturing algorithm has high detection rate. Finally find the percentage for detection rate and false alarm rate.

Abhilasha A Sayar, et.al.,[16]In this paper the author discuss about the classification of Intrusion detection system, advantageous and disadvantageous and its types. In this the IDS uses the artificial intelligence, fuzzy logic and neural network. The techniques are used to detect the intrusions in the images. For example, in military the original information's are changed into images and then send to another location. By using the artificial intelligence with IDS the user can easily identify the unknown attacks. This paper is useful for beginners to study the basic concepts of Intrusion detection system and also detect all kind of images.

III. ISSUES AND CHALLENGES IN IDS

Today intrusion detection system is still in infancy and need lot of research work to be done to make the intrusion detection even more successful. There are a huge number of issues and challenges in current intrusion detection system which needs the immediate and strong research attention. In this paper, we have identified some important issues and challenges which need to be addressed by research communities. The issues and challenges are as:

- Deficiency or incomplete Data set
- Algorithms for Detection
- Integration of multiple formats of data
- Platform dependencies
- Weak Design
- Evaluation of IDS

Let we explain these issues in detail:-

A. Incomplete Data Set

Data set can be defined as a collection of all the data or information during the survey which needs to be analyzed. Since in intrusion detection system, the data sets play important role in accuracy of results. Thus it became very much important to have datasets which are almost near to real time system. Now a days, the researchers are using data set DARPA 98, 99, New Mexico university immune system etc. but being outdated, we are not able to mitigate those attacks which are very much new.

B. Algorithms for Detection

This is the main part while find whether the packet/ information come is attack or the useful information which the user needs to implement the process or jobs. The detection algorithm should be competent enough that it should match all the case in small time and also should match the terms efficiently. The detection policy may be either anomaly or mis-use based. In anomaly based detection, the behavior is identified and if behavior is identified as reverse of normal, it is declared as attack and in another scenario, the pattern is matched using some pattern matching algorithm for known attacks and if pattern matches fully with some suspicious data, it is declared as attack. But there are also drawbacks that there are no rules for new attacks to be matched, hence new attacks are not detected or if it makes some changes in data so that it cannot match the pattern, the attack is detected. Hence we are in need of good and fast algorithm which will detect the pattern thoroughly and fast to match the most of the attacks.

C. Integration of Multiple formats

As we are well aware of the fact that the incoming frames or data may be in different formats. So there is need that different formats shall be integrated on a single intrusion detection system. i.e on the fly it should check for the formats and check the stream for intrusions.

D. Platform Dependence

In current technological world, we have different / number of intrusion detection system available some are free source while other are commercial. While implementing these intrusion detection systems all of them have system requirement to implement the intrusion detection software. Therefore needs some platform for implementation. As we do have different platforms, we need intrusion detection software which may be platform independent so that we can implement the same intrusion detection software on all the platforms.

E. Weak design

The design of all the intrusion detection systems are compact i.e. if a user want to change some part of the intrusion detection system, we have to stop the intrusion detection system, then made the changes as desired and re-deploy it again. Hence the design of the intrusion detection system must be like as mentioned below [13].

It should have two parts, one core part which consists of detection algorithm and second part will be the part associated with pattern matching. This part should be updated on the fly. I.e. it should not affect the detection process of the system but only updates the other parts without touching core part of the system. Thus every update should be added on the fly without stopping the intrusion detection system.

F. Evaluation of IDS

As discussed in the paper, data is growing enormously and IDS has now become a standard for securing large network. Companies are investing huge amount in IDS technologies, but there is no such scientific methods to test the effectiveness of these IDS. Even though some quantitative measurable methods have been design to test the effectiveness, but they do not evaluate the effectiveness on same scale. These methods consider coverage or probability of false alarm or probability of detection or resistance to attacks directed at IDS or ability of handling bandwidth and traffic or ability to identify attacks etc. Hence are not sufficient enough to figure out effectiveness of IDS. Also there should be common scale for evaluating or testing the effectiveness of IDS. The different issues are as [14] [15]

- Collecting script and victim software
- Different requirements for testing different types of IDS
- Testing with different parameters

IV. IMPORTANCE

Since security is of paramount importance in a corporate IT infrastructure, there are a lot of commercial offerings from various vendors in the intrusion detection and protection space. While most products carry a high price tag, there are moderately priced products, as well as open source solutions for those interested.
Visibility: -AN ID provides a clear view of what's going on within your network. It is a valuable source of information about suspicious or malicious network traffic. There are few practical alternatives to an ID that allow you to track network traffic in depth.

Defense: -AN ID adds a layer of defense to your security profile, providing a useful backstop to some of your other security measures.

Response capabilities: - Although they probably will be of limited use, you may want to enable some of the response features of the IDS. For instance, they can be configured to terminate a user session that violates policy. Obviously, you must consider the risks of taking this step, since you may accidentally terminate a valid user session. However, in certain cases it can be an important tool to prevent damage to the network.

Tracking of virus propagation: -When a virus first hits your network, an IDS can tell you which machines it compromised, as well as how it is propagating through the network to infect other machines. This can be a great help in slowing or stopping a virus's progress and making sure you remove it.

Evidence: - properly configured IDS can produce data that can form the basis for a civil or criminal case against someone who misuses your network.

V. DISSCUSSION

In above various literature survey presented by many Authors, we analyze regarding various or many existing research concept in terms of Support Vector Machine (SVM), NSL-KDD, IDS system, HYBRITQ-4(J48, Boyer Moore, KNN) which are given us to emerging method about intrusion detection system on the basis of energy security theme that provide consistent communication and aware from the intrusion. In WSNs environment every nodes are maximize the information delivery in each session and will increase the performance of the network like packet delivery magnitude relation, throughput, and network life time and minimize the end-to-end delay.

VI. CONCLUSION

Intrusion detection techniques have improved dramatically over time, especially in the past few years. Initially developed to automate tedious and difficult log parsing activity, IDSs have developed into sophisticated, real time applications with the ability to have a detailed look at traffic and to sniff out malicious activity. They can handle high-speed networks and complex traffic, and deliver detailed insight – previously unavailable – into active threats against critical online information resources. IDS technology is developing rapidly and its near-term future is very promising. It is increasingly becoming an indispensable and integral component of any comprehensive enterprise security program, since it complements traditional security mechanisms. This work provides an overview of the current state of the art of both computer attacks and intrusion detection techniques. The overview is based on presented taxonomies exemplified with the most illustrative paradigms.

REFERENCES

[1] R. Base, P. Mell, “Special publication on intrusion detection systems”, NIST Infidel, Inc., National Institute of Standards and Technology, Scotts Valley, CA, 2001.

[2] J. Anderson, “An introduction to neural networks”, Cambridge: MIT Press, 1995.

[3] P.G. Teodoro, J.D. Verdejo, G.M. Fernandez, E. Vazquez, “Anomaly-based network intrusion detection: techniques, systems and challenges”, Computers Security, 2009.

[4] J. Viinikka, H. Debar, L. Mé, A. Lehikoinen, M. Tarvainen, “Processing intrusion detection alert aggregates with time series modeling”, Information Fusion Journal, vol. 10(4), 2009.

[5] R. Vaarandi, “Real-time classification of IDS alerts with data mining techniques”, in Proc. of MILCOM Conference, 2009.

[6] K. Julisch, “Clustering intrusion detection alarms to support root cause analysis”, ACM Trans. Inf. Syst. Secur. 6, 2003

[7] G.C. Tjhai, S.M. Furnell, M. Papadaki, N.L. Clarke, “A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm”, Computers & Security 29, 2010.

[8] Yogita B. Bhavasar, Kalyani C. Waghmare “Intrusion Detection System Using Data Mining Technique: Support Vector Machine” 2013 International Journal of Emerging Technology and Advance Engineering volume 3, Issue 3, March 2013.

[9] WenkeLee ,Salvatore J. Stolfo “Adaptive Intrusion Detection: a Data Mining Approach” 2000

[10] HuyAnh Nguyen, Deokjai Choi “Application of Data Mining to Network Intrusion Detection: Classifier Selection Model”

[11] S.A.Joshi, VarshaS.Pimprale, “Network Intrusion Detection System (NIDS) based on Data Mining”, International Journal of Engineering Science and Innovative Technology, Vol. 2, No. 1, January 2013, ISSN. 2319 5967.

[12] Sushil Kumar Chaturvedi, Prof. VineetRichariya. Prof. NirupamaTiwari, “Anomaly Detection in Network using Data mining Techniques”, International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 5, May 2012, ISSN. 2250-2459.

[13] OmprakashChandrakar, Rekha Singh, Dr. LalBihariBarik, “Application of Genetic Algorithm in Intrusion Detection System”, International Institute for Science, Technology and Education, Vol. 4, No. 1, 2014, ISSN. 2224-5774.

[14] A.R. Jakhale, G.A. Patil, “Anomaly Detection System by Mining Frequent Pattern using Data Mining Algorithm from Network Flow”, International Journal of Engineering Research and Technology, Vol. 3, No.1, January 2014, ISSN. 2278-0181.

[15] R. Venkatesan, Dr. R. Ganesan, Dr. A. Arul Lawrence Selvakumar., “A Survey on Intrusion Detection using Data Mining Techniques”, International Journal of Computers and Distributed Systems, Vol. 2, No. 1, December 2012, ISSN. 2278-5183.

[16] Abhilasha A Sayar, Sunil. N. Pawar, Vrushali Mane., “A Review of Intrusion Detection System in Computer Network”, International Journal of Computer Science and Mobile Computing, Vol. 3, No. 2, February 2014, pp. 700 - 703.