IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. III (Jul.-Aug. 2016), PP 20-25
www.iosrjournals.org

Comprehensive Review: Intrusion Detection System and Techniques

Sheenam[1], Sanjeev Dhiman[2],
Dept. of CSE/ DAV University,Jalandhar,India
Dept. of CSE/ DAV University,Jalandhar,India

Abstract: *Security becomes an important challenge to secure the network from cyber attacks. Up till now, threats on the network and security are significant research issues. With increasing the amount of network, there is a chance to secure the network. Number of methods is used to secure the system; our focus is on the study of intrusion detection System. Any hostile attacks on weakness of networks; computer might raise certain serious problems and exploit its Security Policies, Confidentiality, Integrity and Availability (CIA). Many techniques are used to check the system vulnerabilities and to detect the behavior of the system .i.e. anomalous behavior. Threats on the network become the significant research issue. There are number of literature surveys on IDS. This paper gives review on different techniques.*

Keywords**:** *IDS, SNORT, SPADE*

I. Introduction

Over the past years, network security issues have been raised due to the rapid growth of networks. Organization's network system is naturally displayed to the increasing number of threats from the outside hackers as well as internal hackers. The results can be alterations of business data, obstruction in services and violation of the security policies, i.e., Confidentiality, Integrity and Availability (CIA).Many methods, processes, technology and tools are deployed to secure the system by the security organization to counter threats. Firewall, authentication mechanisms methods are used for handling the computer system incidents. This method aim to detect, to prevent, to recover the system and provides a lesson to learn. In this paper, we will discuss the Intrusion Detection System and its techniques that is one of the latest technologies in Information Security.

1.1Why review the IDS?

There is lot of literature survey on IDS. Various techniques are occurring on IDS. Researchers have been done a work on these existing techniques and they prevent system or network from the attacks. Attackers find vulnerabilities in existing system. When they found vulnerabilities they attack on system. So, by reviewing we made IDS which gives less negative rates. There are also many systems which are capable to detect any type of intrusion or malicious attack from which we can create an accurate system to detect the signs of intrusions by reviewing the IDS. There are false positive and negative rates in anomaly based detection and these rates can be reduced by using different techniques. It is difficult to reduce these rates.

1.2Need for IDS

Due to the attacks occurring in the system by the intruders, it causes financial loss, social loss, crashes the system or loss of confidentiality, integrity and availability (CIA). So, there is a strong need of IDS to manage these problems and prevent these kind of losses. Firewall protects the enterprise from the unauthorized access or malicious attacks. Firewalls are used to prevent the system from malicious attacks but new kind of attacks are there which penetrate through the firewalls, so IDS is used to detect all types of attacks occurring on the network.

1.3Intrusion detection system

Intrusion Detection System is competent to detect the intrusions and alerting the administrator of system about the signs of possible intrusions. It provides the information against any lack of confidentiality, integrity and availability to the enterprise's cerebral resources. Firewalls are used to prevent the system from unauthorized access but firewalls are not effective to monitor the system where seniority of attacks occurs. These attacks could be employed by disappointed users and who have a valid access to use the network and they may harm the network system. Now, wireless technology is used and deployed everywhere, therefore it becomes so much easier to attack on wireless than the wired networks. Many types of wireless denial of service (WDOS) attacks have been analyzed[2].
There are two types of IDS:

- Host-Based Intrusion Detection
- Network Based Intrusion Detection

1.3.1Host based IDS: In HIDS, the basic motive is monitoring state and dynamic behavior of the computer. It examines all activities like inspect packet on network targeted at host. HIDS detect what resources are being used and which program accesses those resources. If any modifications occur on the network, alerts are sent to system administrator.

1.3.2Network based IDS: In NIDS, packets are passed through the entire subnet. It matches the packets passing through subnet with the known attacks. NIDS has functional modules are following: *Attribute formation*, *observation stage* and *Espial stage*[14]. *In Attribute formation* Target system are inspected with the pre-defined manner based on observed forms. In *observation stage,* depending the NIDS, It can be done in different manners (automatically and manually). *In Espial stage,* system model is matched with the experimental traffic[14].

1.4Why study the existing techniques in anomaly detection

By deep studying existing techniques of anomaly detection, we will make a new intrusion detection system also used to detect the anomalous behavior of the system by creating a profile of the user normal activities. Compare the results of current traffic on network with observed one to detect the abnormal behavior.

II. Detection categories

2.1Signature or Misuse Detection: It is a technique of intrusion detection which seeks predefined attacks of signature. Patterns must be learnt by system from attacks. From the known attacks, patterns are searched through the incoming data so that the intrusions can be found. For Example, consider a security guard is present at the gate who allows a legitimate person to pass through the gate. Guard would maintain a database of culprits' photographs. The culprits' should not be allowed entry. The guard checks database of culprits' with the incoming persons, if incoming person is in the database then entry should not be allowed. The problem here is that, if the person's photograph is not present in the database, then he will be allowed to enter through the gate, irrespective of the fact that he might be the culprit. The drawback of signature based detection is that, it is in capable to detect new type of attacks.

2.2Anomaly detection: Anomaly based detection shows "abnormal" or "anomalous" behavior of system. Firstly, it creates the profile of the normal activities. If normal activity exceeds the given threshold then it is treated as intrusion. Any deviation through the threshold, gives the anomalous behavior. For Example, guard must contain database of the legitimate persons who would be allowed entry. If the incoming person's match is found in the database, the person will be allowed entry. The person whose photographs not found in the database would be treated as a culprit and will not be allowed entry. The advantage of anomaly detection is that, it is capable to detect the unknown or malicious type of attacks. Many techniques are used in anomaly detection to check the anomalous behavior i.e. Statistical Based Anomaly, Knowledge Based and Machine Learning Anomaly Detection.

2.3Alert types in anomaly detection

2.3.1*False negative*: Intrusion detection system fails to examine the activity, such as results are negative but actually they are not. It is intrusive but not anomalous[4].

2.3.2 False positive: Intrusion detection system examines the activities such that results are positive but actually they are not. It is not intrusive but anomalous[4].

2.3.3True negatives*:* Intrusion detection system examines the activities, such that result would be negative. These are not intrusive and not anomalous[4].

2.3.4True positive: Intrusion detection system examines the activities, such that result would be positive. It is intrusive and anomalous[4].

Table1: Brief description of statistical based anomaly detection

Contributions	**Characteristics**	**Techniques**
Haystack	It describes for each feature set the range of values so to model the behavior.	Host based statistical anomaly detection
NIDES	It has both misuse or signature based and anomaly based detection	Network based statistical anomaly detection
Ye et al.	Hotelling's T^2 test used to detect the trail of activities in computer system.	Multivariate statistical anomaly detection
Denning and Neumann	Gaussian random variables as parameters for univariate models.	Host and Network based approaches

III. Related work

Usage of internet has become an essential part of our daily life. CERT reports that intrusions have increased year by year[2]. Any malicious attacks on the network may raise serious calamity. NIST describes any hostile probes on network weakness; systems may compromise with security policies, i.e., Confidentiality, Integrity and Availability (CIA) and detour the security system. To identify abnormal behavior of system, "Anderson" gives the threat model that categorizes threats as: External Penetration, Internal Penetration, Misfeasance[4]

This categorization of threats is used to monitor the system and to detect the anomalies.

- **External Penetrations** are in which intrusions coming from the unauthorized users.
- **Internal Penetrations** are not carried by unauthorized users; these are carried by authorized users who are not authorized to use that system.
- **Misfeasance** is that when a person is authorized to use the system and data but he misuses both.

3.1Statistical based technique, the profile is generated by observing the system activities to represent behavior. The profile includes measures as Activity Intensity Measure, Audit Record Distribution Measure, Categorical Measures(distribution of an activity over categories) and Ordinal Measure(such as CPU usage)[4].It contains two parameters Current and Observed Profile and measures both profiles. Intrusion Detection System generates an alarm, if anomaly score is greater than a baseline. [6]Denning and Neumann, for each variable set the range of values, by which model the parameters as Gaussian random variables for host IDS and network IDS approaches. Later, multivariate models (two or more metrics) were proposed which gives the better discrimination than a single measure of individual. Haystack[4] is one of the examples of statistical anomaly detection. Haystack set the range of values for individual features and system must be modeled as Gaussian random variables just like Denning and Neumann's work. If value of feature goes down outside the normal range, score was high and alarm was raised. Haystack used to detect attacks like DOS attacks, person penetrate through security control system, from masquerading attacks and hostile use. The con of Haystack, is not to work online i.e. on real time systems, only to work offline. SPADE (Statistical Packet Anomaly Detection Engine) is used in detection of port scans. Port scans are used to know the weakness of system by hackers so as to attack on the target machine services. SPADE is used by SNORT as plug-in in statistical based anomaly detection system. Authors define an anomaly detection as a degree of irregularity based on recent past activity[4].The packets were moved to the correlation engine (used to detect port scans) when the score exceeded the given threshold. The drawback of SPADE is that it has a very high false alarm rate[4]. Ye et al.[7] gives the Hotelling's T^2 test to analyze vet stream of activities in the system. It is used to detect the host based intrusions. Hotelling's T^2 test used to detect the correlation anomalies as well as variations in mean. Maxion and Feather[8] distinguishnormal behavior using different arrangement, this arrangement is derived by taking the packet count at different intervals of time. If bound exceeds the predefined baseline, thenit declares anomalous behavior. Maxion et al. did not consider the non-stationary nature of network traffic which would have resulted in minor deviations in network traffic to go unnoticed[4].Lee and Xiang[9] uses measures of theoretic information such as gaining information and predictability, so as to detect the status of anomaly detection methods, by measuring parameters and build model.This will help to understand the properties of inspection of data.

Earliest developed intrusion detection system is IDES (Intrusion Detection Expert System) at Stanford Research institute (SRI). IDES monitors the individual behavior of users and also detect the distrustful behavior of system. By establishing the behavior of individual users, then we know from where the intrusions flagged. SRI developed the new version of IDES that is NIDES (Next Generation Intrusion Detection Expert System) after analysing the IDES. NIDES operate in real time environment by monitoring the users' behavior and it runs in a batch mode (automatic processing).NIDES is Hybrid System whereas IDES is an Anomaly Based Intrusion Detection System. The current values of the system must be compared with the values that are stored in the profile. If current values are far away from the expected behavior, then anomalies detected. The values of variables are calculated corresponding to the random variable. The frequency distribution must be calculated and it must be updated with time. The distribution is calculated with exponential weighted sum average technique. The frequency distribution is represented in the form of histogram and set the range of variables according to the probabilities. Cumulative frequency is also computed by making the bins according to the probabilities. Now, find the anomalous behavior by computing the current value with stored value. Therefore, NIDES is used to measure the abnormal behavior in system/network. Multivariate statistical technique uses two techniques to monitor the system and detect anomalies by using the Multivariate Exponentially Weighted Moving Average (MEWMA) technique and Multivariate Cumulative Sum (MUCUM). It requires less processing delay and gives notification of signs of intrusions early.

3.2 knowledge based statistical anomaly detection technique, there is possibility of previous knowledge. (Denning and Neumann, 1985; Anderson et al., 1995) characterize the inspected data according to the rules.

Firstly, identify the properties from the learning data. Secondly, reduce procedures and rules. Thirdly, classify the inspected data.

3.3Machine learning is defined as capable to learn the system and improve the performance of work over a period of time. Main focus of machine learning is to improve the performance of the system by getting the prior results and build a model of system, and it is capable to change their execution schemes.

3.3.1Bayesian Networks**:** A Bayesian network is computer graphics model that encodes probabilistic relationship among variables of interest where there is a situation of data missing[4]. It has also capability to constitute the causal dependency. Since Bayesian network contains both relationships among the variables and causal dependency, therefore these are used to solve the problems and results are taken. Kruegel et al.[12] gives a model multisensor fusion in which different outputs from different Intrusion detection system are together. These outputs are aggregated from sensor to give an alarm. Bayesian network is used in many application areas and it is dependent on hypothesis based on the accuracy. So, accuracy for this method is dependent on these assumptions based on target system, deviating from assumptions will decrease accuracy[4]. Therefore, it is necessary to select a good model according to the behavior of the system but it is not an easy task to select the model. Valdes et al.[10] gives the Bayesian network so as to detect the intrusions, when large amount of traffic on network. The drawback of Bayesian network is that it requires high effort.

3.3.2Markov Models: There are two schemes one is Markov and other is Hidden Markov models. In Markov models, it examines the abilities of model by connecting to set of states through transition probabilities. Normal behavior of the target system must be examined during first stage of training and transition probabilities are estimated accordingly. Anomaly score must be calculated and anomalies are found by comparing with observed score. The Hidden Markov model is that in which states and transitions are hidden and follow procedures similar to Markov model.

Table2: Anomaly based detection techniques

Techniques	Advantages	Disadvantages	Schemes
Statistical based	Capability to detect “zero-day” attacks. No require prior knowledge but gives exact notification about hostile activities. No need to update signatures and easy to maintain.	Trained attackers can accept the abnormal behavior as normal. Difficult to maintain the false positives and negative rates. Generates false alarms	Univariate models and multivariate models.
Knowledge based	Gives results after failure of system, flexibility	Time consuming	Finite state machines N-grammars, uml.
Machine based	Dependent on hypothesis.	High resource consuming.	Genetic algorithm Markov model Neural networks Clustering and outliers.

3.3.3Neural Networks: Neural networks are made up of interconnection of neurons (like in human brain). It is used in the field of intrusion detection by creating the profile of users and it examines next commands which will be generated from the sequence of priors and determines the intrusion occurred in network. This approach must be used because of its adaptability with environment.

3.3.4Genetic algorithm***:***Genetic algorithm is part of evolutionary methods. It is inspired by biology .i.e. mutation, selection and crossover and inheritance. It gives the appropriate parameters (optimal) and select features for process of detection. It does not give the best results but do provide us with an optimal solution. It does not contain previous knowledge.

3.3.5Clustering and Outliers detection: means similar type of group. By grouping the observed data into clusters they work together. Firstly, select the point for each cluster. When new point is characterized, check this point if it belongs to a cluster that was previously represented. If it does not belong, then such points are named as outliers and they represent anomaly in detection process[6].Cluster and outlier detection is presented in the IDS field. In KNN, for each cluster find the Euclidian distance to define the data points but some system uses the mahalanobis distance to find membership of data points. Detection systems find an outlier for each point[6].

3.3.6Supervisor instruction call:In machine learning, techniques are used to represent the system’s behavior by learning and then identifying the anomaly from normal behavior. Forrest et al.[13] gives correlation human immune system and intrusion detection. They give a model for program supervisor instruction call order to construct a normal profile. In this, it shows the analogy in constant order of supervisor instruction call used to construct a normal behavior and any deviation from normal order is considered as anomalous behavior.The system made by them is offline by collecting the prior data and results and algorithms are used to understand the profile of system. Hofmeyr et al. created a database according to the sequences of supervisor call instructions to monitor the normal behavior of the program and identify anomaly, if the sequences are not found in the database.

IV. Issues and Challenges

Intrusion detection techniques are growing continuously so as to protect the system and improve security on network. There are some issues and challenges regarding systems:

- Detection efficiency low: This issue might grow due to the lack of studies on intrusions and leads to high false positive rate. These can be reduced by exploration, making accurate systems, good processing schemes to model network.
- High cost and low throughput: To detect intrusion from systems, transmission technologies must be used which have high cost.
- Another relevant issue which is a general problem faced by all intrusion detection platforms .i.e. analysis of ciphered data (in wireless environments)[4].

V. Conclusion

Intrusion detection system (IDS) is very popular in security field. Many techniques are used to check the anomalous behavior. In this paper, we discussed about techniques, issues and challenges. So by applying different techniques, make the new intrusion system which is also capable to detect the anomalous behavior quickly as compared to others by reducing false positives and false negative rates in new system. In Statistical anomaly detection technique, we use chi-square approach to find intrusions by frequency distribution.

References

[1]. Ho, Swee Yenn. "Intrusion detection systems for today and tomorrow." *SANS Institute, SANS Institute, InfoSec Reading Room* 8 (2001).

[2]. Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." *Journal of Network and Computer Applications* 36, no. 1 (2013): 16-24.

[3]. Rights, Retains Full. "SANS Institute InfoSec Reading Room." *Risk* 1 (2001): 27.

[4]. Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." *Computer networks* 51, no. 12 (2007): 3448-3470.

[5]. Khan, Rahul Rastogi1 Zubair Khan2 MH. "Network Anomalies Detection Using Statistical Technique: A Chi-Square approach." (2012).

[6]. Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." *computers & security* 28, no. 1 (2009): 18-28.

[7]. Ye, Nong, Syed Masum Emran, Qiang Chen, and Sean Vilbert. "Multivariate statistical analysis of audit trails for host-based intrusion detection."*Computers, IEEE Transactions on* 51, no. 7 (2002): 810-820.

[8]. Maxion, Roy, and Frank E. Feather. "A case study of ethernet anomalies in a distributed computing environment." *Reliability, IEEE Transactions on* 39, no. 4 (1990): 433-443.

[9]. Lee, Wenke, and Dong Xiang. "Information-theoretic measures for anomaly detection." In *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, pp. 130-143. IEEE, 2001.

[10]. Valdes, Alfonso, and Keith Skinner. "Adaptive, model-based monitoring for cyber attack detection." In *Recent Advances in Intrusion Detection*, pp. 80-93. Springer Berlin Heidelberg, 2000.

[11]. Gyanchandani, Manasi, J. Rana, and R. Yadav. "Taxonomy of anomaly based intrusion detection system: a review." *Neural Netw* 2, no. 43 (2012): 1-14.

[12]. Kruegel, Christopher, Darren Mutz, William Robertson, and Fredrik Valeur. "Bayesian event classification for intrusion detection." In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pp. 14-23. IEEE, 2003.

[13]. Forrest, Stephanie, Steven Hofmeyr, Aniln Somayaji, and Thomas Longstaff. "A sense of self for unix processes." In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, pp. 120-128. IEEE, 1996.

[14]. Jyothsna, V., VV Rama Prasad, and K. Munivara Prasad. "A review of anomaly based intrusion detection systems." *International Journal of Computer Applications* Vol.28, No. 7 (2011): pp.26-35.

[15]. Brown, Douglas J., Bill Suckow, and Tianqiu Wang. "A survey of intrusion detection systems." *Department of Computer Science, University of California, San Diego* (2002).

[16]. Tsai, Chih-Fong, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. "Intrusion detection by machine learning: A review." *Expert Systems with Applications* Vol.36, No. 10 (2009): pp.11994-12000.

[17]. Markou, Markos, and Sameer Singh. "Novelty detection: a review—part 1: statistical approaches." *Signal processing* Vol.83, No. 12 (2003): pp.2481-2497.

[18]. Alenezi, Mohammed, and Martin J. Reed. "Methodologies for detecting DoS/DDoS attacks against network servers." In *The Seventh International Conference on Systems and Networks Communications, ICSNC Semi-Markov models*. 2012.

[19]. Depren, Ozgur, Murat Topallar, Emin Anarim, and M. Kemal Ciliz. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." *Expert systems with Applications* Vol.29, No. 4 (2005): pp.713-722.

[20]. Sava, Neha, Priya Budhwani, Sanika Talekar, Shalaka Borle, and Nagesh Jadhav. "Survey on Intrusion Detection Systems." *International Journal* Vol.2, No. 1 (2014).

[21]. Ye, Nong, Xiangyang Li, Qiang Chen, Syed Masum Emran, and Mingming Xu. "Probabilistic techniques for intrusion detection based on computer audit data."*Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* Vol.31, No. 4 (2001): pp.266-274.

[22]. Bayarjargal, Dolgormaa, and Gihwan Cho. "Detecting an Anomalous Traffic Attack Area based on Entropy Distribution and Mahalanobis Distance."*International Journal of Security and Its Applications* Vol.8, No. 2 (2014): pp.87-94.