International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

An Extensive Survey of Intrusion Detection Systems

Ajay Prakash Sahu[1], Amit Saxena[2], Kaptan Singh[3]

[1]*PG Scholar Truba institute of Engineering and Information Technology, Bhopal (M.P.) India*
[2]*Head CSE Dept Truba institute of Engineering and Information Technology, Bhopal (M.P.) India*
[3]*CSE Dept Truba institute of Engineering and Information Technology, Bhopal (M.P.) India*

Abstract - *There are multiple ways detection is performed by IDS. In signature-based detection, a pattern or signature is in comparison to previous events to disclose present threats. But the major difficulty with today's mainly admired IDS. (Intrusion Detection System) is the formulation quantity of false positive (FP) alerts alongside with the true positive (TP) alerts, which is an awkward chore for the operator to audit to organize the proper responses. So, there is an extensive requirement to discover this area of study and to discover a reasonable solution. A main disadvantage of Intrusion Detection Systems (IDSs), despite of their detection method, is the MASSIAVE number of alerts they produce on a daily basis that can efficiently exhaust security supervisors. This constraint has guide researchers in the IDS society to not only extend better detection algorithms along with signature tuning methods, yet to also focus on determining a variety of relations between individual alerts, formally known as alert correlation. There are a various approaches of intrusion detection, like Pattern Matching, Machine Learning, Data Mining, and Measure Based Methods. This paper aims VS the proper survey of IDS so that researchers can make use of it and find the new techniques towards intrusions.*

Key Words: **Intrusion Detection System, KDD Cup99, False positive alert, Anomaly detection, misuse detection, Machine Learning**

1. INTRODUCTION

As the cost of the information technology and Internet usage falls, societies are becoming wide variety of cyber threats. According to a recent survey, the rate of cyber attacks has been more than doubling every year in recent times. It has become increasingly important to make our information systems, especially in the defense, banking, commercial, public sectors. Intrusion detection includes identifying a set of malicious actions that compromise the integrity, confidentiality, and availability of information resources. Data mining based intrusion detection techniques generally fall into one of two categories; misuse detection and anomaly detection [2] but most of the popular IDSs suffer from generating false alarms in a large volume. False alarms could be of two types. One is called false positive which is generated mistakenly by the IDS as an evidence of malicious behavior of the system, but in reality, it is not such a behavior. The other type of false alarms is called false negative. It is generated by the IDS as an evidence of non malicious event, but in reality, it should be an indication of malicious activity in the system [10]. Previous research on this area reports that this value could be as high as several hundred thousand a day but around 99% of them are false alarms while monitoring intrusion in an active operational network [11]. Network security officers need to investigate each IDS alarm manually whether it is a false or a true alarm. So, it is a quite time consuming, error prone and hard task for the network security officer to investigate manually and take proper action accordingly. Thus we have chosen to address the false alarm problem of IDSs in our survey. Intrusion Detection Systems is of two types based on sources of audit information [3].

- Host based Intrusion Detection System (HIDS):

Its data come from the records of various host activities, including audit record of operation system, system logs, application programs information, and so on

- Network based Intrusion Detection System (NIDS):

It is used to monitor the network traffic to protect the system from network based threats. It gets its data from monitoring the network traffic by using sensors and keeps the records in its defined format in the system log. It tries to detect malicious activity like Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS).

1.1General Architecture of Intrusion Detection System

A general Architecture of IDS is shown in figure 1. Typically, IDS uses the information available in system configuration Data, audit storage and previously known attacks (reference data). The IDS can be placed in the system. It can be located in target system or external to it. In former case if target system is compromised the IDS can also be invaded, in later case it IDS can be safe. IDS may use active information that is running in the system for reducing the detection time. On detecting anomaly IDS send alarm to Site Security Officer (SSO). For detection of anomaly we set the baseline for normal behaviour in IDS. For detection of true intrusion it is crucial to set the baseline of normal behaviour in IDS,

because if it not so system may generate false alarms. The objective of this paper is to identify the various attacks and defense system against the intrusions. We describe different techniques and approaches of intrusion detection so that researchers can do better comparative studies and find the new approaches of intrusion detection. Rest of the paper is organized as follow: Section 2 describes traditional IDS briefly, security functions and measures of IDS. Various types of attacks to the network are described in section 3. In section 4 previous work done is analyzed, section 5 states the current problem statement of the ids and finally in section 6 we conclude our paper.

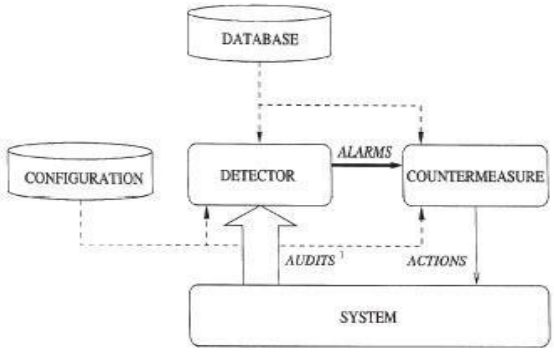

Fig -1: A general Architecture of IDS

1.2 Traditional Intrusion Detection Systems [2]

There are two types of intrusion detection system

A. Anomaly Detection: It refers to detection of abnormal behavior of host or network. It actually refers to storing features of user's usual behaviour hooked on database, and then it compares user's present behaviour with database. If any deviation occurs, and then the data tested is abnormal the patterns detected are called anomalies. Anomalies are also referred to as outliers [2].

B.Misuse Detection (or Signature-based Detection): In misuse detection approach, it defines abnormal system behaviour at first, and then defines any other behaviour, as normal behaviour. It assumes that detecting abnormal behaviour at first has a simple to define model. It produce high intrusion detection rate and raise low percentage of false alarm. However, it fails in discovering the non-pre-elected attacks in the feature library, so it cannot detect the abundant new attacks.

- Data Confidentiality:

It checks whether data/information stored in the system is secured or vulnerable [4] to attack. It is the required security function because sometime system uses the sensitive information.

- Data Availability:

It checks whether the information is available to authorized user or not. Sometimes the valid user cannot access the system information because of DoS attack, so IDS should be tough against the DoS attacks. Again this is a very required security check.

- Detection Rate:

The detection rate is defined as the no. of intrusion instances detected by the system (True Positive) divided by the total no. of intrusion instances present in the test set [8].

- False Alarm Rate:

Defined as the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns [8].

3. Types of Attacks [3]

- DoS Attack:

In this category the attacker makes some computing or memory resources too busy or too full to handle legitimate request, or deny legitimate users access to machine. DOS contains the attacks: 'neptune', 'back', 'smurf', 'pod', 'land', and 'teardrop'.

- Probing Attack(PROBE):

In this category the attacker attempt to gather information about network of computers for the apparent purpose of Circumventing its security. PROBE contains the attacks: 'portsweep', 'satan', 'nmap', and 'ipsweep'.

- Eavesdropping Attack:

It is a network layer attack, in which an attacker captures the packets from the network that are transmitting from a host to others. Attacker can read sensitive and confidential information that is transmitting.

- User to Root Attack (U2R):

In this category the attacker starts out with access to a normal user account on the system and is able to exploit some Vulnerability to obtain root access to the system. U2R contains the attacks: 'buffer overflow', 'loadmodule', 'rootkit' and 'perl'

- Remote to User Attack (R2U):

In this category the attacker sends packets to machine over a network but who does not have an account on that machine and exploits some vulnerability to gain local access as a user of that machine. R2L contain the attacks: 'warezclient', ' multihop', _ftp_ write', 'imap', 'guess_passwd',

'warezmaster', 'spy' and 'phf'.

- Man-in-the-Middle Attack:

In this type of attack the attacker situated himself in the middle of two persons in communication, and both persons in communication think that they both communicating to each other but all the conversation is compromised.

2. Related Work

In related work we explore previous work carried out by various researchers in the field of attack classification of KDD cup dataset in recent years. This section presents brief descriptions of the Data Mining and Machine Leaning approaches used by various researchers.

Kayacik ET. al. [15] proposed a work of feature relevance analysis on KDD'99 dataset on the basis of information gain. Feature relevance is expressed in terms of information gain, which gets higher as the feature gets more discriminative.

Himadri Chauhan ET. Al [16] in this paper, authors presents the comparison of different classification techniques to detect and classify intrusions into normal and abnormal behaviours. J48, Naive Bayes, JRip, and OneR algorithms are used by authors. Authors use the WEKA tool to evaluate these algorithms. The used methods are performed with NSL-KDD intrusion detection dataset.

Prof. N.S. Chandolikar ET. Al [17] in this paper authors present the work on, KDD '99 intrusion detection dataset, which is evaluated to find out most important and relevant features.

Balakrishnan ET. Al [18] proposed a new feature selection algorithm based on Information Gain Ratio. The feature selection decreases the classification time. The author claims that proposed IDS reduce the false positive rates and classification time.

Megha Aggarwal and Amrita [19] present the work on; a comparative analysis which is based on the basis of detection rate, computational time and root mean square error. In this work authors used six feature selection algorithms and their performance is evaluated using Naïve Bayes and C4.5 (J48) classifier. The authors has been observed that Naïve Bayes takes less time to test the dataset but more time in training the set whereas C4.5 does the reverse.

S. Ranjitha Kumari and Dr. P. Krishna kumari [20] in this paper authors have done a survey on four supervised machine learning algorithms: Decision Tree (J48), K-Nearest Neighbour (KNN), Naïve Bayes (NB) and Support Vector Machine (SVM). Authors have shown a comparative analysis of these algorithms based on Accuracy, True Positive Rate (TPR) and False Positive Rate (FPR). Authors have used NSL-KDD dataset for our experiment.

3. Problem Statement

The efficiency of IDS depends on the capability to detect any extraordinary activity in the target system, which is called the sense of IDS. If the IDS are more unstable, the security of the system would be tighter. To making the IDS mor unstable means to apply tighter signature rules or to be less tolerant to anomalies. As a result, the IDS become more sensitive to its input and generate a lot of alarms each day, even though most of the examined events are not illegal events.

Due to large volumes of IDS false alarms, it is a quite tough task for the security officers to investigate manually which are the real doubtful alarms and thereafter take proper action against them. Even sometimes, some real doubtful alarms are ignored mistakenly by the security officer due to large volumes of false alarms and thereby mistakenly interpret a real alarm to be a false alarm. This is the most dangerous situation when a real instance of an attack is ignored by the security officer and thus the IDS become useless though its functionality remains the same. We have chosen to investigate about this problem in our research and thus our research Problem is whether we can reduce the IDS false alarm problem to a reasonable amount, or not.

4. Conclusion

Data mining can help improve intrusion detection towards the enhancement of IDS by adding a level of focus to anomaly detection. Implementing an intrusion detection system and finding more dynamic techniques for detecting attacks in network will be examined in further study it's required to find out and analyze the techniques that are already investigated by several researchers. Keeping that in view here, we have made an attempt to review the well known intrusion detection approaches. Comparison of various approaches is made to show the strength and weakness of these approaches. We hope this study will be useful for researchers to carry forward research on system security for designs of IDS that not only will have identified strengths but also overcome the drawbacks.

REFERENCES

[1] Adriana-Christina Enache, Victor Valeriu Patriciu, "Intrusions Detection Based on Support Vector Machine Optimized with Swarm Intelligence", 9th IEEE international symposium on Applied. Computational Intelligence and Informatics", P.P. 978-1-4799-4694-5/14, May 2014.

[2] Abhaya, Kaushal Kumar, Ranjeeta Jha, Sumaiya Afroz "Data Mining Techniques for Intrusion Detection: A Review" *International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6,*

*June 2014.*R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[3] Subaira.A.S, Anitha.P, "Efficient Classification Mechanism for Network Intrusion Detection System Based on Data Mining Techniques: a Survey" International conference on Intelligent System and Control (ISCO), IEEE, P.P. 978-1-4799-3837, July 2014.

[4] Deepthy K Denatious, Anita John, "Survey on Data Mining Techniques to Enhance Intrusion Detection", International Conference on Computer Communication and Informatics (ICCCI -2012), IEEE, P.P. 978-1-4577-1583, Jan 2012.

[5] A Murali M Rao, "A Survey on Intrusion Detection Approaches", IEEE, P.P. 0-7803-9421-6, 2005.

[6] Ming Xue,Changjun Zhu. "Applies Research On Data Mining Algorithm In Network Intrusion Detection", International Joint Conference on Artificial Intelligence, IEEE, 2009.

[7] Nitin Mattord, Verma (2008). Principles of Information Security. Course Technology. Pp. 290–301. ISBN 978-1-4239-0177.

[8] Www.Users.Cs.York.Ac.Uk/~Jac/Publishedpapers/Adhocnetsfinal.Pdf.

[9] W. Feng, Q. Zhng, G. Hu, J Xiangji Huang,"Mining Network Data for Intrusion Detection Through Combining Svms with Ant Colony Networks" Future Generation Computer Systems, 2013.

[10] Gula, Ron. "Correlating ids alerts with vulnerability information." (2002).

[11] Pietraszek, Tadeusz. "Using adaptive alert classification to reduce false positives in intrusion Detection." In Recent Advances in Intrusion Detection, pp. 102-124. Springer Berlin Heidelberg, 2004.

[12] Mittal, Mitali, Alisha Khan, and Chetan Agrawal. "A Study of Different Intrusion Detection and Prevension System" International Journal of Scientific & Engineering Research 4, no. 8 (2013): 1526- 1531.

[13] Asak, Midori, Takefumi Onabura, Tadashi Inoue, and Shigeki Goto. "Remote attack detection method

[14] in IDA: MLSI-based intrusion detection using discriminant analysis." In Applications and the Internet,2002. (SAINT 2002). Proceedings. 2002 Symposium on, pp. 64-73. IEEE, 2002.

[15] Sathya, S. Siva, R. Geetha Ramani, and K. Sivaselvi. "Discriminant analysis based feature selectioninKdd intrusion dataset." International Journal of Computer Applications 31, no. 11 (2011): 1-7.

[16] Kayacik, H. Günes, A. Nur Zincir-Heywood, and Malcolm I. Heywood. "Selecting features for Intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets."In Proceedings of the third annual conference on privacy, security and trust. 2005.

[17] Chauhan, Himadri, Vipin Kumar, Sumit Pundir, and Emmanuel S. Pilli. "Comparative Analysis and Research Issues in Classification Techniques for Intrusion Detection." In Intelligent Computing,Networking, and Informatics, pp. 675-685. Springer India, 2014.

[18] Chandolikar, N. S., and V. D. Nandavadekar. "Selection of Relevant Feature for Intrusion AttackClassification by Analyzing KDD Cup 99." MIT International Journal of Computer Science &Information Technology 2, no. 2 (2012): 85-90.

[19] Balakrishnan, Senthilnayaki, K. Venkatalakshmi, and A. Kannan. "Intrusion Detection System Using FeatureSelection and Classification Technique."International Journal of Computer Science andApplication (2014).

[20] Megha Aggarwal, Amrita. "Performance Analysis of Different Feature Selection Methods In IntrusionDetection" International Journal of Scientific & Technology Research Volume 2, Issue 6, June 2013

[21] Kumari, S. Ranjitha. "Intrusion Detection-A Comparative Analysis using Classification Algorithms." Networking and Communication Engineering 5, no. 2 (2013): 85-89.

[22] Olusola, Adetunmbi A., Adeola S. Oladele, and Daramola O. Abosede. "Analysis of KDD'99 Intrusiondetection dataset for selection of relevance features." In Proceedings of the World Congress onEngineering and Computer Science, vol. 1, pp. 20-22. 2010.

[23] Chauhan, Himadri, Vipin Kumar, Sumit Pundir, and Emmanuel S. Pilli. "Comparative Analysis andResearch Issues in Classification Techniques for Intrusion Detection." In Intelligent Computing,Networking, and Informatics, pp. 675-685. Springer India, 2014.

[24] T.S.Meenatchi, K. Mythili, M. Gayathri "DATA MINING APPROACHES FOR NETWORK INTRUSION DETECTION SYSTEM" September 2016 IJSDR | Volume 1, Issue 9.

[25] Kruegel, Christopher, Fredrik Valeur, and Giovanni Vigna. Intrusion detection and correlation: challenges and solutions. Vol. 14. Springer Science & Business Media, 2005.

BIOGRAPHIES

AJAY PRAKASH SAHU
Qualification-B.E (CSE)
PG Scholar Truba institute of Engineering and Information Technology.

Prof. AMIT SAXENA
Associate Professor & HoD (truba)
Qualification-B.E(CSE) ,M.TECH , PhD(MANIT) Bhopal
Publication-18 international & 05 National Paper

Prof. KAPTAN SINGH
Qualification-B.E(CSE) ,M.TECH , PhD*(MANIT) Bhopal
Publication-01 international & 01 National Paper