Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.7, No.10, 2016

A Survey on Attacks and Advances of Intrusion Detection Systems

Ravi kishor Ahirwar*
PG Scholar, CSE, VITS, Bhopal, India

Prof. Sumit Sharma
HOD CSE, VITS, Bhopal, India

Abstract
Now day's information of an organization floating over the internet that increases the traffic on the network as well as threats from attackers. To protect these sensitive material Intrusion Detection System (IDS) is situated in the scheme. It is an application software program or hardware mechanism that compacts with assaults by assembling information from a mixture of systems and network resources, then analyzing indications of defense dilemmas. Network Intrusion Detection (NID) is a method that efforts to determine unauthorized entrance to a network through analyzing traffic on the network. There are a variety of advances of intrusion detection, for instance Data Mining, Pattern Matching, Machine Learning and Measure Based Methods. This survey paper aims towards the proper learning of intrusion detection system with the intention that researchers could create employ of it and discover the new methods towards intrusions.
Keywords: Intrusion Detection System, Data Mining, Pattern Matching, Anomaly detection, misuse detection, Machine Learning.

1. Introduction

Intrusions are the activities that violate the security policy of the system or intrusions are the set of rules that meant to compromise the system's integrity, confidentiality and availability of any resources in a computing platform [1]. Intrusion Detection System (IDS) is hardware mechanism or application software that observes the network or organization for malefic actions or policy contravention and generates reports to administration location where it is investigated for additional avoidance and recognition. The objective of IDS is to monitor network assets in order to detect misuse or anomalous behavior [2]. An IDS dynamically monitors the system's events and decide whether the use of the system is legitimate or symptomatic of an attack. It also maintains the historical records of a user activities and attack signatures. Based on these records IDS detect the threats in future and could prevent the system from them. Generally, IDSs do not act or take operative action when an intrusion detected, IDSs usually do report the system administrator about the intrusion. An IDS is a watch dog that alerts the administrator whenever any suspicious activity detected.

Intrusion Detection Systems is of two types based on sources of audit information [3]:

I. ***Host based Intrusion Detection System (HIDS):*** It refers to intrusion that take place on a single host system. This type of IDS gets it audit data from host audit trails and monitors activities such as file changes, integrity of system, system logs and host based network traffic. When any suspicious activity found by IDS, it alerts the system administrator or alert the central management server. Server or user or both could block the user request, this judgment is based on the mechanism installed in the local host system.

II. ***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).

1.1. Intrusion Detection System Model

A generic model 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 could be placed in the system. It could be located in target system or external to it. In former case if target system is compromised the IDS could also be invaded, in later case it IDS could 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 activities in IDS. For detection of true intrusion it is crucial to set the baseline of normal activities in IDS, because if it not so system may generate false alarms.

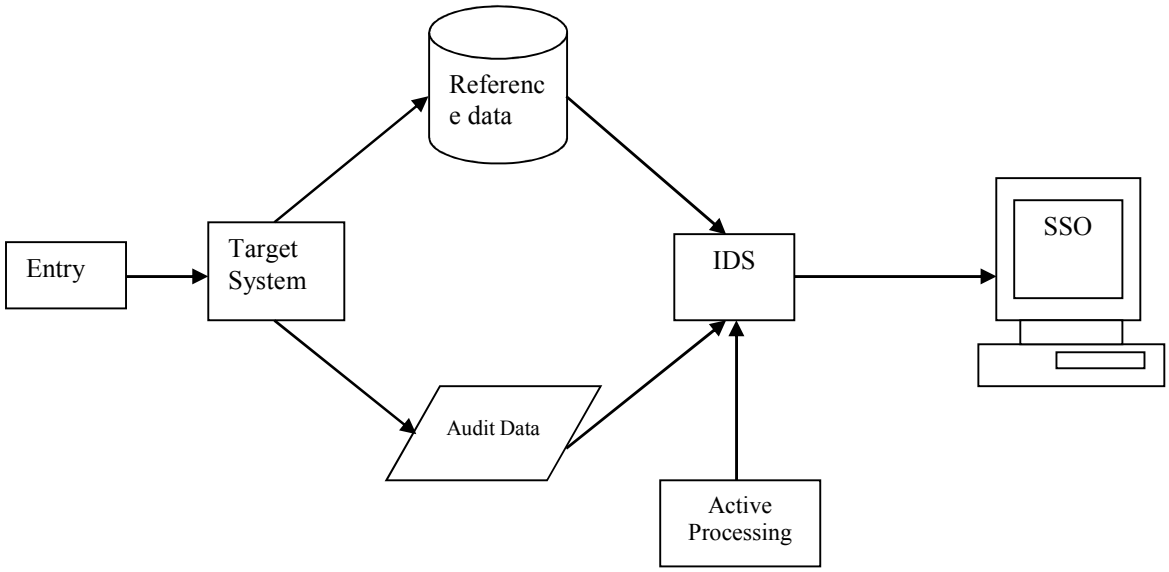

Figure 1: Generic architectural model of typical IDS

The objective of this paper is to identify the various attacks and defence system against the intrusions. We describe different techniques and approaches of intrusion detection so that researchers could do better comparative studies and find the new approaches of intrusion detection.

This paper consists of 5 sections. Section 1 describes the intrusion detection system, its techniques and its very basic architectural model. Section 2 describes types of IDS, security functions and measures of IDS. Various types of attacks to the network are described in section 3. Section 4 having different approaches to IDS, and section 5 having concluding remarks.

2. Traditional Intrusion Detection Systems

There are two types of intrusion detection system [4].

Anomaly Detection: It refers to the technique which is used to detect the malicious activities based on deviation from normal behavior. These activities are considered as an attack to the system. It could also detect the unknown intrusions. All that could happen because we could train this type of IDS for unknown abnormal behavior. For training set we could use the system logs of past activities, database of normal and abnormal behavior, and systems configuration files. The detection rate of anomaly based IDS are high but it also generates false alarms proportionally.

Three wide classifications of anomaly detection methods are as follow:

I. *Unsupervised anomaly detection method:* These methods to identify anomalies in an unlabeled experiment dataset below the hypothesis that the most of the illustrations in the dataset are standard.
II. *Supervised anomaly detection method:* These methods want a dataset that has been flagged as "standard" and "anomalous" and occupies learning a classifier.
III. *Semi-supervised anomaly detection method:* build a model signifying normal activities from a specified standard training dataset, and then experiment the probability of a trial illustration to be produced by the trained model.

Misuse Detection or Signature based Detection: Misuse detection or Signature based detection mostly depends on identifying known signatures. It means in this system we first need to determine the normal activities of the user, based on that IDS could define an activity as a normal or a threat to the system. So, this IDS system is used only for detecting known attacks (intrusions). The drawback of this system is that, a slight modification in activity could lead the system to not to generate the alarm, it could or could not be a malicious activity. The detection rate of these IDS is low but it generates very low false alarms.

IDS provide following security functions [5]:

- ***Data Confidentiality:*** It checks whether data/information stored in the system is secure or vulnerable 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 could not 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.
- ***Data Integrity:*** It ensures that data is consistent and correct throughout the life cycle of an event. The

data should not be changed in between of an event and also a valid/authorized user could have rights to change the data.

Primary criterions of measurements for IDS are as follows [6]:

- ***Burglar Alert:*** A signal is suggesting that a system has been or is being attacked [7].
- ***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

Any kind of malicious [20, 21] activity that tries to collect, infest, decline, debase, or impair information to the system resources or the data itself. An attack could be active or passive. Fig. 2 shows the types of attacks in the network.

***1) Passive attack*:** Trying to learn or concoct use of information from the system but does not clash the system resources.

- Wiretapping: Third party monitors the covert information from a telephone line or network. The secret connection will be a real electrical tape of the telephone line.
- Release of message content: Telephone conversation/Email messages/ Transferred file contain some secret data. Attacker monitors the content of these secret transmissions.
- Traffic Analysis: Attacker analyzes the traffic, determine the location, identify communication hosts, and observe frequency and length of messages. All incoming & outgoing traffic of network are analyzed but not altered.

***2) Active Attack*:** The motto of the attacker is to change the information in the network.

- Denial of Service: In a network the host could get the same information from the same server for multiple times. This causes overloading of data. By using this limitation the attacker tries to get that server for multiple times. Resulting which the services to the genuine host will be blocked.
- Spoofing: One program successfully pretense as another by sending wrong data. E.g. DNS spoofing.
- Man-in-the-middle: The attacker continuously watching the communication between two parties. The attackers make independent connection between them and relay the messages.
- ARP Poisoning: The attacker sends spoofed ARP messages onto the Local Area Network. Spoofing may allow an attacker to modify or stop all traffic.
- Buffer Overflow: While writing data to a buffer replaces adjacent memory location. This is a special case of the violation of memory safety.
- Cyber Attack: Any type of aggressive operation utilized by individual that target the computer data, infrastructure, network information.
- Phishing attack: It obtain sensational information such as user name, password and credit card details. The attackers try to get these details and they are modifying these messages.

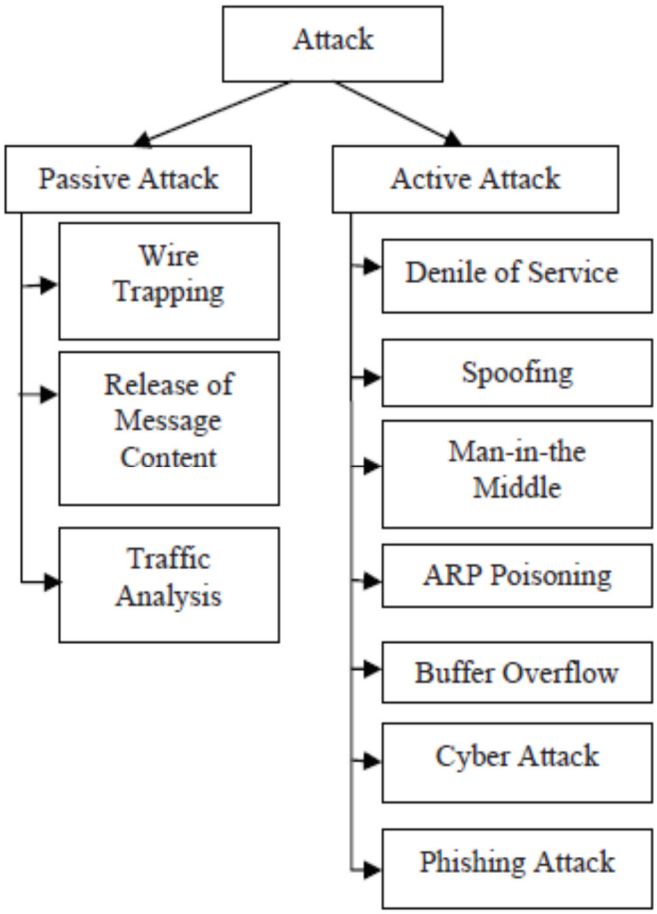

Fig. 2: Types of attack in network

4. Intrusion Detection Approaches

We give detail study about different research carried out previously and explore previous work carried out by various researchers in the field of attack classification of KDD cup dataset in recent years. We present brief descriptions of the Data Mining and Machine Leaning involved in the studies that we have done [9].

Asak et al. [10] proposed a method for discriminate analysis of Machine learning based Intrusion Detection. In which a feature selection based method is utilized for the classification of individual attack. Author's utilizes system log information as experimental purpose.

Ramani et. al. [11] proposed a Discriminate Analysis based Feature Selection of KDD Intrusion Dataset. In this paper [3], important features of KDD Cup 99 attack dataset are extracted by the use of discriminate analysis method. Author's mentioned that proposed method is suffering by two- class classification or multiclass classification problems.

Table 1: Merits and Demerits of existing intrusion detection system

Techniques used	Merits	Demerits
Fuzzy using SRPP	Compare to existing algorithm detection accuracy is high.	No of Fuzzy rule should be decreased
parallel neuro-fuzzy classifiers	Effectively detecting various intrusions.	It takes long time to detect the anomaly for the first time.
Fuzzy C-means and Support Vector Machine (F-CMSVM)	Overcome the difficulty in clustering number determination.	Over fitting occur for generation of clustering number.
Bayes factor	Successfully detect varying the attacks.	Less detection rate and require more training.
Combing SVM & Clustering based on Self Organized Ant Colony Network (CSOACN)	High detection accuracy and faster running time	Less effectiveness and less flexibility of IDS system.
Multilayer SVM classifier	Successfully overcomes the difficulties in network connection data and Maintaining high detection accuracy.	False alarm rate is higher when the data sharing gets increased in each node difficult to detect the unknown attack.
Combing Genetic algorithm (GA) & Support Vector Machine (SVM)	Higher predictive accuracy, faster convergence speed and better generalization.	High rate of false alarm while detecting the intruder.
Neural Network (NN) using shell-code identification	Simple method, high detection accuracy, differentiates various shell codes.	The approach does not differentiate good shell-codes from the bad (malicious) ones
GA using Divide & Conquer Learning Scheme	Improve the individual accuracy for the different classes of problem.	Detect only some types of attacks not all attacks.
Coupled Hidden Morkov Model (CHMM)	Best performance in terms of detection delay and accurate detection.	It is generic. It takes more resting time.
Activity sequence-based indoor pedestrian localization	Robustness, found the activity detection error and estimation error.	Detect the activity but could not match the correct location.

Kayacik et. al. [12] 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. On the basis of result authors sagest that normal, Neptune and smurf classes are highly related to certain features that make their classification easier. On the other hand authors told about certain features have no contribution to intrusion detection.

Balakrishnan et. Al [13] 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.

Adetunmbi A.Olusola et. Al [14] proposed the relevance of each feature in KDD '99 intrusion detection dataset to the detection of each class. Rough set degree of dependency and dependency ratio of each class were employed to determine the most discriminating features for each class. Empirical results show that seven features were not relevant in the detection of any class.

In this paper, selection of relevance features is carried out on KDD '99 intrusion detection evaluation dataset. Empirical results revealed that some features have no relevance in intrusion detection.

N.S.Chandolikar et. Al [15] in this paper authors evaluate performance to two well known classifiers Bayes Net and J48 algorithms for attack classification. The key ideas are to use data mining techniques efficiently for intrusion attack classification. J48 learning algorithm was found to be performing better than Bayes Net in terms of better accuracy and lower error rate. Experiment performed on KDD cup dataset demonstrates that J48 algorithm is an efficient algorithm for classification. Accuracy demonstrated helps to improve efficiency of intrusion detection system.

Prof. N.S. Chandolikar et. Al [16] in this paper authors present the work on, KDD '99 intrusion detection dataset, which is evaluated to find out most important and relevant features. Proposed work based on selection of appropriate feature for reducing the analysis effort and time. Authors suggest that feature identification helps to improve efficiency of intrusion detection system.

Megha Aggarwal and Amrita [17] 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.

Himadri Chauhan et. Al [18] in this paper, authors presents the comparison of different classification techniques to detect and classify intrusions into normal and abnormal activities s. J48, Naive Bayes, JRip, and OneR algorithms are used by authors. Authors use the WEKA tool to evaluate these algorithms. The experiments and assessments of these methods are performed with NSL-KDD intrusion detection dataset. The main task of this paper to show the comparison of the different classification algorithms and find out which algorithm will be most suitable for the intrusion detection.

S. Ranjitha Kumari and Dr. P. Krishna kumari [19] 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. On the basis of experimental result, Authors have shown that the performance of Decision Tree (J48) and K-Nearest Neighbour are better than other two algorithms in terms of Accuracy, True Positive Rate (TPR) and False Positive Rat (FPR).

In addition to the mentioned research in the previous works, my approach of machine learning is on top of Comparative Analysis based Classification of KDD'99 Intrusion Dataset.

5. Motivation

Information security is serious problem in today's extensively interconnected cyber space. Unauthorized network intrusions and computer-related fraud initiated abuses have dramatically increased due to the popularity of Internet and the implicit anonymity of network users. The commercial sectors, academic institution, government even individual desktop users are now victimized at risk from the increasing network attacks. That's why Security is one of most important issue in network management and detection of Intrusion based security attacks. To have a holistic picture of the network intrusion detection, Classification of appropriate feature is very important; it reduces analysis effort and time too. Identification of most astute feature for attack classification plays significant role in intrusion detection. Data mining could be very fruitful for feature classification and intrusion detection. In this Work, KDD '99 intrusion detection dataset is evaluated to find out most important and best classifiers features.

6. Conclusion

This survey paper describes special categories of intrusion detection system and best parts of methods of intrusion detection systems. We draw attention to Pattern Matching, Measure Based method, Data Mining method, Machine Learning Method techniques, which is used to execute Intrusion Detection System (IDS). We also describe special types of attack from which we need to take precautions in IDS. We do the comparative analysis of various Intrusion detection approaches. We sure this brief survey is useful for all researchers that want to investigate more efficient methods against intrusions.

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] K. Asif, Talha A. Khan, Sufyan Yakoob, "Network Intrusion Detection And Its Strategic Importance", Ieee Beiac, P.P 978-1-4673, Sept 2013
[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] Midori Asak a, Takefumi Onabura, T adashi Inoue, Shigeki Goto. 2002. Remote Attack Detection Method in IDA: MLSI-Based Intrusion Detection using Discriminant Analysis. Proceedings of the 2002 Symposium on Applications and the Internet (SAINT.02), IEEE.
[11] Dr. R.Geetha Ramani, Dr.S.Siva Sathya, K.Sivaselvi. 2011. Discriminant Analysis based Feature Selection in KDD Intrusion Dataset, International Journal of Computer Applications (0975 – 8887) Volume 31– No.11, October 2011.
[12] H. Günes Kayacık, A. Nur Zincir-Heywood, Malcolm I. Heywood, Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets.
[13] Senthilnayaki Balakrishnan, Venkatalakshmi K, Kannan A. 2014. Intrusion Detection System Using Feature Selection and Classification Technique. International Journal of Computer Science and Application (IJCSA) Volume 3 Issue 4, November 2014.
[14] Adetunmbi A.Olusola., Adeola S.Oladele. and Daramola O.Abosede.2010. Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features. Proceedings of the World Congress on Engineering and Computer Science 2010 Vol I WCECS 2010, October 20-22, 2010, San Francisco, USA.
[15] N.S.Chandolikar & V.D.Nandavadekar.2012. Comparative Analysis of Two Algorithms for Intrusion Attack Classification Using Kdd Cup Dataset. International Journal of Computer Science and Engineering (IJCSE) Vol.1, Issue 1 Aug 2012 81-88
[16] N.S. Chandolikar & Prof. (Dr.) V.D. Nandavadekar. 2012. Selection of Relevant Feature for Intrusion Attack Classification by Analyzing KDD Cup 99. MIT International Journal of Computer Science & Information Technology, Vol. 2, No. 2, Aug. 2012, pp. (85-90)
[17] Megha Aggarwal, Amrita. 2013. Performance Analysis of Different Feature Selection Methods In Intrusion Detection. International Journal of Scientific & Technology Research Volume 2, Issue 6, June 2013
[18] Himadri Chauhan, Vipin Kumar, Sumit Pundir and Emmanuel S. Pilli. 2013. Comparative Analysis and Research Issues in Classification Techniques for Intrusion Detection. Intelligent Computing, Networking, and Informatics, Advances in Intelligent Systems and Computing Volume 243, 2014, pp 675-685
[19] S. Ranjitha Kumari, Dr. P. Krishna kumari. 2013. Intrusion Detection- A Comparative Analysis using Classification Algorithms. CIIT International Journal of Networking and Communication Engineering Vol 5, No 2 (2013)
[20] Patcha, A. and Park, J.M., 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12), pp.3448-3470.
[21] Jabez, J., and B. Muthukumar. "Intrusion Detection System (IDS): Anomaly detection using outlier detection approach." Procedia Computer Science 48 (2015): 338-346.