SURVEY ON INTRUSION DETECTION SYSTEM

Ms. Kasbe Amrapali[1], Ms. Morde Priyanka [2], Mr. Dhoble Saket[3], Mr. Bhosle S.B.[4]

[1] *Student, Computer Engg., JCOE, Maharastra, India*
[2] *Student, Computer Engg., JCOE, Maharastra, India*
[3] *Student, Computer Engg., JCOE, Maharastra, India*
[4] *Assistant Prof., Computer Engg., JCOE, Maharastra, India*

ABSTRACT

Network is connecting to the rest of the world through the internet. In interconnected system servers are under threads from network attackers. The Denial-of-Service (DoS) attack is the most common attack, which cause serious impact on these computing systems. DoS attack reduce the efficiency of server, in order to increase the efficiency of the server it is necessary to detect the DoS attacks. This paper presents survey of intrusion detection techniques that were proposed by various researchers. There are various techniques that were proposed but the problem of false positive rate still present. It is necessary that detection rate must be high and false positive rate is small enough that alarm from intrusion detection system can be trusted.

Keyword: - *Intrusion Detection, Anomaly Based Detection, Misuse Based Detection, DoS attacks.*

---

1. INTRODUCTION

In modern days, security has been a large priority during the transmission of data in wireless network. This is due to the existence of hacking and other malicious activities that occur just like any other common day-to-day routine. Due to the progress in technology, computer networks are getting more advanced and well equipped. The wireless networks are more accessible and it is more vulnerable to attacks than wired network. The widely known actuality about the wireless network is that, it's easy to accessible and shareable nature of medium. This attack can be the disruption of network operations [1]. It is termed as Denial of service attack or jamming. Depending on whether one looks at the consequence or the cause of attack, a most common example of such an attack is web site is not getting loaded properly. This is an example of jamming or the Denial of Service attack initiated by attacker. This attack can also be done deliberately. It's become a race between attacker and security experts in which one tries to find new methods of attacking system and other one tries to block the attacks.

The data must be transmitted between legitimate nodes irrespective of the attack induced by the attacker. There must not be any interruption between the legitimate users. It is also not ethically and morally accepted if the legitimate node user communicates with the attacker. At such times the node involved in such scam must be identified and warned of any other misleading activities in the network may compromise both the network and the data. The DoS attack detection uses the network based detection mechanism [1][2]. The detection system having two approaches misuse detection [3] and anomaly detection [2]. Misuse detection techniques used to identify the known attack by using the signature i.e. predefined rules for detecting attacks. Anomaly detection technique builds normal profile of monitored entity and the baseline is selected to differentiate normal vs anomalous traffic. When there is large deviation from baseline it is classified as intrusion. The rest of the paper contains survey of different network intrusion detection systems [3].

2. LITERATURE SURVEY

Intrusion Detection is a system that is particularly designed to detect intrusions. It consists of set of techniques and methods used to detect suspicious activities. The objective of IDS is to detect and inform about intrusions. The intrusion detection system is categorized into two types Host Based Intrusion Detection Systems (HIDS) and Network Based Intrusion Detection Systems (NIDS).

Host-based IDSs (HIDS) – monitors and analyses data of individual host machine to find sign of attacks.

Network-based IDSs (NIDS) – monitors network traffic at router or server. Such system detects threat and then alerts the system or network administrator for further action [02].

Intrusion Detection Systems can also be categorized based on mechanism employed for detection such as signature based detection and anomaly detection. Anomaly detection technique uses normal profile of user and any large deviation to this normal activity is considered as intrusion. But anomaly detection system suffers from large false positive rate in which activities that are not intrusive are flagged as intrusive. The signature based detection mechanism uses rules for detecting intrusions and each activity is cross checked against the rule for detecting sign of intrusion. Whenever signature matches with activity of user then system generates alarm [1][2]. There are various technique that were previously used by researchers for building anomaly based detection mechanism such as machine learning, data mining, statistical analysis, etc. In this paper we will review some of these techniques.

NIDES are real-time IDS that monitor user activity on multiple target systems. NIDES are placed on a single host that analyses audit data collected from interconnected systems. Intrusion detection on NIDES is a hybrid of misuse detection and anomaly detection; a rule based signature analysis and a statistical profile-based anomaly detector. The notation expert in NIDES means a system that is intelligently processing intrusion alarms to decide whether further investigation from a security guard is needed or not. Further development of NIDES evolved into SRI's project called EMERALD [5].

A protocol based anomaly detection monitors protocols for deviations from the protocol standard specifications. The detector creates models based on TCP/IP protocol specification which is then matched against the network traffic. If the monitored traffic operates with a protocol that is in conflict with the specification, it is then marked as an anomaly. Most of the protocol based anomaly detectors are built as state machines. This is understandable as all connection oriented protocols have a state. The detector is therefore monitoring transitions from one state to another and if the anticipated transition is different from the transition that has occurred, an alarm is triggered. [6] All of these methods have their pros and cons depending on what is the monitoring target. A protocol based detection method is efficient on analyzing network protocols but is not capable of detecting malicious payload. The same applies vice versa, payload based detection method can be efficient in detection malicious data in payloads but is not efficient in detecting intrusive use of protocols [6].

Forrest et al. (1996) work on intrusion detection found that in normal use most UNIX processes make highly predictable sequences of system calls. Network anomaly detectors look for abnormal traffic ADAM (Audit Data and Mining) [12] is an network intrusion detection system trained on both normal and anomalous traffic with labeled attacks. ADAM monitors IP addresses, port numbers, subnets, and TCP state for detecting sign of intrusion. It uses naive Bayes classifier that finds probability of traffic record to which it belongs, it depends on the probability of the class, and the combined probabilities of a large collection of rules [7]. Dasgupta et al. [19] focusses on the recent improvements in Artificial Immune System [AIS]. Yang et al. [20] use a related method in AIS to enhance the performance of IDS, using antibody concentration to evaluate the damaging power of the intrusion in the network.

Data mining is a technique used for uncovering patterns, associations, changes and statistical structures that are impossible for human to find from large amount of data. Analyzing large amounts of data is possible due to advances in computer science and machine learning. Classifiers are constructed based on these features which are used to classify the monitored features into anomalies and known intrusions. Data mining is an example of method that combines algorithms used in different methods like in machine-learning, statistical and signal processing based methods. [10] Saboori et al. [14] proposed an Apriori Algorithm to detect an anomaly in the system. It predicts a novel attack and generates a set of real-time rules for the firewall, and functions by extracting the correlation relationships among large data sets. In paper [15] author applied k-means clustering over a training samples so that it can categorize the samples into different clusters thus enabling categorization of samples into normal or attack group.

In a statistical based method anomalies are detected from statistics. Statistical based methods create models based on history. These models are then compared to the current situation and deviations between these models are considered as anomalies. Once a deviation is monitored its severity is then evaluated and graded. The more severe the anomaly is the higher the grade is. For example, the average number of times a user has accessed the network daily is compared to the current amount. If the current number of access to the network exceed the average number by one or two it is not maybe considered as a severe anomaly. But in case the number is, for example, ten times or even hundred times higher, it might be a severe anomaly. This of course depends on how the grading rules are defined [12]. Matthew et. al [9] developed system learns the normal range values of packet header field at the network, data link, transport/control layers (TCP, UDP, ICMP) and uses it as baseline parameter to detect anomalous event. There system is able to detect some of the attacks in the DARPA data set that involve exploits at the transport layer. Tan et al. [12] applied multivariate correlation analysis technique to determine correlation between different features by generating triangle area map technique, to identify DoS attacks. Author also applied covariance matrix technique [12] for identifying DoS attacks.

In a machine-learning based method anomaly detection models are constructed based on past behavior. The learning algorithm analyses, for example, previously recorded data sets containing network traffic and create a model of normal behavior. After the learning period the detector monitors deviations from this created model. A machine-learning based detector can adapt to changes in the network traffic when, for example, some application is distributed to all local machines in the network and this application generates previously unknown traffic to the network [8].

Network intrusion detection system can be tested using publicly available datasets such as KDD99 dataset, NSL-KDD dataset. The KDD 99 dataset contains seven weeks of training data and two weeks of testing data. The raw data consist of about four gigabytes of compressed binary TCP dump data from the generated network traffic. Finally this data is pre-processed into five million connection records, in which each line is a vector representing feature values of that network connection. Although not without its drawbacks, KDD 99 benchmark provides the only publicly available labeled datasets for comparing IDS systems, which the authors are aware of. Each connection was labeled as normal or as exactly one specific kind of attack. There were a total of 37 attack types in the data set. The simulated attacks fell in exactly one of the four categories: User to Root; Denial of Service; Remote to Local; and Probe [12].

Denial of Service (dos): Attacker tries to prevent legitimate users from using a service.
Remote to Local (r2l): Attacker does not have an account on the victim machine, hence tries to gain access.
User to Root (u2r): Attacker has local access to the victim machine and tries to gain super user privileges.
Probe: Attacker tries to gain information about the target host.

4. CONCLUSIONS

Network Intrusion Detection System is a latest kind of defense technology which is one of the vibrant areas in network security. In recent years many techniques are available for intrusion detection. In this paper, a detailed survey of important techniques based on intrusion detection is presented. Also the classification of the techniques based on rule based, k-means, hybrid techniques, statistical analysis etc., is provided.

REFERENCES

[1]. V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Computing Surveys, vol. 41, no. 3, 2009.
[2]. Denning D.E., “An Intrusion-detection Model,” IEEE Transactions on Software Engineering, pp. 222-232, 1987.
[3]. B. Mukherjee, L. Heberlein, and K. Levitt, “Network Intrusion Detection,” IEEE Network, 8(3), pp. 26-41, May/Jun. 1994.
[4]. P. Casas, J. Mazel, and P. Owezarski, “Unsupervised Network Intrusion Detection Systems: Detecting the Unknown without Knowledge,” Computer Communications, Vol. 35, pp. 772-783, 2012.
[5]. Debra Anderson,Thane Frivold, Alfonso Valdes,"Next-generation Intrusion Detection Expert System (NIDES) A Summary",Computer Science Laboratory,SRI-CSL-95-07, May 1995

[6]. K. Wang, S. Stolfo, Anomalous payload-based network intrusion detection, in: E. Jonsson, A. Valdes, M. Almgren (Eds.), Recent Advances in Intrusion Detection, Springer, Berlin, Heidelberg, 2004, pp. 203–222
[7]. Forrest, Hofmeyr, et al.,"A sense of self for unix processes", Proceedings of the 1996 IEEE Symposium on Security and Pri v ac y , IEEE Computer Society Press, Los Alamitos, CA, pp. 120–128 (1996), 1996
[8]. H. Om and T.K. Sarkar, "Neural network based intrusion detection system for detecting changes in hardware profile," Journal of Discrete Mathematical Sciences & Cryptography, vol. 12(4), pp. 451-466, 2009.
[9]. F..M. Sabri, Md. Norwawi, and K. Seman, "Identifying False Alarm Rates for Intrusion Detection System with Data Mining," International Journal of Computer Science and Network Security, Vol.11 No.4, Apr. 2011.
[10]. P. G. Teodoro, J. D. Verdejo, G. M.Fernandez, and E.Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", computer & security, Vol. 28, Issues 1–2, pp. 18-28, Feb.–March 2009.
[11]. C.F. Tsai and C.Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," Pattern Recognition, vol. 43, pp. 222-229, 2010.
[12]. Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Denial –of Service Attack Detection Based on Multivariate Correlation Analysis," Proc. Conf. Neural Information Processing, pp. 756-765, 2011
[13]. S. Axelsson, Intrusion detection systems: a survey and taxonomy, in: Technical Report, 2000, pp. 1–27.
[14]. E. Saboori, S. Parsazad, Y. Sanatkhani, "Automatic firewall rules generator for anomaly detection systems with Apriori algorithm," 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE),Chengdu, China,Vol.6 , Aug. 20-22, 2010, pp.V6-57-V6-60.
[15]. M. Varaprasad Rao, A. Damodaram, N. Ch. Bhatra Charyulu,"Algorithm for Clustering with Intrusion Detection Using Modified and Hashed K – Means Algorithms",Advances in Computer Science, Engineering & Applications,2012, Volume 167, pp 737-744