Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review on Intrusion Detection Approaches with Machine Learning

Shakil Ghalib*, Kapil Dewan
CSE & PTU
India

Abstract— With the increasing amount of network throughput and security threat, the study of intrusion detection systems (IDSs) has received a lot of attention throughout the computer science field. Current challenges to find the way of detection the intrusion ,Machine learning approaches improve the intrusion detection. in this paper we have review these machine learning approaches

Keywords— machine learning, intrusion detection, network

I. INTRODUCTION

The network security is becoming an essential need of modern society to protect the confidential information flowing over the networks. Detection of Intrusion over the network is one the most extremely important task to prevent their unlawful use by the attackers [1]. Efficient intrusion detection is needed as a defense of the network system to detect the attacks over the network. A feature selection and classification based Intrusion Detection model is presented, by implementing feature selection, the dimensions of NSL-KDD[5] data set is reduced then by applying machine learning approach, we are able to build Intrusion detection model to find attacks on system and improve the intrusion detection using the captured data. With the increasing number of new unseen attacks the purpose of this model is to develop a system for intrusion detection, and the model will be capable of detecting new and previously unseen attacks using the basic signatures and the features of known attacks.

The important and valuable information always attract attackers and is always liable to maximum attacks over the network. Intrusion is getting into the system or system server by the attacker by sending the malicious packet to the user system and then stealing, corrupting or modifying any confidential information or important information, the sending of network packet over the network for illegal purpose is known as attack. The intrusion can occur over the system or server due to any existing system weakness or vulnerability, such as system misconfiguration, user misuse or program defects. An intelligent intrusion can also be made by putting multiple vulnerabilities together. In a global network there are millions of big servers and large number of on-line services running in the system while such networks attract more attackers and need intelligent intrusion detection model as a defense for their network system [2]

An Intelligent intrusion or system attack includes following step:

- **Collecting Information**: Collecting information about the target getting all the knowledge and details about the user who is attacked. This can be done by using the query tools like ‘‘whois”, ‘‘nslookup” or by using network commands in command prompt to get IP addresses, domain name server etc.[3]
- **Probing and scanning:** Scanning the Target host and check the unguarded or unprotected area on system and seek for the sensitive information in them.
- **Remote to Local access**: It is gaining the access of user system by R2L (Remote to Local) type of attack, like password guessing, network sniffing, buffer overflow attack, etc. An R2L attack means a person who is unknown to user machine send the network packet to get local access of user machine to execute command on a target. This attack can be done by using the system vulnerabilities, using open ports of the target machine, password guessing etc. [3]
- **User to Root access**: In this attack a normal user of system tries to gain a root access of the system by using system vulnerabilities. These attacks are quite similar to R2L attack but in this attacker are already a normal user of machine and try to gain root access of machine.
- **Launch attacks**: Finally attacks are made like stealing confidential information, modifying web pages, accessing another person accounts and creating a backdoors for future attacks.

An Intrusion Detection System (IDS) is security technique to detect the attacks over the network. Intrusion detection has been classified under two categories, namely misuse detection and anomaly detection.

1.1 Types of Intrusion Detection:

- Network based
- Host based

Network based: Network based intrusion detection system (NIDS) monitors is used to monitor the information flowing over the internet network and detect the intrusions. In a network-based system, or NIDS, the individual packets flowing through a network are analyzer. In this method NIDS is applied before the Firewall, so that it can examine all the data packets flowing through the network.

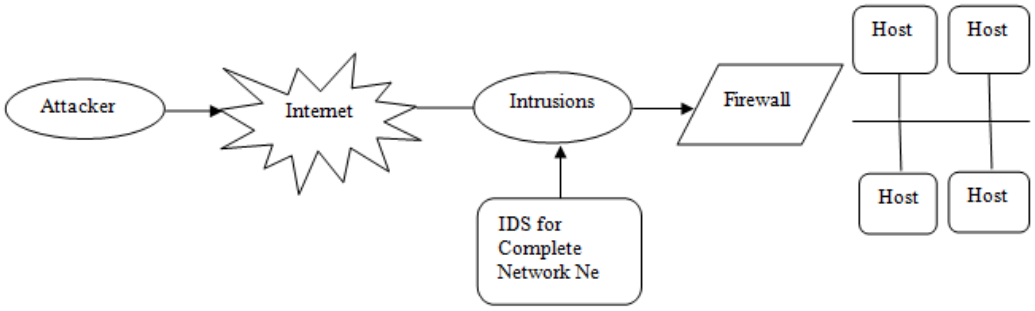

Fig.1.1.Showing network based intrusion detection system.

Host based: Host based intrusion detection system (HIDS) also monitors the flow of information and detects the attacks over the system, but based on network events. In host based intrusion detection operating system events are monitored. In host based system, the Intrusion Detection System (IDS) examine at the activity on each individual computer or host.[4] In this approach the IDS is applied on Individual systems.

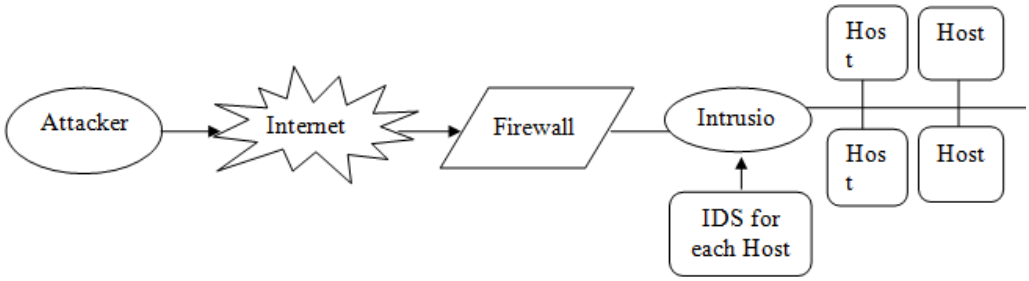

Fig-1.2. Showing host based intrusion detection system.

II. LITERATURE SURVEY

The two prime motives to make an attack are to force the network to stop some service or to steal some confidential information from the network [3]. An intrusion detection system must be able to recognize the Anomalous behavior of data. Some previous work done by the authors for the Intrusion Detection are described which laid foundation for present work.

Anup K. Ghosh, Aaron Schwartzbard & Michael Schatz [3] et.al has proposed learning Program Behavior Profiles for Intrusion detection. This paper is based on learning the behavior of attack indicators from the data set and then detecting the intrusions. Author first has used equality matching algorithm for intrusion detection, which is quite simple attack detection approach based on comparing the patterns. Second author used Back propagation network, in this he has used ANN machine learning method for the detection of intrusions. This approach is used basically used for new unknown attacks detection in data.

This disadvantage of author approach is first detection is done on learning the patterns of old attacks and second author haven't used many learning algorithms for testing the intrusion detection.

Kumar J. Das [4] et.al has proposed Attack Development for Intrusion Detection Evaluation. In modern word attacks on systems and software are becoming a major concern. The dependence on computers and networks for all kind of business and organizational works has increased the risk of damaging the confidential information flowing over networks. Firewalls, security policies and encryption etc are not sufficient to protect the systems from the attacks. Intrusion detection systems are required to enhance the capabilities of current protection models.

Lisong Pei, Jakob Schütte, Carlos Simon in 2007[5] et.al explained that intrusion detection can be either host based or network based. In host based to detect the intrusion every system is monitored independently in the network, where as in network based intrusion detection the detection of intrusion is monitored at the entry level means before the firewall of the network.

Sabhnani, M.& Serpen, G.[6] et.al has proposed application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context. In this paper a simulation study was performed on KDD-99 cup data set for intrusion detection. Various classifier algorithms are applied over the data set and a learning model is tested. The results shows that none of the model was able to detect the User to Root and Remote to Local attack successfully and further no method tried for reducing the dimension of data set for improving the efficiency of intrusion detection.

Aarthy. R, and P.Marikkannu,[7]. Et.al has proposed the Lightweight Network Intrusion Detection System (LNID) which is an intrusion detection model. This model purposes a filtering scheme in which there are two packet filters: Tcpdump Filter and LNID Filter. The Tcpdump processes the initial packets and extracting the TCP packets towards Telnet servers of internal local area network.

Meera Gandhi,G, Kumaravel Appavoo ,Srivatsa,S.K[8] et.al has proposed several decision trees and rules. To perform the classification the learning algorithms used are JRIP, Decision Tabel, PART, and One R) and trees (J48, Random Forest, REPTree, NBTree). Attack shows the vibrant properties, daily new attacks are discovered in such a rapid environment of attacks learning algorithms can optimize with the changing properties of attacks, this is the main advantage of using the learning algorithms. Learning is based on acquired knowledge gained during the processing of data used for training the learning algorithms. Here the machine learning is used as a technique for making the selection, using as training data. Based on the outcome of machine learning, a best algorithm for each attack category is chosen and two classifier algorithm selection models are proposed The model shows performance improvements. The classification learning algorithms were trained over the captured Knowledge Discovery Databases (KDD) data set for identifying the attacks. Then the learned models were used for indicating the risk of the attacks in a web server environment or by any network administrator. To classify the accuracy the author used 10-fold Cross Validation approach and the results have been compared to obtain the accuracy .The authors' purpose attack detection model based on various learning algorithms. The performance of model is evaluated using 10-fold cross validation, due to cross validation the obtained accuracy was only for the known attacks. In cross validation training and train data set are same therefore model will show the accuracy only for the previously known attacks.

Aarthy.R and P.Marikkannu,[7] et.al. has proposed that security system for IDS by using data cleaning in large database. This process is based on by first making the policies in database and then matching the policies with the information coming to the system to detect the intrusion .So this method is good for the attacks whose policies are already defined, it means for each time when a new unseen intrusions are coming policy database need to be updated that is hard to implement.

Guy Helmer, Johnny S.K. Wong, Vasant Honvar, Les Miller, Yanxin Wang, [9] has proposed Light weight agents for intrusion detection. This approach is designed and implemented for intrusion detection system (IDS) prototype based on mobile agents. In this approach the mobile agents detect the intrusion by travelling over the networks of distributed system. These agents classify and correlate information, and report the information to a user interface and database through mediators. Agent systems allow the addition of new features to the agents. This technique is planned and implemented for intrusion detection system (IDS) prototype based on mobile agents , but limited for only mobile agents.

Anna Sperotto,A, Schaffrath,G, Sadre,R, Morariu,C, Pras,A and Stiller,B, [2] et.al has proposed IP Flow-Based Intrusion Detection system, this approach detect the attacks my monitoring the contents of every packet in the network, but having a disadvantage that monitoring the contents of every network packet cannot be done in high speed networks. Therefore alternative approach is created where flow of data instead of packets is monitored in the network, but still intrusion detection is more accurate when the analysis of individual packet is done. Therefore there is still a need of detection model that analyzes the individual packet in network even then when there are high speed networks.

III. CONCLUSION

The study of intrusion detection systems (IDSs) has received a lot of attention throughout the computer science field. Current challenges to find the way of detection the intrusion ,Machine learning approaches improve the intrusion detection. in this paper we have review these machine learning approaches .This approach is designed and implemented for intrusion detection system (IDS) prototype based on mobile agents. In this approach the mobile agents detect the intrusion by travelling over the networks of distributed system. These agents classify and correlate information, and report the information to a user interface and database through mediators. Agent systems allow the addition of new features to the agents.

REFERENCES

[1] Sharmila, K, Wagh, Vinod K, Pachghare, Satish R, Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques," *IJCA International Journal of computer Applications*, vol.78, no.16, pp. 30-37, Sept 2013.

[2] Bajaj, K. Arora, A., "Dimension Reduction in Intrusion Detection Features Using Discriminative Machine Learning Approach," *IJCSI International Journal of Computer Science Issues*, Vol. 10, no. 4, pp. 324-328, July 2013.

[3] Chen, M. C, Chen, Y. L, Chung L. H, "An efficient network intrusion detection," *Elsevier, Computer Applications*, vol.33, no.4, pp. 477-484, March 2010.

[4] Marcus A. M, "*Machine Learning and Data Mining for Computer security*," Springer, 2006.

[5] Richard A. Kemmerer and Giovanni V, "Intrusion Detection: A Brief History and Overview". *IEEE explore, Journals & Magazines, computers*. vol.35, no.4, pp. 27-30, August 2002.

[6] Tavallaee,M, Bagheri, E, W, Lu, and Ali A,G, "A Detailed Analysis of the KDD CUP 99 Data Set" *IEEE Symposium on computational intelligence in security and defense application*, pp. 1-6, 8-10 July 2009.

[7] Stolfo, S,J, Fan W, Lee, W, Prodromidis, A, and Chan, P,K, "Cost based modeling for fraud and intrusion detection: Results from the jam project," In *Proc. of DARPA Information Survivability Conference and Exposition.DISCEX'00,* vol.2 pp 130-144, January 2000.

[8] Lippmann,P,R, Fried,D,J, Graf,I, Haines,J,W, Kendall,K,R, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," In *Proc. DARPA Information and Exposition,DISCEX'00,* pp. 12-26, 25-27 January,2000.

[9] Shrivastava, G, Sharma, K,R,S, "The Detection & Defense of DoS & DDoS Attack: A Technical Overview," In Proc. of ICC, 27-28, pp. 274-282 ,December 2010.

[10] Cowan C, Walgle P, Pu C, "Buffer overflows: Attacks and defenses for the vulnerability of the decade," In *Proc. Information Survivability Conference and Exposition.DISCEX'00,* vol.2, pp. 119-129, 25-27 January 2000.

[11] Uppuluri, P, Sekar, R, "Experiences with specification-based intrusion detection.," *In Recent Advances in Intrusion Detection, Springer Berlin Heidelberg*, pp. 172-189, 10-12 October 2001.

[12] Baumann, R. *Ethical Hacking* GSEC Practical Version 1.4, November 2002.

[13] Anup K. Ghosh, Schwartzbard A, Schatz M, "Workshop on Intrusion Detection and Network Monitoring," Santa Clara, California, USA.,1999.

