A SURVEY to Track Intrusion Detection in the System by using Data Mining

Ms. Ashwini D. Motghare[1], Ms. Archana A. Nikose[2]

[1]Student, Depart. of computer science and engineering, Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
[2]Professor, Depart. of computer science and engineering, Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India

---***---

Abstract - *In recent years, security of computer network has become main stream in most of everyone's lives. Intrusion detection is the method of identifying unauthorized use, misuse, harmful and abuse of computer systems by both system insiders and external attackers. There are several techniques for intrusion detection, many researchers used machine learning techniques for intrusion detection, but some shows poor detection, some techniques takes large amount of training time. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify malicious behaviors launched from the outside world of the system only. In this paper, presents an intelligent learning approach using Hybrid Algorithm to detect intrusions in the distributed network. The algorithm improves the efficiency of intrusion detection, reduces false positives of intrusion detection by monitoring Hardware (keyboard, mouse) as well as software activity (web based, IDE, tools with Computer) activity.*

Key Words: Intrusion detection**,** Insider attackers, Hybrid, Hardware, Software*.*

1. INTRODUCTION

With the rapid expansion of computer networks during the past years, security has become a crucial issue for computer systems. An intrusion detection system (IDS) [1] is an active process or device that analyzes system and network activity for unauthorized and nasty activity. IDS maintains a set of historical profiles for users, matches and audit record with appropriate profile, update the profiles whenever necessary, and reports any anomalies detected. There are two main approaches to the design of IDS [2].

In a misuse detection based IDS, intrusions are found by looking for activities that correspond to known signatures of intrusions. On the other hand, anomaly detection based IDS, intrusions are detected by searching for abnormal network traffic. One of the most commonly used approaches in IDS is expert system based intrusion detection systems i.e. rule-based analysis but it is a static. In Soft computing approach includes an intelligent agent in the system that is capable of disclosing the latent patterns in abnormal and normal connection audit records, and to derive the patterns to produce connection records of the same class. In neural network approach [3] training is provided for intrusion detection.

2. LITERATURE SURVEY

Sufyan T. Faraj Al-Janabi and Hadeel Amjed Saeed.[1] in this paper, a back propagation artificial neural network (ANN) to learn system's behaviour. One of the issues comes in this that ANN requires a very large amount of data and considerable time to ensure that the results are accurate. Another issue is that there is some kind of compromise between increasing the classification levels and the percentage of identification.

Kapil Wankhade, Sadia Patka, Ravindra Thool[4] in this paper, describes the system architecture for intrusion detection system (IDS) based on hybrid data mining techniques. It is based on K-means clustering, which is a typical clustering algorithm. It overcomes the drawbacks of K-means thereby employing a hybrid approach.

Bini V. C, Ms. Nimmy K, Prof. P. Jayakumar[5] in this work, they explain a security system called Internal Intrusion Detection System (IIDS) using data mining and bevaviometric technique to detect the internal intrusion. Behavioral biometric includes the user behavior such as speed of typing, sound of typing on a keyboard. It is also known as keystroke dynamics. Because of uniquely find user, it is more popular among strong authentication techniques.

Hu Zhengbing, Su Jun, Shirochin V. P. [9] By defining user profiles previously, it can easily find out the anomalies and malicious accesses instantly. With the help of user's profiles, we can't only uncover which account has been misused, but also realize who the true intruder is. There is no need to update the knowledge databases of HFIDS manually, it is a self-organized and self-training system. Furthermore, we can discover cooperative attacks simultaneously submitted by the users as well by using data mining and forensic techniques as the attacks are performing. The paper proposes a framework for tracing the intruding and the infecting paths so that the vulnerabilities on the devices and hosts along the paths can be easily discovered and repaired. As new network device called Lightweight Intrusion Detector (LID) which used to figure out these paths quickly is designed and developed.

Miss Prajkta P. Chapke, Miss Rupali R. Deshmukh[12] in this paper, IDS is the Signature Based IDS. The system is designed which detects the signatures. Normally the signatures are embedded in the Packet and are sent to the client system to destroy the machines. Now we have to find out these signatures using the fuzzy rules. Information about these signatures is used to create rules. The detection system is based on rules. These rules are based on intruder signatures. These rules may be used to check various parts of a data packet. For the comparison of content C4.5 Algorithm is used. The packets are capture using WinPcap and JPcap software's. A report for all the protocols which are running is generated. Also the log files generated.

D. Dhanavandhini , Mrs. S.Umadevi.[15] It analyzes what attackers have done such as spreading computer viruses, malwares, and malicious codes and conducting DDoS attacks. The SC monitor and filter, as a loadable module inserted in the kernel of the system being considered, collects those SCs submitted to the kernel and stores these SCs in the arrangement of uid, pid, SC in the protected system. It also stores the user inputs in the user's log file. To find out what SCs are typical ones generated by a shell command, the statistic model of term frequency-inverse document frequency (TF-IDF) is used to analyze the importance of intercepted SCs collected in a user log file. The mining server analyzes the log data with data mining techniques to identify the user's computer usage habits as his/her behavior patterns, which are then recorded in the user's user profile. An attack pattern (or a signature), can be identified in the same method. The detection server compares users' behavior patterns with that SC-patterns collected in the attacker profile, called attack patterns, and those in user profiles to respectively detect malicious behaviors and identify who the attacker is in real time.

3. CONCLUSION

We proposed new methodology which focus on both hardware and software activity which result in higher accuracy as compared to previous intrusion detection methodology. It is a convenient way of extracting patterns and focuses on issues relating to their feasibility, utility, efficiency and scalability. Thus data mining techniques help to detect patterns in the data set and use these patterns to detect future intrusions in similar data.

REFERENCES

1) Sufyan T. Faraj Al-Janabi and Hadeel Amjed Saeed, "A Neural Network Based Anomaly Intrusion Detection System" 2011 Developments in E-systems Engineering , IEEE Publication - 978-0-7695-4593-6/11 , DOI 0.1109/DeSE.2011.19

2) George S. Oreku, Fredrick J. Mtenzi, "Intrusion Detection Based on Data Mining", 8th ed., IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009

3) Mohammad Taghi Jafari1 , Hamdollah Ghamgin2, "Artificial immune intrusion detection system", Intl. Res. J. Appl. Basic. Sci. Vol., 4 (8), 2080-2087, 2013

4) Kapil Wankhade, Sadia Patka, Ravindra Thool, "An Efficient Approach for Intrusion Detection Using Data Mining Methods", IEEE Publication- 978-1-4673-6217-7/13/$31.00 c ,2013

5) Bini V. C, Ms. Nimmy K, Prof. P. Jayakumar, "Internal Intrusion Detection Using Data Mining and Behaviometric Technique", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056, Volume: 03 Issue: 07 , July -2016

6) Dr Sreepathi .B1, Santhamma2, Goutami Sri Rai3, Shanthala .J 4, Sowjanya .M.V5, "Protection and Detection System by using Data Mining and Rhetorical Techniques ",World Journal of Science and Technology April 2018, 2(3):127-133

7) Prof. D.P. Gaikwad, Sonali Jagtap, Kunal Thakare, Vaishali Budhawant,"Anomaly Based Intrusion Detection System Using Artificial Neural Network and fuzzy clustering.", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 1 Issue 9, November- 2012

8) A.M.Chandrashekhar, K. Raghuveer "Intrusion Detection techniques by using K-means, fuzzy neural network and SVM classifier", IEEE Computer Society-2013

9) Hu Zhengbing , Su Jun ,Shirochin V. P, "An Intelligent Lightweight Intrusion Detection System with Forensics Technique", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany

10) Loye Lynn Ray "Training And Testing Anomaly-Based Neural Network IDS" INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE 2013

11) Deepika P Vinchurkar, Alpa Reshamwala, "A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 1, Issue 2, November 2012

12) Miss Prajkta P. Chapke, Miss Rupali R. Deshmukh, "Intrusion Detection System using Fuzzy Logic and Data Mining Technique", published in ICARCSET '15, March 06 - 07, 2015

13) K.Rajasekhar, 2B.Sekhar Babu , 3P.Lakshmi Prasanna, 4D.R.Lavanya, 5T.Vamsi Krishna, "Data Mining and Forensic Techniques for Internal Intrusion Detection and Protection System", IJCST Vol. 2, Issue 4, Oct .- Dec. 2017

14) Lawton,G, Computer,"Biometrics A new era in security," vol. 31. Issue: 8, Aug. 1998, pp.15-18.

15) D. Dhanavandhini , Mrs. S.Umadevi, "An Internal Intrusion Detection and Protection System Using Data Mining and ACO Techniques", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.3, March- 2016, pg. 114-119

16) Shahbaz Pervez, Iftikhar Ahmad, Adeel Akram, Sami Ullah Swati, "A Comparative Analysis of Artificial Neural Network Technologies in Intrusion Detection Systems", Proceedings of the 6th WSEAS International Conference on Multimedia, Internet & Video Technologies, Lisbon, Portugal, September 22-24, 2006

17) Hu Zhengbing, Shirochin V.P. "An introduction of intrusion detecton systems," Computer and Information Technology (J), vol. 1, 2005, pp.100-103.

18) Hu Zhengbing, V.P. Shyrochin, "Data mining approach for signatures search in network intrusion detection," Proceedings IEEE Third International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2005, SOFIA, BULGARIA, 2005.

19) X.Wang, D.Reeves, S.F. Wu, and J.Yuill, "Sleepy watermark tracing: an active network-based intrusion response framework," Proceedings of IFIP Conference on Security, March 2001.

20) A.Leuski, "Evaluation document clustering of interactive information retrieval," ACM CIKM'01, November 2001, pp.33-40.

21) V. K. Pachghare, Parag Kulkarni, Deven M. Nikam, "Intrusion Detection System Using Self Organizing Maps", In Proceedings of IAMA 2009, IEEE, 2009.