ISSN 2320 -2610
Volume 9, No.3, May - June 2020
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis03932020.pdf
https://doi.org/10.30534/ijmcis/2020/03932020

Security Risk Assessment System for Detection and Prevention Of Unauthorized Access

Haritha Sajikumar[1], Kripa Sara Thomas[2], Jithu Biju[3],Thomas T[4], Syamamol T[5]
[1]Student, Mangalam College of Engineering, India, harithasajikumar597@gmail.com
[2]Student, Mangalam College of Engineering, India, kripasarathomas26@gmail.com
[3]Student, Mangalam College of Engineering, India, mail@achachan.in
[4]Student, Mangalam College of Engineering, India, tomas.tommy@gmail.com
[5]Assistant Professor, Mangalam College of Engineering, India, syamamol.t@gmail.com

ABSTRACT

A cyber-attack is the process of stealing, alteration or destroying a specified target by hacking into the target system. Attacks can be of very different types like installing spyware on a personal computer and thereby attempting to destroy the data in the system or to steal data and ask for ransom and also there can be attacks that would affect the infrastructure of entire nations. The proposed systemTracePot is a security system designed to detect and counteract unauthorized access to a computer system. Tracepot works in such a way that it traps unauthorized users, such as hackers or spammers so they can be identified and prevented from causing further problems. It prevents attackers from accessing critical data and thereby protects the system.

Key words: Spyware, Data breaches, TracePot, Intrusion Detection Technology

1.INTRODUCTION

Computer security aren't often taken seriously until a problem arises and at that point so many people don't know what to do and by that time the attackers would have created many problems which might have severe effects on social and personal life. As information technologies advance, organizations are increasingly able to collect, store, and use personal data for personalized services, advertisements, loyalty programs, and so forth and even though several countries have enacted laws and regulations to request organizations to protect personal data, incidents of personal data leakage are commonplace[5]. Computer security is important because it keeps your information protected and also important for our computer's overall health. Proper computer security prevents viruses and malware, which allows programs to run efficiently and results in better performance of the system. Many organisations realise the urgency of utilising security protection tools to preserve their computer servers and reduce the impact of catastrophic attacks[1].A company's network plays a vital role in its business projects and keeping the computer network up-to-date with the latest software and security techniques is essential for success and progress[8].

With the development of the internet and its wide application in all domains of everybody's life, intrusion detection is becoming a critical process in computer network security[3].With tremendous growth of internet, attack cases are increasing each day along with the modern attack method[7].When people don't understand the ramifications of installing unverified freeware, they open their computer to a slew of attacks. Typically, these free applications will have a checkbox installation that some people might miss, which creates the way for installation of spyware or toolbars and viruses. This spyware, in many cases, can track everything you do in your web browser and these toolbars potentially slow down our entire system. Exploit code based on system vulnerability is often used by attacker[10]. There are many techniques that can be implemented throughout the application lifecycle like code reviews as it helps to spot vulnerable code early in the development phase, dynamic and static code scanners which can perform automatic checks for vulnerabilities, and bug bounty programs that isprocess of enabling professional pen testers to find bugs in the website. Even with these best practices in place, we may still find ourselves under attack.Intrusion behavior has the characteristics of fast upgrade, strong concealment and randomness, so that traditional methods of intrusion detection system (IDS) are difficult to prevent the attacks effectively[6].Due to the fact that most risk factors are inevitable, an effective security system is vital to information systems. That is why this proposed system named TracePot is here in order to make computer systems or servers more secure.

2.RELATED WORKS

This section describes some of the related works associated with Tracepot. All these focuses on the need for a security system that protects valuable data from attackers. The study "A LogitBoost-Based Algorithm for Detecting Known and Unknown Web Attacks" states that the rapid growth in the field of web communication throughout the Internet has heightened the need for better security protection since the increasing number and frequency use of web-based applications and webservers have resulted in a greater necessity for effective security defence in both in home network and enterprise networks[1]. Based on the study "Genetic-fuzzy rule mining approach of feature selection techniques for anomaly intrusion detection", classification of intrusion attacks and normal network traffic is a challenging and critical problem in pattern recognition and network security[2]. Panda in [3] says that as traditional methods cannot detect the unknown intrusion patterns efficiently because of the problems faced by a human analyst during analysing a faster and complex network, concentration is on data mining based intelligent decision technology to make effective decisions to this. Intrusion detection and prevention system technologies detect and react to unauthorised access to network systems, providing real-time monitoring of network traffic. They can be software- or hardware-based, or can be a combination of both. Hardware-based IDPSs are very costly and are effective for large organisations and companies, whereas software-based IDPSs running on the same devices or servers can identify and deal with attacks generated from inside or from outside the network, and can also protect the security policies of that network and their internal threats[8]. In the study "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors", it proposes a novel feature representation approach, namely the cluster center and nearest neighbor approach. The experimental results show that CANN performs better than k-NN and SVM classifiers over the original data-set providing higher accuracy and detection rates.There can be different pattern classifiers like feature representation method which provides correct classifications, but the problem is there are very few related studies on how to extract more features for effective detection of attacks[4].

In "A Data-Driven Security Risk Assessment Scheme for Personal Data Protection", a data-driven risk assessment approach for personal data protection is explained. It is such that the organization can model flows of collected personal data using extended DFDs. The organization identifies components used to process, store, and transmit data and recognizes the personal data collection and usage. The proposed method diminishes risks to assets associated with sensitive personal data[5]. Yu Ren in his paper named "An integrated intrusion detection system by combining SVM with AdaBoost" presents an integrated network intrusion detection algorithm by combining support vector machine (SVM) with AdaBoost. The SVM is used to construct base classifiers, whereas the AdaBoost is used for training learning modules and generating the final intrusion detection model[6]. The paper[9] present a method designed to assess the overall utility of cyber security management alternatives. it does so by decision□analysis□based approach that quantifies threat, vulnerability, and consequences through a set of criteria. This framework bridges the gap between risk assessment and risk management. One of the solutions to the increasing attacks is presented in "Comparison of machine learning algorithms performance in detecting network intrusion" by using Intrusion Detection System (IDS). As IDS are related to machine learning, Machine Learning Intrusion Detection system has been giving high accuracy and good detection on novel attacks. The performance of a Machine Learning algorithms can be evaluated by other algorithms for example an algorithm Decision Tree (J48) is evaluated and compared with two other Machine Learning algorithms namely Neural Network and Support Vector Machines[7].

3.PROPOSED APPROACH

Organization has come to realize that network security technology has become very important in protecting its information[7].The Tracepot system is designed in order to provide security to the network systems. There will be users or clients who will be accessing the server or systems through network and for them they can login through id and password. The server system will be containing credential data which are being tried by the attackers. Only the users or the intended persons can take over it. The attackers continuous to hijack the server and stole the data, and this is prevented using Tracepot virtual server. Tracepot will block the attackers from accessing original data and mimic them by providing data from Tracepot server. The attackers continue to receive these data and by the time, Tracepot will track the attacker's details and trace them out.

The user and the attacker send request for data to the client system. It is the client system in turn will process the requests and forward the request to either of the two servers, client server and TracePot virtual server by analysing from where the request has come. If the request is coming from user, the client system will forward the request to the client server. The client server in turn response to the request by providing the user the data or services requested by them. It is through client system that the data flows to the user.

When the request to access the server is coming from an unknown address and the type of network traffic entirely vary from normal user, the client system can understand that the current request is for unauthorised access. It will be an attacker who is trying to enter the server. Most probably attackers are granting access to the server for stealing critical data and resources. How a client system come to identify an attacker can be explained using an example that is a normal user login into the system using the username and password assigned to them while an attacker is not having these credentials, he or she will try to enter using attacking methods like Brute force attack or from the back side of the system. And if the request is coming from a masked IP address, it will also be considered as an attacker. Once an attacker is identified, the client system forwards the attacker's request to the TracePot virtual server. TracePot will provide the attacker some fake data that will be in encrypted form. The attacker thinks that he is receiving data from server which he requested and will continue to receive the data. By this time, the TracePot server will do steps to locate the attacker's geo location, IP address, the method of attack used etc. so any further attacks of this type can be prevented eventually.

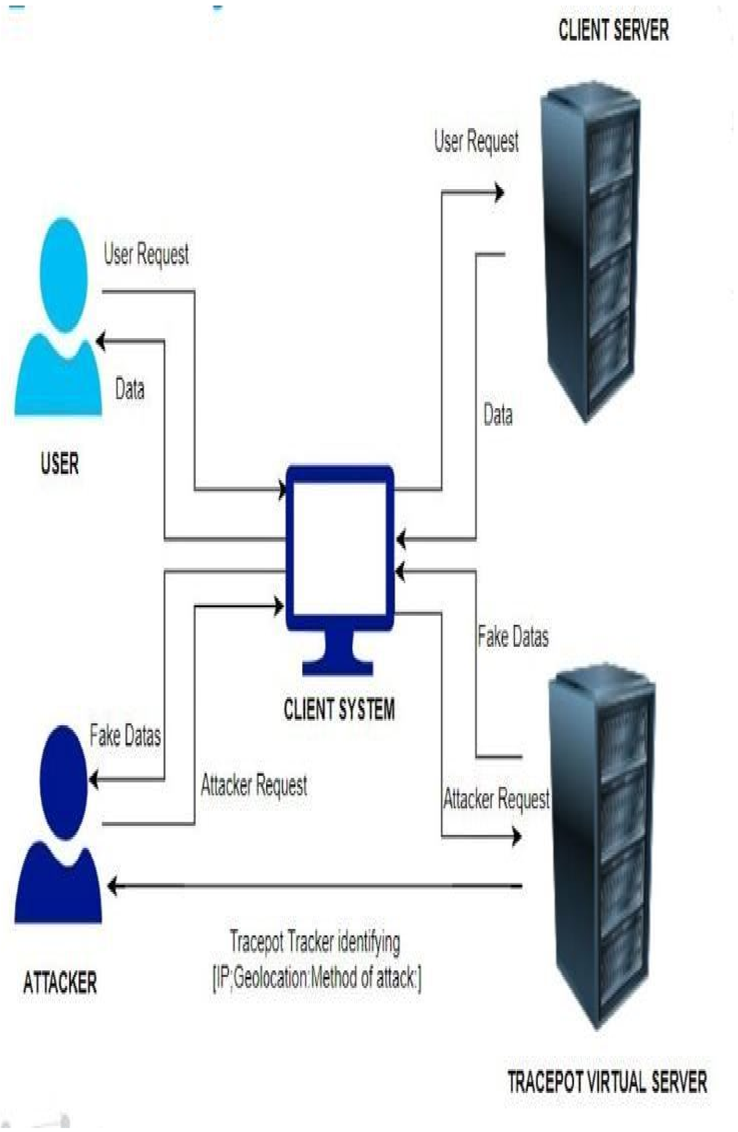

Figure 1: The proposed TracePot system

4.RESULT

Tracepot creates a series of fake servers on selected or default TCP and, if selected, UDP ports. If anyone or anything connects to them, their input will be recorded in the log files, the log files can be viewed as in sheet format or in as a GUI from Splunkinterface. From there it can be monitored down the activities of intruders and can kill the process of attacking with a command to the server sudo -s kill -9 tracepot.The Tracepot is tested based on some features to know the working of the system. It is as that initially user have to login then enter the user name and password then click the login button, the expected result is user get logged in and the actual result is user logged in. The user can access the data and do what he wants. Next if the attacker attacks through backend, the Tracepot server getting activated is the expected result and the actual result also Tracepot got activated. In both the cases the status of the system is successful.

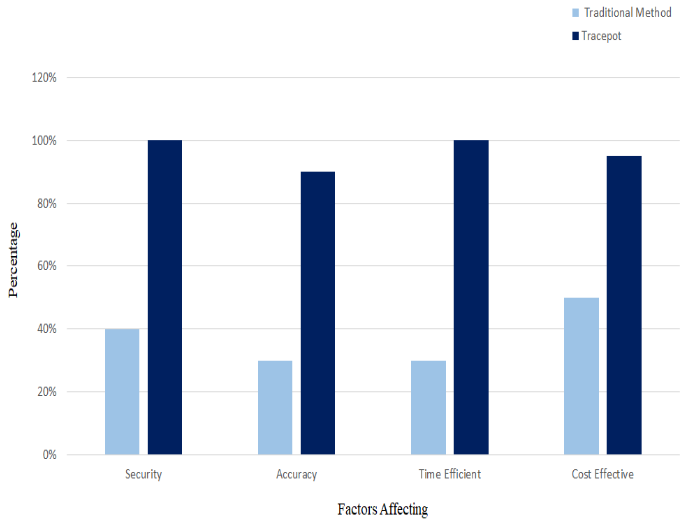

Figure 2: Experimental analysis

Analysis of data is an important part of research in general. The experimental analysis of Tracepot is shown in the below figure 2 that is having factors affecting in the x-axis of graph and the percentage in y-axis. The Tracepot system analyses the security vulnerabilities on the basis of number of illegal logins of the intruders and through intrusion detection system that is Tracepot will get activated and will create a communication path to intruder by sending him a series of fake data. The accuracy of the system is judged as how accurately the Tracepot system is able to detect the intruder correctly to prevent them from further attacks as their inputs are recorded in log files and hence their activities can be monitored continuously. It is found that the accuracy of Tracepot is 90%. The other factors effecting experimental analysis are time and cost efficiency. It tells that the time taken is less to complete the process of detecting the intruder and their activities and about the cheap cost of the system.

5.CONCLUSION

This study proposes a security risk assessment approach for detection and prevention of unauthorized access in which when an attacker tries to intrude into the system then the proposed system TracePot recognises and prevents it from unwanted intrusion. The main aim of the system is to collect the information about the intruder’s activities, deviate them from accessing the critical systems and boost them to stay on top of the system. The system is fabricated to look like real systems by putting real looking information into them so that they appear valuable to the potential intruders. TracePot is equipped with different modules and logs to detect the access and tracks the intruder’s activities.

Hence, the system analyses the network traffic securely efficiently. It promises to provide safety and quick results by reducing the time to troubleshoot and resolve issues. The system generates reports and alerts for the desired search and it is said that World War III which will be a Cyber-attack can be reduced tremendously. Thesystem also prevents the unauthorised and malicious access to the system networks. For example, if the FTP port is allowed and the intruder can use a brute force attack to crack the systems password, then the proposed system TracePot will be separated from the rest of the network. And if an intruder or attacker enter into the system breaking the password and username using the brute force method and the attacker breaks into the system if he or she comes to know that it is a real system with all network connections. Then that system is nothing but it's like a honeycomb in which the attacker is fooled. Therefore, it is one of the latest intrusion detection technology.

ACKNOWLEDGEMENT

We thank God Almighty for giving us this opportunity. This study was done with the support of Department Of Computer Science and Engineering, Mangalam College of Engineering and we express our sincere gratitude to all the faculty members there.

REFERENCES

1. M. H. Kamarudin, C. Maple, T. Watson and N. S. Safa, **A LogitBoost-Based Algorithm for Detecting Known and Unknown Web Attacks**, *IEEE Access*, Vol. 5, pp. 26190-26200, 2017
2. Tsang, C.-H., Kwong, S, Wang, H., **Genetic-fuzzy rule mining approach of feature selection techniques for anomaly intrusion detection,** Pattern Recognition, Vol 40(9), pp.2373–2391,September 2007
3. Panda, M., Abraham, A.,Patra, M. R, **A Hybrid Intelligent Approach for Network Intrusion Detection,**Procedia Engineering, Vol 30, pp.1-9, 2012, doi: 10.1016/ j. proeng. 2012.01.827
4. Lin, W.-C., Ke, S.-W.,Tsai, C.-F, **CANN:An intrusion detection system based on combining cluster centres and nearest neighbors**, Knowledge-Based Systems, Vol 78, pp.13–21,April 2015, doi:10.1016/j.knosys.2015.01.009.
5. S. Cha and K. Yeh, **A Data-Driven Security Risk Assessment Scheme for Personal Data Protection**, *IEEE Access*, Vol. 6, pp.50510-50517, September 2018.
   doi: 10.1109/ACCESS.2018.2868726
6. Y. Ren,**An integrated intrusion detection system by combining SVM with AdaBoost**, J. Softw. Eng. Appl, vol. 7, no-12, pp. 1031-1038, Nov. 2014.
7. K. A. Jalil, M. H. Kamarudin, and M. N. Maseru,**Comparison of machine learning algorithms performance in detecting network intrusion**; in Proc. Int. Conf. Netw. Info Technol. (ICNIT),pp. 221_226, June 2010.
8. W. Bul&ajoul, A. James, and M. Pannu,**Improving network intrusion detection system performance through quality of service configuration and Parallel technology**, J.Computer. Syst. Sci., vol. 81, no. 6, pp. 981-999, 2015.
9. A. A. Ganin et al.,**Multicriteria decision framework for cyber security risk assessment and management**, Risk Analysis., Sep. 2017,
   doi: 10.1111/risa.12891.