Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 11, November -2016

An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques

Wayal Rupesh[1], Jadhav Sagar[2], Sale Rahul[3]

[1,2,3]*Department Of Comp.Engg, Jaihind college of engineering*

Abstract — *Currently, most pc systems use user IDs and passwords because the login patterns to demonstrate users. However, many people share their login pattern with co employees and request these co employees to help co-tasks, there by creating the pattern in concert of the weakest points of pc security. Corporate executive attackers, the valid users of a system UN agency attack the system internally, area unit arduous to observe since most intrusion detection systems and firewalls establish and isolate malicious behaviors launched from the skin world of the system solely. Additionally, some studies claimed that analyzing supervisor call instruction (SCs) generated by commands will establish these commands, with that to accurately observe attacks, associated attack patterns area unit the options of an attack. Therefore, during this paper, a security system, named the inner Intrusion Detection and Protection System (IIDPS), is planned to observe corporate executive attacks at SC level by victimization data processing and rhetorical techniques. The IIDPS creates users' personal profiles to stay track of users' usage habits as their rhetorical options and determines whether or not a legitimate login user is that the account holder or not by scrutiny his/her current pc usage behaviors with the patterns collected within the account holder's personal profile. The experimental result demonstrate that the IIDPS's user identification accuracy is ninety four.29%, whereas the interval is a smaller amount than zero.45 s, implying that it will stop a protected system from corporate executive attacks effectively and expeditiously.*

Keywords- *Spatial, Intrusion detection, Batch, attack patterns*

INTRODUCTION

In the past decades, laptop systems are wide utilized to produce users with easier and additional convenient lives. However, once folks exploit powerful capabilities and process power of laptop systems, security has been one in every of the intense issues within the laptop domain since attackers terribly sometimes attempt to penetrate laptop systems and behave maliciously, e.g., stealing important knowledge of an organization, creating the systems out of labor or maybe destroying the systems. Generally, among all well-known attacks like pharming attack, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack, corporate executive attack is one in every of he most troublesome ones to be detected as a result of firewalls and intrusion detection systems (IDSs) sometimes defend against outside attacks. To evidence users, currently, most systems check user ID and word as a login pattern. However, attackers could install Trojans to filch victims' login patterns or issue an oversized scale of trials with the help of a lexicon to amass users' passwords. once flourishing, they'll then log in to the system, access users' non-public files, or modify or destroy system settings. fortuitously, most current host-based security systems and network-based IDSs ,can discover a acknowledged intrusion during a time period manner. However, it's terribly troublesome to spot WHO the aggressor is as a result of attack packets area unit usually issued with cast IPs or attackers could enter a system with valid login patterns. though OS-level system calls (SCs) are rather more useful in detection attackers and distinctive users, process an oversized volume of SCs, mining malicious behaviors from them, associate degreed distinctive attainable attackers for an intrusion area unit still engineering challenges.

I. LITRATURE SURVEY

1 Analyzing log files for postmortem intrusion detection
AUTHORS: K. A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera
Description: Upon associate degree intrusion, staff should analyze the IT system that has been compromised, so as to see however the aggressor gained access to that, and what he did afterwards. Usually, this associate degree analysis reveals that the aggressor has run an exploit that takes advantage of a system vulnerability. Pinpointing, during a given log file, the execution of 1 such associate degree exploit, if any, is extremely valuable for pc security. this can be each as a result of it accelerates the method of gathering proof of the intrusion, and since it helps taking measures to stop an extra intrusion, e.g., by building associate degreed applying an applicable attack signature for intrusion detection system maintenance. This downside, that we have a tendency to decision post mortem intrusion detection, is fairly complicated, given each the overwhelming length of a regular log file, and also the problem of characteristic precisely wherever the intrusion has occurred. During this paper, we have a tendency to propose a unique approach for post mortem intrusion detection, that factors out repetitive behavior, thus, dashing up the method of locating the execution of associate degree

exploit, if any. Central to our intrusion detection mechanism may be a classifier, that separates abnormal behavior from traditional one. This classifier is constructed upon a way that mixes a hidden Andrei Markov model with k -means. Our experimental results establish that our technique is in a position to identify the execution of associate degree exploit, with a accumulative detection rate of over ninetieth. Additionally, we have a tendency to propose associate degree entropy-based approach that accelerates the development of a profile for standard system behavior.

2] An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques
AUTHORS: Fang-Yie Leu, Kun-Lin Tsai,Yi-Ting Hsiao, and Chao-Tung Yang.
Description: Currently, most laptop systems use user IDs and passwords because the login patterns to attest users. However, many people share their login patterns with coworkers and request these coworkers to help co-tasks, thereby creating the pattern as one of the weakest points of laptop security. business executive attackers, the valid users of a system UN agency attack the system internally, are hard to find since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system solely. Additionally, some studies claimed that analyzing system calls (SCs) generated by commands will identify these commands, with that to accurately find attacks, associated attack patterns square measure the options of an attack. Therefore, during this paper ,a security system, named the interior Intrusion Detection and Protection System (IIDPS), is projected to find business executive attacks at SC level by victimization data processing and rhetorical techniques. The IIDPS creates users' personal profiles to stay track of users' usage habits as their rhetorical options and determines whether or not a legitimate login user is the account holder or not by examination his/her current computer usage behaviors with the patterns collected within the accountholder's personal profile. The experimental results demonstrate that the IIDPS's user identification accuracy is ninety four.29%, whereas the latent period is a smaller amount than zero.45 s, implying that it will stop a protected system from business executive attacks effectively and expeditiously.

3] Biometric Authentication Using Mouse, Gesture Dynamics
AUTHORS: Bassam Sayed, Issa Traor´e, Isaac Woungang, and Mohammad S. Obaidat
Description: The mouse dynamics biometric may be a behavior al biometric technology that extracts and analyzes the movement characteristics of the mouse device once a computer user interacts with a graphical computer program for identification purposes. Most of the prevailing studies on mouse dynamics analysis have targeted primarily continuous authentication or user re-authentication that promising results are achieved. Static authentication (at login time) exploitation mouse dynamics. However, seems to face some challenges thanks to the limited amount of information which will fairly be captured throughout such a method. during this paper, we have a tendency to gift a brand new mouse dynamics analysis framework that uses mouse gesture dynamics for static authentication. The captured gestures square measure analyzed employing a learning vector quantization neural network classifier. we have a tendency to conduct an experimental analysis of our framework with thirty-nine users, in which we bring home the bacon a false acceptance magnitude relation of five.26% and a false rejection ratio of four.59% once four gestures were combined, with a test session length of twenty six.9 s. this is often Associate in Nursing improvement each in the accuracy and validation sample, compared to the prevailing mouse dynamics approaches that would be thought-about adequate for static authentication. moreover, to our data, our work is the first to gift a comparatively correct static authentication scheme based on mouse gesture dynamics.

4] A Model-based Approach to Self-Protection in SCADA Systems
AUTHORS: Qian Chen,Sherif Abdelwahed
Description: Supervisory management and information Acquisition (SCADA) systems, that square measure wide utilized in watching and dominant essential infrastructure sectors, square measure extremely at risk of cyber attacks. Current security solutions will shield SCADA systems from illustrious cyber assaults, however most solutions need human intervention. This paper applies involuntary computing technology to watch SCADA system performance, and proactively estimate approaching attacks for a given system model of a physical infrastructure. We have a tendency to additionally gift the practicability of intrusion detection systems for illustrious and unknown attack detection. A dynamic intrusion response system is intended to judge suggested responses, and acceptable responses square measure dead to influence attack impacts. we have a tendency to used a case study of a water tank to develop AN attack that modifies Modbus messages transmitted between slaves and masters. Experimental results show that, with very little or no human intervention, the planned approach enhances the safety of the SCADA system, reduces protection time delays, and maintains water tank performance.

5] Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment
AUTHORS: Junho Choi, Chang Choi, Byeongkyu Ko, Dongjin Choi, and Pankoo Kim
Description: A distributed denial of service attacks square measure the foremost serious issue among network security risks in cloud computing surroundings. This study proposes a way of integration between protocol GET flooding among DDOS attacks and MapReduce process for a quick attack detection in cloud computing surroundings. This technique is feasible to confirm the supply of the target system for correct and reliable detection supported protocol GET flooding. In

experiments, the time interval for performance analysis compares a pattern detection of attack options with the Snort detection. The projected technique is healthier than Snort detection technique in experiment results as a result of process time of projected technique is shorter with increasing congestion.

III. PROPOSED SYSTEM

The proposed system offer a security system, named Internal Intrusion Detection and Protection System (IIDPS), that detects malicious behaviors launched toward a system at SC level. The IIDPS uses data processing and rhetorical identification techniques to mine supervisor call instruction patterns (SC patterns) outlined because the longest supervisor call instruction sequence that has repeatedly seem many times during a user's log file for the user. The user's rhetorical options outlined as associate degree SC pattern oftentimes showing during a user's submitted SC sequence however seldom getting used by different users, square measure retrieved from the user's pc usage history. The system got to study the SCs generated and also the SC-patterns made by these commands in order that the IIDPS will find those malicious behaviors issued by them so stop the protected system from being attacked.

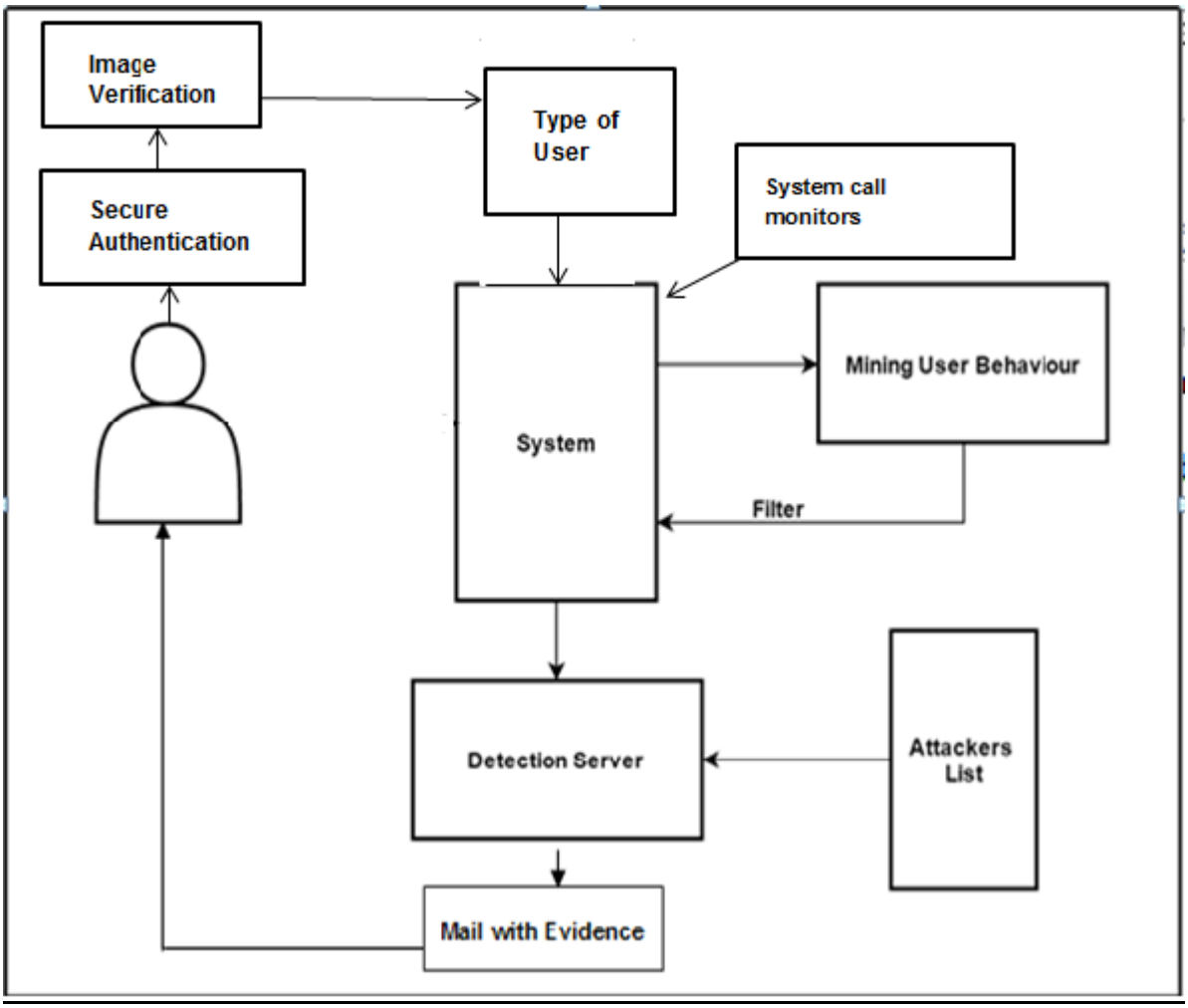

Fig: System Architecture

Advantages of Proposed System:

1. Accuracy of detecting suspicious user is efficient than existing system.
2. Internal Intrusion Detection and Protection System(IIDPS), which detects malicious behaviors of users.
3. Although other systems consume longer time for data analysis than the IIDPS does.
4. This can also detect malicious behaviors for systems employing GUI interfaces.

IV MATHEMATICAL MODE

INPUT:-

Let W is the Whole System Consists:

W = {U, S,UA, A,D,SC}.
Where,

1. U is the set of number users.
   U={U1,U2…Un}.
2. Sis the IIDS which detects the internal malicious activities of user.
3. UAis set of user activites.
   UA={ua1, ua2, ua3, . . . uan}.
4. A be set of attack i.e. malicious activities of user.
   A={a1,a2, . . .an}.
5. D be the detection server which detects the malicious activities of user from which id detected in A.
6. SC be the set of system calls which are running continuously inside the system.

Step 1: user U login to the system.
U={U1,U2…Un}.
.

Step 2: The IIDS system S will authenticate the user U by sending the OTP to user mail and verify the user.

Step 3: the use U will perform some activities like attaching USB device, copying some content from one place to another place, installing new software etc. , the activities may be malicious activities.

The system generated call i.e. SC (system calls) are always monitors the user activities from user history details i.e. log files.

Step 4: The IIDS system will filter the user log files i.e. user activities from attack list A with the help of detection server D.

Step 5: the system S will reports the malicious user activities by taking snapshots of activities at time of performing those activities.

Output: The system will detect the malicious activity of user.

V. SCOPE OF PROJECT

The IIDPS uses data processing and rhetorical profiling techniques to mine call patterns (SC patterns) defined because the longest call sequence that has repeatedly seem many times during the users log file for the user.

VI. CONCLUSION

The IIDPS (Internal Intrusion Detection and Protection System) employs data processing and rhetorical techniques to identify the user behavioral patterns for a user. The time that a habitual behavior pattern seems within the user's log file is counted, the foremost unremarkably used patterns square measure filtered out, and so a user's profile is established. By characteristic a user's behavior patterns as his/her laptop usage habits from the user's current input, the IIDPS resists suspected attackers. the long run work of business executive attack detection analysis are regarding aggregation the important information so as to study general solutions and models. it's onerous to gather information from traditional users in many alternative environments. it's particularly onerous to amass real information from a masquer or traitor whereas performing arts their malicious actions. Albeit such data were offered, it's additional probably to be out of reach and controlled underneath the foundations of proof, instead of being a source of valuable info for analysis functions.

ACKNOWLEDGMENT

We might wish to convey the analysts and additionally distributers for creating their assets accessible. we tend to in addition appreciative to commentator for his or her important recommendations moreover convey the college powers for giving the duty-bound base and backing.

REFRENCES

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers—Or how to thwart a phisher with trusted computing," in *Proc. IEEE Int. Conf. Avail., Rel. Security*, Vienna, Austria, Apr. 2007, pp. 120-127.

[2] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," *ACM Trans. Int. Technol.*, vol. 10, no. 2, pp. 1–31, May 2010.

[3] Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in *Proc. ACM Cloud Autonomic Comput. Conf.*, Miami, FL, USA, 2013, pp. 1–10.

[4] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," *J. Parallel Distrib. Comput.*, vol. 68, no. 4, pp. 427–442, Apr. 2008.

[5] H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation based malware behavioral concise signature generation," *Inf. Commun. Technol.*, vol. 7804, pp. 271–284, 2013.

[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," in *Proc. ACM Int. Conf. Autonomic Comput.*, Karlsruhe, Germany, 2011, pp. 111–120.

[7] M. K. Rogers and K. Seigfried, "The future of computer forensics:A needs analysis survey," *Comput. Security*, vol. 23, no. 1, pp.12–16, Feb. 2004.

[8] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web based DDoS attack using MapReduce operations in cloud computing environment,"*J. Internet Serv. Inf. Security*, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.

[9] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–5.

[10] Z. A. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," *Comput. Commun.*, vol. 34, no. 3, pp. 468–484, Mar. 2011.

[11] H. S. Kang and S. R. Kim, "A new logging-based IP traceback approach using data mining techniques," *J. Internet Serv. Inf. Security*, vol. 3, no. 3/4, pp. 72–80, Nov. 2013.

[12] K. A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera, "Analyzing log files for postmortem intrusion detection," *IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev.*, vol. 42, no. 6, pp. 1690–1704, Nov. 2012.

[13] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Proc. Int. Conf. Commun. Softw. Netw.*, Singapore, 2010, pp. 313–317.

[14] S. O'Shaughnessy and G. Gray, "Development and evaluation of a data set generator tool for generating synthetic log files containing computer attack signatures," *Int. J. Ambient Comput. Intell.*, vol. 3, no. 2, pp. 64–76, Apr. 2011.

[15] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Appl. Soft Comput.*, vol. 10,

