IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

A Literature Survey on Intrusion Detection and Protection System using Data Mining

Chaitali Choure
Priyadarshini Institute of Engineering and Technology, Nagpur, Maharashtra
chaitalichoure13@gmail.com

Leena H. Patil
Priyadarshini Institute of Engineering and Technology, Nagpur, Maharashtra
lhpatil10@gmail.com

Abstract: In the modern world of security many researchers have proposed various new approaches; among those techniques application of data mining for Intrusion detection is one of the best suitable approaches. The system proposes a security system, name the Intrusion Detection and Protection System (IDPS) at system call level, which creates a personal profile for the user to keep track of user usage habits as the forensic features.

The IDP uses a local computational grid to detect malicious behavior in a real time manner. In this paper, a security system named the IDPS is proposed to detect insider attacker at SC level by using data mining and forensic techniques.

Keywords: Forensic Features, Identify User, Data Mining, Internal Intrusion Detection and Protection, System call (SC).

I. INTRODCTION

The complexity of security attacks is very high. these attacks are difficult to handle. The solution of these issues is a creating an effective Intrusion Detection system(IDS).Intrusion means any set of activity that tries to harm the security goals of the information.It is very difficult to identify who the attacker is because attacks packages are often issued with valid login pattern. Most current computers check UID and password as an authentication. But hackers may install Trojans to pilfer victim's security patterns or issue a large scale of trials with the assistance of a dictionary to access users' passwords before they can legally log in to a system. When successful, hackers may access user's private files or even destroy system settings. Most host-based security systems can discover an intrusion from a user's logged history afterward. And most network-based systems can detect an intrusion online. However, to identify who the attacker is in real-time is difficult since attack packets are often issued with forged IPs.

In this paper, we propose a security system, named the Intrusion Detection and Identification System (IDIS), which mines log data to identify commands and their sequences(together named command sequences) that a user habitually submits and follows respectively as the user's forensic features. When an unknown user logs in to a computer, the IDIS starts monitoring the user's input commands to detect whether the users are issuing an attack. IIDPS can block internal intruders and identify the attacker in the network.

II. 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 exploits, 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 paper, we have a tendency to propose an intrusion has occurred. During this 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 in 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 an accumulative detection rate of over ninetieth. Additionally, we have a tendency to propose an 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 with 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 use 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.

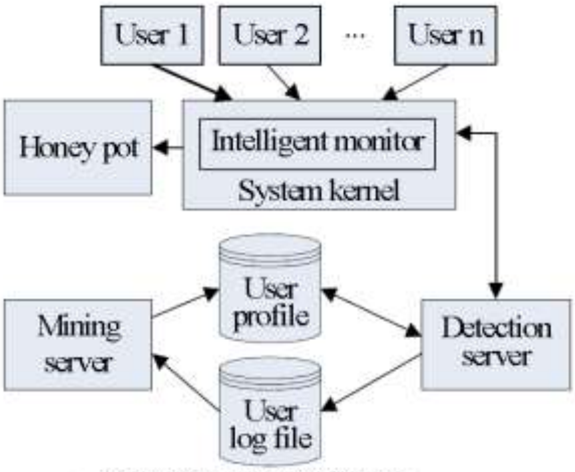
III. PROPOSED SYSTEM

we propose a security system, named the Intrusion Detection and Identification System (IDIS), which mines log data to identify commands and their sequences (together named command sequences (C - sequences in short)) that a user habitually submits and follows respectively as the user's forensic features. When an unknown user logs in to a computer, the IDIS starts monitoring the user's input commands to detect whether he/she is issuing an attack. In the following, we use hacker, attacker, and intruder interchangeably as the same terms are even defined differently by different authors.

ADVANGENTS

1. IDPS system provide comprehensive protection against identity theft, information mining, and network hacking
2. Constant Network Monitoring while user asleep or away from the computer.
3. The IDPS system is able, to monitor both the outside attacks and patterns of behaviour which may be detected within the system.
4. The main disadvantage of intrusion detection systems is their inability to tell friend from foe, is overcome using IDPS system.
5. Techniques used for intrusion detection provide effective attack resistance.
6. Average detection accuracy is higher.

Comparison between Existing System and IIDPS



The IDIS system architecture

By studying this paper three types of attacks observed, Type-I attack in which users group members are not allowed to submit system calls. While in Type-II attack generates sensitive system call which modifies settings or data and last third Type-III, it successfully enters into the security system. Table I indicates comp comparison results of these schemes are shown in which "Y" means that the system has the designated function, "*N*" represents that the system does not provide this function. All these systems, except the IIDPS, do not have the function of identifying a possible user. The response times of a system for all attack types are also shown in Table I in which IIDPS outperforms the other tested systems.

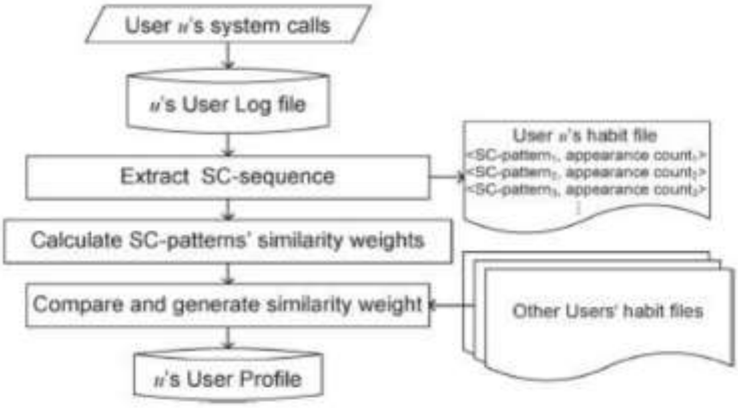
Table I Comparative Analysis of the Existing Systems & IIDPS

Existing systems	Attack type/Response time(seconds)			
	Identify user	Type –I	Type -II	Type -III
AIDE	N	Y /60	Y /60	N
SAMHAIN	N	Y /60	Y /60	N
SYMANTE CSP	N	Y /60	Y /60	N
IIDPS	N	Y /2	Y /3	Not Completely/3
OSSEC	Y /0.45	Y /0.001	Y /0.001	Y /0.045

IV. METHODOLOGY

The IDPS, as shown in Fig. 1, consists of an SC monitor and filter, a mining server, a detection server, a local computational grid, and three repositories including

1. User log Files
2. User Profiles
3. Attacker Profile.


User u's system calls
u's User Log file
Extract SC-sequence
User u's habit file
<SC-pattern$_1$, appearance count$_1$>
<SC-pattern$_2$, appearance count$_2$>
<SC-pattern$_3$, appearance count$_3$>
Calculate SC-patterns' similarity weights
Compare and generate similarity weight
Other Users' habit files
u's User Profile

Control Flow of the Generation of a User Profile.

When user update his data to server user need to match his highly secure digital signature.

For matching digital signature pattern user make a request to the server. The server sends matrix of water marked images for user digital signature matching.

The user selects his pattern images and make a temporary signature and match with user original digital signature which stores into the database. When both signature match user data modification process start and inform the user.

When both signatures do not match server make alert to the user. When user update his data to server user need to match his highly secure digital signature. For matching digital signature pattern user make a request to the server. The server sends matrix of water marked images for user digital signature matching.

The user selects his pattern images and make a temporary signature and match with user original digital signature which stores into the database. When both signature match user data modification process start and inform the user. When both signatures do not match server make alert to the user.

V. CONCLUSION

This paper focuses on a survey of techniques for data mining and forensic to internal intrusion detection and protection. IIDPS system enables data mining and forensic technique to identify system calls, creating a user profile and isolated from attacker profile to protect the user from internal attack.

REFERENCE

1.Fang-YieLeu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao-Tung Yang,'' An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques", IEEE Int. Conf. Avail., Rel. Security, Taiwan, pp 1932-8184,2015

2. B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2, pp. 262–274, Jun. 2013.

3. 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.

4. 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.

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

6. 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.

7. 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.

8. 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.

9. 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.
10. 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.
11. H. S. Kang and S. R. Kim, ―A new logging-based IP trace back 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 a 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,