Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 1, January-2019

ANONYMOUS ACTIVITY DETECTION USING IIDS

Tejas Patil [1], Vinayak Patil [2] , Mohan Yewale [3], Akash Somvanshi [4]
Prof. Deepali Degale [5]

[1]tejaspatil1296@gmail.com,[2]vinayak01patil@gmail.com,[3]mohanyewale4@gmail.com, [4]akashsomvanshi97@gmail.com

[5]deepali.dagale@gmail.com

[1]Computer Engineering, Indira College of Engineering and Management, Pune University
[2]Computer Engineering, Indira College of Engineering and Management, Pune University
[3]Computer Engineering, Indira College of Engineering and Management, Pune University
[4]Computer Engineering, Indira College of Engineering and Management, Pune University
[5]Computer Engineering, Indira College of Engineering and Management, Pune University

Abstract *— Today in the age of computer and Smartphone's, it has become a tedious task for us to remember or Ids and passwords. Especially for working professionals where one needs to enter N numbers of user Ids and passwords, we start opting for a common pattern or password for every authentication. Thus it becomes easy for us to remember but as from security point of view, it becomes very easy and vulnerable for an attacker to attack a system or network. Intrusion basically refers to some outsider who does not belong to the group or community and is trying to intrude i.e. get into our system by wrong means. Thus intrusion detection basically refers to an act of detecting network system for malicious or harmful activity. It is an application which tries to identify and raise an alarm if any suspicious activity is tracked and observed. However here we are proposing a system which aims to identify internal intrusion in network or system. We are going to use data mining techniques to identify internal intruders and take action accordingly.*

Keywords: *Intrusion Detection Systems, data mining, network, vulnerable, malicious, authorisation.*

I. INTRODUCTION

In this digital age, computer and its subsidies have become so handy that all our day o day life are dependent on it. But due to increased chances of attacks we are asked for authentication at each and every step. We need to login into system or any application or any network, we require and need to successfully pass through authentication step. But in order to remember and store password, we have human tendency to keep a simple or mostly a common password or pattern for every authentication purpose. This in turn increases the chances of intrusion. Security till date remains one of the biggest challenges and continuous efforts are taken to improve it. Still we face with large number of attacks such as DOS attack, phishing attack, eves dropping attack, spa email attack, Trojan horse attack, etc. All these attacks are easy to be detected at system call i.e. operating system level. Thus in this paper we are proposing a system that detect malicious harmful behavior basically called as Advance Intrusion Detection and Prevention System. Intrusion prevention monitors system structures for malicious activity or threat. It's an proactive approach which every organization should follow for safety and security purpose.

II. LITERATURE SURVEY

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

Author: Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao- Tung Yang

Description:

Currently, users and systems as well as applications mostly worldwide use user ids and password for authentication purpose. But its also a common practice to share passwords while working to get any task done. This is unethical also gives unauthorized user a chance to do any malicious activity under someone else account name and credentials. This paper aims at detecting intrusion attacks, keeping a trend and logs of same and alerting system and network if any activity is found.

2. A Model-based Approach to Self-Protection in SCADA Systems
Author: Qian Chen,Sherif Abdelwahed

Description:
Supervisory Control and Data Acquisition (SCADA) systems are highly venerable and easy catch for cyber attacks. Currently we are having many systems that detect attacks and monitor for suspicious activity. In this paper we present a self prevention system to detect attacks. This proposed system does not rely on any external source and does self prevention. This system is dynamic in nature. This approach has reduce d downtime as compared to current systems and has better efficiency and performance. We have developed this system using autonomic computing technology.

III. PROPOSED SYSTEM

This proposed system aims at improving and providing high efficiency for intrusion detection. The analysis method monitors and provides details of routers, firewalls, packets, servers for detecting unauthorized entities. As we are using system calls to detect the intrusion attacks, this can be complimented using data mining and forensic techniques. It would help to identify and provide detailed information about a user and its SC patterns. IPS can be configured to monitor log and report activities. Here the duration of time is counted as it appears in the user's log file. After which the most commonly used SC patterns are filtered. These are then compared with user's daily habits and if any deviation is found then the reason for that needs to be identified. If the user has an exception on that particular instance than it can be ignored as a warning. But if no special particular instance is found then it needs to be alarmed and reported to the right authorities. Thus this would help in nay harmful after effect and prevent from any type of attacks. This helps to stop threat of attacks and is typically located between companies firewall and rest of network.

IV. APPLICATIONS

1. System can be used in corporate organizations.
2. System also used in industries.
3. System also useful in the cyber cafes.
4. System also used for the government organizations.

V. HARDWARE REQUIREMENT

System	: Intel I3.
Hard Disk	: 40 GB.
Monitor	: 15 VGA Colour.
Mouse	: Logitech.
Ram	: 4 GB.

VI. SOFTWARE REQUIREMENT

Operating system	: Windows XP Professional/7LINUX.
Coding language	: JAVA/J2EE.
IDE	: Eclipse Kepler.
Database	: MYSQL

VII.CONCLUSION

In this paper that we have proposed, we have successfully implemented an internal intrusion detection and preventions system. As the saying goes that prevention is better than cure, similarly we have aimed to build a system that prevents intrusion attacks and activities. This can be implemented from small scale to large corporate and non technical areas as well. Also we have provided multiple modules and scenarios where we can keep a track and record of all the users and their activities. It will also help us generate trends which we can store in database and use it for future reference. It will also serve the purpose of maintaining logs which can be sent to higher and dedicated authorities for checking and preventing intrusion detections and harmful attacks or activities which do not have good intentions.
.

VIII. REFERENCES

[1] C. Yue and H. Wang, BogusBiter: A transparent protection against phishing attacks,ACM Trans. Int. Technol., vol. 10, no. 2, pp. 131, May 2010.

[2] 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. 110.

[3] H. Lu, B. Zhao, X.Wang, and J. Su, DifiSig: Resource dier- entiation based malware behavioral concise signature generation, Inf. Commun. Technol., vol. 7804,pp. 271284, 2013.

[4] Z. Shan, X.Wang, T. Chiueh, and X. Meng, Safe side eects commit- ment for OS-level virtualization, in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe,Germany, 2011, pp. 111120.

[5] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environ- ment, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 2837, Nov. 2013.

[6] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer stream- ing, in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 15.

[7] Z. A. Baig, Pattern recognition for detecting distributed node ex- haustion attacks in wireless sensor networks, Comput. Commun., vol. 34, no. 3, pp. 468484, Mar. 2011.

[8] H. S. Kang and S. R. Kim, A new logging-based IP traceback ap- proach using data mining techniques, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 7280,Nov. 2013.