JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Advance Intrusion Detection and Protection System by Self-Monitoring using Data Mining Techniques

[1]Priyanka Jadhav,[2]Prof. Sunil Yadav
[1]Student, [2]Professor
[1]Computer Engineering,
[1]Siddhant College Of Engineering, Sudumbare, India

Abstract : *Intrusion means some outsider who is not part of the organization and who is trying to intrude i.e. trying to access something into our system by wrong intention. Therefore intrusion detection means detection of harmful or malicious activity. It is a web based application which identifies and raise the notification if any harmful activity is observed. In this paper we have explained our propose system which is basically used for identifying internal intrusion in system which is connected in the network. We are going to use data mining techniques for catching internal attackers and take action accordingly.*

Currently There lot of ways for protection the network attacks for example firewall but as per the observation the firewalls basically used for protect systems from the outside attackers or attacks. So in this paper we are trying to focus on different forensic techniques and data mining techniques for detection of insider attacks at System call level.

IndexTerms - Intrusion Detection Systems, data mining, network, vulnerable, malicious, authorization.

I. INTRODUCTION

The attackers and malicious users are focusing on weak machines such as unpatched systems, The computer systems which are infected insecure services which is running the network. The assurance of safety is expected computer systems. The Internet has made the information flow to the large extent. Also at the same time it has to face many attacks and threats. Thus the security alert is very important to control the attacks. A notification should be sent to the security team members or Administration about the various attacks which have occurred so that they can respond in real-time to the threat. In this paper we have discussed various techniques for anomaly detection techniques.

II. LITERATURE SURVEY

1. Internal Intrusion Detection System (IIDS) by using Forensic Techniques and Data Mining
Author: Yi-Ting Hsiao ,Fang-Yie Leu, Kun-Lin Tsai, and Chao- Tung Yang

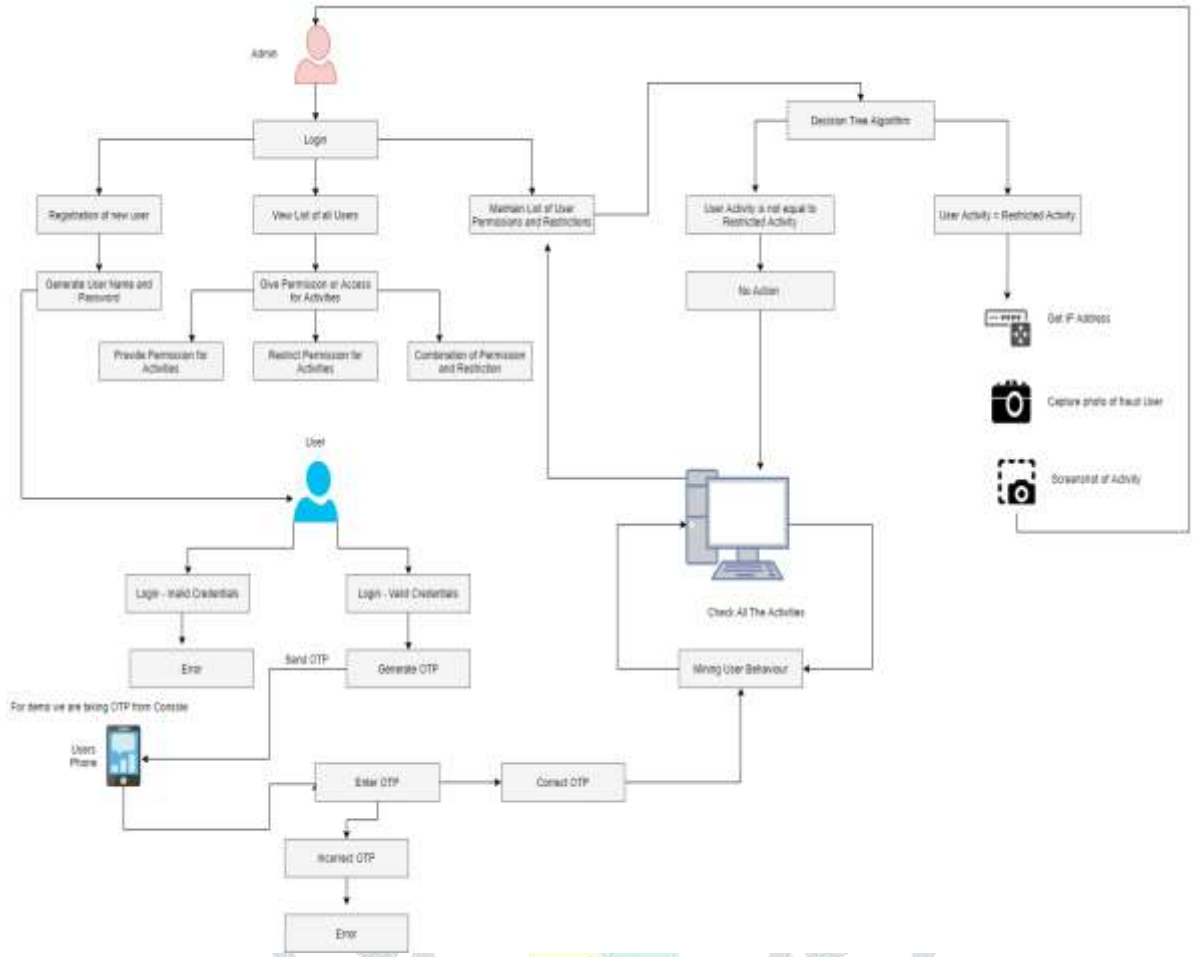
Description:
Currently, users and systems as well as applications mostly worldwide use user ids and password for authentication purpose. But its also a common practice to share passwords while working to get any task done. This is unethical also gives unauthorized user a chance to do any malicious activity 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 Self-Protection in SCADA Systems - Model-based Approach
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 focus on improving and providing high efficiency for detection of intrusion. As we are going to use system calls technique for detection of the intrusion attacks, the expected outcome can be achieved using forensic techniques and data mining techniques. It will help to detect and provide information about a user. After that we are going to use System calls, which will detect the malicious activities or restricted activities which are happening in the network. This system uses forensic profiling techniques and data mining to mine system call patterns.



- Admin Module:
  Admin will be holding rights to register the user and restrict the activities of user.

- User Module:
  User will be able to login in system and getting the valid credential from admin after getting registered.

- System Module:
  System will continuously watch the restricted activities and raise the alert hen activities are caught..

- System after malicious attack
  It will capture the screenshot of screen, capture the picture of user, and will capture the IP address of system from where the attack took place.

- Sending mail and required details Module:
  As soon as the malicious attack takes place .i.e. user tries to access the restricted activities. System will catch this behavior and send the all details to admin.

IV. APPLICATIONS

1. Corporate organizations.
2. Educational Institutes.
3. The cyber cafes.
4. Government organizations where 24/7 surveillance is needed.

IV. ACKNOWLEDGMENT

In this paper that we have proposed, an internal intrusion detection and preventions system. As prevention is better than cure, similarly we have focused on to build a system that prevents intrusion activities and attacks. This can be implemented from small scale to large corporate and non technical areas as well. Also we have trying to provided multiple scenarios and modules 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.

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, 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.

[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.

[9] VIRTUAL KEYBOARD. 2007. Hacker demos how to defeat Citibanks virtual keyboard. http://blogs.zdnet.com/security/?p=195