International Journal of Advance Research in Engineering, Science & Technology

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

Volume 8, Issue 6, June-2021

INTRUSION DETECTION SYSTEM FOR INTERNAL ATTACKS USING DATA MINING TECHNIQUES

Jarad Vikas Balasaheb [1], Mane Sagar Angad [2] , Kolhe Abhijeet Vasudeo [3], Korake Pandurang Mahadeo [4]

[1]vikasjarad@gmail.com,[2]sagarmne7777@gmail.com,[3]akolhe98@gmail.com, [4]p9881952543@gmail.com

[1]Computer Engineering, P K Technical Campus, Pune University
[2]Computer Engineering, P K Technical Campus, Pune University
[3]Computer Engineering, P K Technical Campus, Pune University
[4]Computer Engineering, P K Technical Campus, Pune University

***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. So intrusion detection basically points to an act of detecting network system for harmful or malicious activity. It is a web based application which identifies and raises the notification if any harmful activity is observed. Here we are proposing a system with intention to identify internal intrusion in system or network. We are using data mining techniques to catch internal intruders and take action accordingly.**

There so many ways to protect the networks and data from attackers for example firewall but it is observed that firewalls commonly try to protect computer system against outsider attacks. So in this paper we are focusing different data mining and forensic techniques to detect and protect internal computer system from intrusion using Internal Intrusion Detection and protection systems using Forensic Techniques and Data Mining to find out insider attacks at System call level.

Keywords: *Data mining, network, Network attacks, malicious, insider attacks.*

I. INTRODUCTION

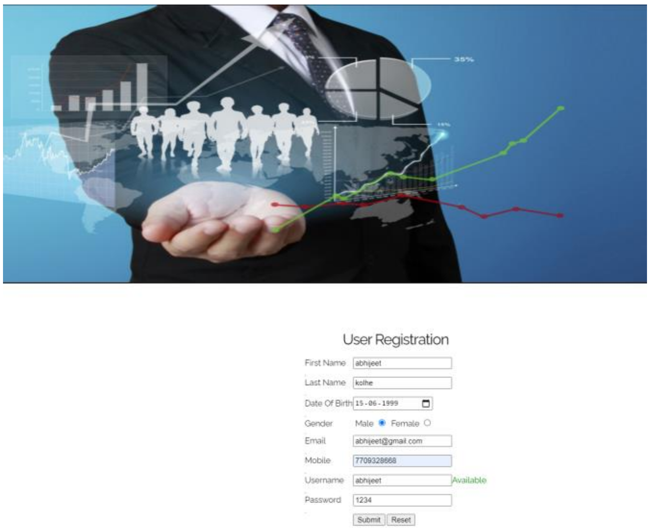
The crackers and malicious users are looking for weak targets such as unpatched systems, systems infected with networks running insecure services The assurance of safety should be applied to data and computer systems. The Internet has the information flow to the large scale. Also at the same time it 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. PROPOSED SYSTEM

This proposed system focus on improving and providing high efficiency for detection of intrusion. As we are using system calls to detect the intrusion attacks, this can be complimented using data mining and forensic techniques. It will help to detect and provide information about a user. Here the time is counted in the user's log file. After which the commonly used SC - patterns will be filtered, which detects malicious behaviors launched toward a system at SC level. This system uses forensic profiling techniques and data mining to mine system call patterns. The system needs to study the SCs generated and the SC-patterns produced by these commands so that the IIDS can detect those malicious behaviors issued by them and then prevent the protected system from being attacked.

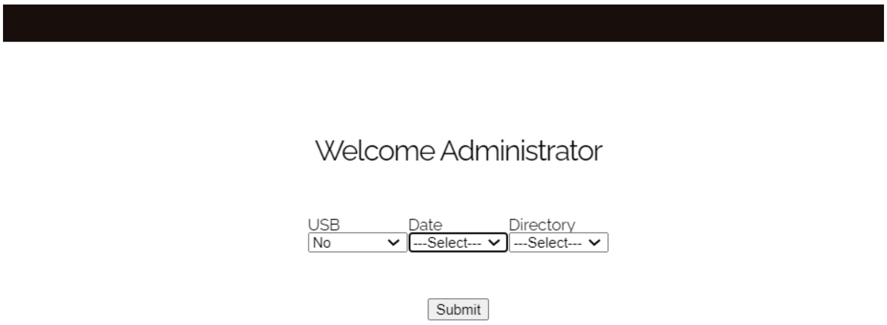
III. Modules with Screenshots

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



User Registration

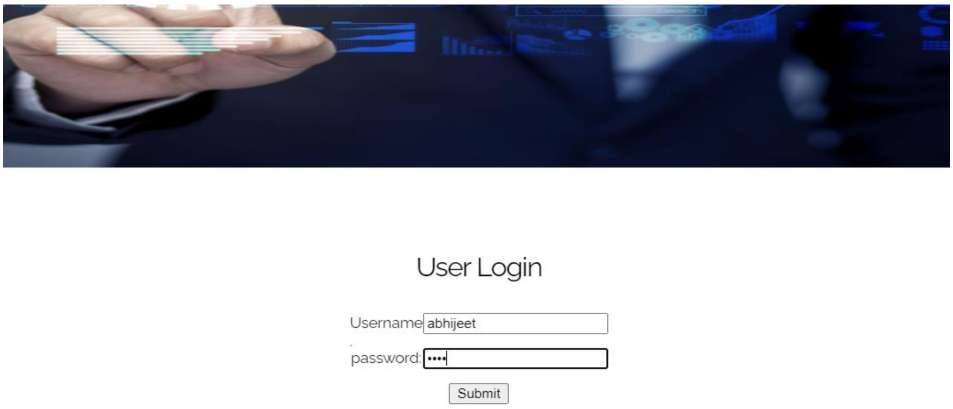
First Name	abhijeet
Last Name	kolhe
Date Of Birth	15 - 06 - 1999
Gender	Male ● Female ○
Email	abhijeet@gmail.com
Mobile	7709328668
Username	abhijeet Available
Password	1234



Welcome Administrator

USB	Date	Directory
No	---Select---	---Select---

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



User Login

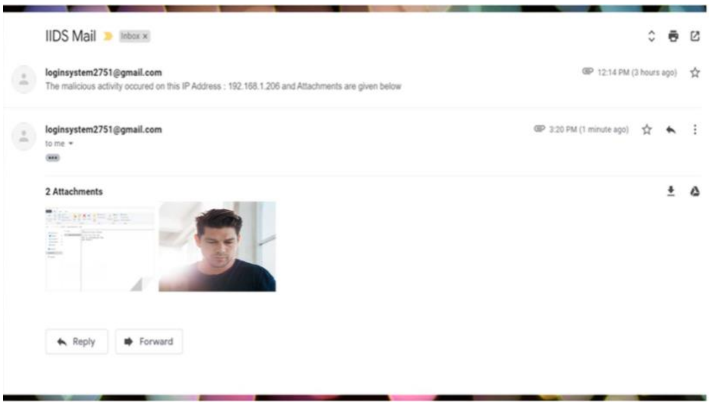
Username	abhijeet
password:	••••

- System Module:
  System keeps the track of restricted activities and triggers the alert if any activities are caught of users.

- 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 generate the alert and send the details of attack.



IIDS Mail

loginsystem2751@gmail.com
The malicious activity occured on this IP Address : 192.168.1.206 and Attachments are given below
12:14 PM (3 hours ago)

loginsystem2751@gmail.com
to me
3:20 PM (1 minute ago)

2 Attachments

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. CONCLUSION

In this paper that we have explained our system i.e. an internal intrusion detection and prevention system. This system can be used in multiple organizations or in school, colleges. if any user performs activity which is restricted by the admin then our system will automatically detects this attack and inform to admin immediately with IP address of system, photo of the user and screenshot of restricted activity. So admin can take immediate action on that user.

VI. REFERENCES

[1] H. Wang, BogusBiter and C. Yue: A transparent protection for ACM Trans, phishing attacks. 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, Safe side commitment 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.