Scientific Journal of Impact Factor (SJIF): 5.71

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

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

DATA-STREAM BASED INTRUSION DETECTION SYSTEM BY USING DATA MINING AND FORENSIC TECHNIQUES

Miss. Pranjali Yadav Deshmukh [1], Pooja Bhosle[2], Rutuja Jadhav[3]
,pallavi Danawale[4], Snehal jadhav[5]

Department of Information Technology
Dr. D. Y. Patil Polytechnic, Akurdi

Abstract — *In today's technology, there are new attacks are emerging everyday due to that the system makes the Insecure even the system wrapped with number of security measures. To detect the intrusion, an Intrusion Detection System (IDS) is used. To detect the intrusion and respond in timely manner is its prime function. In other words, IDS Function is limited to detection as well as response. The IDS is unable to capture the state of the system when an intrusion is detected. So that, in original form, it fails to preserve the evidences against the attack. New security strategy Is very much needed to maintain the completeness and reliability of evidence for later examination. In this research Work, there proposed an automated Digital Forensic Technique with Intrusion Detection System. It sends an alert Message to capture the state of the system, to administrator followed by invoke the digital forensic tool Once an IDS detects an intrusion. To prove the damage Captured image can be used as evidence in the court of law.*

KEYWORDS: *Intrusion Detection Systems, Digital Forensic, Logs, Cryptography*

I. INTRODUCTION

Now a day, to safeguard the organization electronic assets, Intrusion Detection System (IDS) is crucial requirement. To determine whether the traffic is malicious or not Intrusion detection is a process of monitor and analyzes the traffic on a device or network. It can be a software or physical appliance that monitors the traffic which violates organization security policies and standard security practices. To detect the intrusion and respond in timely manner as a result risks of intrusions is diminished it continuously watches the traffic. Based on the deployment IDS broadly classified into two types i.e. Host based Intrusion Detection System (HIDS) and Network based Intrusion Detection System (NIDS). Host -based Intrusion Detection System is configured on a particular system/server. It continuously monitor and analyzes the activities the system where it is configured. Whenever an intrusion is detected HIDS triggers an alert. For instance, when an attacker tries to create/modify/delete key system files alert will be generated. Major advantages of the HIDS that it analyzes the incoming encrypted traffic which cannot be detected NIDS. To detect the attack like Denial of Service (DoS) attacks, Port Scans, Distributed Denial of Service (DDoS) attack, etc Network Intrusion Detection System (NIDS) continuously monitor and analyze the network traffic. To classify as malicious or non-malicious traffic it examines the incoming network traffic. If any predefined patterns or signatures of malicious behavior are present it re-assembles the packets, examine the headers/payload portion and determine.

Recently "Intrusion investigations with data-hiding for computer Log-file Forensics" technique has been proposed. In this approach, log file is stored in two different places as well as in two different forms. On target host the Log file in plain text from is stored and a copy of same log file is stored in another host called log manager and it is hidden in image using steganography. IDS running on target host detects an intrusion and sends an alert message to security administrator about the intrusion when an intruder tries to alter log file on target host. Security administrator use the stego image to extract log file and compares it with log file available in the target host To verify whether the intrusion occurred or not. Intrusion is confirmed If the result of the comparison is unequal else not. Forensic technique is unable to capture the evidence of the attack is the major limitation of this approach. So to preserve the log file damage for forensic analysis, it is not possible and to prove in the court of law, evidence cannot be collected immediately against the attack. In this work automated Digital Forensic Technique with Intrusion Detection System is proposed to overcome this limitation. Because the current IDS are not designed to collect and protect evidence against the attack this new technique is crucial requirement. Digital forensics plays an important role by providing scientifically proven methods to gather, process, interpret and use digital evidence to bring a decisive description of attack.

II. LITERATURE SURVEY

1. Analyzing log files for postmortem intrusion detection

Author: K. A. Garcia, R. Monroy, L. A. Trejo, and C. MexPerera

Description:

Upon an intrusion, security staff must analyze the IT system that has been compromised, in order to determine how the attacker gained access to it, and what he did afterward. Usually, this analysis reveals that the attacker has run an exploit that takes advantage of a system vulnerability. Pinpointing, in a given log file, the execution of one such an exploit, if any, is very valuable for computer security. This is both because it speeds up the process of gathering evidence of the intrusion, and because it helps taking measures to prevent a further intrusion, e.g., by building and applying an appropriate attack signature for intrusion detection system maintenance. This problem, which we call postmortem intrusion detection, is fairly complex, given both the overwhelming length of a standard log file, and the difficulty of identifying exactly where the intrusion has occurred. In this pa- per, we propose a novel approach for postmortem intrusion detection, which factors out repetitive behavior, thus, speeding up the process of locating the execution of an exploit, if any. Central to our intrusion detection mechanism is a classifier, which separates abnormal behavior from normal one. This classifier is built upon a method that combines a hidden Markov model with k -means. Our experimental results establish that our method is able to spot the execution of an exploit, with a cumulative detection rate of over 90that speeds up the construction of a profile for ordinary system behavior.

2.An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques
Author: Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao- Tung Yang

Description:
Currently, most computer systems use user IDs and passwords as the login patterns to authenticate users. How- ever, many people share their login patterns with coworkers and request these coworkers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system only. In addition, some studies claimed that analyzing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns are the features of an attack Therefore, in this paper, a security system, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. The IIDPS creates users personal profiles to keep track of users usage habits as their forensic features and determines whether a valid login user is the account holder or not by comparing his/her current computer usage behaviors with the patterns collected in the account holders personal profile. The experimental results demonstrate that the IIDPSs user identification accuracy is 94.29s, implying that it can prevent a protected system from insider attacks effectively and efficiently.

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

Description:
Supervisory Control and Data Acquisition (SCADA) systems, which are widely used in monitoring and controlling ritical infrastructure sectors, are highly vulnerable to cyber-attacks. Current security solutions can protect SCADA systems to monitor SCADA system performance, and proactively estimate upcoming attacks for a given system model of a physical infrastructure. We also present the feasibility of intrusion detection systems for known and unknown attack detection. A dynamic intrusion response system is designed to evaluate recommended responses, and appropriate responses are executed to attack impacts. We used a case study of a water storage tank to develop an attack that modifies Modbus messages transmitted between slaves and masters. Experimental results show that, with little or no human intervention, the proposed approach enhances the security of the SCADA system, reduces protection time delays, and maintains water storage tank performance. From known cyber assaults, but most solutions require human intervention. This paper applies autonomic computing technology

III. PROJECT IDEA

Our idea to provide secure system which detects malicious behaviors launched toward a system at SC level. The IIDPS uses data mining and forensic profiling techniques to mine system call pat- terns (SC patterns) defined as the longest system call sequence that has repeatedly appear several times in a user's log file for the user.

IV. MOTIVATION OF THE PROJECT

In current system it is very difficult to identify who the attacker is because attack packets are often issued with forged IPs or attackers may enter a system with valid login patterns. Hence we got motivation to developed a system which detects malicious behaviors launched towards a system at SC level.

IV. EXISTING SYSTEM AND DRAWBACKS

Specific network topology-based patterns are defined to model normal network traffic flow, and to facilitate differentiation between legitimate traffic packets and anomalous attack traffic packets. This intrusion detection mechanism is a classifier, which separates abnormal behavior from normal one. This classifier is built upon a method that combines a hidden Markov model with k -means. Packet sniffer is not just a hacker's tool.

Drawbacks:

1. It can be used for specific network topology-based patterns.
2. Detection accuracy is less.
3. Difficult to detect the malicious behaviors of users.
4. Tools used to detect malicious user which is not efficient technique.

V. PROPOSED SYSTEM AND ADVANTAGES

1. A novel approach named Internal Intrusion Detection and Protection System (IIDPS), has been proposed.
2. Capturing the screen when suspicions attacks detected and send that information to victim.
3. Taking snapshot of misbehavior of normal user.
4. This can also detect malicious behaviors for systems employing GUI interfaces.

Advantages:

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.

VI. ARCHITECHTURE

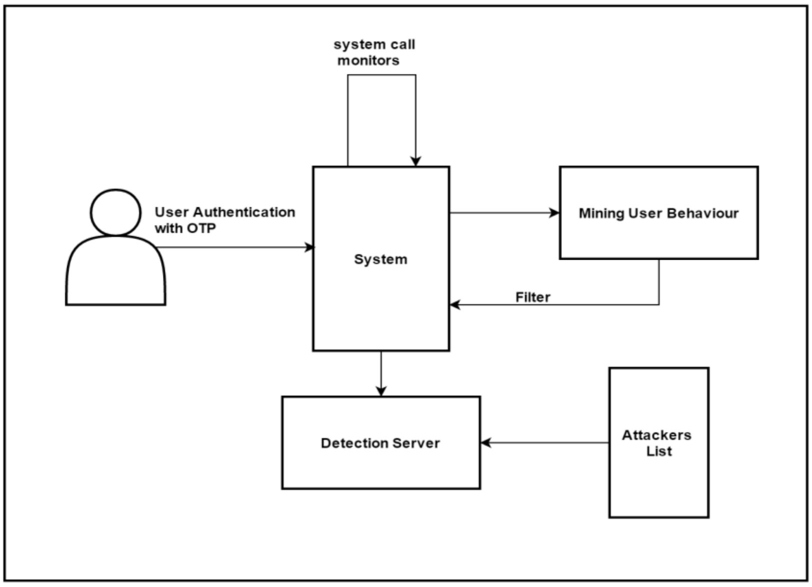


Fig. : System Architecture

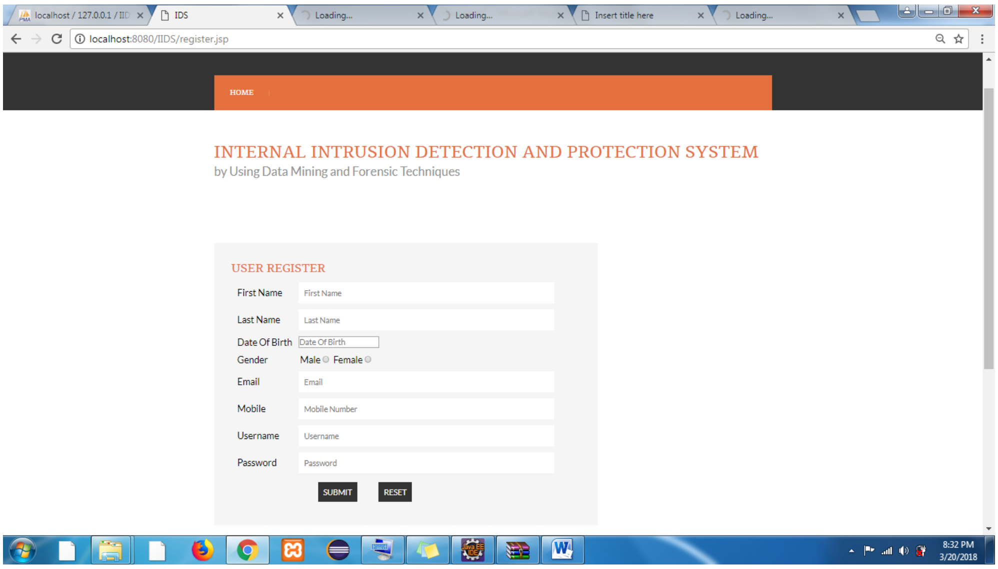
VII. APPLICATIONS

1. System can be used in college.
2. System also used in organizations.
3. System also useful in the cyber cafes.
4. System also used for the personal use.

VII. FUTURE WORK

This system can be used to detect the host intrusion detection where host machine comprises the confidential files. Attackers can attack on host machine that attacks would be detected by the system and updated files can be recovered by system. This system can detect the files modification and also prevent the file modification. If files deleted from the host machine permanently then system can recovered the files.

VIII. OUPTPUT

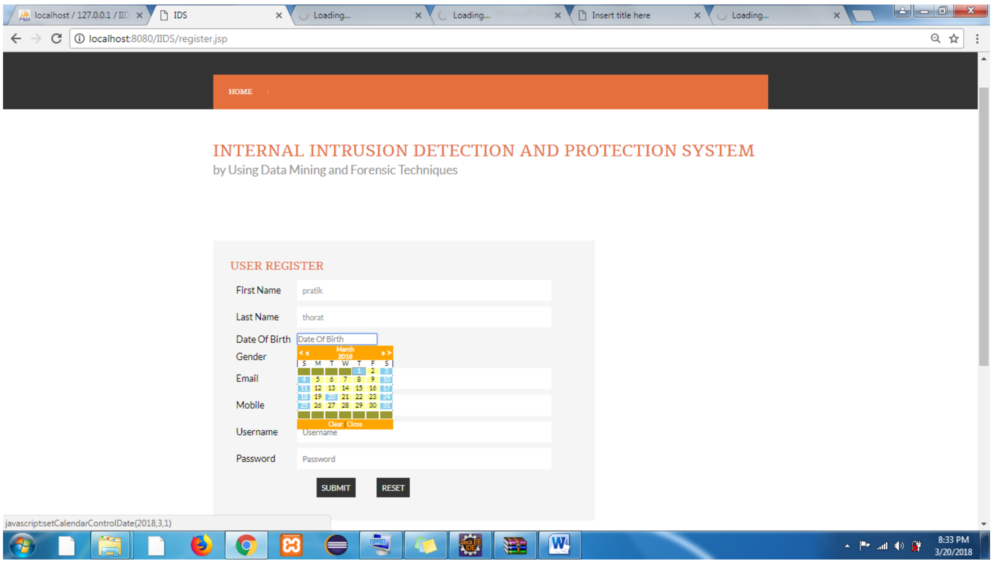


INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM
by Using Data Mining and Forensic Techniques

USER REGISTER

First Name	First Name
Last Name	Last Name
Date Of Birth	Date Of Birth
Gender	Male ○ Female ○
Email	Email
Mobile	Mobile Number
Username	Username
Password	Password

SUBMIT RESET



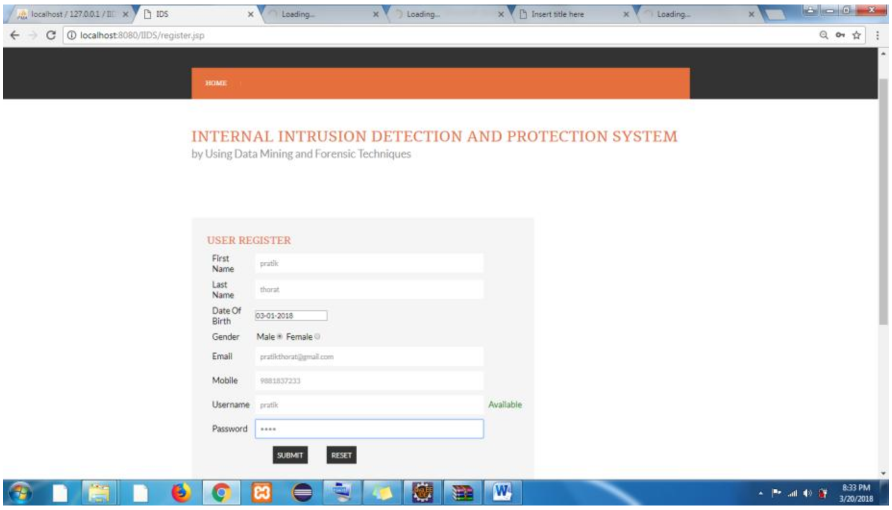
INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM
by Using Data Mining and Forensic Techniques

USER REGISTER

First Name	pratik
Last Name	thorat
Date Of Birth	Date Of Birth
Gender	
Email	
Mobile	
Username	Username
Password	Password

SUBMIT RESET

javascript:setCalendarControlDate(2018,3,1)

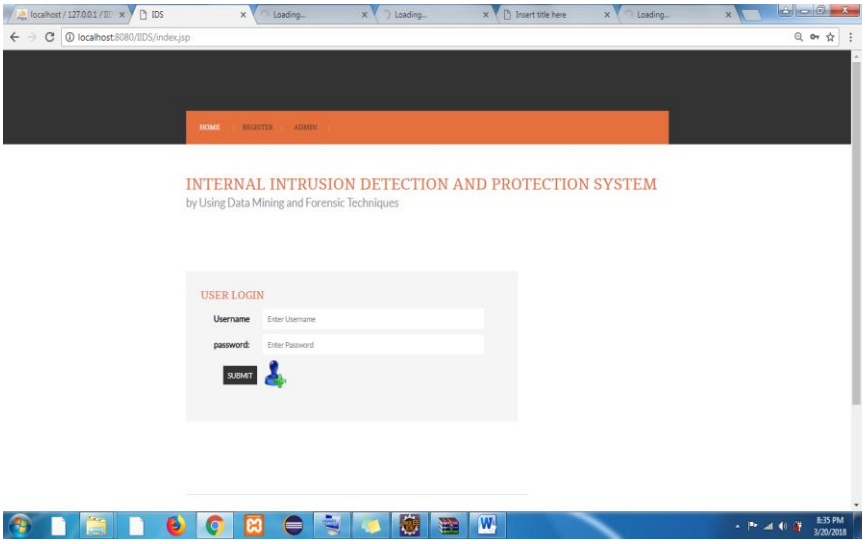


INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM
by Using Data Mining and Forensic Techniques

USER REGISTER

First Name	pratik	
Last Name	thorat	
Date Of Birth	03-01-2018	
Gender	Male ● Female ○	
Email	pratikthorat@gmail.com	
Mobile	9881837233	
Username	pratik	Available
Password	••••	

SUBMIT RESET

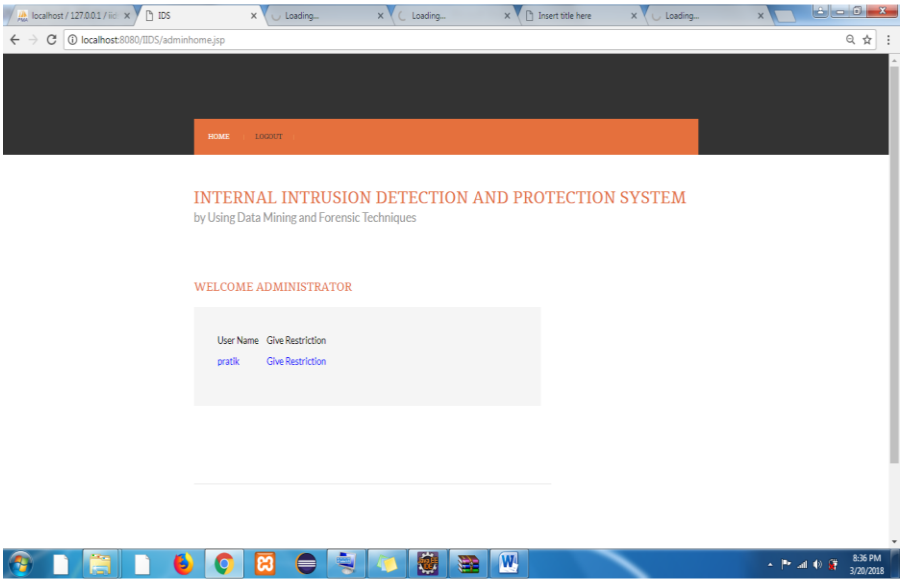


INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM
by Using Data Mining and Forensic Techniques

USER LOGIN

Username: Enter Username

password: Enter Password



INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM
by Using Data Mining and Forensic Techniques

WELCOME ADMINISTRATOR

User Name	Give Restriction
pratik	Give Restriction

IX. CONCLUSION

In this work, intrusion detection system is proposed. IDS is used to determine the intrusion. We can easily detect which activities are performed by user. So that we can recover all the modified file. By using web cam system take pictures of user which performs malicious activities and save that activity in folder and send that activity log and image of user on clients email id. So that we know this particular user. So that our system is very effective and efficient for detecting intrusion of system.

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.