ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 02, pp.46102-46106, February, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

INTRUSION DETECTION SYSTEM FOR COLLEGE ERP SYSTEM

***Dhairya Shah, Jigar Kataria and Harsh Vora**

Department of Information Technology, K.J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai, Maharashtra, India

ARTICLE INFO

Article History:
Received 08th November, 2016
Received in revised form
26th December, 2016
Accepted 18th January, 2017
Published online 28th February, 2017

Key words:

Intrusion Detection System (IDS),
Network Intrusion Detection System (NIDS), Cyber security,
Enterprise Resource Planning (ERP).

ABSTRACT

Importance of cyber security cannot be denied in the current evolving era of the Internet – where safety is no longer just a concern, it has become a #1 priority, as it affects both big reputed organizations as well as small business and individuals. Intrusion detection systems (IDS) are considered to be an efficient way for detecting and preventing cyber security threats. However, there has been not enough attention and awareness on intrusion detection and prevention systems, especially among small business and individuals. Due to this, selection and deployment of IDS is significance in regard to this subject being considered highly technical, expensive and time consuming process. To overcome this, it is necessary to understand the underlying concept of IDS, its role in Cyber Security & thus create an awareness of IDS tools which form the basis of this paper. Further, this will also help in identifying suitable IDS functions needed for developing IDS Software for respective organizations, personal use etc.

Citation: Dhairya Shah, Jigar Kataria and Harsh Vora, 2016. "Intrusion Detection System for College ERP System", *International Journal of Current Research*, 8, (12), 46102-46106.

INTRODUCTION

With the recent advances in technology, people are sharing more and more information among each other. Some organizations like medicine, military etc. are sharing data which is highly sensitive and important. For secure communication, people are using cryptography, using secret key, so that only authenticated receiver can decrypt the message and authenticity of message remains intact. But intruders are not interested to decrypt message. They can use sophisticated tools to attack the host on the network and get access to the sensitive data. Here, IDS comes as a savior. IDS provide three important security functions of *monitoring*, *detecting* and *responding* to unauthorized activities (Defeng *et al*., 2007). It usually provides three services: Observing and analyzing the host and the network activities, audit system configurations and evaluating of integrity of critical information by estimating abnormal activities. IDS are generally classified as follows:

- Host-Based (HIDS): Host based intrusion detection systems run on individual hosts / devices on the network. It monitors the incoming and outgoing packets from the device and alerts the administrator on detection of suspicious activity.
- Network-Based (NIDS): Network based intrusion detection systems monitor traffic between all devices on the network. On performing an analysis for a passing traffic on

The entire subnet (in a promiscuous mode), it subsequently matches the traffic on the subnets to the collection of known attacks. On finding a match, alert is sent to the administrator. Today, IDS becomes necessary for every organization to secure their sensitive data from intruders. In the next sections, we will discuss about various tools & techniques used in Host and Network Based Intrusion Detection Systems.

Host based IDS

Host based IDS is aimed at collection and analysis of information on a particular host or system (3). This Host agent monitors and prevents intruders to compromise system security policy. HIDS plays different role from Anti-virus. Anti-virus is supposed to monitor all the activities inside the system but not concerned with buffer overflow attacks on system memory nor malicious behavior of operating system process but HIDS checks and collect system data including File System, Network Events and System Calls to verify whether any inconsistency has occurred or not. HIDS system relies heavily on audit trail and system logs to detect unusual activities inside the system. Host-based systems can monitor access to user specific information which is a major advantage (Bace, 1998;

****Corresponding author: Dhairya Shah,***
Department of Information Technology, K.J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai, Maharashtra, India.

Brackney, 1998). HIDS can identify an improper user of company resources. On detection of similar pattern (similar to past attacks or suggestive of an attack); activity with that workstation can be stopped, thus blocking the attack. This is greatly useful in systems where system resources are accessed remotely in a routine manner. Some major disadvantages as follows: (1) they cannot see the network traffic (Bace, 1998); (2) HIDS rely heavily on audit trails which can exhaust a lot of resource and space in server and (3) lack of cross-platform interoperability.

Network based IDS

Network Based Intrusion Detection Systems (NIDS) are active systems. These are deployed on networks to primarily monitor the network traffic. NIDS are operated under promiscuous mode without exposing itself to the potential attackers. NIDS systems generally work by identifying attacking signature within the networks. NIDS are OS independent and also compromising one NIDS will not affect the system if multiple NIDS are deployed to monitor the traffic flow. Sometimes network people raise a question like what can NIDS do that Firewall can't?

The firewall is the equivalent of a security fence around a property and the guard post at the front gate. But Firewall is not able to detect what is happing inside (Bace, 1998). Firewalls are subject to many attacks, tunneling attacks and application-based attacks are most prominent. On the other hand a NIDS system works like a body guard which is monitoring both inside and outside of a property. It monitors packets, matches pattern; find attacking signature from already existing attacks done in the past and sometime statistical analysis of the information to detect abnormal behavior. However NIDS system cannot scan the content if network traffic is encrypted, it cannot efficiently handle high speed networks.

SURVEY ON EXISTING SYSTEMS

For the purpose of getting a clear view on the IDS systems, we studied about the currently existing systems that include HIDS & NIDS systems open-source systems being used for the detection & prevention of attacks in real-time. ELM Enterprise Manager (http://www.tntsoftware.com), an enterprise class event log Management solution, collects event logs from different Devices in real-time. On detection of critical events, immediate email alerts are helpful in activating more stringent security policies. Network Based Intrusion Detection Systems (NIDS) are active systems, examples of which include Snort (http://www.sans.org/security-resources/idfaq/limitations.php), an open source network intrusion prevention system, are capable of performing real-time traffic analysis and packet logging on IP networks.

It can handle various intrusion detection techniques like buffer overflow, protocol analysis, CGI attack and many more. Trivedi *et al*. (2006) proposed an Intrusion Detection System which defines a term called "Reputation" that is assigned to every node in the network. Every node monitors the behavior of its next-hop neighbor through promiscuous mode. A reputation manager keeps track of all the "Reputation" values from all the nodes, for updating the reputation value. A node is declared as malicious whenever it crosses a predefined threshold. A warning message is sent only to the immediate neighbors. Each node also contains an Avoid list. It contains a list of malicious nodes and no further communication is done through these already identified malicious nodes. Toosi *et al*. (2007) presented a method to classify the normal and the intrusive behavior in a network. They used a combination of neuro-fuzzy networks, fuzzy interference and genetic algorithm to classify the network. Parallel neuro-fuzzy classifiers did the initial classification and its output was the basis of the fuzzy inference system. Finally, the genetic algorithm approach was used to optimize the decision. Faysel and Haque (12) surveyed various methods of cyber-attack detection and classification technique. These are based on neural networks and data mining. They have also discussed IDS evaluation criteria and dataset for IDS validation.

TYPES OF ATTACKS

Denial of service

DoS is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users access to machine. Having network connectivity available through more than one service provider can be part of the answer to this problem. At least that way, when the main entrance is blocked, you can use the emergency exit to maintain at least minimal communications such as email. There are many varieties of DoS attacks. Some DoS attacks abuse a perfectly legitimate feature. Others create malformed packets that confuse the TCP/IP stack of the machine that is trying to reconstruct the packet. Still others take advantage of bugs in a particular network daemon

User to Root Attacks

This is a class of exploit in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system. There are several different types of U2R attacks where the most common is the buffer overflow attack. Buffer overflows occur when a program copies too much data into a static buffer without checking to make sure that the data will fit.

Anomaly detection

Designed to uncover abnormal patterns of behavior, the IDS establish a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion n. What is considered to be an anomaly can vary, but normally, we think as an anomaly any incident that occurs on frequency greater than or less than two standard deviations from the statistical norm. It identifies anomalies as deviations from "normal" behavior and automatically detects any deviation from it, flagging the latter as suspect. Thus these techniques identify new types of intrusion as deviations from normal usage. It is an extremely powerful and novel tool but a potential drawback is the high false alarm rate, i.e. previously unseen (yet legitimate) system behaviors may also be recognized as anomalies, and hence flagged as potential intrusions. If a user in the graphics department suddenly starts accessing accounting programs or compiling code, the system can properly alert its administrators.

Target Monitoring

These systems do not actively search for anomalies or misuse, but instead look for the modification of specified files.

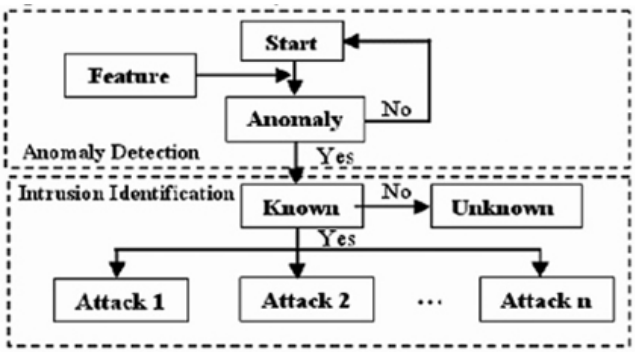


Fig.1. Anomaly Detection & working

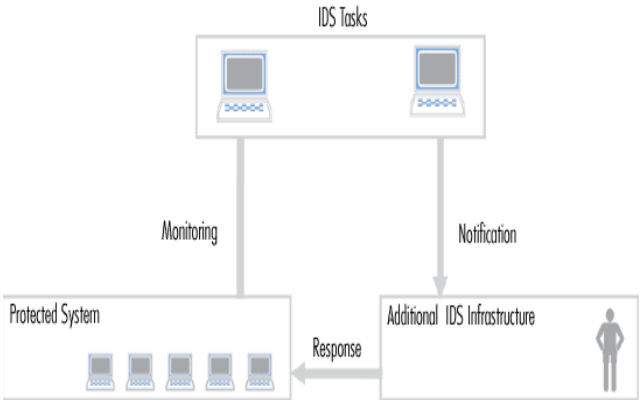


Fig.2. Target monitoring in IDS

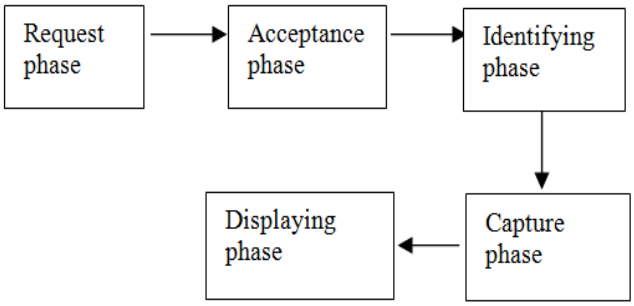
This is more of a corrective control, designed to uncover an unauthorized action after it occurs in order to reverse it. One way to check for the covert editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the mission/system critical files.

ERP SYSTEMS & COLLEGE ERP SYSTEM

It is a general tendency to think that Enterprise Resource Planning (ERP) systems are beneficial to certain industries, organizations or specific sectors, but this is not true. People, products & markets use ERP or sort of Integrated Information Management Systems (IIMS) to improve the efficiency of their input-output systems as well as for efficient utilization of resources. Educational Institutions do need ERP systems or some sort of related software's for maintaining student data, admission process, library management, examination processes etc.

But not all colleges or institutes have these kinds of facilities available or deployed, thus they have a burden of manhandling all sorts of work -- manual labor increases. To ease it up for such colleges, we try to develop a general framework of ERP systems for colleges (involving modules such as administrative, exam-related, staff & students modules as well as inventory & other management modules) -- also customized Intrusion Detection System focused on providing security to these modules isn't readily available, thus we focus on developing an IDS integrated into ERP systems that can be used by colleges, institutes as well as it can be modified & tweaked to work accordingly with companies or other corporate levels.

Proposed System



Request phase: - In this phase the user is requested to enter the user name and appropriate password. Thus, the login details of user are accepted here, it becomes the Login form of College ERP System.

Acceptance phase: - The system will check whether the user is authorized or not. If the user is authorized then the access is granted to the system. If the login credentials are matched then the user will be allowed to access the College ERP System as per the permissions granted to user (depends whether user is staff, student etc).

Identifying phase: - After gaining access the system checks that any unauthorized entry has been made to the system before. The work of IDS system for monitoring College ERP system starts here, the four layers of IDS system: Dos layers, Probe Layer, U2R Layer & R2L Layer are enabled to detect the incoming attacks on the system.

Capture phase: - In this phase the intruder is captured by the system and blocked. Hence, security is maintained. An attack made by the intruder at any level or phase, depending on type of attack, its vulnerability, its detected & its blocked before it causes further damage.

Displaying phase: - Here the system will display the list of authorized and unauthorized users. Also, the type & vulnerability of attack being made on the system, and how it is being blocked, preventive solutions can be guided to users too. A log for these incidents can be maintained separately.

Thus the four layers of IDS: Dos Layer, Probe Layer, U2R Layer & R2L Layer will work to monitor & detect attacks on the different modules & sub-modules of College ERP System.

SYSTEM OVERVIEW

Fig (1), Fig (2), Fig (3) shows the Login Screen, System Modules and Module with Functionality respectively. System Modules involve Principal, Office, Admission, Library, Exam & Inventory modules. Login Screen simply consists of user credentials & server name. Module with functionality shows the internal functions contained in Principal Module.

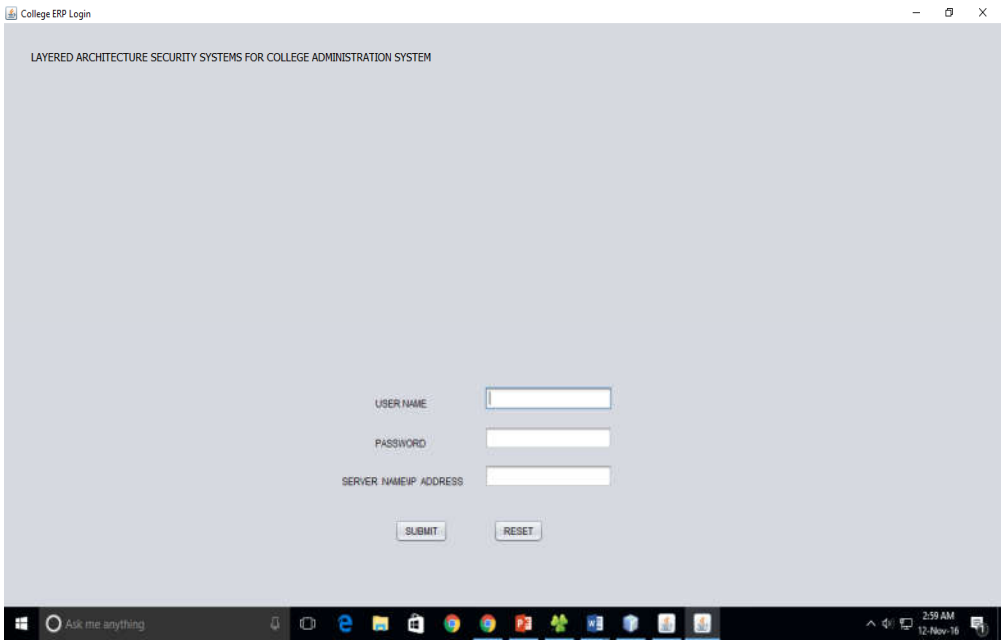


Fig. 1. Login Screen

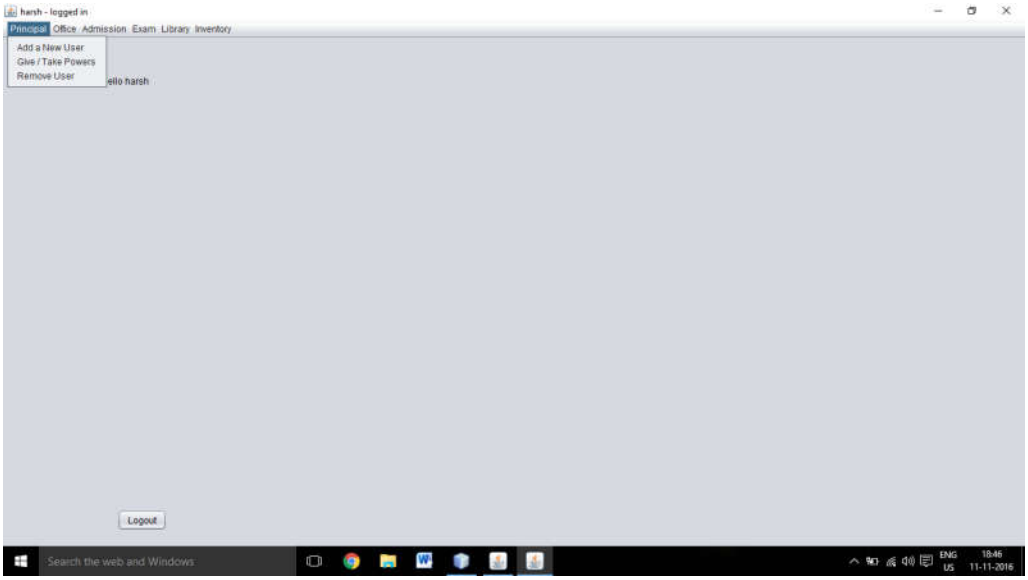


Fig. 2. System Modules

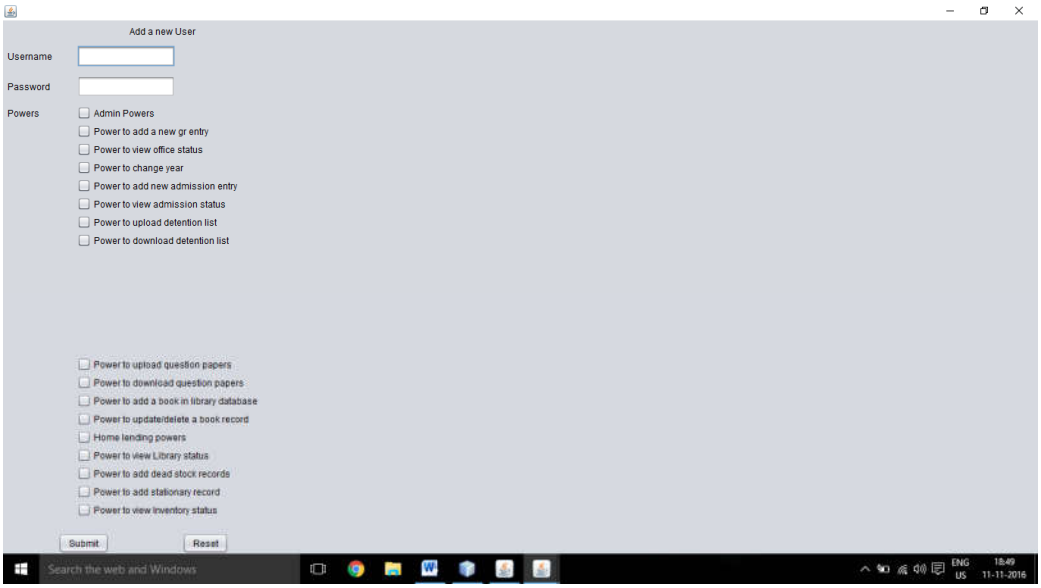


Fig. 3. Module with Functionality

Conclusion

The primary problem concerned with Internet is security & maintaining data integrity & consistency, while the system can be prevented from attacks, no assurances or assumptions can be made on the types & severity of attacks due to the complexity involved in systems, its heterogeneous nature & also the loopholes detected in them. But, preventive measures along with security mechanisms such as IDS allows the system to sustain in different environments. IDS for College ERP systems enables colleges & organizations to deploy needed security measures for securing their confidential data in a comprehensible manner. Colleges & organizations where such types of facilities are already deployed can use this as an additional security measure, whereas colleges & organizations where such facilities or security measures are not used can make use of this simple IDS security infrastructure.

Acknowledgement

We wish to express our sincere gratitude to Mrs. Vijaya Pinjarkar, Project Guide for providing us an opportunity to do our project work in Security domain. We sincerely thank Mr. Uday Rote, HOD of IT Department and Mr. Harsh Bhor, Project Coordinator for their guidance and encouragement in carrying out this project work. We also wish to express our gratitude to the officials and other staff members of K.J Somaiya Institute of Engineering and Information Technology, who rendered their help during the period of our project work.

REFERENCES

"Comprehensive Windows Event Log Monitoring - Servers, Desktops & Devices", http://www.tntsoftware.com/, June 12, 2014.

Ajith Abraham, Ravi Jain, Johnson Thomas, and Sang Yong Han. "D-SCIDS: Distributed soft computing intrusion detection system." *Journal of Network and Computer Applications* 30, no. 1 (2007): 81-98.

Ajith Abraham, Ravi Jain, Sugata Sanyal, Sang Yong Han, "SCIDS: A Soft Computing Intrusion Detection System", *6th International Workshop on Distributed Computing (IWDC-2004), Springer Verlag, Germany, Lecture Notes in Computer Science,* Vol. 3326. 2004, pp. 252-257

Animesh Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal, Bace, Rebecca: An Introduction to Intrusion Detection & Assessment. Infidel Inc., prepared for ICSA Inc. Copyright 1998.

Brackney, R: "Cyber-Intrusion Response", *Proceedings of Seventeenth IEEE Symposium on Reliable Distributed Systems,* West Lafayette, IN, 20-23 Oct,1998, pp. 413-415. Matthew Richard, "Intrusion Detection FAQ: Are there limitations of Intrusion Signatures?" http://www.sans.org/security-resources/idfaq/ limitations. php, April 5, 2001.

Defeng Wang, Yeung, D.S., and Tsang, E.C., "Weighted Mahalanobis Distance Kernels for Support Vector Machines", *IEEE Transactions on Neural Networks,* Vol.18, No. 5, Pp. 1453-1462, 2007

http://en.wikipedia.org/wiki/Intrusion_detection_system

Mohammad A. Faysel, Syed S. Haque, "Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems", *IJCSNS International Journal of Computer Science and Network Security,* Vol.10No.7, July 2010, pp. 316-325.

Sugata Sanyal, "RISM - Reputation Based Intrusion Detection System for Mobile Ad hoc Networks", *Third International Conference on Computers and Devices for Communication (CODEC-06), Institute of Radio Physics and Electronics, University of Calcutta,* December 18-20, 2006, pp. 234-237.

Toosi, A. N., Kahani, M. 2007. "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers." *Computer Communications 30,* no. 10: 2201-2212.

Toosi, A. N., Kahani, M., Monsefi, R. 2006. "Network Intrusion Detection based on Neuro-fuzzy classification," *International Conference on Computing & Informatics, (ICOCI '06), Kuala Lumpur, Malaysia*, June 6-8, pp. 1-5.

****