International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Host Based Intrusion Detection System

Vishal Parande[1], Prof. Sharada Kori[2]

[1, 2]Modern Education Society's College of Engineering, Savitribai Phule University, Bandgardan Road, Pune, India

Abstract: ***In today's technology, new attacks are emerging day by day which makes the systems insecure even the system wrapped with number of security measures. Intrusion Detection System (IDS) is used to detect the intrusion. Intrusion Detection System (IDS) is crucial requirement to safeguard the organization electronic assets. Intrusion detection is a process analyze the traffic on a device or network to determine whether the traffic is malicious or not. In other words, intrusion is any unauthorized attempt to access private data of which the intruder doesn't have access rights. It can be a software or physical entity that monitors the traffic which violates organization security policies and standard security practices. An Intrusion Detection System is made to mainly avoid the intruder from being successful in accessing the prohibited files. It continuously analyzes the traffic to detect the intrusion and respond in timely manner as a result of which risks of intrusions are diminished. It not only stops the intruder from getting access but also captures an image of the changes that he makes in the files. An added feature of capturing a webcam image of the intruder at the time of intrusion can also be collected.***

Keywords: Intrusion detection system, logs, cryptography, digital forensic.

1. Introduction

Intrusion Detection System (IDS) is crucial requirement to safeguard the organization electronic assets. Intrusion detection is a process to monitor and analyzes the traffic on a device or network to determine whether the traffic is malicious or not. It can be a software or physical appliance that monitors the traffic which violates organization security policies and standard security practices. It continuously analyzes the traffic to detect the intrusion and respond in timely manner as a result risk of intrusions is diminished. IDS broadly classified into two types based on the deployment i.e. **Host based Intrusion Detection System (HIDS)** and **Network based Intrusion Detection System (NIDS).**

The HIDS that it analyzes the incoming encrypted traffic which cannot be detected NIDS. Network Intrusion Detection System (NIDS) continuously monitors and analyzes the network traffic to detect the attacks like Denial of Service (DoS) attacks, Port Scans, Distributed Denial of Service (DDoS) attack, etc. It examines the incoming network traffic to classify as malicious or non-malicious traffic. It re-assembles the packets, examine the headers/payload portion and determine if any predefined patterns or signatures of malicious behaviour are present.

Real-time and computing resource restraint: An intrusion should be detected during or immediately after it happened. However, traditional HIDS techniques (e.g., log analysis, offline integrity checking) bring undesirable delays. NIDS usually detect intrusions in real-time.

2. System Description

In this approach, log file is stored into two different forms as well as in two different places. Log file in plain text from is stored on target host and a copy of same log file is stored in another host called log manager and it is hidden behind an image using steganography. When an intruder tries to alter log file on target host, IDS running on the target host detects an intrusion and sends an alert message to the security administrator about the intrusion which in turn takes the required steps to mitigate it.

2.1 Target Host

Crucial data (i.e. log files) is stored in the Target Host. Continuous monitor of log file is prime requirement to preserve the integrity and confidentiality of the data stored in it. To achieve this, IDS is deployed on target host and it is a continuous process round the clock. Whenever an attacker tries to intrude the target host, IDS running on target host detects the intrusion; sends an alert message to security centre as well as log server. Further, it invokes the digital forensic tool to capture the state of the system (RAM image and log file image). Newly captured log file image is compared with previous log file image to confirm the intrusion. Our Target Host is nothing but our Operating System as it is a Host based System. The intruder shall be able to access the system but if he tries to alter any of the system properties and manipulate the records then the IDS comes into picture.

2.2 Log Server

It stores the copy of the log file in an encrypted form. Encryption key maintained only by the log server and it kept secret. Periodically back up of the Target host log file is taken and it is stored on the log server. Upon receiving the log file as a backup, it encrypts the received log file and stores within it. Whenever the log server receives an alert message from target host, it decrypts the log file, computes the image of the decrypted log file using digital forensic tool and sends it to the target host to perform the comparison. The main job of the Log server is encryption and decryption of log files such that the intruder doesn't have access to them. If the intruder gets to know the location and condition of the log files then their safety comes under scrutiny. The most important part will be the key. The key that is used to encrypt and decrypt the log files shall only be available with the owner and nobody else. It shall be provided at the time of delivering the software as a complete product.

2.3 Security Centre

This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Once the target host has sent the alert to the Security Centre, the job of the Security Centre starts. The attack is hence detected and looked into at the Security Centre. The Security centre is the most essential component of the IDS. Its job is to track the intrusion in such a way that as soon as he/she tries to access the system, an alert should be sent to the real owner. This shall be accompanied by the webcam image capturing activity in order to prove the offence in the court of law. If the intruder tries to access the files without the net connection, the system shall shut down by itself within 10 seconds, and if he has the net connection intact, then we shall also be able to inform the true owner about the intrusion with the help of an e-mail.

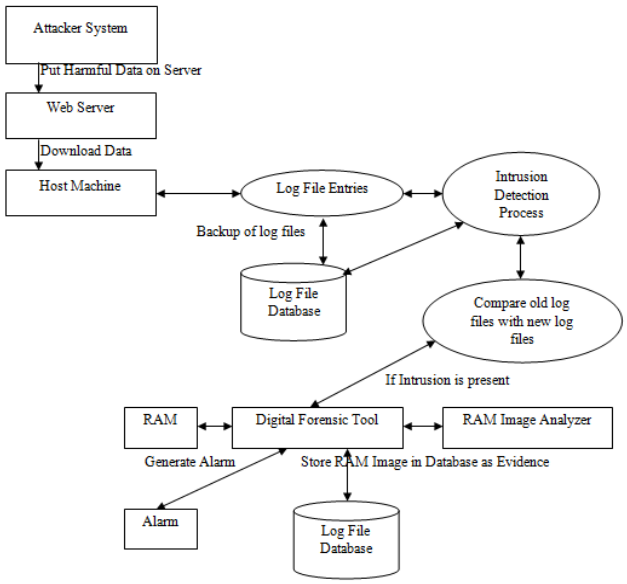
3. Proposed System Features

The proposed system comprises of advanced automatic log updation and log sending module where in the realtime intrusion done on any host is. Proposed system features include:

1. Realtime monitoring of each host over the network
2. History monitoring of each host over the network.
3. Realtime Image capture module for Intruders image as an evidence of intrusion.
4. Network monitoring for network connectivity ensuring.
5. File integrity detection on realtime basis.
6. Running process monitoring for detecting any backdoor entry.
7. Drive directory monitoring and Log encryption for security.

All the log files are stored in the encrypted format for security purpose.

4. System Design



5. Interfaces Used in IDS

External Interface Requirements

5.1 User Interfaces

The user interface includes GUI (Graphic User Interface) which contains all basic plug-ins that constitute the basic functions of the program. The most common features of Intrusion Detection System GUI are:

- Working Environment
- Log file Database
- Searching for Information (log file entries)
- Image capturing technique

5.2 Hardware Interfaces

- The minimum Hardware requirements for a PC are:
- Maximum memory usage: 512MB*(default)
- Disk space needed: 200MB
- User can change the default value of memory with the appropriate commands if he/she has to handle a large database.

5.3 Software Interfaces

- Intrusion Detection System is compatible with every system that supports a JRE, i.e. it is independent of the operating system of the computer system on which it runs. Intrusion Detection System runs on every platform where a JAVA Virtual Machine is available.

6. Non Functional Requirements

6.1 Performance Requirements

The Intrusion Detection System is an application that needs a few resources to work. It is designed not to delay the system from other key processes. It shall not increase the time required for the operation from the user. It is meant to work on parallel lines such that only verified users are able to view the log file entries such that no changes in them shall be permitted. If any such activity is found to be taking place then it shall take the appropriate steps to mitigate this intrusion.

6.2 Safety Requirements

The application must ensure that it leaves the original database untouched. No modification is allowed to these database entries. Also, the database is backed up at regular intervals of time to ensure that no data is lost as a result of power failure or other mishaps.

6.3 Security Requirements

- Backup of important data like database should be maintained.
- The database is set for automatic backup after every two hours and if back up is successful then previous backup is removed or else new attempt for backup is initiated.

- Antivirus tools must be installed to protect the system from malpractice.

7. Software Quality Attributes

- The system should be accurate to give the correct results.
- System should be reusable.
- System should be reliable.
- System should be complete such that the security of the important documents remains intact.

8. Conclusion

In this work, automated digital forensic technique (image capture) with intrusion detection system is proposed. An ID is used to determine the intrusion followed by invoking the digital forensic tool to capture the state of the system (RAM image and log file image). During our experimental study, Ossec is used as User Interface and wind32dd is used to capture the RAM image and the time of intrusion which shall be useful to prove the intruder in the court of law. To test the proposed idea, rules were written in Java and interfaced in Ossec to detect the intrusion. Ping command sent from one system to another system where the system is readily deployed and the IDS system has successfully detected the packet as intrusion followed by invoked the webcam to take the image of the RAM. Captured RAM image is analyzed using RAM Image Analyzer.

Our main job is, to provide security, to obtain better accuracy and optimized results, to get false accept and reject rate as low as possible and to compare the algorithm with the system as whole.

9. Acknowledgment

I would like to express my deep sense of gratitude towards my project guide, Prof. S. KORI for guiding me through the entire process right from doing the research till penning my thoughts in the form of this paper. I would also like to thank my parents and colleagues for their valuable time and inputs that have helped me making this paper a reality.

References

[1] Ya-Ting Fan1 and Shiuh-Jeng Wang, "Intrusion Investigations with Data-hiding for Computer Log-file Forensics", IEEE 2010.
[2] R. Araeteh, M. Debbabi, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence," Digital Investigation 4S, pp, 82-91, 2007.
[3] Bhagyashree Deokar, Ambarish Hazarnis, " Intrusion Detection System using log files and reinforcement learning", *International Journal of Computer Applications (0975 – 8887) ,May 2012*
[4] Qing Si-han. Cryptography and Network Security [M].Bei Jing: Tsinghua University Press, 2009.
[5] Bo Pang and Lillian Lee, "Opinion Mining and Sentiment Analysis", Foundations and Trends in Information Retrieval Vol. 2, No 1-2 (2008)
[6] Aditya Pal & Scott Counts, "Identifying Topical Authorities in Microblogs", WSDM'11, February 9–12, 2011, Hong Kong, China, Copyright 2011 ACM

Author Profile

Vishal S. Parande is pursuing his Bachelors Engineering degree in Computer Engineering. He is currently studying final year in Modern Education Society's College of Engineering, Bandgardan road, Pune- 411001, Maharashtra, India.

Prof. Sharada M Kori, Department of Computer, Modern Education Society's College of Engineering ,University of Pune, Pune – 411001, India.