International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Survey on Detection and Prevention of Intrusion

Ms. Deepali D. Rane, Mrs. Shraddha T. Shelar, Mr. Vinod Mane
Assistant Professor, Department of Information Technology,
D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India

ABSTRACT
Intrusion Detection and Prevention System using GSM modem is proposed, which is designed to detect unwanted attempts of accessing, manipulating and/or disabling computer system. If intruder cracks or guess the password then proposed system will deny access of system resources with the help of security question known to owner of the system. Proposed system will take snapshot of intruder using webcam. Unwanted attempts can be avoided by using cell phone and GSM modem. System will send alert message to authorized user on mobile phone. Authorized user can control or prevent own machine by sending commands through message like lock desktop PC, shutdown PC etc.

Keywords: *Intrusion, Security*

I. INTRODUCTION

An intrusion is a deliberate, unauthorized attempt to access or manipulate information or system and to render them unreliable or unusable. The detection of intrusions or Intrusions attempts either manually or via software expert systems that operate on logs or other information available from the system or the network.

An Intrusion Detection and prevention can be an interface designed to detect unwanted attempts and prevent accessing, manipulating, and/or disabling computer systems.

Intrusion Prevention and Detection system's main role in a network is to help computer systems to prepare and deal with the network attacks. This will help computer systems on how to deal with attacks**.** A **GSM modem** is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages.

A. Detection Techniques of IPD

1. Host based IPDS

A host-based intrusion prevention and detection system (HIPDS) is an intrusion prevention and detection system that monitors and analyzes the internals of a computing system. A host-based IPDS monitors all or parts of the dynamic behavior and the state of a computer system. Much as a NIPDS will dynamically inspect network packets, a HIPDS might detect which program accesses what resources and discover that, for example, a word-processor has suddenly and inexplicably started modifying the system password database. Similarly, a HIPDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected. One can think of a HIPDS as an agent that monitors whether anything or anyone, whether internal or external, has circumvented the system's security policy.

2. Network based IPDS:

A network intrusion prevention and detection system (NIPDS) monitors the packets that traverse a given network link. Such a system operates by placing the network interface into promiscuous mode, affording it the advantage of being able to monitor an entire network while not divulging its existence to potential attackers. Because the packets that a NIPDS is monitoring are not actually addressed to the host the

NIPDS resides on, the system is also impervious to an entire class of attacks such as the “ping-of-death" attack that can disable a host without ever triggering a HIPDS.

NIPDS monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. On a heterogeneous network, a NIPDS generally does not possess intimate knowledge of all of the hosts on the network and is incapable of determining how a host may interpret packets with ambiguous characteristics.

II. RELATED WORK

In the existing system, the notion of public auditability has been proposed in the context of ensuring remotely stored data integrity. Public auditability allows an external party, verifies the correctness of the remotely stored data. However most of the schemes do not consider the privacy protection of the user’s data against external auditors. Indeed they may potentially reveal the users data to auditor. This severe drawback greatly affect the security of these protocols in cloud computing. From the perspective of protecting the data privacy, users who are owners of the data and rely on the TPA for storage security

III. PROPOSED SYSTEM

A. The problem domain

To design a system which will provide security to machine as well as to specific nodes in network by host-based intrusion prevention and detection system (HIPDS) and network intrusion prevention and detection system (NIPDS) using GSM modem technique as well as electronic mail that will help to maintain confidentiality and integrity.

B. System overview

The proposed system is distributed as follows:

1. Login

User must crack two-level security credentials to get access and if one of the authentication is failed then access will denied. First User have to provide authorized user id and password then he have to provides second level security credentials i.e. OTP

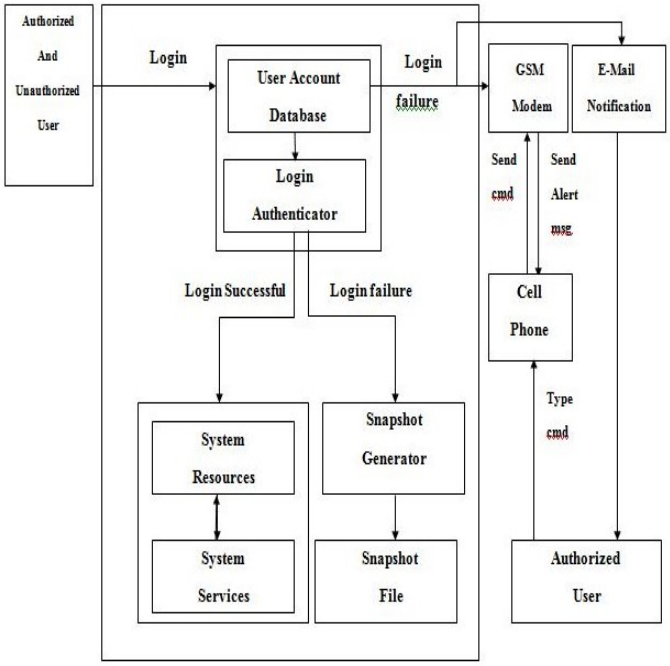

Fig: 5.1 “System Overview”

2. Email notification

To keep track of intruder’s attempts system will generate an e-mail notification and sends to the authorized user entity If user failed to satisfy the credentials then E-mail will get send to authorized person that will help to detect intrusion activities.

3. Command processing

When the intruder tries to manipulate or access the confidential data then the authorized user can control or prevent his PC by sending commands through SMS like lock desktop PC, shutdown PC. System accepts commands and takes appropriate action according to the commands.

4. Storage

All the information of authorized user’s like password, user ID, & security question etc. is store in file. It will also store snapshots of intruders to detect malfunction. User credentials are stored for the authentication and authorization purpose.

5. Captures Snap of Intruder

User must crack two-level security class credentials to get access and if one of the authentications is failed then access will get denied and systemwill capturethe snapshot of the intruder.

IV. RESULT ANALYSIS

- Proposed system will provide security to authorized user’s system resources.

- Proposed system will provide two-way security notification i.e. SMS security notification, E-mail notification and two-level security class i.e. login ID or name, password and question, password.

V. CONCLUSION

Using this system user can tighten the security constraints so as to avoid intruders attack on crucial data like hospital or military data.

VI. REFERENCES

1. Mehmood, Y., Shibli, M. A., Habiba, U., Masood, R.: Intrusion detection system in cloud computing: challenges and opportunities. In: IEEE 2nd National Conference on Information Assurance (NCIA), pp. 59–66 (2013)
2. Mr. Bilal Maqbool Beigh, Mr. M. A. Peer "Intrusion Detection and Prevention System: Classification and Quick Review", *ARPN Journal of Science and Technology,*ISSN 2225-7217, Volume No.2, Issue No.7, August 2012
3. Mr. Harley Kozushko "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", *International Journal of Engineering Research and Applications,* ISSN 2248-9622, Vol. 3, Issue 6, September 2003
4. Ms. Shivani Sharma, Mr. AmitAsthana, Mr. Manik Chandra Pandey "Intrusion Detection Solution Using Anomaly Detection Scheme", *International Journal Of Advance Research In Science And Engineering,* ISSN-2319-8354(E), Volume No.2, Issue No.5, May 2013, pp.16-19
5. Mr.Tom Dunigan, "Intrusion Detection and Intrusion Prevention on a Large Network", Proceedings of the Workshop on Intrusion Detectionand Network Monitoring, Volume No.5, April 2012.