Volume-5,Issue-5 (May-16)
ISSN (O) :- 2349-3585

Design Intelligence Data Gathering and Incident Response Model for Data Security Using Honey Pot System

[1]Sutharsan M, [2]Logeshwaran J
Assistant professor, Department of ECE,
Apollo Engineering College, Chennai, India.
[2]Assistant professor, Department of ECE,
Mahendra College of Engineering, Salem, India.

Abstract - Now a day's protecting our Networks from the Attackers was much challenged task. Achieving data Security is really massive work between the user and server. Network forensics is basically used to detect attacker's activity and to analyze their behavior. Data collection is one of the important tasks of network forensics and honey pots are used in network forensics to collect useful data. Honey pot is an exciting new technology with enormous potential for security communities. In this paper we are discussing about the data security in Java, based on user and server network model. We are also deployed the cryptographic procedure for maintains the security and prevent our data's from the attackers. In this concept, the alternate path selecting is the major factor for eliminate the intruder in the network and also utilize the network in better manner. For the result of this work we will provide reliable communication between the users and server.

Keyword:. Networks, Security, network forensics, Honey pot, Java, communication

Introduction

Increasing privacy for small and business networks is an essential one. Now days there are several algorithms and security solutions are available but still we are unable to create a complete solution for the system security and network security. Hacking experts and system attackers find very different methods to steal our data. As a result management of newly constructed network flows often surprised attacks from the unknown peoples. Exploit automation and massive global scanning for network flows enable adversaries to compromise computer systems shortly after Network Flows become known. Network Management especially in flow control creates some creative ideas for prevent and guard the data's between the user and server. In this paper we create a new security and data protection techniques to protect and assist in a business and organizational networks. A Guarded honey pot offers secured features that can help us to protect our network also assist with intelligence data gathering, incident response for a better understanding to find the attackers, what method the attacker used to break the access.

Existing Work

Most of the existing systems need manual explanations for normal and abnormal behavior of network access. It is really a massive task to identify the abnormalities automatically using network algorithms and data mining techniques. The existing works analyze network or system usage logs to create models or rules which the system can use to detect intrusions that can potentially compromise the system integrity or reliability also the imposition and abnormal behavior detection focus on activities generated by a single source, resulting in many fake positives and undetected instructions. In the existing an interloper or attacker can easily enter into networks and access it likes a very common user. So we have to prevent our network from this interloper entry for the security purpose.

Proposed System Model

The proposed system based on the concept of Permit Pointer (PP). The main idea of a permit Pointer is the use of issued and verified the permissions of network users to access the network resources. Our new proposed model makes use of this idea for assigning permissions and priority to an authenticated network users. The back end server will compare the requested operation with the user's permissions to determine whether the requested operation is allowed.

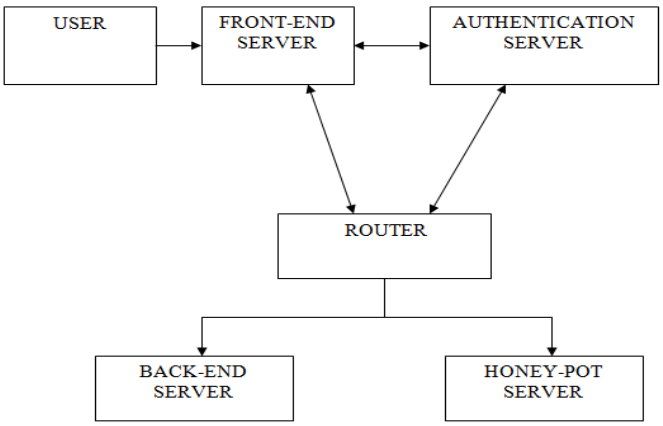

Fig 1 : Proposed System Block Diagram

Suppose the back end server identifies a difference between permissions and requested operations of a network user, the back end server will move the particular packet to the deployed Honey pot for verification.

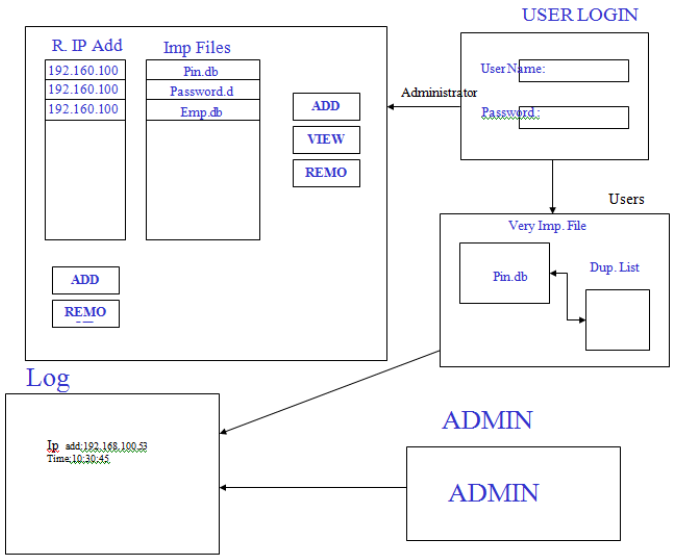

Fig 2 : DATA SECURITY Architecture Diagram

Proposed System Modules

User Module

In this module, the Network user sends the inquiry to the back end server. Based on the query the server sends the corresponding file to the user. Before this process the user authentication process is involved. In the server side it checks the User Name and the password. If the details are satisfied then server received the queries from the user and searches the corresponding files in the database. Finally find that file and send to the user. If the server finds the interloper means, it set the alternative path to those interlopers.

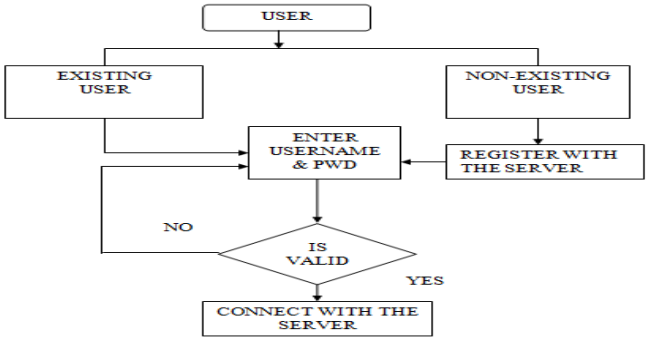

Fig 3 : Proposed System User module

Front-End Server

The front-end server is only responsible for responding user requests to the router for processing. The presence of masked router is transparent to the user and even Front-end Server. The only load upon Front-end server is to forward the user message packet to the router and if the request from the user involves back-end computation and to connect to AS to authenticate the user as a lawful user. This basically involves forwarding the user request to the AS and accepting the user request or denying the user request based on the AS response contained in the reply message.

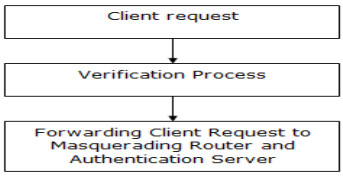

Fig 4 : Front End Server

Authentication Server

The Authorization Server (AS) functions as any AS would with some extra tasks to add to the typical user authorization protocol. The first task is to sending the user authorization information the Masking Router. The AS in this model also functions as a permit Pointer (PP), controlling permission on the application network. The other functions that should be supported by the AS is the updating of users lists, causing a reduction in authorization time or even removal of the user as a valid user depending upon the request.;

ISSN:-2349-3585 |www.ijrdt.org

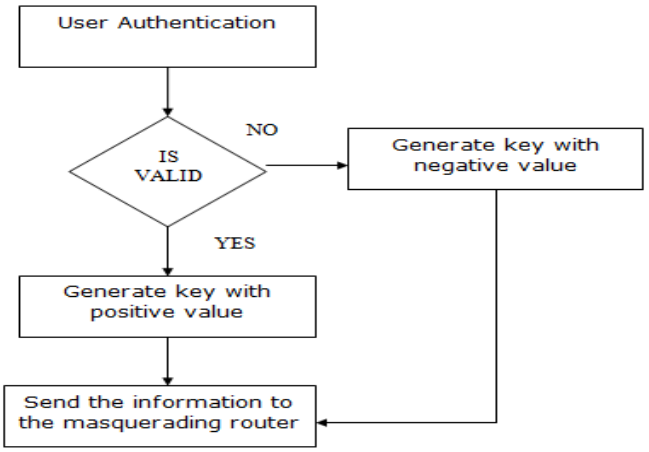

Fig 5 : Authentication Server

Router:

The masking router is responsible for handling the users destined to the back-end server and deciding which user is legitimate and which user should be deflected to the honey pot. The masking router is the only entity on the network that can automatically distinguish between the true back-end server and the honey pot. It verify the key of each user, based on the key forward them to either the true back-end server or the honey pot. It is therefore suggested that the communication between the back-end server, the honey pot.

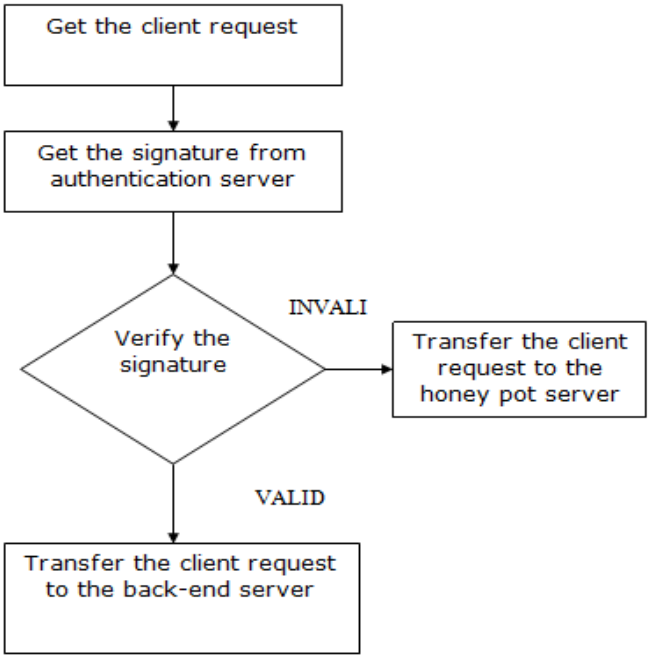

Fig 6 : Router

Honey-pot Server:

The honey pot server is charged with handling unauthenticated user from either an external source or a misbehaving insider.

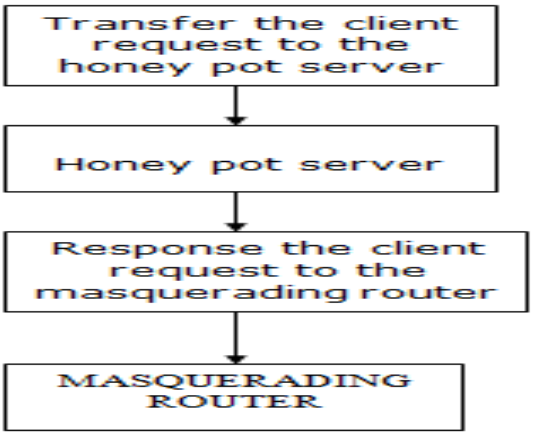

Fig 7 : Honey pot Server

The Honey Pot is a fake protection Environment that can perform a simulation of as small or huge functionality as required. Its messages are handled in the same way as the back-end server messages. The authenticated request and respond messages are processed by the honey pot without any change. The advantages of this system come in the fact that honey pot messages are sent to the application network along with the back end server messages. A user never tells the difference whether the message is being sent from the lawful back end or the honey pot. This makes the honey pot untraceable and unavoidable unless the hacker can authenticate as a lawful user.

Back-End Server:

The back-end server handles request and response messages normally used in the security system; it offers the functionality for the more difficult executions. The user information is not recorded within the back-end server. Instead, permissions are assigned to accessed objects or queries and compared to the permissions assigned to the users to test whether the users is able to legally access the desired information. The indirection between the user and the back-end server is therefore kept highly confidential via use of the masking router, so that the back-end server is much more secured from attacking by the unknown and misbehaving users.

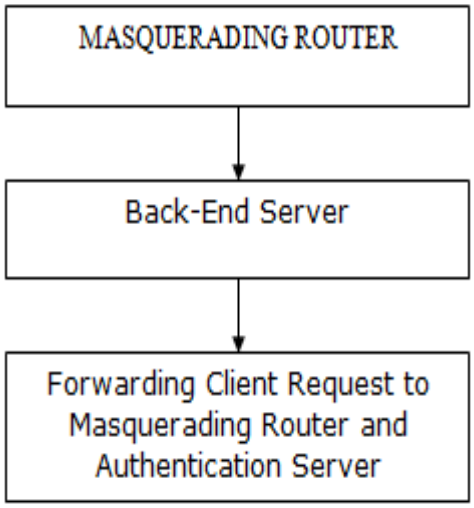

Fig 8 : Back end Server

Proposed System Design

In order to restrain harmful attacks against a back-end server, this paper introduce a network model that allows for separation from unauthenticated traffic, blacklisting of unauthenticated and misbehaving users, and limitation on the effectiveness of back-end DoS attacks. These proposed techniques are accomplished by using four network equipments within a network masked first through fourth. The first of these is the, back-end server itself that manages the responsive data and functions of a web application. The overhead required of the back-end server is consistent with any Role-Based Access Control (RBAC) system in which the server must compare the permissions and accessing limits of users with the request to access a assured resource or carry out a dedicated operation; the only change to this system is the handling of an unauthenticated request. This back-end server is remote usage from the network by a separate connection to a masking router; this is a router that performs its function in a particular way and converts all IP and MAC access on packets exiting the router to the current values for the router itself. In effect, this router operation as a blinder to any traffic sent through its other network connections; this is assumed to occur only on packets designed to the network on which the back-end server is supposed to reside. This layer of indirection prevents the discovery of the actual MAC address of the back-end server's network card. This indirection facilitates the choice of the masking router to allow traffic to pass to the back-end server or deny the unauthenticated message packets. This will secured the server from unauthenticated traffic and misbehaving network users, but further measures can be taken to improve the security of the network. To that end, a honey pot should be organized on the separate network connected by the masking router; a honey pot is a trap system used to create a center of attention of a misbehaving users. The masking router can then decide whether traffic is lawful or not and re-transmit it to either the attached back-end server or to the attached honey pot. Since the router mask the back-end server, any communication traffic out of the honey pot will also appear to be from the masking router and hence appear to be from the back-end server, misbehaving attackers to the fact that they are in reality communicating with a honey pot.

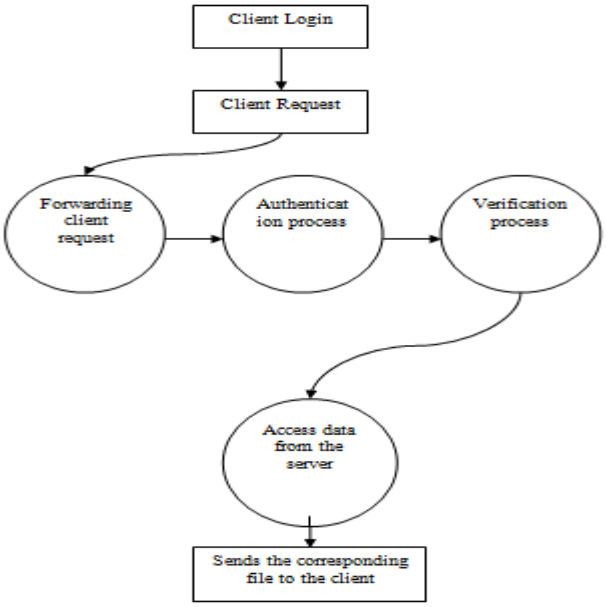

Fig 9 : Complete Flow

Flow Chart

The problem remains of identifying which traffic is lawful. Therefore, the final component necessary for this model is an Authorization Server (AS). This server has the responsibility of authenticated network users and allowing them to utilize the responsive information on the network via a connection to the front-end servers. This is the normal function of an AS with the extra responsibility of assigning tickets based on user permissions for use by the backend server. As part of each user authorization, the ID and the IP address of the users are forwarded to the masking router for storage in its routing table. Therefore, the masking router will be able to determine

which traffic originated from authenticated users and which traffic has been inserted into the network or sent through a front-end server by unauthenticated users.

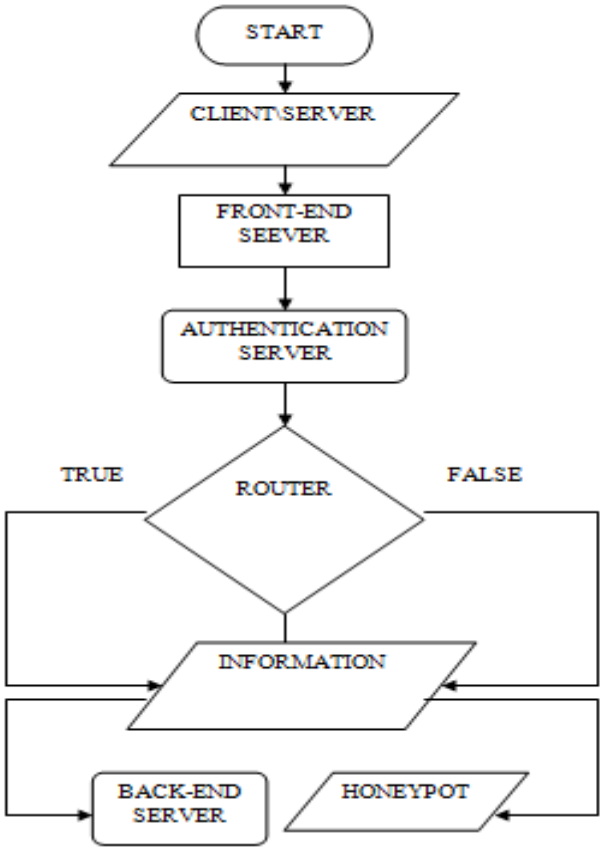

Fig 10 : Flow Chart

REFERENCES

[1] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987

ISSN:-2349-3585 |www.ijrdt.org