Implementation of Security Mechanisms using Honeypots in Banks

Dr. Sonal Bordia Jain
Associate Professor
S.S. Jain Subodh P.G. College, Jaipur
sonalbordiajain@gmail.com

ABSTRACT - In today's world various new threats are frequently emerging for the security of data and any organization's information system infrastructure. A variety of control measures like Firewall and VPN are implemented to prevent intrusions and attacks from outside and within the organization itself. Now a day, Network Intrusion Detection Systems (NIDS) or Intrusion Detection Systems (IDS) has been recognized as one of the most proficient techniqueof discovering attacks. But, the network traffic hasbeen increased innumber and diversity which has resulted in growing costs of hardware and so it is the difficult to analyze the number of false alerts generated in bulk effectively. NIDS are incompetent to identifylatest new kind of attacks as they are growing so rapidly and the encryption prevents them to examine the traffic altogether. So, to cope up with such type of problems, a diverse approach is required. However, the users of electronic banking system still face the security related risks in the form of unauthorized access into their banking accounts by non-secure electronic transactions; hence the need arises to build a reliable system which seizes the identity of both the sender and the receiver. Here, in this paper, a secure system is proposed to be implemented in the banking applications using the concept of honeypots. The integrity of data can be ensured using this system besides with noticing the interaction to identify possible attacks.

KEYWORDS - Honeypots, Information Security and Attacks.

1. INTRODUCTION

In this era of technology, each and everyone is using internet at a very large scale and so the security of the network and data both has become the focal point in each and every organization. Honeypots are set to trap hackers or methods of some new unconventional hacking. Honeypots are basically traps intended to purposely engage and mislead hackers and discover the malicious activities carried out over the internet. Multiple honeypots can be placed on a network to form a honey net. Honeypots are the budding current technology to secure such networking system.

To offer secured platform to any organization, honeypots are incorporated in network with firewall and Intrusion detection systems. Firewall provides the ways to filter and produce logs which further deals with any malevolent activity, firewall rules or any violation policy of access control list. Many diverse approaches like firewall demilitarized zone (DMZ) have been used but they are not successful for today's network security. Then, the Intrusion detection systems are established to overcome the limitations of existing network. Intrusion detection system look for the network's traffic and provide the alerts to notify about any kind of intruders depending upon the database of signatures of existing intrusions. There were a lot of issues with IDS too such as facing an increase in the number of false negatives and false positives. Here the honeypots are then set up in the network to make the most of the unused IPs of the network and the activities of attacker are thus assessed on the basis of these honeypots. Honeypots makes IDS better by making the numbers of false positives lesser in number. The accuracy of network security implemented through honeypots increases with the integration than the security measures of implementation of network Intrusion detection system. For instance, the renowned company Amazon which possess the world's largest database, make use of database honeypots to mislead attackers to reach their actual honeypots.[1]

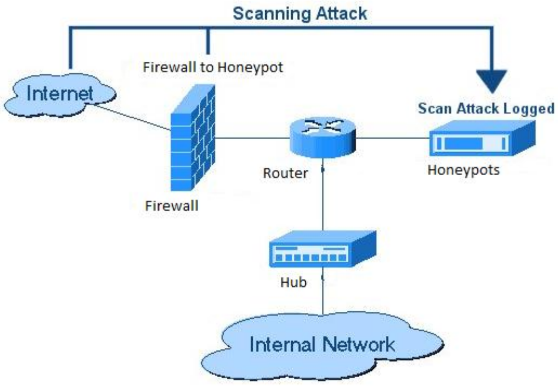

Fig. 1: Architecture of Honeypot Security System

2. CLASSIFICATION OF HONEYPOTS

The classification of honeypots is done based on two parameters primarily; (a) the interaction level (Low and High) and (b) the purpose (Research and Production). [2]
The interaction level defines the degree of activities that honeypot allows an attacker to perform.

1. Interaction Level

a. Honeypots with High-Interaction: High-interaction honeypots are complex solutions as they include real operating systems and the applications of it. This permits an intruder to gain complete access to the system and make use of it to instigate network attacks further. With the help of such security measures implemented through honeypots, the users can gain information about targeted attacks against their systems or even about attacks from inside the system.

b. Low-Interaction Honeypots: In disparity, the low-interaction honeypots put on only services which cannot be exploited to get whole access to the honeypot security system. These honeypots are limited but are useful to collect information about intrudes at a higher level.

2. Purpose of Honeypot (Deployment Method)

a. Research Honeypot – The purpose of a Research Honeypot is to study and analyze about the strategies and techniques of the attackers. It is utilized as a watch to see how an intruder is working when compromising a system.

b. Production Honeypot – These types of honeypots are mostly used to identify errors and to protect the systems in organizations. The major objective of a production honeypot is to assist in lowering the possibility of any kind of risk in an organization.

3. WORKING OF HONEYPOT

a. Data Capture

The major objective of data capture is to document all the attacker's activities. There are two sources of data in Honey Analyzer System: Honeypot log into network traffic log with the help of TCP dump. The framework of Honeypot supports various kinds of logging into network activity. It has the capability to create connection logs that informs about attempted and computed connections for all the protocols. But to study the total attack scenario, the system needs to know complete payload of the packets entering and leaving the honeypot security system. The second element that is TCP dump perform this task by capturing every packet full pay loaded. TCP dump is a tool which monitors the network and known as one of the well-known sniffers for Linux. It then further dumps the packets header information in the log file.

b. Data Analysis

A Data Analyzer has been developed in order to extract the more precise attack signature as shown below:-

The interface of the web gives a graphical output with the use of which, the security administrator simply find out the most attacked ports. So these are the IP address to detect the location of the attacker or hacker. The proposed way of realization of the Honey Analyzer for extracting more precise attack signature is described below:-

- Configuring honeypots for network stimulation
- Run TCP dump for the analysis of network traffic
- Invoke the auto run shell script that runs in a precise gap of time and execute the parser utility that parse the data from the honey log file and insert the data into the database. The realization of the parser utility can be done in any language, which has abilities of strong string tokenization as in java programming language
- Execute the auto-run shell-script to push the honeyed logs data into the database
- In the last, to visualize the patterns of the attack, login to the web interface and analyze the data for extraction of good quality signature

The web GUI has the following features to allow the security administrator to choose the suspicious data: -

i. Capacity to exhibit information of packets from the database.
ii. Ability to display real time network traffic from data stored in database, as well as statistics of historical traffic.
iii. Ability to display the ports, which were attacked within a certain frame of time interval.
iv. A timeline based hit statistic showing how many hits per second Honeypot got in a certain time range.
v. Now the main scenario that is to find which remote IP-addresses were "visited" by Honeypot in a certain time range. Here it's possible to specify a port number to show activity on a specific port.
vi. A textual hit statistic over a certain time range. By specifying an IP or a port number it is possible to focus on specific events.

c. Signature Extraction

The graphical interface has supported for application of LCS algorithm on the data of interest while present system apply LCS algorithm on whole data. The process of finding attack signatures is not fully automated rather it also depends upon the wisdom and experience of security administrator (SA). The Security Administrator can select the traffic on which the LCS algorithm is to be applied. The Resulting precise signature will provide us with the information of less number of false positive and false negatives. The steps followed for finding the good quality attack signature are as follows:-

i. Identify the data of interest from the database by looking at the web GUI. The technique of signature extraction is done by detecting the intruder from the Graphic websites.

ii. Analyze combined data from different data sources that is Honeypot and TCP dump Initiate the following sequence of activities for each received packet:-

- Identify data of interest (i.e. of significance) from the database by looking at the web GUI
- Analyze data from sources i.e. honeypot and TCP dump

4. REFERENCES

[1] Maximillian Dornseif, Thorsten Holz, and Sven M•uller.Honeypots and limitations of deception.

[2] Xiaoyan Sun, Yang Wang, JieRen, Yuefei Zhu and Shengli Liu, "Collecting Internet Malware Based on Client-side Honeypot", 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2008.

[3] C. H. Nick Jap, P. Blanchfield, and K. S. Daniel Su, "The use of honeypot approach in software-based application protection for shareware programs", IEEE International Conference on Computing & Informatics, (ICOCI '06), pp. 1-7, 2006.

[4] JianBao and Chang-pengJi, and Mo Gao, "Research on network security of defense based on Honeypot", IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302, 2010