

Blocking Misbehaving Users using Fake Database

Ambika S¹ Ms. P. Devki²

²Associate Professor

^{1,2}Department of Computer Network Engineering

^{1,2}The National Institute of Engineering, Mysore

Abstract— In the IT world, information is the most important asset for any organization. Protecting this asset is the critical factor and the method of securing this asset is known as information security. In today’s competing IT business, network administrator must be always available to protect the network and the information on the network with extreme measures. One of them is fake database. Fake database reduces the overhead of the network administrator to always be on the network and always monitoring it. Fake database is a setup to imitate a real network. The idea is to make the attacker believe that the fake database is a legitimate system. This Paper proposes the methodology to identify and trap the misbehaving user.

Key words: Anonymizing Networks, NIDS, Fake Database, Nymble, Anonymous Access

I. INTRODUCTION

In today’s world the data that an organization holds is very much valuable and any compromise regarding the data with the unauthorized usage is intolerable by the organization. This may result in huge damage to the same it may be in terms of economy, research; etc securing the data on the file server is of main concern these days. Many organizations have some kind of sensitive data, which are used to develop the market competitive products. These are the data which are frequently in the radar of the intruders. There are different kinds of attacks that an intruder tries to pour on the file server of the targeted organization and fetch the data of their interest. The different kinds of attacks could be any one of the following:

- 1) The intruder pretends to be the genuine user and send the message to the fileserver collects all the data on file server or causes damages the data on the file server.
- 2) The intruder attempts to capture the data units, which is transmitted from the genuine user to file server this unauthorized access may result in data leakage.
- 3) The intruder tries to collect the login privileges and get access to vital information’s in file server.

II. EXISTING SYSTEM

Dealing anonymous network the user IP address is hidden, where the blocked user can use different IP’s to gain access to server. If the user is blocked, the misbehaving user may become anger and launch a more hostile attack against the server. Anonymous networks were operated by small and friendly communities of developers. As interest in anonymous peer to peer increased and the user base grew, malicious users inevitably appeared and tried different attacks. This is similar to the Internet, where widespread use has been followed by waves of spam and distributed denial-of-service attacks.

III. PROPOSED SYSTEM

The proposed work uses the concept of ticket to access a resource with the fake database technology combines to form a new architecture that is used to trap the misbehavior user in fake database instead of blocking. This helps in survey in what kind of data the misbehavior user is interested on server or what kind of attack the misbehavior user is trying to in order to damage the data. The fake database contains all the duplicate files present in the file server but the contents of these duplicate files present on fake database will have junk data. The architecture proposed to trap the misbehaving user.

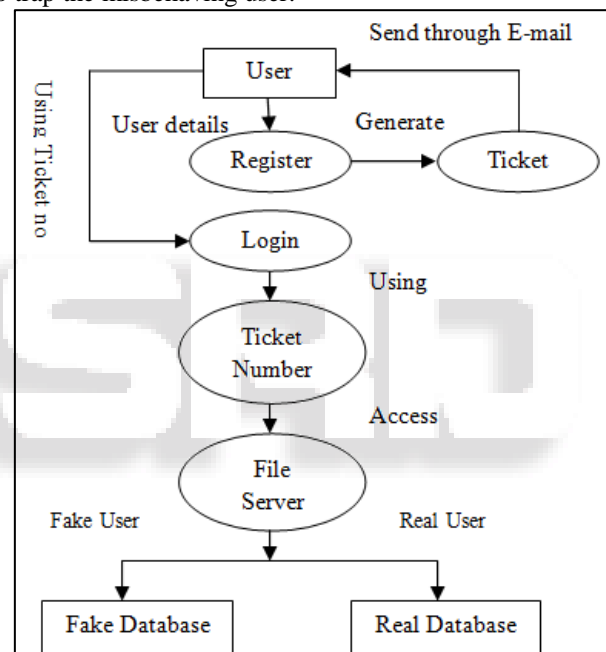


Fig. 1: The Architecture Proposed To Trap the Misbehaving User

The user registers the required details with the administrator (Network Intrusion Detection System (NIDS)). After registering, a ticket number will be generated by a ticket manager. The ticket manager will contain the ticket number and also the IP address and MAC address of the user. The ticket number will be send to the user through the E-mail. Then the user logs in using the user name, password and ticket number. If the user name, password and ticket number is valid the NIDS will compare the current IP address and MAC address with the IP and MAC address of the particular user name and password. If it matches then the user is directed to the real database. If it does not match then the user is directed to the fake data base. By using this system the data will be more secure. Here the intruder cannot access the data.

IV. LITERATURE SURVEY

A. Nymble: Blocking Misbehaving Users in Anonymizing Networks [1]:

The advent of anonymizing networks assured that users could access Internet services with complete privacy avoiding any possible hindrance. This arrangement where series of routers form a network, hide the user's IP address from the server. However malfeasance of few malpractitioners has left this system with a loophole where users make use of this anonymity to deface popular websites. Administrators who cannot practically block a user using IP address are forced to shut all possible nodes that lead to exit. Thus deny access to both behaving and non-behaving user altogether. And so end up blocking users with no compromise to their anonymity. Hence we propose a system which is undogmatic with different servers. Thus we aim at giving the administrator the right to block the malicious user without hindering the anonymity of the rest.

B. Review of Implementing a Working Fake Database System [2]:

A fake database is used in the area of computer and Internet security. It is a resource used to trap attacks, records intrusion information about tools and events of the hacking process, and avoids attacks outbound the compromised computer system. It can also be deployed to attract and divert an attacker from their real targets. The goal of our paper is to show the overview of fake databases and their use in a research as well as productive environment.

A fake database can be anything from Windows to UNIX. Compared to the other intrusion detection systems, fake databases have the big advantage that they do not generate incorrect alerts or large log files like other intrusion detection systems because no productive components are running on the system. Other big advantage of fake database system is that we don't need to manage the data base of intrusions signature or definition. The fake database system logs every byte that flows through the network. This log data helps the researcher to draw a picture of an attack and the attacker.

C. Fake Databases for Distributed Denial of Service Attacks [3]:

Distributed Denial-of-Service attacks are still a big threat to the Internet. Several proposals for coping with the attacks have been made in the recent past, but neither of them are successful on themselves alone. In this paper, we present a system that helps in the defence in depth of a network from DDoS attacks. In addition to state-of-art active and passive security defences, we propose a fake database for such attacks. The goal is to convincingly simulate the success of the compromise of a system to a potential DDoS attacker. Thereby, we can implement the lessons learned by the fake database in our other systems to harden them against such attacks. On the other hand, we protect the rest of our network infrastructure from the impact of such an attack.

D. Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Fake Database [4]:

This research presents an intrusion detection system (IDS) with fake database over distributed networks. The main objective is to compare the effectiveness of attacks between

IDS and IDS with fake database by unicast IP address attack and multicast IP address attack. These attack forms generating by NESSUS. NESSUS is an attack program via wire network and wireless network consists of Snort. Snort is a program that is used to detect intrusion and Honey pot to simulate a fake database computer, which is installed on the system practical for Linux with a number of more 2 points (Sensor) to detect each program will be sent to the primary database for the analysis of experimental results.

V. CONCLUSION

With this proposed method the access to the file on file server can be secured as such, not only the identity but also the ticket place a role in securing the files on the file server, as all the connection to the file server has to go through the NIDS only. Since, NIDS keeps the complete information of the registered users, the file server can be accessed by the registered user with the valid ticket only. With this the system can secure the accessing of files from the file server because there is only one path to the file server that is through the NIDS which acts as a secured gateway.

REFERENCES

- [1] Patrick P. Tsang, Apu Kapadia, "Nymble: Blocking Misbehaving Users in Anonymizing Networks.
- [2] Amandeep Singh, Satwinder Singh, Saab Singh M.Tech CE & Punjabi University Punjab, India "Review of Implementing a Working Fake database System".
- [3] Nathalie Weiler "Fake databases for Distributed Denial of Service Attacks".
- [4] Auttapon Pomsathit, "Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Fake database".