Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Proposed Method to Enhance the Strength of Honeypot Through the use of IP-Spoofing Detection Method

Praveen Kumar
M. Tech (cs)
Department of computer science
BBAU, lucknow, U.P., India

Ram Singar Verma
(assistant professor)
Department of computer science
BBAU, lucknow, U.P., India

Abstract: Worldwide correspondence is getting more critical consistently. In the meantime, PC violations are expanding. Countermeasures are produced to distinguish or forestall assaults. The greater part of these measures depends on well establish truths and known assault designs. By knowing assault methodologies countermeasures can be enhanced and vulnerabilities can be settled.
Honeypot is an advanced way to deal with system security. It is an asset, which is planned to be assaulted and bargained to acquire data about the assailant and the utilized usage. The Honeypot empowers the framework to log each byte that moves through the system, through and The essential convention for sending information over the Internet organize what's more, numerous other PC systems is the Internet Protocol ("IP"). The header of every IP bundle contains, among other things, the numerical source and goal address of the parcel. The source address is the address that the parcel was sent from. By fashioning the header so it contains a diverse address, an aggressor can make it give the idea that the bundle was sent by an alternate machine. The machine that gets satirize parcels will send reaction back to the produced source address, which implies that this procedure is for the most part utilized when the assailant does not think about the reaction or the aggressor has some method for speculating the reaction.

Keywords: Honeypot, IP-Spoffing, internet, protocol

INTRODUCTION

In specific cases, it may be workable for the assailant to see or divert the reaction to his own machine. The most common case is the point at which the aggressor is caricaturing an address on a similar LAN or WAN. Subsequently the assailants have an unapproved access over PCs. In this paper we will propose a method in which we will be discuss how the strength of Honeypot can be increased. We use the concept of IP-spoofing detection method to increase the strength of the Honeypot.
There are many IP-spoofing detection methods. IP-spoofing detection is mainly based on the spoofed packet detection methods.Bundles sent utilizing the IP convention [1] incorporate the IP address of the sending host. The beneficiary guides answers to the sender utilizing this source address. Nonetheless, the accuracy of this address is not checked by the convention. The IP convention indicates no technique for approving the validness of the bundle's source. This infers an aggressor could fashion the source deliver to be any he seeks. This is a notable issue and has been very much depicted [2][3][4]. Identification techniques can be named those requiring switch bolster, dynamic host-based strategies, aloof host based techniques, and authoritative strategies. Authoritative techniques are the most ordinarily utilized strategies today. At the point when an assault is watched, security faculty at the assaulted site contact the security work force at the gathered assault site and request certification. This is amazingly wasteful and for the most part unbeneficial. Methods used for the IP-spoofing detection are:

1. **Routing Method**
2. **Non-routing Method**

RELATED WORKS

Open and private associations exchange a greater amount of their data through the Internet. Today, aggressor or interloper to the framework is the most concerning issue for the security of the system. Hoodlums have greater chance to access touchy data through the Web application. The initial phase in assurance against online assaults is to comprehend the nature and apparatuses of the assaults.
To give security to server information, it is proficient to execute fake administrations utilizing honeypot. Honeypot is only a fake server that gives copied administrations like the genuine administrations running on the real server. So at whatever point aggressor tries to assault genuine server, assailant is diverted towards the fake server that is honeypot and inevitably gets caught in the honeypot. Honeypot then gives the profitable data with respect to the gatecrashers. This data can be utilized to hinder the aggressor and it can be utilized to take the legitimate activities against them [5].
Look into around there has brought about various papers examining particular themes concerning honeypots and how honeypots can be made and sent [6]. It is hard to discover data from a solitary source that gives a general picture of honeypots including their advantages, the ideas driving honeypots, the way to deal with utilizing honeypots, and the difficulties included while executing honeypots.
A few papers and ventures have investigated the strategy of Honeynet as an instructive apparatus for IT understudies and scholarly foundations [7].This inquire about demonstrates that Honeynet can be a successful device in security training. A lot of work is accessible that subtle elements the advantages of honeypots.
Different papers really expound about model PC security lab and outline of system security ventures utilizing Honeypots

[8]. There are additionally papers that depict the procedure and strategies of how honeypots are utilized against insider dangers [9].
To distinguish bizarre or wrong exercises, as of now there are a few strategies, for example, IDS, Firewalls and so forth. Be that as it may, they have a few impediments of inconsistency identifications, for example, high rate of false caution, alarms produced does not contain adequate point by point data for examination and so on.

INVOLVEMENT OF HONEYPOT IN SECURITY

There are two main purposes due to which the Honeypot is used:

1. To figure out how gatecrashers test and endeavor to access your frameworks and pick up understanding into assault strategies to better secure genuine generation frameworks.
2. To accumulate criminological data required to help in the anxiety or arraignment of interlopers.

EXISTING METHODOLOGY OF HONEYPOT

The idea of honeypots was first depicted by Clifford Stoll in his book. This honeypot effectively utilized different virtualized frameworks facilitated on a solitary equipment part. From that point forward, the improvement of advanced honeypots and Honeynets has proceeded. Lately, honeypots have turned out to be relentlessly more adaptable. Honeyed can make various virtual has on a system and can be adaptably arranged to run self-assertive administrations.
The primary target of the honeypot is to befuddle the assailant that the aggressor is parodying the data from the true blue client, all things considered that was not the authentic client, initially that was the copy or the false PC where the aggressor assault the data. So the goal of honeypot is to befuddle the assailant.
Frameworks are utilized for particular examinations and to limit false-positives. In this kind of honeypot system movement which is by all accounts abnormal is diverted toshadow servers and a criminological module gathers valuable data about executed assaults.
In PC phrasing, a honeypot is a trap set to identify, avoid, or, in some way, neutralize endeavors at unapproved utilization of data frameworks. By and large, a honeypot comprises of a PC, information, or a system site that gives off an impression of being a piece of a system, however is really detached and observed, and which appears to contain data or an asset of significant worth to aggressors. This is like the police bedeviling a criminal and afterward leading covert observation [10].
Its basic role is not to be a trap for the dark cap group to catch them in real life and to press charges against them. The attention lies on a quiet accumulation of much data as could reasonably be expected about their assault designs, utilized projects, and the dark cap group itself.This data is utilized to take in more about the dark cap procedures and thought processes, and additionally their specialized information and capacities. This is only a basic role of a honeypot. There is a considerable measure different conceivable outcomes for a honeypot-redirect programmers from gainful frameworks or grab a programmer while leading an assault are only two conceivable illustrations.

PROPOSED ARCHITECTURE

Design

In this system we have considered that all those users are intruder who tries to spoof their IP address. So the proposed method is based on that if any user spoof their IP address then, considered as attacker and redirected to the Honeypot. There will be a Honeywall before the Honeyppot and the real system. At this Honeywall the request is checked that it is request from an attacker or from a genuine user. At the Honeywall the steps involved in this proposed method is shown in the figure below:

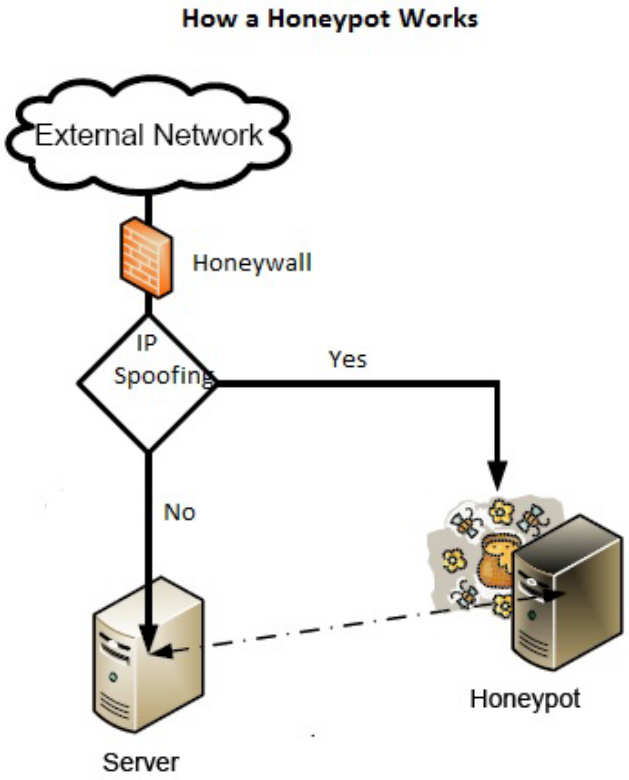

Fig.: How a Honeypot will work with IP Spoofing detection.

ALGORITHM INVOLVED IN THE PROPOSED METHOD

Steps

1. Start
2. Request arrived at the Honeywall.
3. Request is captured by Honeywall and checked with IP-Spoofing detection methods.
4. If(IP-Spoofing==Yes)
5. Request is redirected to the Honeypot.
6. Request is captured at Honeypot.
7. Alarm is triggered for Administrator.
8. A log file starts to maintain.
9. Fake information is replied to involve the attacker for long time and collect more information.
10. Else If(IP-Spoofing==No)
11. Redirect the request to real system.
12. Correct information is replied.
13. End.

COMPARISION BETWEEN PREVIOUS AND PROPOSED METHOD OF THE HONEYPOT

PREVIOUS METHOD OF HONEYPOT	PROPOSED METHOD OF HONEYPOT
Log file is created for every request.	Only the suspected user redirected to honeypot will log file be created.
Log file will capture the large amount of memory.	Only the log file related to attacker will capture the memory, unnecessary memory is not captured.
Every request is not checked before response.	Every request is checked before response and only attacker will be send to honeypot.
Many false alarms are triggered.	False alarms are reduced as only for IP-Spoofed request.

CONCLUSION AND FUTURE WORK

Honeypot is used for the collection of the tricks and techniques involved in the attacking process by the attacker. For this purpose a log file is created for every user when any one tries to enter to the system. It does not detect the user that it is a genuine user or an attacker. It only collects the data and information about and the processes and tools used to enter into the system. For this purpose a log file is created by the system for every user comes into interaction of the system. Now in future these log files are user for the forensic purposes if required. But Honeypot never detect that the user is an attacker or a genuine user.

In the proposed method of Honeypot in this paper the concept of IP-spoofing is used which detect that the user is attacker or not. If the user is found as an attacker then it is redirected to the Honeypot. After the redirection the alarm is triggered for the administrator and the log file is created. In this way the log file is created only for the attacker, which reduces the use of the storage. Also the false alarms are reduced, because the alarms are triggered only for those who try to spoof their IP address. Any genuine user will not spoof their IP address so any user with spoofed IP address will be an attacker. The proposed method has a technique to distinguish the attacker from the genuine users along with the whole quality of the Honeypot. In other words we can say that the proposed method is the advanced version of the Honeypot.

In future the proposed method may come into existence and improve the working quality of the present Honeypot. It will also reduce the unnecessary use of the memory space. If the proposed method will come into existence then the false alarms will also reduce. In the future the proposed method may also be used with different other types of attacking tricks at the place of the IP-spoofing, such as if any attacker tries to hide their IP address, etc.

REFERENCES

[1] Daemon9. IP Spoofing Demystified. Phrack Magazine Review, Vol 7, No. 48, June 1996, pp. 48-14.

[2] Computer Incident Advisory Committee (CIAC) (1995). Advisory Notice F-08 Internet Spoofing and Hijacked Session Attacks.[On-Line],Available:http//ciac.llnl.gov/ciac/bulletins/f-08/shtml,retrieved August 2006.

[3] Donkers, A. (1998, July). Are You really Who You Say You Are? System Administrator, Vol 7, No. 7, 69-71.

[4] D. Schnackenberg, K., Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response," Proc.DARPA Information Survivability Conference and Exposition January 2000.

[5] M.Balamurugan , B Sri Chitra Poornima "Honeypot as a service in cloud", InternationalConference on Web Services Computing ,IJCA 2012.

[6] Karthik, S., Samudrala, B. and Yang, A.T., "Design of Network Security Projects Using Honeypots.", Journal of Computing Sciences in Colleges, 20 (4)

[7] A. Chandra, K. Lalitha, "Honeypots: A New Mechanism for Network Security", Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College A. Rangampet , Tirupati. Vol 04, Special Issue01; 2013**.** http://ijpaper.com/

[8] Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang. "Design of Network Security Projects Using Honeypots". Journal of Computing Sciences in Colleges, Vol. 20, Issue *4*. April 2005.

[9] "Honeypots: Catching the Insider Threat", by LanceSpitzner. Proceedings of the 19th Annual Computer Applications Conference (ACSAC)2003, Honeypot Technologies Inc.

[10] "Honeypots" available at :http://en.wikipedia.org/wiki/Honeypot_%28 computing %29.