International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 04, April 2016
www.ijirse.com
ISSN: 2454-9665

HONEYPOT: AN EXTERNAL LAYER OF SECURITY AGAINST ADVANCE ATTACKS ON NETWORK

Aaditya Jain[1], Bhuwnesh Sharma[2], Pawan Gupta[3]

[1,2] M.Tech Scholar, [3] Assistant Professor, Department of Computer Science & Engg.,
R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, (India)

ABSTRACT

The number of people connecting to the internet is increasing very rapidly but the risks involved and new types of attacks are also increasing day by day. It is necessary to have tool for detecting and preventing attacks. A perfect tool for this can be a Honeypot. It has a huge potential for the security community and can achieve several goals of other security technologies. This paper discuss about the honeypot technology with its classification and deployment strategy. Paper also throws light on how honeypot can be used as defence tool against advance attacks like Denial of service attack, Distributed denial of service attack, Botnet attack, and Polymorphic worm attack.

Keywords: Honeypot, DOS, DDOS, Botnet, Polymorphic worm.

I. INTRODUCTION

In the era of information technology security of network has become the core issue, because exploitation of network is getting more common. Protection of information availability, its access and data integrity are the basic security characteristics of information sources. Firewall and Intrusion detection system are two broadly used solutions for protecting network against advance attack but both have their limitations [2]. Firewall cannot protect from internal threats and from attacks that bypass the firewall. For proper working Intrusion Detection System needs signature of attacker or his attacks and if new attack is launched then it is fail to detect such attack. So there is a need of an external layer that works against attacks that are not detected by the Intrusion Detection System.

A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information system. Its primary goal is not to ambush attackers but the focus lies on silent collection of as much information as possible about their activities and used strategy. Honeypot is a simple and cost effective tool for securing network. It is an information system resource whose value lies in unauthorized or illicit use of that resource. It provides direct and indirect values to an organizations information security [1]. The direct value of honeypot is based on their detection capabilities and design concept. Its indirect value is based on the analysis performed on captured data. It is clear that if intruders do not interact with honeypot then it has little value.

II. HONEYPOT WORKING PRINCIPLE

Honeypot is an advance decoy based technology, is an elective means to save the network and search in order to design a tough system on a descriptive environment. It works by fooling attackers into believing that it is a legitimate system, attackers attack the system without knowing that they are being observed. When an attacker

attempts to compromise a honeypot, its attack related information such as the IP address etc. will be collected, and generates an alarm to the administrator of the system [3].

The overall functionally of honeypot is depends on three major task done by it. First luring the intruders for attacks, if the system is compromised by intruders then second task is providing fake details so that intruder spend more time such system. At last analysis the activities performed by intruders and generate alerts.

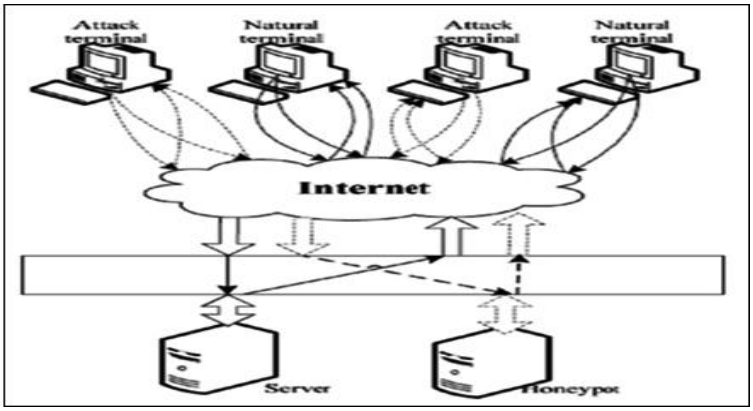

Fig. 1 Honeypot working principle [3]

III. CLASSIFICATION OF HONEYPOT

For better understanding, honeypot can be classified their level of involvement with intruders and their deployment purpose.

3.1 According To Level Of Involvement With Intruders

The level of involvement does measure the degree an attacker can interact with the real system [4].

Low Involvement Honeypots: Low involvement honeypots does not provide operating system access to intruders. It only provides fake services to fool the attackers. They involve low risks, easy to install, configure, deploy, and maintain because of their simplicity. But they provide limited information about intruders and attacker can easily detect them. Example a facade is a software emulation of a target service or application that provides a false image of a target host and honeyed is another one.

Medium Involvement Honeypot: The working of such honeypot lies between low involvement and high involvement honeypots and do not provide operating system access to attackers but chances to be probed are more than low interaction honeypot . These honeypots are more capable than low-interaction honeypot but involve high risk compare to it. Examples of medium interaction honeypot are Napenthes, Dioneae, and honeytrap.

High Involvement Honeypot: Such Honeypots uses real operating systems and applications so difficult to design. Primary aim is to capture more malicious activities from attacker's side. These honeypots involve high risk also because it is not impossible that attackers might take over such system and use it as stepping stone to attack other systems in the network. Honeywall is the best example.

3.2 According to Deployment Purpose

Honeypots comes in many shapes and sizes according to purpose for which it is developed [2]. Broadly they can classify as production and research honeypot [5].

Production Honeypot: This type of Honeypot helps to mitigate risk in the organization by protecting their internal IT infrastructure. These honeypots are placed along with production server inside the production network to improve overall security. These types of honeypots are easy to deploy and have limitation of capturing limited information because they are actually low interaction honeypots.

Research Honeypot: Research honeypots work on the principal of knowing about the tricks used by the attackers and by his communities. Research honeypots give a platform to study cyber threats and fill the lack of information on the enemy so used by educational entities, military or government organizations. These honeypots are difficult to maintain and complex to deploy and does not add direct value to the organization.

IV. HONEYPOT DEPLOYMENT STRATEGY

Honeypots are integrated in network with firewall and Intrusion detection systems to provide solid secure platform to an organization as described in [6]. Honeypots introduced in the network to utilize the network's unused IPs and the attacker's behavior is analyzed on these honeypots. Honeypots improve IDS too by decreasing the numbers of false positives. With the integration honeypots network security accuracy increases than the only implementation of network Intrusion detection system. These are the increasing trends in information security mechanism. For instance, the well known company Amazon possessing the world's largest database uses honeypots to deceive attackers to reach their actual honeypots.

To maximize the strengths and minimize the risks consider following strategies:

- Install Honeypots along with regular production servers.
- It will likely need to mirror some real data and services from the production servers in order to attract attackers.
- The security of the Honeypot can be loosened slightly so as to increase its chance of being compromised.
- Pair each server with a Honeypot, and direct suspicious traffic from server to the Honeypot.
- Build a honeynets [1], [7], which is a network of Honeypots that imitate and replicate an actual or fictitious network.

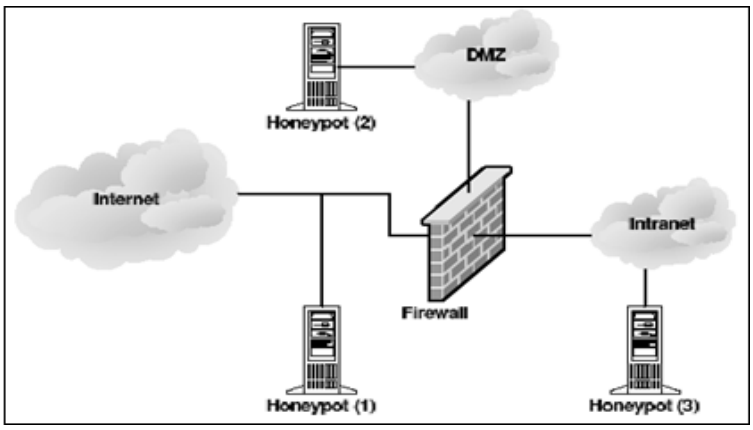

Fig. 2 Placement of Honeypot in the Network

V. HONEYPOT AGAINST ADVANCE ATTACKS

Honeypots play a great role in the area of network security. Honeypots have evolved in diverse directions to cope with various new security threats against not only security defenders but also novice users in the Internet today. Yu Adachi et al. in [8] describe about various harmful attacks that occur on internet to disturb the users and their working. To cope with the recent changes in the network security new forms of honeypots are introduced, they act against the new vulnerable activities or against advance attacks which is not detected by IDS [2]. Some proposed solutions by multiple authors in their research papers are surveyed in this section.

5.1 Honeypot Against Botnet Attack

Botnet is one of the major internet threats now a day, mainly focus on compromising and controlling victim computers. Each compromised computer is installed with a malicious program called a "bot", which is used to communicate with other bots in the botnet as shown in figure3.

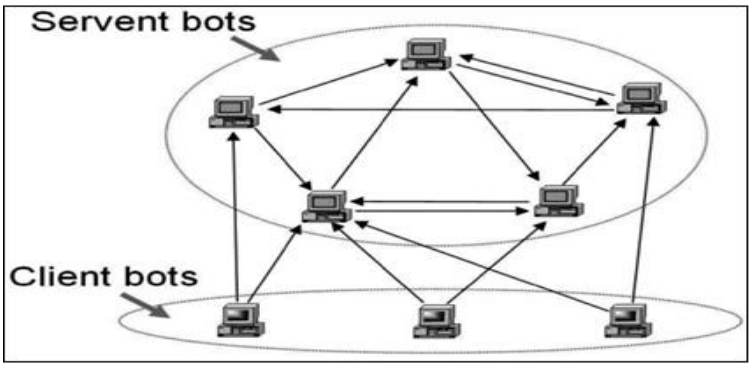

Fig. 3 Architecture of Botnet

Rajab Challoo et al. in [9] use honeypot to expose botnet membership and its behavior. Authors deploy honeypot in the network in such a way that it lures the attacker. When attacker gain control on honeypot system

Alberdi et al. in [10] proposed a solution in which honeypots monitor actual malicious activities by bots, worms, and viruses without letting them leave the honeypots. Author proposed a "Redirection Kit", which redirects outgoing attacks, such as messages bots used to coordinate attacks, to other honeypots to prevent the malicious attacks to other production servers through honeypots at the same time it prevents detection of the honeypots by the attackers. Using this mechanism, the bot masters still believe that their bots communicate with hosts outside of the network, while they are actually communicating with another honeypot in the same network.

Cooke et al. studied the possible threats to honeypots by bots [11]. Cook performed experiments in which a honeypot was installed to observe that the honeypot was repeatedly compromised by attacks from bots, sometimes by two bots at once. These stunning findings imply that the recent bots are strong so that special honeypots to protect honeypots are needed. Cooke proposed "Super Honeypots" that are honeypots for honeypots. Cook designed the super honeypot in the following way. First, deceptive honeypots that intentionally let bots infect and compromise them are set up. Then, the super-honeypot monitors the deceptive honeypots to capture, learn, and prevent such bots.

ISSN: 2454-9665

5.2 Honeypot Against Denial Of Service (Dos) And Distributed Dos Attack

Denial of Service attacks is the most ubiquitous, easy to implement and unavoidable for most of the time. The attack gets worse when a distributed denial of service attack is implemented which attempt to make a service usually one offered over internet, unavailable to its legitimate users. Figure 4 describe basic of DOS attack.

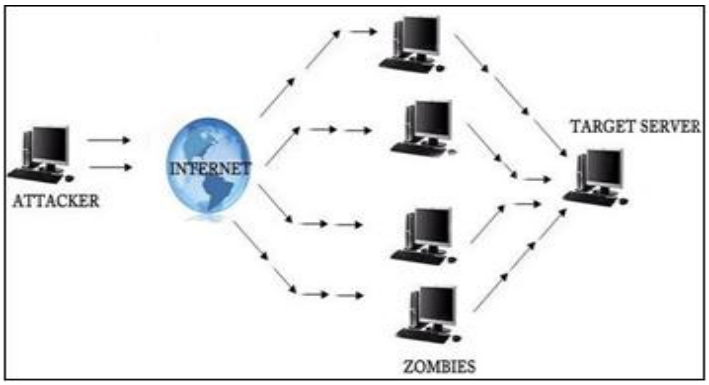

Fig. 4 Denial of Service Attack [12]

Vinu V. Das in [12] proposed a solution to mitigate denial of service attacks by hiding production servers behind an access gateway, called "Active Server (AS)". Each AS authenticates its clients and once a client is authenticated, a path is opened between the client and a server. If an AS does not authenticate a client, it behaves as a honeypot, trapping the client there. Since authentication done prior it will prevent DoS attackers from clogging the path from an AS to the protected server.

Khattab et al. proposed a solution against denial of service attack in [13]. In the strategy honeypots and production servers are continuously shuffled within a network. Honeypots trap attackers, which prevented, reduced, and delayed the impacts from the DoS attacks. The production processes automatically became honeypot when they migrate to other hosts. This solution will be effective when the majority of the incoming requests are DoS attacks. But if majority of traffic is legitimate and only few requests are DoS attacks, the solution is ineffective since a certain number of servers function as honeypots irrespective of the traffic.This method will be an effective solution for a large scale distributed DoS attacks.

Sridhar et al. proposes the usage of honeypots to prevent DDoS attacks for cloud infrastructure [14]. This solution proposes a network of honeypots to monitor attacker activities but doesn't provide satisfactory solutions to mitigate flooding attacks. In the same direction Natalie Weiler in [15] proposes implementation of a cluster of physical honeypots servers that mimic the activities of real servers. This solution is expensive since every honeypot needs a separate physical server which results in wastage of resources and high maintenance costs.

Arun Deshpande in [16] proposed an effective and new solution against DDOS attack by using virtual Honeypots called "Honeymesh". Author creates a network of virtualized Honeypots (i.e. Honeypot as virtual machine) within the existing infrastructure with minimal cost and maintenance overheads. Since VM's share resources, multiple honeypots can be hosted on a single server. These VM's continuously monitor the incoming traffic for potential malicious activities and once an attack is discovered, all the traffic from the attack source is routed to the honey VM network.

ISSN: 2454-9665

5.3 Honeypot Against Polymorphic Worm Attack

Polymorphic worm attack is very harmful and destructive or intrusive that changes its signature constantly. So it is difficult find the signature, but honeypot in this direction work well.

Hyang Ah Kim et al. proposed "Autograph" [17]**.** It is a distributed, automated worm signature generation scheme to detect polymorphic worms. Autograph takes input from across DMZ traffic. Payloads partition is done into different content block and using COPP algorithm. The content blocks are analyzed and autograph selects most frequently occurring byte sequence across the flows in suspicious flow pool. Prevalence histogram is generated for each content block which acts as worm signature. Polymorphic worms may change their payloads in each injection. Autograph fails to address this problem.

Mohssen M. Mohammed et al. proposed a concept of "Double Honeypot and Principal Component Analysis (PCA)" in [18] to enhance accuracy in signature generations for polymorphic worms. Authors used two honeynets first honeynet catches a worm and then allowed to infect other systems in the second honeynet. The worm can move back and forth between the two honeynets, evolving as it goes. Each version of the worm is captured as the worm repeats infection between the two honeynets. All versions are analyzed using PCA to produce a signature that can be used to detect the polymorphic worm using intrusion detection systems.

James Newsome et al. developed a solution called "polygraph" in [19] to cope with polymorphic worms in automating their signature generations with low false negatives and low false positives while using network flows that may contain noise to generate the signatures. The solution extracts a signature that consists of multiple disjoint content substrings for a polymorphic worm, instead of a particular fixed substring to achieve the accuracy. The solution first discovers tokens, which are the substrings that have to appear in a specific order or the special case of regular expression using clustering techniques. To efficiently extract signatures, the solution classifies the contents to three major sections of invariant, wild card, and code bytes data sections. The authors concluded that content-based filtering with effective signatures would be still useful, contrary to the wide-spread rumors that are skeptical about their usefulness.

5.4 Honeypot Against other Advance Attack

Shujan Li et al. proposed a new concept called "Phoneybots" in [20] specially designed for monitoring bank transactions using fake accounts to trap behavior of attackers or phishers. In the existing systems, after spam traps capture spam emails from phishers, the human administrators analyze them and launch a client-side honeypot to the phishing sites to examine whether they are phishing sites or not. This causes significant delay in responses that lets attackers detect such investigations.

Steave Webb developed a high-interaction honeypot in [21] to cope with currently popular social spamming. Social spamming is sending spam messages to innocent human users in social networking services to guide them to malicious web sites. The proposed high-interaction honeypot analyzes friend invitation requests spams in MySpace. Webb created 51 dummy personal profile accounts in MySpace. Running behind each dummy page, the honeypot waited for incoming friend invitation requests from spammers, downloaded the spammers' profiles, recorded their origin network addresses, and identified the spammer's geographical location for further analyses. Webb also found that the spamming behaviors in spam profiles follow distinct temporal patterns.

Lance Spitzner presented techniques for detecting insider threats using honeypots and honey tokens [1]. Spitzner pointed out that insider threats have challenges different from outsider attacks, as that the malicious insiders are given access to the system and are much more familiar with it. To help catch such malicious insiders, honeypots should be moved into the network and can take up all unused IP addresses. Also, because they are familiar with the system, all of the honeypots must be high interaction. The malicious insiders must be directed to the honeypots rather than hoping they come across them on their own. Attackers of this type are after information that they can use, therefore the honeypots must provide data that the attackers will want but do not need to know. This could include false business plans and design specifications. These false documents, as well as the password to log in such servers can be honey tokens.

VI. CONCLUSION

Over recent years area of network security achieves the biggest progress because nobody wants that his system will be attacked by intruders. Honeypot technology is useful and extremely important part of an overall network security strategy if security professionals and researchers are to know their enemies, and insure that network security keeps pace with the rapid changes in network attacks. No other mechanism is comparable in the efficiency of a honeypot if gathering information is a primary goal. This paper describe new ways with honeypot to enhance network security policies against advance attacks but we also have to consider the fact that if attacker know about such system or bypass from it than the whole mechanism is meaningless, so develop a honeypot in such a way that attacker will definitely believe that it is a original production server. Strong control mechanism is required because if attacker is successful in controlling the honeypot system than it will not used by attacker for further attacking purpose.

REFERENCES

[1]. L. Spitzner, "Honeypot: Catching the Insider Threat", 19th Annual Computer Security Applications Conference, 2003.

[2]. Aaditya Jain, Dr. Bala Buksh, "Advance Trends in Network Security with Honeypot and its Comparative Study with other Technologies", International Journal of Engineering Trends and Technology, Vol. 29 , No. 6, 2015.

[3]. Snehil Vidwarshi, Atul Tyagi, Rishi Kumar, "A Discussion about Honeypots and Different Models Based on Honeypot", 28th IRF International Conference, ISBN: 978-93-85465-37-6, June 2015.

[4]. Navneet Kambow and Lavleen Kaur Passi, "Honeypots: The Need of Network Security", International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 5, 2014.

[5]. Niharika and Ranjeet Kaur, "Honeypot for Network Surveillance", International Journal of Research in Engineering & Technology, ISSN (E): 2321-8843, ISSN (P): 2347-4599 Vol. 2, Issue 5, May 2014.

[6]. Snehal B Rase and Pranjali Deshmukh, "Summarization of Honeypot: A Evolutionary Technology for Securing Data over Network" International Journal of Science and Research, ISSN: 2319-7064, 2013.

[7]. http://www.honeynet.org.

[8]. Yu Adachi and Yoshihiro Oyama, "Malware Analysis System using Process-Level Virtualization", Proceedings of IEEE Symposium on Computers and Communications, pp. 550-556, July 2009.

[9]. Rajab Challoo, Raghavendra Kotapalli, "Detection of Botnets Using Honeypots and P2P Botnets", International Journal of Computer Science and Security (IJCSS), Vol. 5, Issue 5, 2011.

[10]. Ion Alberdi, Éric Philippe, Owezarski Vincent, and Nicomette M. Kaâniche, "Shark: Spy Honeypot with Advanced Redirection Kit", Proceedings of the IEEE Workshop on Monitoring, Attack Detection and Mitigation, November 2012

[11]. Evan Cooke, Farnam Jahanian, and Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets", Proceedings of the USENIX Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, July 2005, pp. 39-44.

[12]. Vinu V. Das, "Honeypot Scheme for Distributed Denial-of-Service", Proceedings of the 2009 International Conference on Advanced Computer Control, January 2009, pp. 497-501.

[13]. Sherif M. Khattab, Chatree Sangpachatanaruk, Daniel Moss, Rami Melhem, and Taieb Znati, "Roaming Honeypots for Mitigating Service-Level Denial-of-Service Attacks," Proceedings of the International Conference on Distributed Computing Systems, March 2004, pp. 328–337.

[14]. Kumar Shridhar and Nikhil Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot", International Journal of Science and Research, Volume 3 Issue 11, November 2014, pp. 2378-2383.

[15]. Natalie Weiler, "Honeypots for distributed denial-of-service attacks", Proceedings of Eleventh IEEE International Worksops on Enabling Technologies, 2002.

[16]. Hrishikesh Arun Deshpande, "Honeymesh: Preventing Distributed Denial of Services Attacks Using Virtualized Honeypots", International Journal of Engineering Research & Technology, Vol. 4 Issue 8, 2015.

[17]. Sounak Paul and Bimal Kumar Mishra, "Honeypot Based Signature for Defence Against Polymorphic Worm Attack in Networks", IEEE International Advance Computing Conference (IACC), 2013.

[18]. Mohssen M. Z. E. Mohammed, H. Anthony Chan, Neco Ventura, Mohsim Hashim, Izzeldin Amin, and Eihab Bashier, "Detection of Zero-Day Polymorphic Worms Using Principal Component Analysis," Proceedings of International Conference on Networking and Services, March 2007, pp. 277-281.

[19]. James Newsome, Brad Karp, and Dawn Song, "Polygraph: Automatically Generating Signatures for Polymorphic Worms," Proceedings of IEEE Symposium on Security and Privacy, May 2005, pp. 226-241.

[20]. Shujun Li and Roland Schmitz, "A Novel Anti-Phishing Framework Based on Honeypots," Proceedings of eCrime Researchers Summit, October 2009, pp. 1-13.

[21]. Steve Webb, James Caverlee, and Calton Pu, "Social Honeypots: Making Friends with a Spammer Near You," Proceedings of the Conference on Email and Anti-Spam, August 2008.

[22]. Upendra Joshi , Sumeet Sehrawat, Taranjeet Singh Huda. "RELIABILITY PARAMETER ESTIMATION AND ANALYSIS FOR ELECTRICAL UPS SYSTEM." International Journal of Advanced Technology in Engineering and Science 3.Special Issue No. 01 (2015): 280-284.