Proceedings of the 10th INDIACom; INDIACom-2016; IEEE Conference ID: 37465
2016 3rd International Conference on "Computing for Sustainable Global Development", 16th - 18th March, 2016
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

Honeypot-Based Intrusion Detection System: A Performance Analysis

Janardhan Reddy Kondra
National Institute of Technology
Rourkela - 769008, India
Email Id: 9494566535jana@gmail.com

Santosh Kumar Bharti
National Institute of Technology
Rourkela - 769008, India
Email Id: sbharti1984@gmail.com

Sambit Kumar Mishra
National Institute of Technology
Rourkela - 769008, India
Email Id: skmishra.nitrkl@gmail.com

Korra Sathya Babu
National Institute of Technology
Rourkela - 769008, India
Email Id: ksathyababu@nitrkl.ac.in

***Abstract*— Attacks on the internet keep on increasing and it causes harm to our security system. In order to minimize this threat, it is necessary to have a security system that has the ability to detect zero-day attacks and block them. "Honeypot is the proactive defense technology, in which resources placed in a network with the aim to observe and capture new attacks". This paper proposes a honeypot-based model for intrusion detection system (IDS) to obtain the best useful data about the attacker. The ability and the limitations of Honeypots were tested and aspects of it that need to be improved were identified. In the future, we aim to use this trend for early prevention so that pre-emptive action is taken before any unexpected harm to our security system.**

Keywords- Control center; Firewall; Honeypots; Honeypssot farm; Honeywall; Sebek; Snort; Virtual honeyd.

I. INTRODUCTION

With the ease of connecting through the internet, threats of internet attacks also came along with it. Various technologies have been widely used for the improvement of network security [1]. To detect the black-hats society, it is necessary to keep up-to-date with the hacker innovations. In recent times, two types of security scenario activities observed namely, black-hats and white-hats. Black-hats destroys the network while white-hats protects the network. Honeypots were used for combat attacks. Honeypots can be defined as "An attractive defence tool placed in a network that attracts the attackers towards it, detects them, and observe them with the actual intention to know them" [2]. Honeypots can be used for various purposes such as prevention, detection, and information gathering about network threats [3, 4]. To study about hackers in social network and how they communicate with each other. It is necessary to offer a real operating system to the attacker so that the attacker can gain root privileges on the system and information about the attack can be identify. The amount of activity perform by the attacker with the honeypot is called interaction level. Honeypots are divided into two broad categories, namely low-interaction Honeypots and high-interaction Honeypots [5, 7, 13, 14]. Low-interaction honeypots provides the minimum interaction between the attackers and the system and captures only a small amount of data regarding the attacks [7, 14]. It can emulate numerous operating systems and offers diverse TCP/IP services to them. A large network topology that can be simulated with different routers to work with various types of network topology. High-interaction honeypots interacts maximum with the attacker, also allows the attacker to access the real operating system to experiment with [7, 13]. High-interaction honeypots are not predicting that how an attacker will attack, and they prepare the services to respond accordingly. These honeypots explore the attacker with the real operating system and applications [7].

According to the capabilities, honeypots can be categorized into three different categories namely, preventive honeypots, deceptive honeypots and detective honeypots. Preventive honeypots are deployed for network prevention and it can be classified into two sub-categories such as sticky honeypots and deceptive honeypots. Sticky honeypots are the low-interaction honeypots that protects the network from automated attacks like worms. These attacks, scans the networks for vulnerable systems and if found, the system is overtaken and slows the attacker down by TCP tricks. On the other side deceptive honeypots are the honeypots that can have low interaction honeypot or high interaction honeypot which protects from human attacks. The main goal of these honeypots is to waste the attacker time and till the time attacker is interacting with the machine all the relevant information about the attacker is extracted like the tools, techniques used by the attacker, how they take over the system. Detective honeypots generates alerts as an early warning and detects unauthorized attempt in the network. An example of detective honeypots is honeyd. Responsive honeypots are the honeypots those are used only to educate us against the black-hats community so that effective measures can be taken against them.

In recent years, honeypots have been focussed on mainly three types of architectural approaches, namely conventional honeynet, modified honeynet and hybrid honeynet [2]. Conventional honeynet combines intrusion detection system, intrusion prevention system, and other security related resources to offer high performance, however it is costly to

 ISSN 0973-7529; ISBN 978-93-80544-20-5

manage the resources or to work out research purpose as well [2,7]. Another type of honeynet architecture is "Modified Honeynet" architecture which improves the shortcomings of the conventional honeynet design, also its management system manages all the security resources and has less hardware cost when compared to the previous design [2]. Although problem with this approach is its complexity and reliability to combat the attackers. To improve with the above two approach challenges "Hybrid Honeynet" was introduced. Hybrid honeynet combined the concept of conventional honeynet and modified honeynet design. Hybrid honeynet offers flexible, cost-effective, better reliability. It uses the concept of virtualization techniques within a single platform [15]. Unfortunately, the only disadvantage of this approach is its low performance.

In this paper, we proposed a new virtual Honeynet architecture that implements virtual honeynet collaboration systems (VHCS). Proposed approach is able to overcome the honeypot module and security module problem.

The rest of the paper is organized as follows: In Section 2, related work is presented. Proposed work is given in Section 3. Performance analysis is discussed in Section 4. Finally, we conclude in Section 5.

II. RELATED WORK

Previous section gives a brief introduction of the Honeypots. This section will address more about the work done in this field and related in the field of research on decoys in different areas to combat the attackers. An experiment conducted by Reto Baumann, who performed it for 14 days and honeyd system was configured to host with three different virtual machines and each listening on its own IP addresses [13]. To let traffic pass to the network interface, it is necessary to answer to the respective address resolution protocol (ARP) requests. Honeyd listens on the network interface and then answers to the ARP requests for some IP addresses. Different virtual honeypots on a single machine with different simulated operating systems increase the performance for detecting victims so that relevant information can be gathered. A script can be attached to a certain port that allows a very flexible setup with efficient capabilities for detection where the number of alerts that was generated in two weeks were 11 and 121. Top attacker named Telstra, who belongs to an Australian company who is an Internet Service Provider (ISP), offers Internet connectivity to the customers. Another top attacker, belongs to France University. The next attacker again belongs to the ISP, who belongs to China [1].

Disk imager makes the forensic image of the target's file system and there is the low communication latencies in between the two new components introduced [4]. When all the Honeynet machines are located on the same physical machine, it is directly proportional to the latency (results in low latency). FSLog was again introduced and described by the author which efficiently logs 18 virtual file systems out of the 60 virtual file systems, where the system calls the Linux 2.4 kernel machine. This approach removed the disadvantages of virtual honeynets in terms of Security and detectability. But the only disadvantage is that the flexibility remains a problem [4]. The Author has focused on the most frequently targeted destination ports as the port that was targeted is directly being linked to the malicious activity types [5]. It was observed that compared to the external traffic, the internal traffic contained different malicious types. They also provide the information that the stability of the external malicious performs over the week, but the internal traffic is not stable as a function of the user's activity profile [5]. Adding to this, Honeypot is a terminology to detect any malicious activity of information system, current size of the size touching the term big data. By combining both concepts, Puthal et al. proposed novel techniques for big data stream security verification [9]11]. These concepts perform security verification at server side without communicating sources after handshaking.

Zhi-Hong *et al.* [6] introduced a prevention model for the solution of the honeypot problem and they also show the experimental results. According to Mohssen *et al.* [16], since every year availability and integrity of the world-wide internet and based services has been affected by internet worms generally by changing their payload on every infection attempt. Here, they have proposed a mechanism for the automated signature generation for Zero-day polymorphic worms. They have also planned and designed a novel double-Honeynet system. This system is capable of detecting unknown new worms and the system utilizes an algorithm that uses the worm's binary representation for pattern matching and is capable to generate an accurate signature for different (single or multiple) worms [7].

Further, Chang *et al.* [2] have proposed the Virtual Honeynet collaboration System (VHS) for the improvement of the Honeynet architecture by the use of some virtualization technologies. Herrero *et al.* [8] proposed some algorithm such as Honeypot Redirect Outbound (HRO) and the Honeypot Redirect Inbound (HRI) algorithms. The advantage of the proposed approach is that it has higher flexibility and usability and each module can be customized according to different needs, making the VHS superior to the existing Honeynet designs by cost, and also is more flexible security platform.

Unfortunately, this high-interaction client honeypots is not as efficient for detecting malicious web pages, carrying rootkit which is used for hiding the malicious object. Because of this problem, the authors in [16] proposed a detecting technique for kernel integrity which is based on System Services Descriptor Table (SSDT). The experimental results indicate that the detection ratio increases for most of the malicious servers.

According to L. Li *et al.* [3], an application of honeypots in the LAN system, where the physical honeypots as well as virtual honeypots are placed in a specific location. Honeypots can lure hackers to attack the internet, and logs the activities, analyze of the logs gathered and study about

the attacker. By this way information about the latest attack, methods and tools, can be known. The traditional defense system generally gives an inadequate performance, this is the reason why honeypot is deployed to the LAN for active defense [10]. When proposed virtual system is used, then the connections that seems to be suspicious who are visiting the server are shunted to the virtual honeypot that effectively reduce the risk of server attacks and is cost-effective. Information about the attacks is recorded with the help of the intrusion attraction and also capture functionalities of physical honeypot without attacker's awareness. This research enhances the security of local area network and attacker always wants to choose the optional path which is not a honeypot [10].

Honeypots have advantages as well as few shortcomings also. Although it has proved itself in various areas of security for detection purpose. The related work review reveals that a honeypot is a very efficient detecting tool which can be used in many areas for defense purpose by the researchers. The most important feature is that it has the capability to offer a real time defense system and to catch newly born attacks and the information about them, the tool they use, the methods they used, and the way of attacking. Because of this effectiveness of the decoys the attackers always try to skip honeypot path as they know they will be caught. This section focused the previous work done by the researchers in different areas of honeypots, to detect and catch the attackers and prevent our secure network. The next section shows our proposed approach and the summary of the work we have done on honeypots.

III. PROPOSED APPROACH

This paper proposes a new approach as compared to the existing shortcomings in the security scenario as shown in Figure 1. It uses the virtualization technique to overcome the existing security problem. It overcomes the limitation of honeypots from single network detection to network across the organization and improves the existing security design to waste the attackers' time as much as possible to get the best useful information.

The proposed approach collaborates the concept of Honeynet, honeyd and honeypots related security resources. Honeyd is a low-interaction honeypot which can detect and also log any activity on any port (UDP or TCP), and also for some ICMP port. Honeyd must be configured with attack signatures so that it can recognize the type of attacks. Honeyd has the capability to interact with the attackers. This is the reason why Address Resolution Protocol Daemon (ARPD) is required in order to detect in the first place that there is someone who is trying or requesting to interact with a non-existent host. ARPD [12] is a software that actually monitors the unused IP space and directs attacks to the Honeyd honeypot.

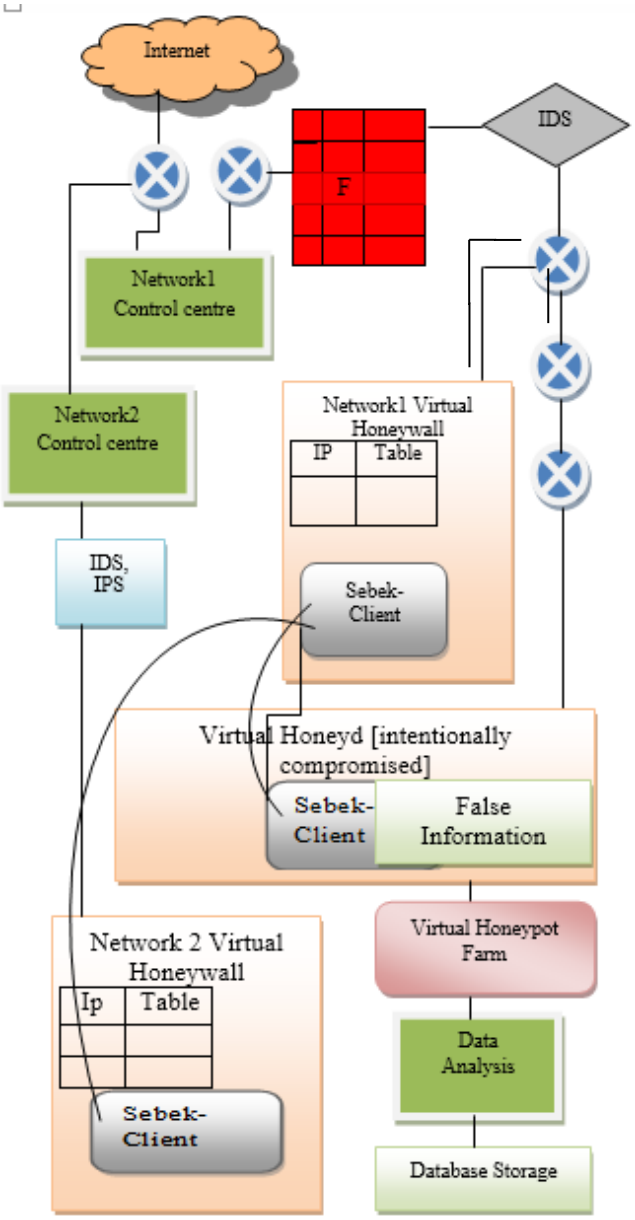

Fig. 1. Proposed approach

If ARPD sees any packets going to the unused IP, it spoofs the victim machine IP address with the MAC address of the machine which is hosting Honeyd. Snort [14] is used as an intrusion detection, it has real time alerting capability and generates an alarm of each incoming and outgoing packets. It uses a pattern matching technique to detect attacks. Some Snort rules were developed to restrict the incoming and outgoing data packets. If a malicious packet is found, then snort generates a real-time alarm and all the suspicious connections are forwarded through the security resources. Also by using three routers a good amount of time is taken by the attacker to find the link or the interface between the routers.

The general intention of the attacker is there should be some interface between the routers otherwise there is no reason to connect it without any reason. But in actuality, there is no interface. And virtual honeyd has the important information related to the machine which is not real. This machine is intentionally kept to be attacked so that the ways, techniques of attacks may be known during the attack and relevant proper security measures are taken. The Sebek client does the hidden communication and stores the information to the server such that the configured machine itself does not know about the communication. The MAC address of the Sebek is kept same as that of the Ethernet and UDP port is kept same as of the honeypot. The database is stored in the MYSQL database in Ubuntu environment 'Perl scripts', 'Cisco router', and 'Telnet' are used for some management related resources. The information gathered from the analysis with the help of different analysis tools used to extract the possible information about the attacker. Logs generated were stored on the server and analysis tools were used for analysing the logged activities.

IV. PERFORMANCE ANALYSIS

Since log analysis involves analysis and mining of malicious packets that came to the network. To study the malicious packets ethereal and tcpdump analysis was done using an ethereal packet sniffer. To perform statistical analysis of log files ACID (analysis console of intrusion databases) analysis helps in classifying different security-related alerts. After analysing the logged activities of the different honeypots and IDS, various information has been found which is described in table 2. The port which has been attempted the most and the port with maximum alerts is TCP port number 80. *GetRequest*, *GetNextRequest* and *SetRequest* messages are the signatures by which denial of service (DoS) takes the control of a system. These signatures indicate that the attacker tried to attack the hosts in a network and makes for the real users the services unavailable for a certain period. After the analysis, it was found attacker was more interested to attempt DoS attacks or web-based vulnerabilities. A large amount of proxy port scans, IIS access attempts were there, so that the real host must make the information unavailable for their requests. The attacker used Trojan signature to flood the host in a network by sending many UDP packets by the attempt of UDP flooding.

Table 1 shows the list of generated attacks and the number of attempts in each protocol. Maximum number of attempts were on Transmission Control Protocol (TCP) port, it also generated the maximum number of alerts. Different attack signatures were generated which are described in Table 2. Most of the attack attempt signatures were 'bad unknown' and the most attempted protocol was TCP/IP protocol and the least attempted protocol was Internet Control Message Protocol (ICMP). Honeyd gives destination unreachable message on ICMP attempt. However, there was no change in the number of users' attempts during the attack.

TABLE I. LIST OF ATTACK ACTIVITIES

Attack Activities			
Ports	***TCP/UDP***	***Attempts***	***Alerts***
80	tcp	1400	15
138	udp	800	1
161	tcp	2460	12
162	tcp	417	1
0	udp	285	4
1	tcp	245	2
177	udp	71	0
69	tcp	47	2

TABLE II. LIST OF ATTACKS WITH SIGNATURES

Attacks	***Alerts***	***Signatures***
Unclassified	1032	212
Bad-unknown	7331	5
Dos attack	73	6
Web application activity	3614	81

Next, the different honeypots according to the level of interaction to detect attacks are shown in Table 3.

TABLE III. HONEYPOTS INTERACTION LEVEL

Honeypots Interaction			
	Low-INTR	***Med-INTR***	***High-INTR***
Alerts	Med	Low	High
Direct Attack	High	Null	Med
Efficiency	Low	Low	High
Info in-depth	Low	Low	High

Where,

Info:-Information, INTR- Interaction, Med- medium, Avg.-average, IDS- intrusion detection system.

V. CONCLUSION

The objective of this research is to analyse the performance of different honeypots based intrusion detection systems and get the best possible data about the attack and relevant information. Here, we study and use different types of honeypots, intrusion detection systems and related analysis tools. When honeypots was implemented, log file was generated. By the help of the data gathered, it was found that most of the attacks were on protocols which are based on TCP/IP. HTTP port was one of the most vulnerable port. Another vulnerable port found was FTP port. It was also found that the number of vulnerabilities increased when this

port was opened. Also, there exists Proxy scan attempt, IIS attempt using the get command. To attempt a denial of service (DoS) attack on the host by sending large number of UDP packets, the attacker used Trojan which floods the UDP packets in a network. During the analysis phase, the number of ICMP attempts was the least. Analysis part has been tried in this, but technology can be used in further areas of defence.

VI. FUTURE WORK

Work can be done in different areas in this field to overcome the limitations. Honeypots can be worked with using Grid services. Honeypots can be worked with anti-spam technology to achieve real time detection and prevention system to minimize the attack and sources.

REFERENCES

[1]. Y. Yun, Y. Hongli, M. Jia, Design of distributed honeypot system based on intrusion tracking, in: 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011, pp. 196-198.

[2]. J.C. Chang, T. Yi-Lang, Design of virtual honeynet collaboration system in existing security research networks, in: 2010 International Symposium on Communications and Information Technologies (ISCIT), 2010, pp. 798-803.

[3]. L. Li, H. Sun, Z. Zhang, The Research and Design of Honeypot System Applied in the LAN Security, in, Beijing, 2011, pp. 360-363.

[4]. L.-j. Zhang, Honeypot-based defense system research and design, in: Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, 2009, pp. 466-470.

[5]. T. Holz, F. Raynal, Detecting honeypots and other suspicious environments, in: Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, 2005. IAW '05. , 2005, pp. 29-36.

[6]. T. Zhi-Hong, F. Bin-Xing, Y. Xiao-Chun, An architecture for intrusion detection using honey pot, in: Machine Learning and Cybernetics, 2003 International Conference on, 2003, pp. 2096-2100 Vol.2094.

[7]. I. Kuwatly, M. Sraj, Z. Al Masri, H. Artail, A dynamic honeypot design for intrusion detection, in: Pervasive Services, 2004. ICPS 2004. IEEE/ACS International Conference on, IEEE, 2004, pp. 95-104.

[8]. A. Herrero, U. Zurutuza, E. Corchado, A Neural-Visualization IDS for Honeynet Data, International Journal of Neural Systems, 22 (2012).

[9]. D. Puthal, S. Nepal, R. Ranjan, and J., Chen, "A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream." In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[10]. Y. Mai, R. Upadrashta, X. Su, J-Honeypot: A java-based network deception tool with monitoring and intrusion detection, in: P.K. Srimani, A. Abraham, M. Cannataro, J. Domingo-Ferrer, R. Hashemi (Eds.), Las Vegas, NV, 2004, pp. 804-808.

[11]. D. Puthal, S.Nepal, R. Ranjan, J,.Chen, "DPBSV-An Efficient and Secure Scheme for Big Sensing data Stream."In Tustcom/BigDataSE/ISPA,2015 IEEE(Vol. 1, pp.246-253).

[12]. R. Talabis. Honeypots 101: A Brief History of HoneyPots. The Philippine honeynet project, 2002.

[13]. R. Baumann. "Honeyd–A low involvement Honeypot in Action." Original published as part of the GCIA practical (2003): 14.

[14]. X. Li, D. Liu, Automatic scheme to construct Snort rules from honeypots data, Journal of Systems Engineering and Electronics, 16 (2005) 466-470.

[15]. H. Artail, H. Safa, M. Sraj, I. Kuwatly, Z. Al-Masri, A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks, Computers and Security, 25, 274-288, 2006.

[16]. D. Dagon, X. Qin, O. Gu, W. Lee, J. Grizzard, J. Levine, H. Owen, Honey stat: Local worm detection using honeypots, in, 2004, pp. 39-58.