A survey on the approaches in honeypot for implementing network security

Niharika Srivastava[1], Ved Prakash[2]
[1]Reaserch Scholar, Department of Computer Science
[2]Assistant Professor, Department of Computer Science
S.R.M.S College of Engineering and Technology
Bareilly, India
[1]niharikasrivastava17@gmail.com
[2]ved123@gmail.com

***Abstract*- Honeypot is a supplemented active defence system for network security. It traps attacks, records intrusion information about tools and activities of the hacking process, and prevents attacks outbound the compromised system. Integrated with other security solutions, honeypot can solve many traditional dilemmas. It has emerged as a prominent technology that helps learn new hacking techniques from attackers and intruders. Honeypots can initiatively lure hackers to attack the internet, take the record of the ways and means of their invasion, and then analyze and study them. This paper discusses the client and server honeypot approaches for the implementation of network security.**

Keywords- Honeypot; anti-virus; firewall; DMZ; intrusion.

I. INTRODUCTION

Broadband and the great variety of services offered over the Internet have contributed to the success of the World Wide Web. The Internet has become an important source for information, entertainment, and a major means of communication at home and at work. With connectivity to the Internet, however, come certain security threats. Unauthorized access, denial of service, or complete control of machines by malicious users are all examples of security threats encountered on the Internet. Since the Internet is a global network, an attack can be delivered remotely from any location in the world with great anonymity. Security professionals have responded to these threats and are offering a wide range of mitigation and prevention strategies. Machines connected to a network are usually equipped with at least an anti-virus software and a firewall. These measures are usually very successful in fending off a large number of attacks. But, today, since the attackers are barred by defences so they seek out unprotected paths to attack. One of these new major attack types that we are faced with today are client side attacks which led to the development of client honeypots in addition to the server honeypots. On the basis of underlying basic working criteria, honeypots are classified as server honeypots and client honeypots. They are described as under-

***A. Server Honeypots*-** A honeypot [1] is a dedicated security device whose value lies in being probed, attacked, and compromised. The term honeypot usually refers to a server honeypot, a dedicated server that exposes its services to a network and passively waits to be attacked. Therefore, server honeypots should have convincing deception technique to entice the adversary to initiate an attack. However, this set of circumstances ignores the fact that most malicious hacking currently occurs from client-side attacks, because attackers seek out soft targets to attack.

***B. Client Honeypots*-** A client honeypot is a honeypot that finds servers that attack clients. For example, a browser-based client honeypot retrieves web pages from web servers and determines whether the web pages contain malicious code that target vulnerabilities of the web browser. These types of honeypot help in protection from the client side attacks. These attacks target clients. As the client accesses a malicious server, the server delivers the attack to the client as part of the server's response to a client request. Common examples of these attacks are web servers that attack web browsers. As the web browser requests content from a web server, the server returns a malicious page that attacks the browser. If successful, the web server could, for example, install arbitrary programs on the client machine. Traditional defences, such as firewalls and the anti-virus software, are ineffective against these new threats.

II. AN EFFECTIVE SERVER HONEYPOT SYSTEM FOR LAN SECURITY

Firewall and intrusion detection [7][8], that play a very important role in LAN security system, have been widely used. Firewall and intrusion detection systems initially analyse the possible problems in the system, and then set the appropriate defensive strategy. They can discover the existing invasion, so, the systems deploying

honeypot come with a solution to this problem of detecting unknown invasions. In this particular system model [2], virtual honeypot and physical honeypot have been deployed in the LAN. In a LAN, the top priority is to protect the sever as it provides a variety of network services and saves users' information and the virtual honeypot is deployed to protect the server. By installing virtual computer software, a single physical computer has a zone that contains the virtual DMZ honeypot. For hackers, the vulnerable computer has considerable appeal to them, so in this system the physical honeypot should be deployed in a specific location to disguise a number of physical machines as vulnerable personal computers to lure hackers to attack, and then capture and record invasive methods and means.

Though attacks to the virtual honeypot can be identified by experienced hackers, but still once the invaders find they are attacking honeypot and the network has already set the trap, they will give up the attack on the server and escape quickly. But high-level hackers will not easily give up the attack, so in this system physical honeypot deployment is carried out in order to realize better camouflage to capture various attacks information. Several physical computers will be configured as PC's and many security vulnerabilities are left on the OS of the trap host and then it is closely monitored. The overall deployment of the system is shown in Figure 1.

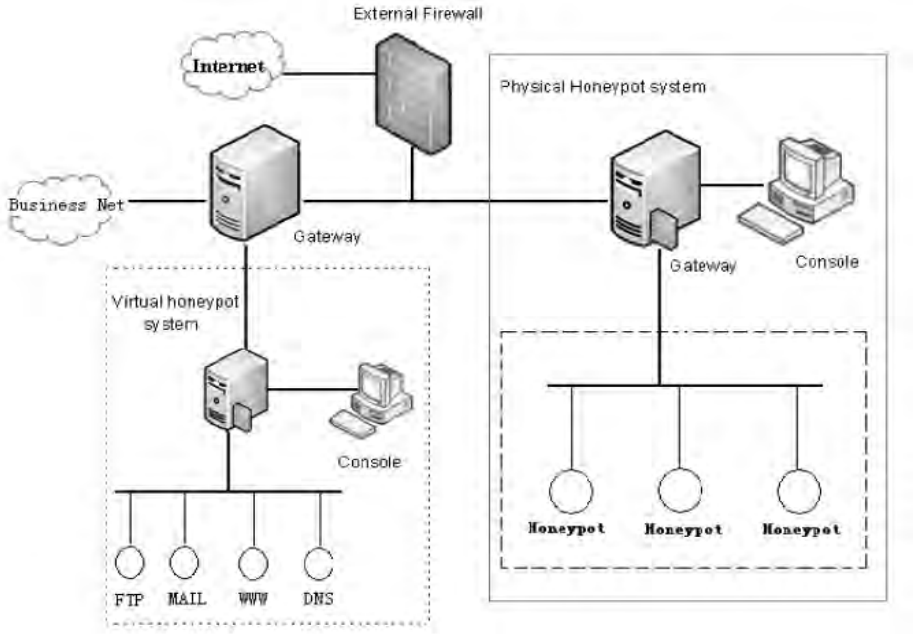

Figure 1. System Deployment Diagram

The system components and the working of the system proposed are discussed below:

A. System Components- The four prominent system components are Virtual Honeypot System, Physical Honeypot System, Gateway and Firewall. The Virtual Honeypot has three parts- DMZ zone, Virtual gateway and console. To protect the servers in DMZ zone, virtual computer software is installed on a single physical computer. Honeypot system is set up on virtual computer, and then similar structure like real DMZ zone is created in the virtual honeypot system. In order to confuse hackers, the appropriate network services are provided and when necessary, even some sensitive data are prepared. Furthermore, Sebek client software is also installed on virtual servers to record the invasion information.

In physical honeypot system, a number of physical computers are disguised as trap computers on which several vulnerabilities are left and some personal information is added to enhance authenticity in order to attract hackers. Sebek Client Software is installed on the honeypot host to capture the invasion information. The firewall is placed on the connection point between LAN and the Internet. It prevents the malicious packets from entering the LAN. The follow-up packets can be dynamically shunted to the honeypot system. Honeypot through the gateway can link the systems and business networks, and monitor data packets going in and out of several subnets, especially external connection initiated from the honeypot system.

B. Functioning of the model proposed- The external data packets are filtered by the firewall and then go through the filtering of IP tables in the gateway. If properly connected to service network, it will be shunted to

the business network else if connection is suspect, then it will be shunted to virtual honeypot system and other suspicious connections are diverted to the physical honeypot system. At the gateway of physical honeypot, suspicious packets arrive and then go into the honeypot after real time monitoring of IP tables and Snort. Sebek client silently records the invasion information.

The Database administrator uses console to make management, analysis and judgement on the database and further this analysis is utilized to update the invasion knowledge base. The outgoing connections should be strictly controlled for it means that the honeypot has been captured.

The operation of Virtual Honeypot system is similar to Physical Honeypot system. Since freedom and camouflage of virtual honeypot system and the latter captures more invasion information, the physical honeypot can be adopted to update knowledge database in virtual system.

III. A HYBRID CLIENT HONEYPOT

Client honeypots are faced with some challenges. First, they are faced with crawling the Internet with its millions of servers. Finding a malicious server might be similar to finding a needle in a haystack. Speed is a crucial aspect in order to identify malicious servers quickly and protect against them. Current client honeypot technology, which detects malicious servers by state change monitoring, is slow. Monitoring the entire state of the honeypot to detect a successful attack is an expensive operation, which requires time and consumes resources. According to the lead researches, Wang of Honeymonkey (a client honeypot developed at Microsoft Research), many websites install the first malicious file within 30 seconds. Faced with the quantities of servers on the Internet, duration of 30 seconds to classify a server as malicious makes comprehensive searches of the Internet infeasible.

Christian Seifert proposed a solution[4] which utilizes the strengths of both the technologies- the low-interaction client honeypot as well as the high- interaction client honeypot. It is expected that a hybrid client honeypot system is able to inspect servers with faster detection speed and an improved false positive/ negative rate over individual client honeypot technologies. A low interaction client honeypot, HoneyC, has been created which can detect malicious web servers via static detection algorithms. This implementation is expanded and evaluated with a group of web servers. Capture, a high interaction client honeypot, has been developed. Similar to HoneyC, it will be evaluated with a group of web servers. HoneyC and Capture have been combined into a hybrid client honeypot system.

The Hybrid Client Honeypot system [4] is targeted at increasing the performance of client honeypots through introduction of a lightweight client honeypot technology, a so-called *low* interaction client honeypots. These client honeypots will detect violation of a security policy by statically analyzing the server response directly. Pattern matching, heuristics and static analysis algorithms will be employed. This approach stands in contrast to already described state-based, so-called *high* interaction client honeypots that detect violations of a security policy via state changes of the underlying operating system that result from the server response.

High interaction client honeypots have a false positive rate of zero. Low interaction honeypots, on the other hand, tend to have a higher false positive rate because certain exploits attack code to cause a fault in an existing vulnerability, mimic benign code and therefore cannot b differentiated by static analysis algorithms. As a result, at times, this client honeypot falsely reports a benign response as malicious. *False negatives*, indicators of how many malicious responses are incorrectly classified as benign, seem to exist in both systems, but are expected to be complementary. A malicious response that is missed by one technology is likely to be correctly detected by the other technology.

Figure 2 shows the hybrid client honeypot. At the forefront stand a cluster of low interaction client honeypot nodes. They crawl the network at high speed. In order to increase detection accuracy, a certain percentage of responses are forwarded to the high interaction client honeypot nodes for an additional classification. The high interaction client honeypot node can confirm the classification of the low interaction client honeypot node, indicating that the server is indeed malicious, or it can reject the initial classification. In the latter case, the low interaction client honeypot node is likely to have raised a false alert. The static detection algorithm of the low interaction client honeypot is adjusted by using the classification of the high interaction client honeypot in the form of a feedback loop. This feedback loop should adjust the static detection algorithm of the low interaction client honeypot to increase detection accuracy.

The result of the hybrid client honeypot system is a client honeypot with a fast detection speed and improved false positive and negative rate over individual client honeypot technologies.

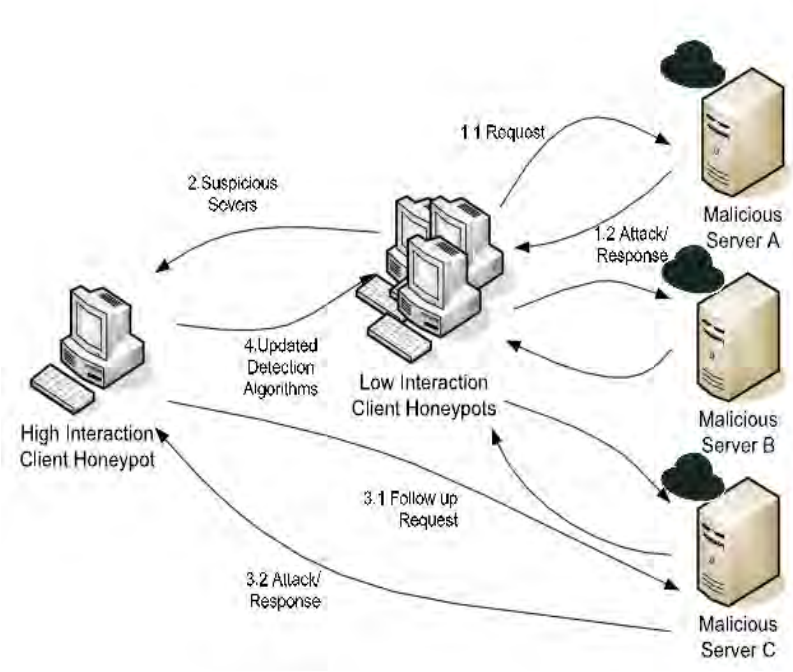

Figure 2. The Hybrid Client Honeypot

Several parameters, for example how many server responses are forwarded to the high interaction client honeypot, determine the speed and detection accuracy of the overall hybrid client honeypot system. The faster identification of malicious servers is expected to enable security researchers to devise additional defence mechanisms against malicious servers.

IV. CONCLUSIONS

The traditional defence [7] usually gives inadequate performance in face of the new invasion, therefore, the honeypot technology has been developed. Either of the honeypot technology- sever honeypots or the client honeypots may be deployed to gather the intrusion information in order to protect the systems in the network. The server honeypot technology discussed above effectively captures the invasion information through the deployment of physical and virtual honeypots in the LAN. When virtual honeypot system is used to protect the security of the server, suspicious connections visiting the server are shunted to the virtual honeypot which can not only reduce the risk of server attacks, but also save cost. By the intrusion detection and capture function of physical honeypot, attack information is recorded without the awareness of hackers. Through the research of their methods and tools, we understand their means and intentions, which make us, take the necessary and timely measures to protect the network system and enhance the security of local area network.

The hybrid client honeypot technology is helpful in detecting the client-side attacks. The low interaction honeypot, HoneyC and the high interaction honeypot, Capture together form the hybrid client honeypot system. Thus, the hybrid system can efficiently detect the malicious response and the malicious responses that are missed by one technology are likely to be detected by the other one. Although client honeypots have obtained a lot of focus in recent years, current client honeypots are still in the developing phase. They have various shortcomings related to their inability to detect various attacks, and easiness of evading them by malicious websites.

REFERENCES

[1] Feng Zhang, Shijie Zhou. Zhiguang Qin, Jinde Liu. Honeypot: a Supplemented Active Defense System for Network Security, 2003.
[2] Li Li, Hua Sun ,Zhenyu Zhang. The Research and Design of Honeypot System Applied in the LAN Security, 2011.
[3] Mahmoud T. Qassrawi, Hongli Zhang. Client Honeypots: Approaches and Challenges, 2010.
[4] Christian Seifert, Improving Detection Speed and Accuracy with Hybrid Client Honeypots, 2008.
[5] Ali Ikinci, Monkey-Spider: Detecting Malicious Web Sites, May 23, 2007.
[6] Niels Provos. A Virtual Honeypot Framework[EB/OL].http://www.citi.umich.edu/techreports/reports/citi-tr-03-l.pdf, October 21,2003.
[7] Karen Scarfone, Peter Mell. Guide to IntrusioDetection and Prevention Systems. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[8] Understanding Intrusion Detection Systems. http://www.sans.org/reading_room/whitepapers/detection/understanding-intrusion-detection-systems_337