International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-1, October 2015

Detection of Intrusion and Honey Net Architecture Approach to Defend in Virtual Network Systems

Lakshmi HV

Abstract— ***Security in cloud is one of the most important issues that drawn interest of research and development in past years. Hackers can explore vulnerabilities of cloud system and to deploy large-scale Distributed Denial-of-Service they compromise virtual machines. Distributed Denial-of-Service attacks involve early stage actions as multi-step exploitation, less frequency vulnerability scanning, and compromising insecure virtual machines, and Distributed Denial-of-Service attacks through the compromised VMs. In cloud system, the detection of zombie attacks is difficult. Because users may install insecure applications on their VMs to avoid insecure virtual machines from being compromised in the cloud, we propose a multi-phase distributed vulnerability finding, and Honey Net approach to fight back the attack. Honeypot is a data system resource and its value lies in unauthorized use of that resource of system. Honey nets are "a security resource whose value lies in being attacked". Honeypots and honey nets are used to collect data about threats that organizations might face and hence protect them.***

Index Terms—*Network Security, Honey Pot, Honey Net, Cloud Computing, Intrusion Detection*

I. INTRODUCTION

RECENT years users moving to cloud believe security as the essential factor. Cloud Security Alliance (CSA) survey accord that among all security problem, abuse and nefar- ious use of cloud computing is reasoned as the top security threat [1], where attackers can exploit fragility in clouds and make use of cloud system assets to arrange attacks. The challenge is to improve an effective attack detection and response system for properly identifying threats and reducing the effect of security problem to cloud users.

In [2] M. Armbrust et al. addressed that protecting "Business continuity and services availability" from service outages is one of the top concerns in cloud computing systems. That type of attacks is more active in cloud environment as cloud users commonly share out computing assets. In this article, we propose intrusion detection technique and honey pot architecture approach to overcome the attack to establish a defense-in depth intrusion detection framework. For better attack detection, this technique includes attack graph procedures to detect intrusion.Richard [l] stated that, with the most forward protection, computers are not cent percent secure. In fact, almost computer security genius agrees that, given user-desired features such as network connectivity, it'll never attain the goal of an absolutely secure system.

Manuscript published on 30 October 2015.
***** Correspondence Author (s)
Lakshmi HV, Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore, India.

Hence, we need to develop intrusion detection techniques and systems to determine and behave to computer attacks.

II. RELATED WORK

In this area, present literatures of several highly related research areas to intrusion detection, including: detection of zombie and prevention, attack graph creation and security analysis, and honey pot for attack countermeasures. The attack graph is able to illustrate a sequence of exploits, called atomic attacks that guide to an unwanted state. There are numerous automation tools to build attack graph. Intrusion Detection System (IDS) and firewall are extensively used to observe and find skeptical events in the network. Honeypots and honey nets have been aimed with gathering important information on computer attackers since their initiation. These devices, whether low or high interaction, have traditionally been deployed manually by a network administrator. A fixed number of devices with fixed characteristics (such as which ports are accessible or which services are started) must be manually configured and deployed. All the while the administrator's network is constantly changing as a result of the addition or removal of machines, updating or adding new operating systems and the addition of services. So for a majority of the time, the predetermined honey net might look nothing like the actual network environment in which they are deployed. The data gathered by this predetermined honey net might be interesting but the data does not accurately represent the administrator's network environment, and is therefore not representative of the types of attacks that the production devices are likely to encounter.

III. HONEY POT AND HONEY NET TECHNOLOGY

A. Description of Honey pot

Honey pot is nothing but resource; whose value is that it will carry out data exchange with the hacker. By itself Honey pot does not change any information; honey pot are just the administrator to give additional, more important information. Under normal circumstances, when the server is an intruder penetrated, the administrator will check while logging information, monitor the intruder changes made on the system, whether the system left the back door. Usually at this time the system logs the credibility of the data recorded is not high, a situation in which the administrator at this time is very passive. In order to be able to get the intruder's information that can be benefited by honey pots to fool the intruder, so that the intruder honey pot to record every move, the last full check attack source, master the attacker's every move, then attack with the corresponding defensive measures [5].

In fact, the honey pot is a cheating technique that makes an attacker to unknowingly transfer to the trap set by honey pot. Honey pot technology can advance the time of detection and response capabilities to efficiently collect evidence of criminal intruders and good tracking environment is provided. But with the wide range of benefits, the short comings of traditional honey pots began exposed, together with three main areas:

(1) Honey pot can only attack against the surveillance and analysis; the intrusion detection system cannot view through the bypass listening techniques to monitor the entire network.

(2) Protection of honey pot technology cannot be directly insecure information systems and may be exploited by attackers to bring some security risk.

(3) The activities of the attacker on the encrypted channel (IPSec, SSH, SSL, etc.) Increased data capture takes time to decipher after this increase in aggressive behavior to the analysis of the difficulties [6].

B. Honey net Introduction

In order to solve the above problems of the honey net technologies, Honey net technology is essentially a kind of high-interaction honey pot type technology, and traditional differences in honey pot technology is Honey net constitute a hacker trap network architecture, in this framework, can contain one or more honey pots while ensuring a high degree of controllability of the network, and offers a variety of tools to facilitate information collection and analysis of attack. One of the most critical components for the network gateway as Honey Wall of honey, including the three network interface card 1 access outside the network, LAN 2 connection honey net, and card 3 as a secret channel, to connect to a monitoring network [7] .Honey Wall is a working bridge in the link layer device, as the Honey net network, the only other connection point, all the inflow and outflow of the Honey net network traffic will be through Honey Wall, and subject to the control and audit, while not on network data decreasing TTL packets and network routing, and will not provide its own MAC address, so hackers run, Honey Wall is completely invisible, so hackers will not recognize it is the Honey net network attacks.

C. Honey Pot in the System

In this system, the use of Honeyd also because it's the defense can be effective for inhibiting DDoS attack sources, transfer attack flows and the role of information gathering attacks. Inhibition of attack source is configured Honeyd system to the DDoS attack; the honey pot can be adjusted in response to the attack source to achieve the slow attack speed, attack blocking proliferation, and even anti-attack purposes. The DDoS attacks, Honeyd ways to respond to the following points: the UDP-based attacks, Honeyd sends ICMP Source Quench messages, so the source host sends the speed slows down; for TCP attack, you can increase session delay, reduce the TCP windows, etc. to limit the attacker to send attack data; Honeyd can be strictly controlled from its own data packets sent to block attacks from the honey pot spread to other targets. According to the working mechanism of Honeyd, we are able to respond flexibly to control the invasion, to realize the invaders cheat, convince them that a successful invasion of the honey pot, while honey can be discarded by the attack packets sent; Through a specific script, take the initiative to eliminate the source of the attack. Generally attack hosts are being infected, or are specific procedures for implantation of the attacker, that is, the host of loopholes, we can use the same communication mechanisms, the appropriate preparation of an anti-virus script, on the contact honey pot host for virus infection clean up and patch and so on. Because Honeyd can simultaneously simulate multiple systems, then the honey pot deployment more efficient clean-up the higher the attack source. This defense is based on understanding of the mechanisms of the spread attack, defense was very obvious, but also the need for policy support. Transfer of attack traffic is Honeyd can be suspicious packets transferred from the actual target honey pot system, so that makes the target host from attack. DDoS is a large flow of data resource consumption attack target, honey pot to achieve its drainage function, we must have guarantees of their own defense, and to ensure its own will not be defeated. Honeyd is a low-interaction honey pot type, while the low-interaction honey pot type shown here on its merits: Honeyd system does not directly access the kernel but by a core set of interacting with the operating system kernel, so that all arriving packet is copied to the honey pot kernel set of procedures, the kernel is not the actual data packet processing, honey pot system programs will not only simulate the allocation of resources to respond to guarantee the security of the operating system itself. Meanwhile, Honeyd will record all incoming traffic, action, this information can be collected more attacks.

IV. INTRUSION DETECTION

A. Lack of Intrusion Detection Technology

Traditional intrusion detection systems work more like anti-virus software. It contains a database of known attack signatures. The system continuously network communications and information in the database for comparison. If the detected attack, intrusion detection system for the issue of attacks reported. Usually by detecting port access through the exchange of data packets, because it only is a passive method to measure the data traffic, so when the attack detection code to the data package, you cannot stop the attack traffic. In general, two methods commonly used to attack blocking, adding to the data stream packets, a session on the target server reset. However, current attacks but may arrive before the reset packets have all arrived at the destination server, so it is too late to respond to [8].

B. Snort Software Introduced

In 1998, Mr. C language developed with the open source Snort. Until today, Snort has evolved into a multi-platform, real-time traffic analysis, network features such as IP packet recorder powerful network intrusion detection / defense system, that is, NIDS / NIPS. Snort meet the General Public License, available online for free download Snort, and only a few minutes to install and start using it. Snort based on libpcap. Snort system components: snort composition of three major subsystems: the packet decoder, detection engine, and log and alarm system. Snort has three operating modes: sniffer, packet logger, network intrusion detection system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Sniffer mode simply reads the packets from the network and displayed as a continuous flow of the terminal. It's packet recording mode to record the data packets to the hard disk. Network intrusion detection mode is the most complex and is configurable. We can snort analysis of network data stream to match some user-defined rules and based on test results to take some action. In this paper, experiment with it as the core of an intrusion detection system.

C. DDoS Defense System Design

The starting point of this design is the use of a variety of ways and the honey pot firewall, intrusion detection systems, multi-faceted protection network security, defense DDoS attacks. The whole system is divided into a firewall, virtual honey pot system, intrusion detection systems, transponders, server farms and network honey pot system within six parts. The entire defense system work together to achieve chart:

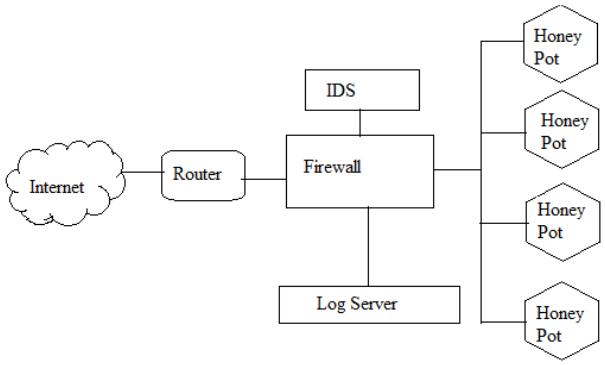

Figure 1 DDoS defense system logic model diagram

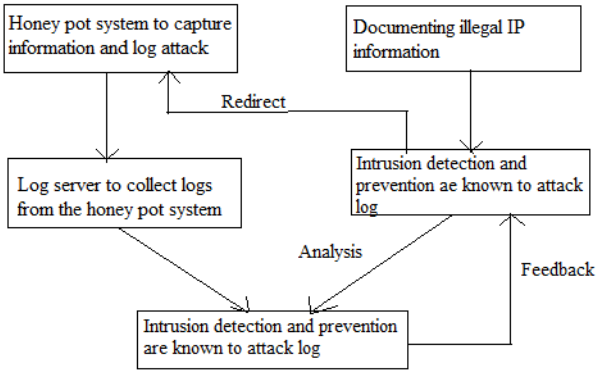

Figure 2 DDOS defense system logic model diagram

V. CONCLUSION

security of network is an important issue which cannot be ignored, it's complicated, difficult and far beyond our imagination. Distributed denial of service attack in the way of all hacker attacks has played an important role; everyone must make great efforts to study.

REFERENCES

1. Cloud Security Alliance, "Top threats to cloud computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010.
2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," ACM Commun., vol. 53, no. 4, pp. 2010.
3. R.Thomas, B. Mark, T. Johnson. NetBouncer: client-legitimacy- based high-performance DDoS filtering [J]. In Pro of DARPA information Survivability Conference and Exposition. Washington, DC, 2003:14-25.
4. T. Peng, C, Leckie, K. Ramamohanarao. Protection from distributed denial of service attacks using history-based IP filtering [J]. In Pro of IEEE International Conference on Communications (ICC03), Anchorage, Alaska, USA, 2003:482-486.
5. Zhu Ge Jianwei. Honeypot and honeynet technology description [J].Peking University Institute of Computer Technology, 2006.
6. Shi Weiqi, Chengjie Ren. Honeypot technologies and applications[J]. Computer Engineering and Design, 2008,29 (22) :5725-5728.
7. J. Mirkovic, G. Prier, P. Reiher. Source-end DDoS defense [J]. In Pro of IEEE International Symposium on Network Computing and Applications (NCA2003). Ca mbridge, Massachusette, 2003:171-178.1989.
8. Yang Shangsen, Hu Bei. Based on Intrusion Deception active honeypot technology system design [J]. Computer Applications and Software, 2008,25 (1) :259-260.

Lakshmi HV, Completed Bachelor's degree from PES Institute of Technology and Management. Masters in Computer Science and Engineering from MSR Institute of Technology.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)