International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:12, 2014

Parallel Hybrid Honeypot and IDS Architecture to Detect Network Attacks

Hafiz Gulfam Ahmad, Chuangdong Li, Zeeshan Ahmad

***Abstract*—**In this paper, we have proposed a parallel IDS and honeypot based approach to detect and analyze the unknown and known attack taxonomy for improving the IDS performance and protecting the network from intruders. The main theme of our approach is to record and analyze the intruder activities by using both the low and high interaction honeypots. Our architecture aims to achieve the required goals by combing signature based IDS, honeypots and generate the new signatures. The paper describes the basic component, design and implementation of this approach and also demonstrates the effectiveness of this approach to reduce the probability of network attacks.

***Keywords*—**Network security, Intrusion detection, Honeypot, Snort, Nmap.

I. Introduction

ALL sectors of society, whether government or private, progressively desires networks to be reliable and secure. In the current digital era of technology computer networks are vulnerable to a variety of activities. These weaknesses compromise their intended operations [1]. In spite many decades of research and knowledge, we are still incapable to make secure computer networks systems. To solve this problem, researcher sought out many solutions like firewall, VPN and intrusion detection system. As a result exploitation, automation and massive global scanning for vulnerabilities enable adversaries to compromise computer systems shortly after they become known. Intrusion detection is to identify, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators, preferably in real time achieve a unique importance [2]-[4]. One type of IDS is Signature or knowledge based technique which is commonly known as signature detection or misuse detection. This technique uses specifically known patterns of unauthorized behavior to forecast and detect subsequent similar attempts. These specific patterns are called signatures [5]. Misuse systems are capable of attaining high levels of accuracy in identifying even very subtle intrusions that are represented in their expert knowledge base. Here we introduce a well-known term “honeypot”, which is normally used to attract and trap something for its own means and use. In network security this technology is used to overcome the drawbacks of traditional intrusion detection system [6]. Honeypot monitors the system resources which are intended to be compromised, probed or attacked. By monitoring data, which enter and leave the honeypot, we can get the information that is not available on a network IDS. Due to nonproductive value any attempt to contact honeypot are considered suspicious. So the data gathered by honeypot is more important as compare to NIDS data because of false positive. In this discussion we will try to demonstrate the power of the honeyed framework with IDS. This approach of detection has several advantages over traditional methods, the most important of which is the fact that every time a honeypot generates an alert, it most likely is a real attack and not a false alarm. The rest of the paper is organized as follows. Section II describes the different types of IDS and honeynet. Section III includes proposed architecture and Section IV evaluates the performance of the framework.

Hafiz Gulfam Ahmad is with the College of Computer Sciences, Chongqing University, Chongqing, 400044 P.R. China (phone: 008618883875624 e-mail: gulfamahmad@uaf.edu.pk).

Chuandong Li is with the College of Electrical and Information Engineering, Southwest University, Chongqing (400044), P.R.China. (e-mail: li.chuandong@gmail.com).

Zeeshan Ahmad is with the School of Electronic & Optical Engineering, Nanjing University of Science & Technology, Nanjing , Jiangsu (210094), P.R. China (e-mail: engr.zeeshan@hotmail.com).

II. IDS Associated Research

A. Detection Techniques

The fundamental goal of intrusion detection is to identify intruders, preferably monitor the network traffic. Traditionally, researchers study intrusion detection tactics from two major understandings, anomaly detection and misuse detection but there is no considerable difference to their characteristics [7]. There are two sources of information host-based information source and Network-based information source. The host based IDS are the only way to gather information about the behavior of the users of a given machine. They are also susceptible to alterations in the case of a successful attack. This creates an important real-time constraint on host based intrusion-detection systems, which adopt the technique of audit trial and generate alarms before an attacker take over the machine control. The network based IDS examines the network protocol data. These data packets are compare with the realistic data to verify them.[8] Intrusion detection methodologies are classified as three major categories and their conceptual descriptions are as follows [9]. Signature based intrusion detection technique is used to describe a set of rules (or signatures) which can be used to decide whether a given pattern is an intruder or normal network traffic. This technique is extremely capable to attain high level of precision and minimal number of false positives.

B. Misuse Detection or Signature Detection

A small variation in known attacks may also affect the analysis and the results if a detection system is not properly

configured. The signature based detection technique flops to identify unknown attacks or distinction of known attacks. One of the inspiring reasons to adopt this technique is easy to maintain and update the rules [10]. These signatures are composed of several elements that identify the traffic. For host- based intrusion detection, one example of a signature is "three failed logins." For network intrusion detection, a signature can be as simple as a specific pattern that matches a portion of a network packet. For instance, packet content signatures and/or header content signatures can indicate unauthorized actions, such as improper FTP initiation. The occurrence of a signature might not signify an actual attempt of unauthorized access, but it is a good idea to take each alert seriously. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response, or notification should be sent to the proper authorities [11]. Fig. 1 describe the different types of the IDS and there source and behavior.

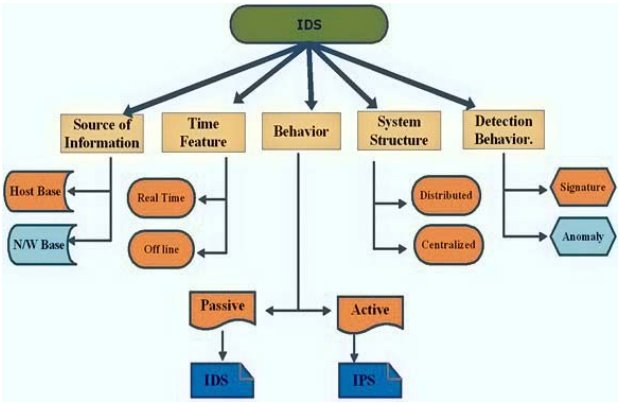

Fig. 1 IDS Types

C.Anomaly Detection (Behavior Base)

Anomaly base or behavioral base detection is related with identifying events that seems to be anomalous with respect to normal system behavior. A wide variety of approaches including data mining, statistical modeling and hidden Markov models have been discovered as different ways to approach the anomaly detection problem. Anomaly based detection is a deviation to a known behavior, and profiles represent the normal or expected behaviors derived from monitoring regular activities, network connections, hosts or users over a period of time. Profiles can be either static or dynamic, and developed for many attributes, e.g., failed login attempts, processor usage, the count of e-mails sent [11]. Anomaly based approach involves the collection of data relating to the behavior of authentic users over a period of time, and then apply statistical tests to the observed behavior, which determines whether that behavior is legitimate or not. It has the advantage of detecting attacks which have not been found previously. The key element for using this approach efficiently is to generate rules in such a way that it can lower the false alarm rate for unknown as well as known attacks [12].What is considered to be an anomaly can fluctuate, but normally, any incident that occurs on frequency greater than or less than two standard deviations from the statistical norm raises an eyebrow. An example can be code here if a user logs on and off of a machine 20 times a day instead of the normal 1 or 2. Also, if a computer is used at 2:00 AM when normally no one outside of business hours should have access, this should raise some suspicions. At another level, anomaly detection can investigate user patterns, such as profiling the programs executed daily. .

III. Honeypots

The general perception of Honeypots is to catch malicious activity in the network with an organized and prepared machine which is used as bait. The researchers are intended to improve network security with Honeypots. In the vast area of network security, to learn more about attack patterns and attacker behavior, the idea of electronic traps, is used with the name of honeypots i.e. network resources (computers, routers, switches, etc.) deployed to be probed, attacked, and compromised in this phenomenon. These electronic baits lure attackers and help in assessment of vulnerabilities. [13]. Honeypots can be utilized as a psychological weapons such as a trick to confuse, slow down, or stop attacks and we can detect and record unknown attacks in addition to known ones. Usually Honeypots are used in conjunction with Intrusion Detection Systems. In these cases Honeypots serve as Production Honeypots and only extend the IDS. But in the concept of Honeynets, the Honeypot is the major part of the security system.

A. Production and Research Honeypot

Production Honeypots typically works as extension to Intrusion Detection Systems and accomplish an advanced detection function. Production honeypots mainly emulate specific services and sometimes operating systems to invite attackers. They can also emulate different backdoors, viruses and trojans to lure the attackers. The value of production honeypots lies in all the three intrinsic security functions detection, prevention and reaction of an organization [14]. Production honeypots are designed in such a way that either there is no false positive or very few because all the activities on production honeypots is taken as illegitimate, hence all the logs are relevant, important and reveal some problem, attack or any attempt made for the same. They are also at par with the risk of false negatives, when IDS systems fail to detect a valid attack. But they can never replace any technology for detection because they can't be placed on production systems. However they are very useful to complement the available detection technology. Often after a system is compromised in a production environment the data gets polluted due to the continuous production work. So it cannot be used for further analyses making it difficult to even detect and preserve the evidences of the attack [15]. The ultimate challenge face by security community is the lack of information about enemy threats. Research honeypot provide a platform to study these threats tactics and techniques who, why and how a threat attack. Research honeypots can capture automated attack for analysis. However research honeypot can't reduce the risk but

the gain knowledge can be applied to improve the detection, prevention and the reaction process of any security mechanism.

B. Level of Interaction

Honeypots are generally allocated into three categories, low medium and high according to the level of interaction. Firstly, we discuss low interaction honeypots that emulates network services and collect the beginning of attack processes but they can't perform any action and just use only for detection and serve as production honeypot. At this level attacker gains only access to the emulated service.

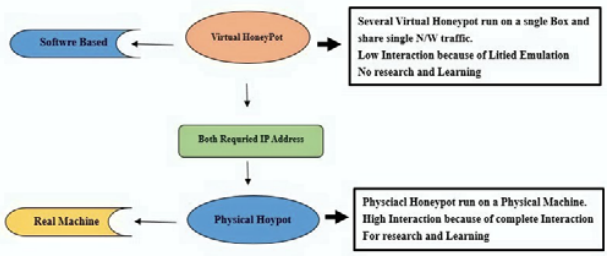

Fig. 2 Low and high level interaction

So it is an effective way for any security system with low risk. Medium interaction honeypots emulate full services and there basic purpose is to detect vulnerabilities. The emulated services at medium level honeypots are more powerful and chances of failure are higher which make it risky. High-interaction honeypots are the most elaborated Honeypots.

They either emulate a full operating system or use a real installation of an operating system with additional honeypot and try to break into it. We can classify the honeypots in term of physical and virtual. Physical is a real machine on network while virtual is a software but the common things is that both required IP address.

C. Honeypots Benefits

Either low- or high-interaction, honeypots are extremely powerful technology to be integrated in any overall security architecture. They are especially well suited to detect and record sources and types of known and unknown probes and attacks. Anyone having worked with network-based intrusion detection systems (NIDS), which are supposed to fulfill the mission of alerting on network attacks, knows that they face two main problems: false positives, alarms triggered by unimportant events mistaken as attacks, and false negatives, real attacks not being reported. Honeypots, on the other hand, excel on these two areas. For one thing, because honeypots serve no real production purpose other than being attacked, any interaction whatsoever with them is by definition illegitimate traffic that should be 9 For more information on these terms and on Honeynets in general, the reader is strongly encouraged to read the book .Know Your Enemy: Learning about Security Threats. Fig. 2 describes the low and high level difference.

IV. Proposed Design Framework

The objective of the parallel IDS based honeynet framework is to decrease the possibility of intruders attacking in a network and to effectively analyze the network attacks [17]. This feature enables it to detect the nature of attacks services, NIDS can identify certain attacks but not without the risk of compromising security. Only can provide the maximum information on an attack, without risk of compromise and also describes a system for automated generation of attack signatures for network intrusion detection systems. Unlike others, our approach is not relying only on signatures of known attacks, so it can detect old and new or 0 day threats, such as new worms, viruses and elite hackers. All TCP, UDP and ICMP traffic is monitored for all ports. The proposed honeypot architecture show honeyed server connected with a LAN switch. Fig. 3 also shows the two physical honeypots to receive the network traffic in and out of data captured and control. Fig. 3 shows the two physical honeypots interaction while the virtual Honeypot lie in the low interaction. The signature based IDS system also captures the incoming and outgoing traffic to detect the attacks by analyzing the traffic. The honeyed engine performs the following functions.

1. First interface run the Network scan tool to acquire the network information about operating systems, open ports and services.
2. To store this information in the Database and analyze the log data of the honeypot traffic by assuming those IP address which engage by intruders or attackers.
   The honeyed engine performs three functions. 1. Network scanning to collect the Network information about ports, Operating system and services. 2. Honeypot traffic log data.3. Storage in the data base.
3. Third function of the engine to create new signatures base on the analysis of log file generated by the scanning tool and honeypots. The number and type of virtual hosts for Honeyed to emulate is defined by the administrator in a configuration file. Honeyed is able to simulate not only some services running on the virtual systems but also the whole TCP/IP stack of those systems, so that they respond to OS fingerprinting.

A. Scanning

Scanning is a bulk target evaluation. To get information about machine is up and what ports Services are open. It focuses on most promising paths of entry. To avoid being detect, these tools can reduce frequency of packet sending and randomize the ports or IP addresses to be scan in the sequence. [16].

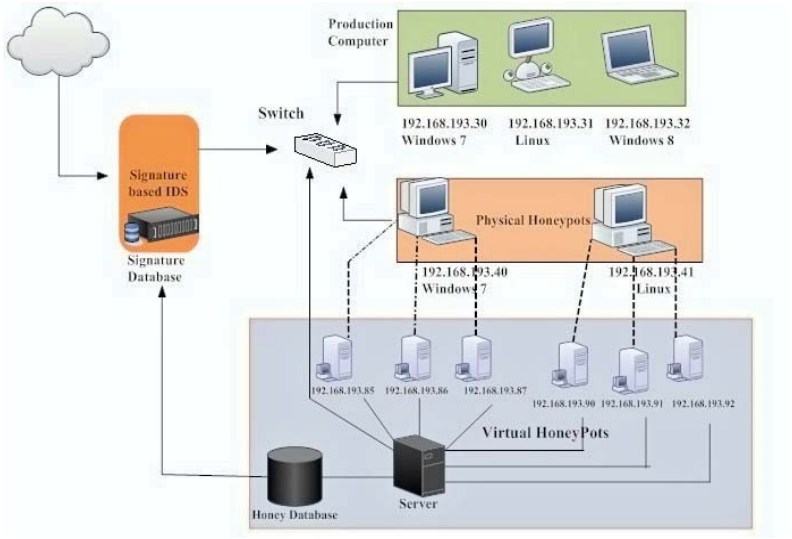

Fig. 3 Parallel Honeypot and IDS architecture

B. New Signature Creation

The Honeyed framework supports several ways of logging network activity. It can create connection logs that report attempted and completed connections for all protocols. Protocol Traffic analysis performs at network and transport layer. The new packet is outbound the process stop and signature engine compare the header in order to detect the IP address of network. Honeypot create the new empty signature and start inspection of packet. [18] Each signature record has unique identifier and stores the different properties about the current traffic which under investigation. As we perform the protocol analysis at IP, TCP and UDP packet headers. Then header comparison of each packet stored in the signature database. If any match with the IP identifier happened .The analysis signature match and become specific and recorded as a new signature. Built with the libpcap (packet capture library) interface, it collects information from packets on the network including those intended for other host machines. It does this through a network interface card's ability to enter into promiscuous mode. It then dumps packet header information in the log file.

V. Experimental Work

The parallel honeypot system was integrated into the network of the computer science Lab at the Chongqing University China (CQU), which comprises at least 40 computers. The parallel Honeypot server is installed on a 3.0 GHz Core i5 computer with 4 GB RAM. After initial scanning of the hardware on the network the server produce the information about the IP addresses and used operating systems. Fig. 4 describes the internal structure of honeyed engine and IDS system.

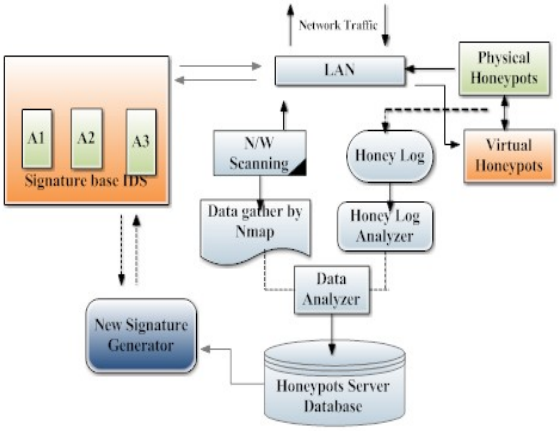

Fig. 4 Honeyed servers and IDS Parallel functional Diagram

For scanning we use the scanning tool Zenmap that is the official Nmap GUI scanner. It is a multi-platform (Linux, Windows, Mac S X, BSD, etc.) open source application which aims to make Nmap easy to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as log files to make them easy to run repeatedly. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

TABLE I
PORT ATTACKS AND HONEYED SIGNATURE

Port	Description	Attack	Signature Detect by Honeyed
TCP-3268	Microsoft Global Catalog part of Active Directory	186	No Service
TCP-22	Defined protocol to communicate	89	DDos attack
TCP-1024	Protocol to communicate	09	No Service
TCP-2968	SG Ports Services and Protocols official, unofficial information.	08	No Service
UDP-2179	VM Connect to Hyper-V hosts	10	No Service
UDP-389	Lightweight Directory Access Protocol	67	No Service
UDP-53	Domain Name System.	43	560 Payloads
TCP-1433	Ms SQL server	56	669 Brute Force
TCP-80	HTTP used by IIS	30	568 Payloads

To collect our honeyed data, we used two windows and Linux based honeypot computers on a sealed-off network that allowed all incoming connections, but severely limited outgoing connections to minimize damage by the attackers. The IP addresses of these honeypots were never publicized. To make the virtual honeypot we use VMware workstation 4.5.2 to emulate two virtual Honeypot machines. VMware Workstation is powerful desktop virtualization software for emulating virtual PCs. The software allows users to run multiple x86-based operating systems, including Windows, Linux, and NetWare, and their applications simultaneously on a single PC. The basic version allows the operation of four machines at the same time. Further those machines can be interconnected by one or more virtual networks. To capture the network intrusion we use Snort a parallel agent base intrusion detection system. To perform this task practically we use Snort. It is an Open Source IDS solution which we will use to capture all network activity, and generate alerts for known attacks. The two high interaction honeypot configured running windows 7 and Linux operating system. During the one week of experiment of different session, we discover the 465707 events and honeyed recorded total 26570 attacks. The ports UDP 389 and TCP 2976 show the low activity inside the network and TCP 80, TCP22, TCP 25 show high activity with a large volume of the traffic and targeted by many attackers. In Table I the overview of the attacks collected by Honeyed per port described. Fig. 5 show the different attacks detected by honeyed IDS.

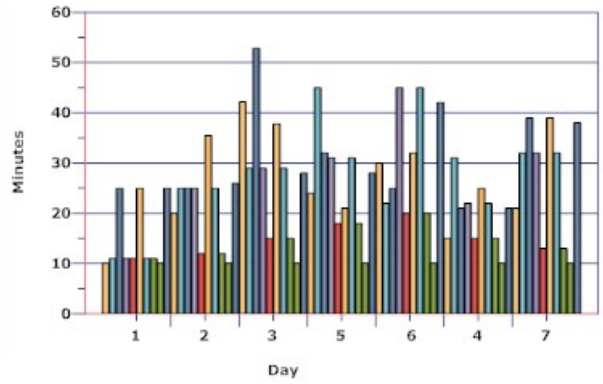

Fig. 5 Attacks detected by honeyed

VI. CONCLUSION

This paper serves as a reference to highlights a framework based on the honeypot and IDS. The architecture engages already developed techniques to enhance performance of the intrusion detection phenomena by implementing the fake system in network as the virtual honeypot. The attacker can't differentiate which one is fake and real system. The installation of the honeypot also help to update data base by generating new signatures .This enhancement play an active role in analyzing and detecting the unknown attack type of the intruder. In the future we want to automate the signature generation process by using the honey pot.

REFERENCES

[1] A.Valses, K, Skinner, "Probabilistic Alert Correlation", LNCS, vol. 2212, Recent Advances in Intrusion Detection, RAID 2001, Springer-Verlag.
[2] Mukherjee, B.; Heberlein, L.T.; Levitt, K.N., "Network intrusion detection," Network, IEEE , vol.8, no.3, pp.26,41, May-June 1994.
[3] R. Srivastava, V. Richhariya, "Survey of Current Network Intrusion Detection Techniques", Journal of Information Engineering and Applications, Vol.3, No.6, 2013
[4] The Symantec Internet Security Threat Report (ISTR) Volume 17 ,2011<http://www.symantec.com/about/news/resources/press_kits/detail .jsp?pkid=threat_report_17> le)," .
[5] Brown DJ, Suckow B, Wang T, "A Survey of Intrusion Detection Systems", Department of Computer Science, University of California, San Diego; 2002.
[6] Yeldi S., Gupta S., Ganacharya T., Doshi S., Bahirat D., Ingle R.,et-al." Enhancing network intrusion detection system with honeypot". Conference on Convergent Technologies for Asia-Pacific Region TENCON 2003; October 2003. p. 1521–6.
[7] Stavroulakis P, Stamp M. Handbook of information and communication security. New York: Springer-Verlag; 2010.
[8] TF Lunt, "A survey of intrusion detection techniques". Computers & Security, 12 (1993), pp. 405–418.
[9] StiawanD, Abdullah, AH, Idris, MY." The trends of intrusion prevention system network". In: Second international conference on education technology and computer (ICETC) 4; 2010: 217–21.
[10] Brown DJ, Suckow B, Wang T, A Survey of Intrusion Detection Systems. Department of Computer Science, University of California, San Diego; 2002.
[11] Chirag Modi a,n, DhirenPatel, "A survey of intrusion detection techniques in Cloud". Journal of Network and Computer Applications 36 (2013) 42–57.
[12] Hung-Jen Liaoa, , Chun-Hung Richard Lin, "Intrusion detection system: A comprehensive review". Elsevier Volume 36, Issue 1, January 2013, Pages 16–24
[13] Holz, Thorsten, and Frederic Raynal. "Detecting honeypots and other suspicious environments." Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005.
[14] Yin, Chunmei, et al. "Honeypot and scan detection in intrusion detection system." Electrical and Computer Engineering, 2004. Canadian Conference on. Vol. 2. IEEE, 2004
[15] Tian, Jun-Feng, et al. "A Study of Intrusion Signature Based on Honeypot." Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005. Sixth International Conference on. IEEE, 2005.
[16] Portokalidis, Georgios, and Herbert Bos. "SweetBait: Zero-hour worm detection and containment using low-and high-interaction honeypots." Computer Networks 51.5 (2007): 1256-1274.
[17] Umar, Hafiz Gulfam Ahmad, Chuangdong Li, and Zeeshan Ahmad. "Parallel Component Agent Architecture to Improve the Efficiency of Signature Based NIDS." Journal of Advances in Computer Networks 2.4 (2014).
[18] Newsome, James, Brad Karp, and Dawn Song. "Polygraph: Automatically generating signatures for polymorphic worms." Security and Privacy, 2005 IEEE Symposium on. IEEE, 2005.