Design and Analysis of Distributed Honeypot System

Ritu Tiwari
Graphic Era University
Dehradun, Utrakhand
India

Abhishek Jain
Graphic Era University
Dehradun, Uttrakhand
India

ABSTRACT

Honeypot technology has been widely used to overcome the limitations of firewall technology, many intrusion detection systems, intrusion prevention systems, which detected several attacks but couldnot detect new attacks. This paper discusses the honeypot technology according to the existed shortage in the honeypot system and proposes a distributed system which remedy the existing deficiency in the centralised control system to improve network security and presents the experimental results which successfully improves the performance of the safety defence systems.

General Terms

Security and protection.

Keywords

Firewall; Honeypots; Honeywall; Sebek-client; Snort IDS.

1. INTRODUCTION

With the ease of communicating with the world through Internet, came the threats that causes unexpected harm and damage to our security networks. To detect the blackhat society it is necesary to keep up-to-date with the hackers innovations. Various security defense systems were introduced for the improvement of network security but couldnot detect attacks inside an organisation network[1]. Also, inspite of the advances in technology, it doesnot recognizes the new attacks. To overcome with the problem honeypot technology was introduced and enhanced.

"Honeypots can be defined as the attractive defence resource placed inside a network that attracts the attackers towards it, with the actual intention to capture new attacks and learn the tools and techniques used by them" .

According to the level of interaction, honeypots can be catagorised into three types: (a) Low-Interaction honeypots, (b) Medium-Interaction honeypots and (c) High-Interaction honeypots [1]-[12]. Low-interaction honeypots can simulate TCP and UDP services. Also different types of network topology can be simulated. It detects some ICMP activity as well. Example: honeyd is a low-interaction honeypot. Medium-interaction honeypots allows limited interaction between the attacker and the system by sending the same request back to the sender. High-interaction honeypots offers a real-time system to the attacker and when the attack is in progress in-depth information can be gathered about the attacker like the tools and techniques used by them. Example: Honeynet is a high-interaction honeypot. To study the blackhats society and how they communicate with each other it is necessary to offer a real system to the attacker so that the attacker can gain root privilidges of the system and information can be gathered [12]-[24].

2. DRAWBACK OF THE EXISTING HONEYPOT SYSTEM

Honeypots has been focussed in research area in recent years against evading attacks. A centralized control, manages all the control center of the network. Agents can be virtual honeypot, Firewall, intrusion detection system. Control centre manages the different agents in a network [2]. It handles the messeges, and performs sample matching. Another function of control center is it generates the alarm, and identifies intrusion [1]. Also attack source can be find out by tracking techniques. Figure 2.1 below shows the existing centralized honeypot system [1].

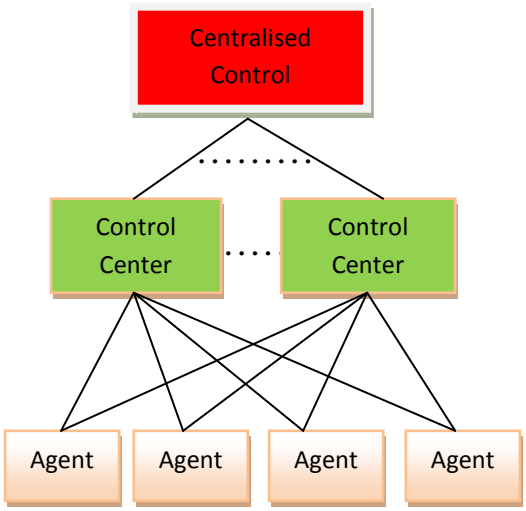

Fig 1: Existing centralised control system

But still there are few shortcomings in the existing system. A honeypot cannot protect a network which is not covered in its network range. It can detect attacks only which are directed towards it. A single honeypot residing in a particular network cannot protect its peered networks. Also, it doesnot automatically trace the information to the honeywall where all the information about the attack is maintained in the form of IP tables. Durability remains a problem.

3.1 Security Resource

3.1.1 Snort IDS

Snort is used as an intrusion detection system which captures the malicious traffic and if any unauthorized or suspicious

aonnection is attempted then snort generates a real-time alarm.

3.1.2 Virtual Honeyd

3. PROPOSED APPROACH

We propose a distributed honeypot system approach which is independent of the centralized control and information can be traced automatically about the source of attack. Even attack information of the other peered network can be gathered immediately by hidden communication. Even the honeypot residing in the same network doesnot know about this communication. This helps in providing better security, better durability, independent of the underlying honeypot network and the centralized control.

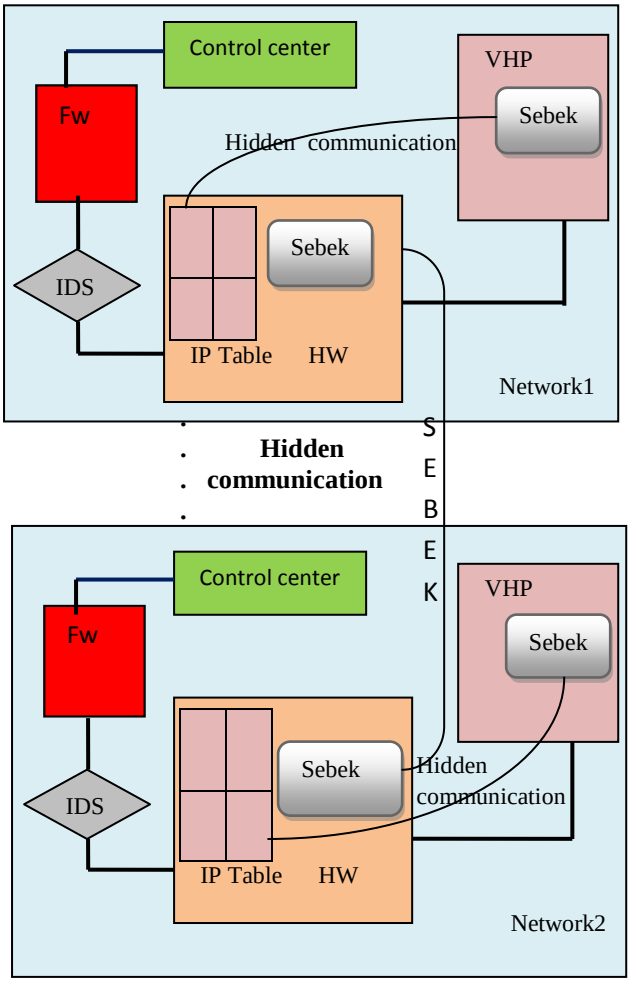

Figure 3.1: Proposed approach work architecture

Symbols used are: FW- firewall, IDS- intrusion detection system, VHP- virtual honeypot, HW- honeywall. Honeyd is a low-interaction honeypot designed to be attacked. It listens to certain ports and can simulate different and large number of network topologies.

3.1.3 Virtual Honeywall

Honeywall is a gateway for honeypots which uses IP table to collect the information gathered from the client sebek residing on the virtual honeypot. Every outgoing connections can be restricted or permitted by some snort rules according to the information gathered.

3.1.4 Sebek Client

Sebek operates on the Kernel of the honeypot in which it is installed. The UDP port should be the same on the honeypots and on the sebek server which has the honeywall so that the sebek communication can be hidden. Even the honeypot in which it is installed doesnot know about this communication.

3.1.5 Hihat

High-interaction honeypot analysis tool can be used to log all the events, keystrokes, fingerprints and much more about the attacker.

3.2 Security Resource

3.2.1 Database storage

The database is stored in the mysql storage center The database is stored in the mysql database storage center.

3.2.2 Data analysis

The informastion gathered uses ‘Perl scripts’, ‘ cisco router’, and ‘telnet’ for the management related resource.

3.3 Interaction Framework

The data collected is stored in the mysql database and is used for further analysis to extract information about the attacker. The work process of the interaction framework of the honeypot is described in the diagram shown in figure 3.3.1. The data collection and analysis structure is described with the help of the diagram shown in figure 3.3.1 .

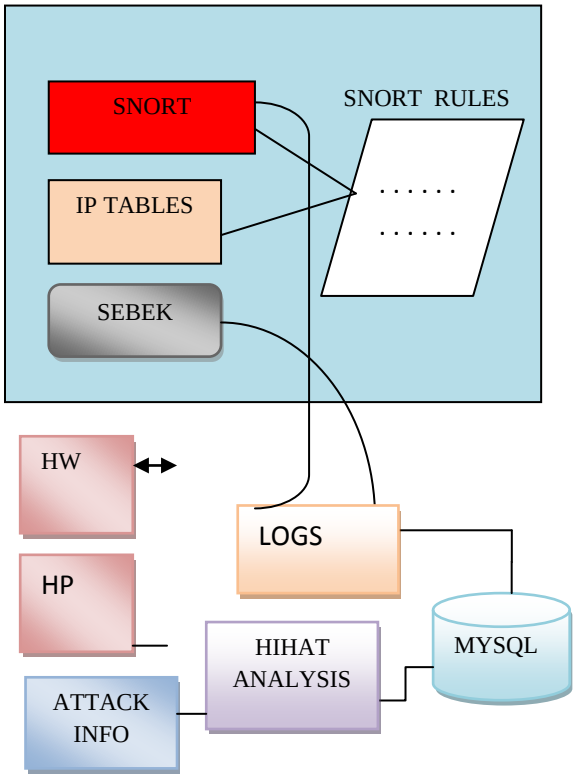

Figure 3.3: Interaction framework of honeypot

Attack information is automatically given to the honeywall by the help of sebek client within a network and the peered network information can be gathered by the help of the

communication between the honeypot server using sebek,using distributed system.

4. DISCUSSIONS AND RESULTS

After analysing the logged activities from virtual honeyd and tcpdump.log file by ethereal analysis usiing ethereal packet analysis tool and analyst notebook 6, sniffer, sawmill, HIHAT analysis tool, the information that has been found for 24 hours period which is described in table 4 below.

Table 4.1: List of attempts and alerts

PORT NO.	CONN	ATTEMPT	ALERTS
80	Tcp	1416	18
138	Udp	800	1
161	Tcp	1800	12
162sss	Tcp	517	2
3128	Udp	43	0
1	Tcp	345	3
177	Udp	74	0
69	Tcp	47	2

Denial of service attack take over the prevelidges of the host in a network by the GetRequest, GetNextRequest and SetRequest messages. This indicates that the attacker tried flooding the hosts and makes for the real users to deny the response or make the request unavailable. The number of port attempt and the number of unique alerts with occurences has been increased as compared to the previous results. Different catagories of attacks, generated signatures and alerts are in below table 4.2 below.

Table 1: List of attacks and signatures:

ATTACK	ALRT	SIG	NEW ALRT	NEW SIG
Unclassified	911	270	1032	212
Bad-unknown	4764	2	7331	5
Trojan	2	1	3	1
Dos attack	52	3	73	6
Web application activity	2357	63	3614	81

ALRT- alerts, SIG- signatures

From the analysed data, we get that the attackers were more interested to attempt DOS based attacks or web related vulnerabilities. There were high amount of proxy port scans and lot of web based attacks using IIS access attempts. This was mainly to attempt DOS attack on the host so that the real host must be made the information unavailable for thseir network requests. Attacker also used Trojan to flood the host in a network by sending many udp packets towards the host which is an attempt of udp flooding.

Table 2: Comparison analysis

	LOW NTR	HIGH-INTR	IDS	FIRE-WALL
Alert	Med.	High	Low	Med.
Directd Attack	High	High	Med	Med.
Emul eff.	Low	Avg.	Null	Null
Depth info	Low	High	Null	Low

Info- information, INTR- Interaction, Emul eff. Emulation efficiencsy, Med- medium, Avg.-average, IDS- intrusion detection system.

5. SUMMARY AND CONCLUSION

The objective of this research is to remedy the limitations of the existing honeypot architecture by a distributed honeypot system approach which is not limited within its network scope. The proposed approach shows better durability, efficiency for better network security. With the wide use of honeypot technology attackers always try to follow the track which is not a honeypot. Because now they know, they can be easily detected. Issues must be focussed in the future about how to secure our systems with the hackers new innovations from causing harm and damage to the network security.

6. FUTURE WORK

Work can be done in different areas in this field to overcome the above limitations. Many honeypot based IDS and different tools can be modeled to provide better efficiency. Combination different honeypots with few IDS can result in knowing much more about the attackers. Honeypots can be worked with using Grid services

7. REFERENCES

[1] Y. Yang, H. Yang, and J. Mi, Design of Distributed Honeypot System Based on Intrusion Tracking, IEEE. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference. Xi'an, China..

[2] L. Li, H. Sun, and Z. Zhang, The Research and Design of Honeypot System Applied in the LAN Security, IEEE. Software Engineering and Service Science (ICSESS), 2011 IEEE 2nd International Conference. Beijing, China.

[3] J. C. Chang & Y. Lang, Design of virtual honeynet collaboration in existing security research network,IEEE. Communications and Information Technologies (ISCIT), 2010 international symposium. Tokyo, Japan.

[4] H. Liu, D. Zhang, G. Wei, and J. Zhong, Detecting Malicious Rootkit Web Pages in High-interaction Client Honeypots, IEEE. Information Theory and Information Security (ICITIS), 2010 IEEE International Conference. Beijing, China.

[5] L. Zhang, Honeypot based Defense System Research and Design, IEEE, Computer Science and Information Technology (ICCSIT), 2009 2nd IEEE International Conference. Beijing, China.

[6] L. K. Yan, Virtual Honeynets Revisited, IEEE. Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC.

[7] M. Cukier, and S. Panjwani, A Comparison between Internal and External Malicious Traffic, IEEE. Software Reliability,2007. ISSRE '07. The 18th IEEE International Symposium. Trollhattan, Sweden.

[8] R. Baumman, Honeyd- a low involvement honeypot in action .2005. GCIA Practical.

[9] R. Chandran, and S. Pakala, Simulating networks with honeyd. 2006.

[10] M. T. Qassrawi, and H. Zhang, Client Honeypots-Approaches and challenges. New Trends in Information Science and Service Science (NISS), 2010 4th International Conference. Gyeongju, South Korea.

[11] M. M. Z. E. Mohammaed, and H. A. Chan, Polymorphic worm detection using double honeynet. Software Engineering Advances, 2009. ICSEA '09. 4th International Conference. Porto, Portugal.

[12] K-H. Yeung, D. Fung, and K-Y. Wong, "Tools to attacking layer 2 network infrastructure", 2008, Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol II, IMECS 2008, 19-21 March, 2008, Hong Kong

[13] J. Oberheide, and M. Karir. Honeyd detection via packet fragmentation.2010. *Networking Research and Development.* Merit Network Inc.

[14] D. Stirling, Enhancing Client Honeypots with Grid Services and Overflows, Master of Science Thesis, Victoria University of Wellington, 2010.

[15] Know Your Enemy: Learning about Security Threats, Addison Wesley 2nd ed., 2004.

[16] P. Wang, L. Wu, R. Cunningham, and C. C. Zou, Honeypot detection in advanced botnet attacks. *International Journal of Information and Computer Security (Vol 4, No.1/2010)*,2004. Inderscience Publishers.

[17] X. Fu, B. Graham, D. Cheng, R. Bettati, and W. Zhao, Comouflaging Virtual honeypots. 2005.

[18] Y. Yang, h. Yang, J. Mi, Design of distributed honeypot based on intrusion tracking , 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 196 – 198, 27-29 May 2011.

[19] E. E. Frederick, Testing a Low-Interaction Honeypot against Live Cyber Attackers, Amazon, 2011.

[20] J. Awad, and A. Derdmezis, Implementation of a high interaction honeynet testbed for educational and research purposes,2005. URL: http://www.aitdspace.gr/xmlui/handle/123456789/245 (4th March, 2012)

[21] The Honeynet Project: Know Your Enemy: Learning About Security Threats, 2nd ed. Boston: Addison-Wesley, 2004, The Honeynet Project & Research Alliance: Know Your Enemy:Honeywall CDROM .

[22] L. Spitzner, Honeypots Tracking Hackers, Addison-Wesley Professional, 2003.

[23] R. Russell, J. C. Foster, J. Posluns, and B. Caswell, Snort 2.0 intrusion Detection. 2004.

[24] Hayati, P. & Potdar, V., 2009. Toward Spam 2.0: An Evaluation of Web 2.0 Anti-Spam Methods. In 7th IEEE International Conference on Industrial Informatics. Cardiff, Wales.