HONEYPOTS andComparison of

Firewall, Intrusion Detection System and Honeypot

Hossein Akhavan Aski[1]

1*Hossein Akhavan Aski ,Computer software engineering graduate student ,Islamic Azad University ,Ayatollah Amoli*

Abstract

Computer networks allow communicating faster than any other facilities. These networks allow the user to access local and remote databases. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network and examining the threats and warningsthe administrator that have been attacked. And IDS provide a solution only for the large scale industries, but there is no solution for the small scale industries, so the model is proposed for honeypot to solve the problem of small scale industries which is the hybrid structure of Snort, Nmap, Xprobe2, and P0f. This model includes series of attackers and intrusion operations. The focus of this report is primarily on preventing the attacks including external and internal attackers and maintaining the log file by using honeypot of virtual machine [3].

Keywords: Intrusion detection system, Honeypots, Network attacker, Network security tools**.**

INTRODUCTION

In the era of information and technology, the main issue is network security in any organization. Honeypots are integrated in network with firewall andIntrusion detection systems to provide solid secure platformto an organization. Firewall provides the filtering andgenerates logs to further analyze any malicious activity orany violation policy of access control list, firewall rules . Different approaches like firewall demilitarized zone (DMZ)have been used but they are not effective for today'snetwork security. Intrusion detection systems thenintroduced to overcome the shortcomings of existingnetwork. Intrusion detection system silently monitor thenetwork's traffic and give the alerts to tell about any kind ofintruders based upon the database of signatures of existingintrusions. A number of issues were with IDS too as facingwith an increasing number of false negatives and falsepositives. Honeypots then introduced in the network toutilize the network's unused IPs and the attacker's behavioris analyzed on these honeypots. Honeypots improve IDStoo by decreasing

ISSN 2519-0814

the numbers of false positives[2]. The small scale industries using LAN have to keep high their own security level as the database, server and clients are all handled by themselves. Since threat from internal network is Always the big challenge for the administrators, so a solution is required for small scale network to secure their internal network. This report provides the solution for the same using honeypot.Honeypots are phony components set up to entice unauthorized users and malicious software (malware) by presenting numerous system vulnerabilities, while attempting to restrict unauthorized access to internal network information systems.

LEVEL OF INTERACTION OF HONEYPOTS

A. Low Interaction Honeypots

On the basis of interaction low interaction honeypots doesn't provide Operating system access to the intruder .It provides only services such as ftp ,http ,ssh etc. these low interaction honeypots plays the role of passive IDS where the network traffic is not modified. Some examples of low interaction honeypots are honeyd, specter, BOF. Honeyd is an opensource tool and the facility of service emulation on hoenyd is unrestricted whereas specter is not an open source tool and developed by Netsec. The well-known example of low interaction honeypot is Honeyd. Honeyd is a daemon and it is used to simulate the large network on a single host [1,4]. It provides a framework to create several virtual hosts using unused IP addresses of the network with help of ARP daemon, For instance, several virtual numbers of operating systems, server, switches, routers, can be configured on a single host. Furthermore, emulated services include FTP service listening on port 21 (Telnet), login to FTP server etc. Another low interaction honeypot is specter and kFsensor. Specter can monitor the total of 14 TCP ports. Out of these fourteen ports, seven ports are called traps and seven are called services. Traps act as listeners of ports i.e. when the attacker makes the connection with these ports the attempt is terminated and then logged. Services are more advanced wherever there is the interaction between attacker and emulating services.

B. Medium Interaction Honeypots

Like low interaction honeypots, these also do not provide OS access to the attacker but chances to be probed are more than low interaction honeypots.Some examples of medium interaction honeypots are Nepenthes, Dioneae, honeytrap, I collect.These honeypots also provide faced services to the attackers.Mwcollect and nepenthes can be used to collect the spreading malware.

C. High Interaction Honeypots

These are the most sophisticated honeypots.These are difficult to design and implementation.These honeypots are very time to consume to develop and have highest risks involved with this as they involve actual OS with them.In high Interaction Honeypots, nothing is simulated or

ISSN 2519-0814

restricted. Some example of High-interaction honeypots is Sebek, Argos. As these honeypots involve real operating system the level of risk is increased by many extents, but to capture a large amount of information by allowing an attacker to interact with the real operating system, it is a kind of trade-off. This helps in capturing and logging of attacker's behavior that can be analyzed in the later stage.

Fig1: shows About the Various factors Associated with different honeypots[2].

Various factors Associated with different honeypots			
	Low interaction honeypot	Mid Interaction honeypot	High Interaction honeypot
Degree of involvement	Low	Mid	High
Real operating system	-	-	X
Risk	Low	Mid	High
Information Gathering	Connection	Requests	All
Compromised wished	-	-	X
Knowledge to run	Low	Low	High
Knowledge to Develop	Low	High	High
Maintenance time	Low	Low	Very High

PURPOSE OF HONEYPOTS

A. Research Honeypots

Research honeypots are basically used to obtain information about the new ways of attacks, new attacks, viruses, worms which are not detected by IDS. These honeypots are used for research purpose. Mostly educational entities, military or government organizations, these kinds of honeypots are used to gather information about motives and new tactics about the black hat community. These honeypots never add direct value to the organization, difficult to maintain and deploy, complex in architecture, but provide extensive information which is worth to develop new policies to protect the organizational network. Research Honeypots are used to gain Information about black hat community. Its primary performanceis that to follow the footprints of the attacker and obtain new way for attacks and threats[16].

B. Production Honeypots

Production honeypots are easy to deploy, use and capture less information and are primarily used by companies or corporations. These honeypots are placed along with the production server inside the production network of the organization to improve overall security. A production honeypot is one which is used within the organization to prevent attacks and mitigate risks.It provides immediate security to production resources [5]. Production honeypot tends to duplicate the production network or provide some services such as Ftp, Http, SMTP to the attackers. Commercial organizations get more benefits from production honeypots. It addresses some challenges to IDS because of its simplicity.Sometimes the attack is too recent

ISSN 2519-0814

to the vendors in such situations IDS doesn't give any alert as it uses it is limited to the signature based database for detection of intruders. Sometimes IDS alarms are impaired too much on normal network traffic. This is called false positive claims. Honeypots address these challenges as all the traffic sent to honeypots is unauthorized that means there are no false positives no false negatives and large data sets to analyze.Fig 2: Represents honeypots based on their interaction level and based on purpose[2].

Fig 2: type of honeypots

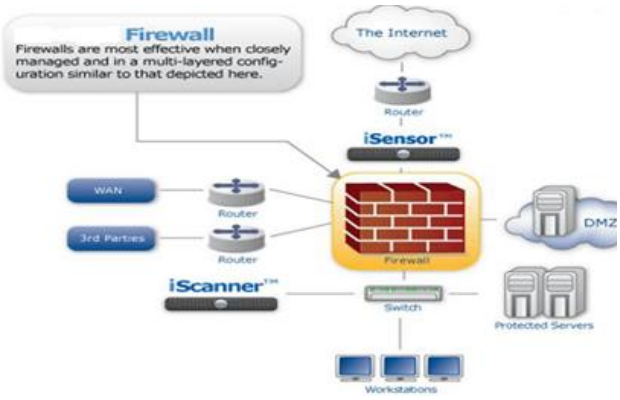
Sr. no	Honeypots	Types of Honeypots	Example
1	On the basis of interaction	1) low interaction honeypots	Honey, Kippo
		2) Medium interaction honeypots	Diona, Napenthes
		3) High interaction honeypots	specter
2	On the basis of purpose	1) Research honeypots	A standalone PC having any operating System installed like Linux.
		2) Production honeypots.	KF sensor, specter, Dionne, nepenthes

Comparison of Network Security tools- Firewall, Intrusion Detection System and Honeypot Currently available network security solutions

The ease of use and the connectivity the Internet provides is highly useful but the risks involved and malicious intrusions are also increasing day by day. Exploitation of computer networks is getting more common. It is completely critical for the business organization as well as individuals to protect their data from serious threats that would aim to steal their information. There are many security solutions available in the market. Some of them are like Firewall, Intrusion Detection System (IDS), Honeypot which is explained below[15].

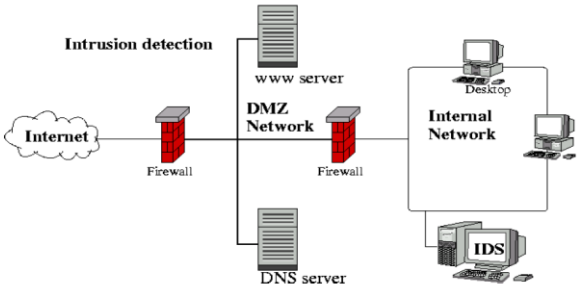
A. Firewall

ISSN 2519-0814



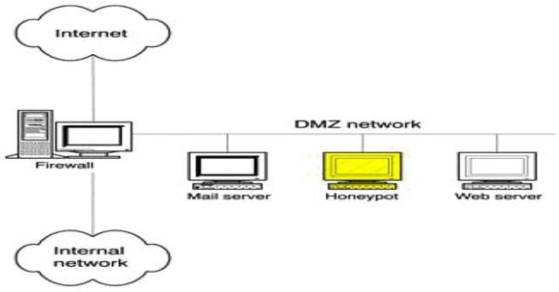
Pic 1: Firewall [6]

B. Intrusion Detection System (IDS)

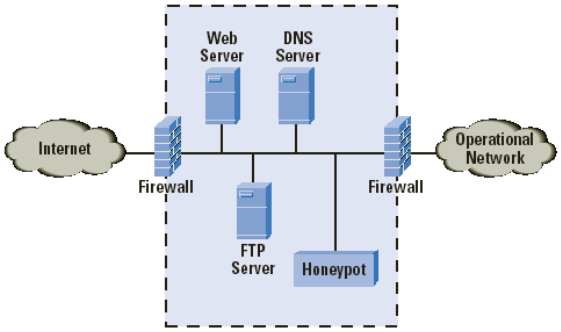


Pic 2: Intrusion Detection System [7]

C. Honeypot



Pic 3: Honeypot[8]



Pic 4: Honeypot

Honeypots compared with Firewall

A firewall is designed to keep the attackers out of the network whereas honeypots are designed to entice the hackers to attack the system. This is done so that a security researcher can know how hackers operate and can know which systems and ports the hackers are most interested in. Also, firewalls log activities and logs also contain events related to production systems. However in the case of Honeypot, the logs are only due to non-productive systems, these are the systems that no one should be

ISSN 2519-0814

interacting with. So a firewall log contains 1000 entries of all the systems of the network whereas the honeypots log only contains 5-10 entries[10].

Honeypots compared with IDS

IDS also suffer from high false positive rates. The value of a honeypot is determined by the information that can be obtained from it. Monitoring the data that enters and leaves a honeypot lets us gather information that is not available to IDS. To detect malicious behavior, IDS require signatures of known attacks and often fail to detect compromises that were unknown at the time it was deployed. On the other hand, honeypots can detect vulnerabilities that are not yet understood. Consequently, forensic analysis of data collected from honeypots is less likely to lead to false positives than data collected by IDS. An ID is used as an alternative for building a shield around the network[12]. The shielding approach is deficient in several ways, including failure to prevent attacks from insiders. IDS often depend upon signature matching or statistical models to identify attacks. This means that unknown or novel threats may not be detected. In contrast, honeypots are designed to capture all known and unknown attacks directed against them. Because any network activity that represents an anomaly, even the secret activity is recorded in a Honeypot[15].

CONCLUSION

A honeypot is not a security solution for the network but it is a complementary tool for other security technologies to form an alternative active defense system for network security. Working with IDS, firewall, and Honeypot provides new way to attacks prevention, detection, and reaction. A honeypot can serve as a good deception tool for prevention of product system because of its ability of trapping attacker to a decoy system. Supplemented with IDS, honeypot reduces false positives and false negatives. Intelligence routing control provides the flexible response to attacks. Different kinds of honeypot share the common technologies of data control and data capture. Experts focus the two to make honeypot easier to deploy and more difficult to detect. From the advances in research and production honeypot now days, I predict the future honeypot has the features of integration, virtualization, and distribution. Integrated honeypot encapsulates all the components in a single device. Virtual honeypot creates the large number of honeypot systems in one machine. Distributed honeypot comprises different honeypot system in an actual network to offer high interaction between attacks and system. All of these cases create

ISSN 2519-0814

the way to make honeypot cheaper in future and perform the functions.

REFERENCES

[1] Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).

[2] NavneetKambow, Lavleen Kaur Passi , " Honeypots: The Need of Network Security " in NavneetKambow et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101

[3] A. Sharma , " HONEYPOTS IN NETWORK SECURITY" in International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 1, Issue 5 (Nov-Dec 2013), PP. 07-12

[4] Provos, Honeypot Background. http://www.honeyd.org/background.php.

[5] Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 2004.

[6] S. Nassar, A.E. Sayed, N. Aiad, "Improve the Network Performance By using Parallel Firewalls," in Proc. of 6th International Conference on Networked Computing, May 2010, pp. 1-5.

[7] HarekHaugerud, "Intrusion detection and firewallsecurity,"Available: http://www.iu.hio.no/teaching/materials/MS004A/html/pictures/ids.png.

[8] Levin, J. and Labella, R., "The Use of Honeynets to Detect Exploited Systems across Large Enterprise Networks", IEEE Proceedings, pp.92-99, 18 June 2003.

[9] Gurleen Singh., Sakshi Sharma, Prabhdeep Singh "Design and develop a Honeypot for small scale organization "in IJITEE. Vol 2, issue-3, Feb2013.

[10] DenizAkkaya – Fabien Thalgott, "Network Security Using Honeypot" IEEE, June 2010.

[11] Y.K.Jain, S. Singh "Honeypot based Secure Network System" in IJCSE. Vol 3.No.2 Feb 2011.

[12] ErwanLemonnier, Defcom, "Protocol Anomaly Detection in Network-based IDSs", http://erwan.lemonnier.free.fr/.

[13] C K Shyamala, N Harini, Dr T R Padomanabhan – Cryptography and Security, May 2011.

[14] D. Rozenblum, "Understanding Intrusion Detection System," www.sans.org/reading_room/whitepapers/detection/understanding-intrusiondetection-systems_337, October 31, 2003.

[15] SonaliGhodke , PoojaPemare, KrittikaGoswami "An Overview of Network Security Tools- Firewall, Intrusion Detection System and Honeypot" International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE)Volume 2, Special Issue , Vivruti 2016.

[16] NavneetKambow et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101

ISSN 2519-0814

ISSN 2519-0814