A Review on Honeypots

Manikandan K[1], Shambhavi Rai[2]

[1]Associate Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
[2]Student, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Abstract - As the number of devices linked to a network is increasing day by day we need to ensure some proper security measures. Honeypots are specially designed networks that mimic the target network and attract the hacker, meanwhile all the activities of the hacker are closely monitored and as soon as any abnormal activity is detected the system is either warned about it or the information of the hacker is stored for future references. In this paper we discuss about the recent trends and advances in honeypots and review three open source and easily available research honeypots and perform a performance analysis based on various parameters.

Key Words: Honeypots, Firewall, Internet Of Things(IoT), Malware, HoneyBOT, KF Sensors, Valhala Honeypot, Zenmap

1. INTRODUCTION

Network Security has become really important as all of our devices nowadays are connected to a network in one form or the other. Various technologies like Firewall, Intrusion Detection systems, Anti-Viruses are used to prevent any unwanted and abnormal activities on our devices and to prevent the loss and misuse of our own data. Honeypots is one such technology that can be used to provide additional security to our device and data. It can either prevent the attacks or help us gain information about the intruders by constantly monitoring their activities. Various honeypots existing these days include the followings.

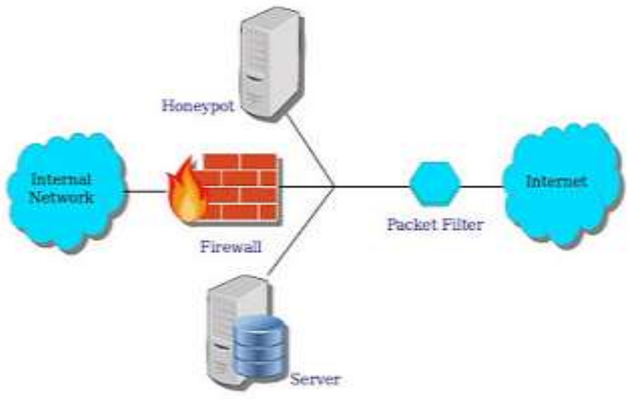

Fig -1: A Simple Honeypot

1.1 Deception Technology

It is an advanced version of honeypot that can help with network security by considering the hacker's perception and technique of exploring, exploiting and stealing the data. It is being widely used nowadays with Internet of Things (IoT) devices, Medical devices and other Embedded Operating Systems.

1.2 Malware Honeypots

In these kind of honeypots existing knowledge about the attackers are used to further prevent any attack on the network. Malware is detected based on previous knowledge about the activity pattern of hackers. Nowadays this technology is widely used in the security of cryptocurrencies theft.

1.3 Spam Versions

Plenty of vulnerable resources are available of internet for example open servers that allows mail from anywhere on the internet and forward it to it's destination. Spammers often abuse this system and in this case honeypots prove be an effective countermeasure. IP address and other information about the spammer can be revealed and thus can be used to prevent the abuse of these open mail relays and proxies.

1.4 Email Trap

Also known as spam traps these kind of systems are specially designed to receive spam mails from the spammer and then the information gained in the process can be used for backtracking the spammer. Project Hoyepot is one such technology that embed honeypot pages in between the webpages of a website and can further be used in the backtracking process.

1.5 Database Honeypots

Theft and loss of data is one of the most crucial threat to the databases and to avoid this one dummy database is created and whenever someone attempt to steal or modify or delete data using SQL injections information about them is recorded in the system and can be further used to prevent such kind of attacks on the main databases.

2. LITERATURE REVIEW

Detect, deflect and counter, these are the three basic functionalities of a honeypot. It can be used alone or with the combination of Intrusion Detection system and Intrusion Prevention System [1]. Various factors that can be used to determine the characteristics of a honeypot are level of interaction, deployment environment, resource type, services, adaptability and implementation [2]. With more and more research and development in this field various new techniques like CAPTCHA, Intrusion Detection Systems and Honeypots are now combined to develop security systems for the network [3]. Based on their role these honeypots can be divided into research and production honeypots each one of them providing security to the system by attracting hacker but in a slightly different way [4]. Auto responsive honeypots has also been developed which can be very useful in prevention of denial of service attacks [5]. With the introduction of honeypots in 1990, a lot of development have been done till 2020. Be it in commercial department or research department, honeypots have emerged as a trending technology [6]. A lot of honeypots were available for kali linux operating system and a few for windows initially, breakthrough came when Java was used to implement user friendly and easily accessible honeypots in windows as well [7]. With more research honeypots started taking new forms and shape for example introduction of game theory in honeypots to manipulate the hacker increased the efficiency of honeypot manifolds [8]. Honeypots can be placed with firewall either behind it or in front of it, or it can be combined with De militarized zone [9]. Other than that various network log manager tools like wireshark can also be combined to produce effective results using honeypots [10].

3. CLASSIFICATION

A honeypot can be classified based on three categories namely, interaction level, deployment modes, deployment categories. These categories are further elaborated in detail in the following subsections.

3.1 Interaction level

Based on interaction level the honeypots can be classified into three categories namely, high interaction honeypots, medium interaction honeypots and low interaction honeypots.

A high level interaction honeypot mimics the target network and provide access to all the resources and other data. In this category of honeypots the information gain about the hacker is very high however the risk involved in the process are significantly high as well since the attacker has complete access to all the resources.

A medium level interaction honeypot mimics the target network and provide access to a few resources and other data. In this category of honeypots the information gain about the hacker is medium and the risk involved in the process is less as compared to high level honeypot since the attacker has access to only a few of the resources.

A low level interaction honeypot mimics the target network and provide access to a very limited number of resources and other data. In this category of honeypots the information gain about the hacker is comparatively low however the risk involved in the process are low as well since the attacker has access to a very limited number of resources.

3.2 Deployment categories

Based on deployment categories the honeypots can be classified into two categories namely, production honeypots and research honeypots.

Production honeypots are employed by an organization where there is an active threat to the resources of the organization. Their purpose is to detect and prevent threats.

Research honeypots on the other hand are used by the network security companies to gain useful information about the hacker by monitoring and recording their activities.

3.3 Deployment modes

Based on Deployment modes the honeypots can be classified into three categories namely, deception mode, intimidation mode and reconnaissance mode.

In deception mode, as the name suggests the attacker is deceived by a mimic network that looks completely like the real time network. The attacker feels that the response it is getting is by the real time network, the purpose is to make sure that the hacker uses every hacking tool he has so that maximum amount of information can be gained about him. This is also an example of high level interaction honeypot.

In intimidation mode, the attacker is warned about the measures taken in case the system detects any abnormal activity. A warning is issued that the activities of the attacker are being monitored and this scares away a few of the attackers, and the others that are still left are monitored and their information is stored for future reference.

In reconnaissance mode, the tools are the techniques used by the hacker are recorded and this information id further used to develop intrusion detection systems. Both the internal as well as external attacks are monitored.

4. EXISTING OPEN SOURCE HONEYPOTS

Various open source and free honeypots are available on internet for our use like HoneyBOT, KF Sensors, Valhala Honeypot. These three honeypots were studied and analyzed by attacking the network using ZenMap which is a software that access the open ports of the system and thus giving honeypots an image of attack. Response time and other information were monitored and recorded by these systems. A trade-off is done based on the study of these systems and experimental observations.

4.1 HoneyBOT

HoneyBot is a medium level honeypot that simulate a number of protocols like echo, radmin, smtp, dcom, telnet, socks, http, ident, pop3 etc. There is an option of adding and deleting normal and abnormal activities. An alert is generated in case of any malicious activity.

4.2 KF Sensors

It is typical commercially used honeypot which is designed in a way to attract the attackers. It simulates vulnerable trojans and system services. It is already configured to track all the UDP and TCP ports. It can be customized by the user after the installation.

4.3 Valhala Honeypot

Compared to HoneyBot and KF Sensors this honeypot covers a lesser domain and can be used to monitor a limited number of ports including ftp, telnet, echo, smtp, pop3 etc. Security settings of these ports and protocols can be modified and customized to a limited extend.

5. TRADE OFF BETWEEN EXISTING HONEYPOTS

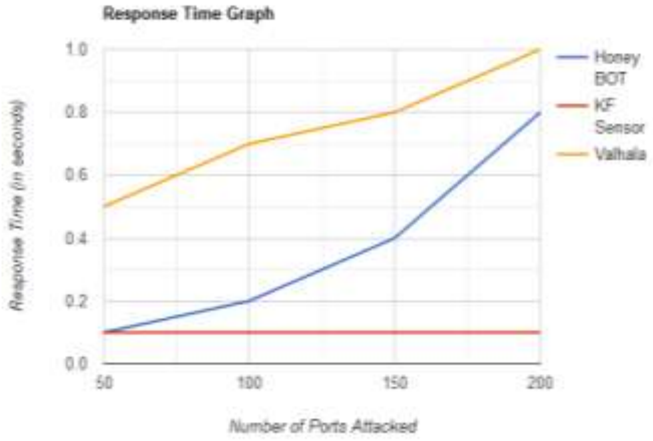

Chart -1: Response Time Graph

Table -1: Comparative study between existing system

	HoneyBOT	KF Sensors	Valhala Honeypot
Level of Interaction	Medium	Medium	Low
Deployment Mode	Deception	Intimidation	Intimidation
Deployment Category	Production	Production	Research
Complexity	Medium	High	Low
Cost	Free	Free	Free
Adaptability	High	Medium	Low
Portability	Medium	Medium	Low
Detection	Yes	Yes	Yes
Prevention	Yes	Yes	No

6. CONCLUSION

Honeypots are a good security measure for small scale industries and a good research tool for large scale industries. Combined with firewall and intrusion detection systems it can act as a security system that is very difficult to penetrate. Focus should be done on making these honeypots more simple and easy to deploy so that even people with minimum knowledge can access and use it similar to Anti-virus. However attackers keep on brushing up their skills and are persistent and thus constant research and development needs to be done in this domain to keep up with the hackers and keep the devices, servers, databases safe.

REFERENCES

[1] Rajbhar, Vivekanand. "INTRUSION DETECTION& PREVENTION USING HONEYPOT." International Journal of Advanced Research in Computer Science 9.4 (2018).

[2] Fraunholz, Daniel, Marc Zimmermann, and Hans D. Schotten. "An adaptive honeypot configuration, deployment and maintenance strategy." 2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE, 2017.

[3] Abdullahi, Mukhtar Ahmad, S. Aliyu, and S. B. Junaidu. "AN ENHANCED INTRUSION DETECTION SYSTEM USING HONEYPOT AND CAPTCHA TECHNIQUES." FUDMA JOURNAL OF SCIENCES-ISSN: 2616-1370 3.3 (2019): 202-209.

[4] Toor, Jashanpreet Singh, and Er Abhinav Bhandari. "DEPLOYMENT OF LOW INTERACTION HONEYPOT IN A PRIVATE NETWORK." International Journal of Advanced Research in Computer Science 8.7 (2017).

[5] Sekar, K. R., et al. "Dynamic Honeypot Configuration for Intrusion Detection." 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2018.

[6] Campbell, Ronald M., Keshnee Padayachee, and Themba Masombuka. "A survey of honeypot research: Trends and opportunities." 2015 10th international conference for internet technology and secured transactions (ICITST). IEEE, 2015.

[7] Kakade, Nilesh, et al. "JAVA Based Honeypot: Intrusion Detection System." (2018).

[8] La, Quang Duy, et al. "Deceptive attack and defense game in honeypot-enabled networks for the internet of things." IEEE Internet of Things Journal 3.6 (2016): 1025-1035.

[9] Kevat, Satish Mahendra. "Review on Honeypot Security." International Research Journal of Engineering and Technology (IRJET) 4.06 (2017): 1200-1203.

[10] Kumar, Dinesh, and Akshay Girdhar. "Network monitoring & analysis along with comparative study of honeypots." 2017 International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2017.