EXCELLENT PUBLISHERS

International Journal of Current Research and Academic Review

ISSN: 2347-3215 Volume 2 Number 4 (April-2014) pp. 65-70

www.ijcrar.com

Advanced Honeypot System for Analysing Network Security

Suruchi Narote[1*] and Sandeep Khanna[2]

[1]Department of Computer Engineering.
[2]PADM. Dr. V. B. Kolte College of Engineering, Malkapur, India

*Corresponding author

KEYWORDS

Honeypot, Information Security, Honey token and Attacks

ABSTRACT

Honey pot is an exciting new technology with enormous potential for the security community. It is a resource which is intended to be attacked and compromised to gain more information about the attacker and his attack techniques. They are a highly flexible tool that comes in many shapes and sizes. This paper deals with understanding what a honey pot actually is, and how it works. There are different varieties of honey pots and based on their category they have different applications. This paper gives an insight into the use of honey pots in productive as well as educative environments. This paper also discusses the advantages and disadvantages of honey pots.

Introduction

As the number of people using internet increasing day by day i.e. traffic on internet increasing faster, so security is a major concern in computing system. Honeypot is a system developed for analyzing and detecting malicious attacks attempting to get access to the network. Honeypot is a decoy machine which looks like a real server, real database and real operating system to the attackers. Honeypot attracts the attackers towards itself, attackers thought that there is some vulnerable weakness at your system which may be used to break and get access to your system. The main aim of honey pot system is to hide its existence from the attackers, honey pot examines the activity of the attacker and create logs for their activity and try to get as more information as possible by asking some questions and the same IP address through which attackers what to get access. Based on this information you know about the attackers even it’s location in the network and it’s purpose. There are two types of attackers: inside attackers and outside attackers. Outside attackers are the person who are unauthorized users means they are not authorized to access the system and the inside attackers are those who have access rights but may use sensitive data to get profit either by leaking information to the competitive or my using this information in wrong way which may loss the organization and to get profit for himself. For creating Honey pot system the widely used tool is honeyed.

The term honey pot was first presented by Lance Spitzner in 1999 in a paper titled To Build a Honeypot (Lance Spitzner, 1999)

Intrusion Detection System (IDS) distinguishes between traffic coming from the client and the traffic coming from the attackers or intruders (Ram Kumar Singh, 2009).

Types of Honeypot

Honeypot systems are classified in many ways based on the purpose (production and research) and level of interaction (low and high).

Based on Purpose

Research Honeypot

Research Honeypot are designed to gain information on black hat community targeting different networks and do not add any direct value to an organization (Karthik et al., 2008). They are used to gather data about the general threats that an organization may faces and allow organization to protect those treats in a better way. It main goal is to monitor the attackers activity, understand their purpose and intention and how they attack i.e. their line of attack. They are complex to both deploy and maintain and captures large amount of data.

Production Honey pot

Production Honey pot captures only limited information, are easy to use and are primarily used by companies and corporations. A production honey pot is one used within an organization's environment to protect the organization and to help to mitigate the risk (Iyatiti Mokube and Michele Adams, 2007) .Production honey pot are place with other production servers inside the production network by an organization to improve the overall security of an organization. They give less information abut attackers and attack then research honey pot.

Levels of Interactions

Low – interaction Honey pots

Low interaction Honey pot is easy to deploy and maintain. There is no operating system for the attackers to interact with (Baumann , R. and Plattner, 2002). They do not modify the network traffic in any way therefore can be compared with passive IDS, and do not interact with attackers. Low interaction honey pot has limited interaction and minimizes the risk associated with the organization. Commercial example of low interaction honey pots are Honeyed, Specter and KFSenseor.

Medium-interaction Honey pots

Medium interaction Honey pots are more sophisticated than low interaction honey pots but less sophisticated than high interaction honeypots.More compel attacks can be logged than low interaction. It provides the attackers with a better illusion of an operating system. Mwcollect and honey trap are the examples of medium interaction honey pot.

High-interaction Honey pots

High interaction Honey pots are more complex and involve highest risk because they involve an actual operating system

(Baumann , R. and Plattner, 2002). They are most time consuming. This honey pot allows attackers to interact with the real operating system and gather large amount of information because nothing is restrictable to access for an attackers, as all activities are logged and analyzed. Honey net is an example of high interaction honey pot.

Working of Honey pot

Honey pot system works on the concept that all the traffic coming to the Honey pot system is suspicious. Honey pot system looks like real server, the only difference between Honey pot system and real server is the location of the machine related to the real server. Honey pot is placed somewhere in DMZ. This means real server is hidden or invisible to the attackers. Honey pot system are generally devised to monitor the activity of an attackers or intruders, save log files, and records events such as processes started, compiles, file adds, deletes and changes. By gathering such information Honeypot system improves the overall security system of the corporation. If sufficient information is gathered it may be used to prosecute in serious condition. This data is used to measure the skill level of the attackers, their intention and even their identity. (www.123eng.com).

Honeypot Implementation

When a programmer wants to develop a honey pot there are two important points to be in considerations: needed complexity to be convincing and how to hide that it is honey pot system not the real system from the attackers. Honeyed and Kippo are two popular open source honey pots.

Honeyed

Honeyed is an application which allows setup of multiple virtual systems (honey pot) on a single machine, each with different services and behavior. It simulates a network stack of various operating systems to the attackers and makes him believe that they are interacting with the real system not with the honey pot system.
Honeyed simulates the network stack not the entire operating system (Mathias Gibbens, Harshavardhan Rajendran, 2012), so this ensures that if honeyed is breached then it will not do much damage. Zto simulate multiple operating system honeyed is combined with virtual machine (VM).

When the attacker sends a packet to the virtual honeypot, then the packet is forwarded to the honeyed host machine by router. After receiving the packet router checks its routing table that the forwarded address of virtual honey pot exist in it or not. If it exists, then router send ARP request for the virtual honey pot to determine the MAC address of honeyed host. This method is known as ARP proxy. If it does not exist then the router dropped the ARP request.

Figure 2 shows the architecture of honeyed. The architecture consists of packet dispatcher, configuration database, personality engine and the protocol handlers. All the incoming packets are dispatched by the packet dispatcher t. Before dispatching the packet, the dispatcher queries the configuration corresponding to the destination address. If a configuration found in the configuration database, then it forwards the packet towards specific protocol handler else discard the packet. On receiving TCP or UDP packet, then the handler establishes

Figure.1 Honey pot system

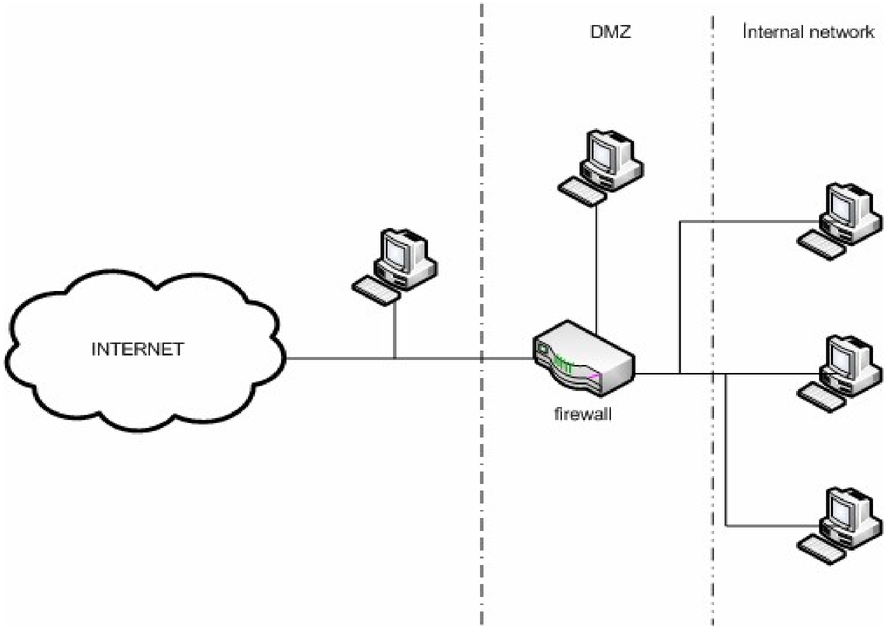
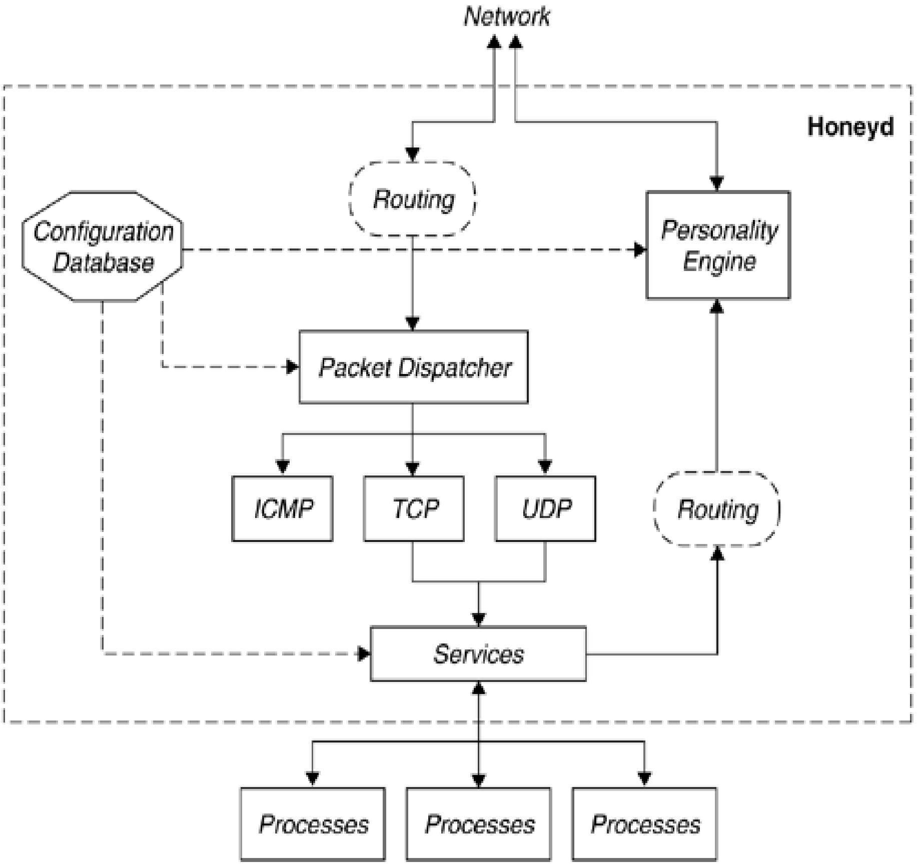


Figure.2 Architecture of Honeyed



the connections to various services. If packets are a part of already started service then all packets are forwarded to the service, otherwise new service is started. At last all the outgoing packets goes through the personality engine to match the characteristics of the configured operation system (Vusal Aliyev, 2010).

Service-specific honey pots

Remote administration is one of the most popular classes of services, like SSH for Linux servers, RDP/VNC for Windows servers (Mathias Gibbens, Harshavardhan Rajendran 2012). One particular SSH honey pot implementation is called kippo, which provides the duplicate of actual SSH server and file system using Python. Kippo is easy to setup and use due to some limitations, it logs both connection attempts and all commands and outputs of the emulated shell of the attacker are saved for later analysis if it allowed access.

Honey tokens

Honeypot is not a computer. A Honeypot is (Amit D. Lakhan)"*An information system resource whose value lies in unauthorized or illicit use of that resource*". Honey token is a Honeypot which is not a computer but some digital entity like credit card number, Microsoft Word file, database entry whose value lies in unauthorized use of that resource. No one should access the honey token only attackers are the possible who access it. Consider an example of Honeypot system.

Assume that there is a bank with a large customer record database going into tens of thousands of entries. Assume that there are thousand numbers of authorized users. Maintaining who is authorized to access what is a complex task and might end up in giving many false alarms. To ignore this situation a bogus record for a customer details or other popular figure is created. This is honey token and has no records. It is accessed by attackers only; no one other than hacker can access it. When attackers attacked for getting sensitive information like account balance and password of any customer, this record will stand out. Therefore attackers access it naturally which results an alarm.

Working Model of Honey token

Honey token detect only invalid activities and therefore need to combine with other security solution to detect the attacker. Honey token plays an important role in detecting internal attacker within an organization. Consider the following example:

Assume that there exists a University: ABC University. The security team had doubt that the mail interaction among the committee members is being monitored illegally. They send out a mail as shown in Figure 2 .An attacker who reads this mail will easily log into that domain with username and password provided in that mail. The attacker does not know that this domain is actually a Honeypot, which will be monitoring his movement and he might get caught eventually.

To: Vice Chancellor
From: Security help desk
Subject: Access to student database
Sir,
The security team has updated your access to university's student database.
Your new login credentials can be found below.
If you need any help please contact us.
https://student.abcuniversity.com
User id: ABCvice
Password: Abc01uVice

Security Help Desk
Figure 2: Example of Honey token.

Advantages and Disadvantages

Advantages

The main advantage of Honeypot is that it provides security to the actual server means if an attacker penetrates the weakness then only the decoy system(Honeypot) get affected, not your real server. Honeypot creates a log files and collect information from this file about the tools and software used by the attackers to harm your system. By this information system administrator provides an additional security to your system and be confident that no sensitive data is leaked to an attacker.

Disadvantages

Every system have disadvantages, honey pot also have some disadvantages. If the decoy system (copy of real system) is not good enough, the gathered data and means of compromise may not match the exact response of the server. Honeypot system may not have the same vulnerable points as the real server; otherwise the intruders will be able to hack the honey pot itself.

Conclusion

Hopefully by reading this paper you have been able to understand what actually honey pot is and how it works and collect information about the attacks and attackers' activity without knowing them. By this short introduction you have been able to know how to bring security in the field of computing system and also know the merits and demerits of honey pot system. One important thing to remember is that honey pot alone is not recommended to secure a system. You have multiple mechanisms which successfully provide security against threats, combining honey pot with other security system is necessary.

References

Amit D. Lakhan, Deception Techniques Using Honey pots.

Baumann , R. and Plattner, C. Honeypots, *Swiss Federal Institue of Technology*, Zurich,2002

Iyatiti Mokube and Michele Adams, Honey pots: Concepts, Approaches and Challenges,*ACM Southeast Regional Conference,page-321-326, ACM*, 2007.

Karthik, S., Samudrala, B. and Yang, A.T. 2008. Design of Network Security Projects Using Honeypots, Journal of Computer Sciences in Colleges.

Lance Spitzner To built a honey pot, http://www.spitzner.net/honeypot.html, Aug 1999.

Mathias Gibbens, Harshavardhan Rajendran, Honey pots, April 2012.

Ram Kumar Singh,Intrusion Detection System Using Advanced Honeypots,*International Journal of Computer Science and Information Security, Vol. 2, No. 1*,2009.

Vusal Aliyev. Using honeypots to study skill level of attackers based on the exploited vulnerabilities in the network. Chalmers University Of Technology, Goteborg, Sweden, 2010

www.123eng.com.