IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 2; Page No. 52-58

Review on: Honey Spot for Analysing Network Security and Related Issues

Rohini Sharma (M. Tech. Scholar)

Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

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 review paper is based upon the introduction to honeypots, their importance in network security, types of honeypots, their advantages disadvantages and legal issues related with them. Research Paper also discuss about the shortcomings of intrusion detection system in a network security and how honeypots improve the security architecture of the organizational network.

Keywords: Honeypot, Information Security, Honey token, Attacks

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 .With the advancement of Internet , whole world become interconnected which uses a no. of technologies to connect and to provide robust level of security . Every domain include its networked group, which having a pool of data stored at a particular location here comes the concept of Network security. 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.

Honeypots

A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. (This includes the hacker, cracker, and script kiddy.). Honeypot is a unique security resource which is a part of security mechanism deployed in an organisation. These are the resources you want the black hat guys to interact with. Yet, honeypot technology is moving ahead rapidly, and, in a year or two, honeypots will be hard to ignore. New developments will advance the lab technology with the catchy name to a full-fledged, enterprise-level security tool.

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. Research honeypots are basically used to attain 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

Corresponding author: Rohini Sharma

protect the organizational network. Research Honeypots are used to gain Information about black hat community Research honeypots are used [3] .Its primary function is to follow the footprints of attacker and gain knowledge about the new ways of attacks performed threats.

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 about attackers and attack then research honey pot. 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.

Levels of Interactions

Low interaction Honey pots

Low-interaction honeypots work by emulating certain services and operating systems and have limited interaction. The attacker's activities are limited to the level of emulation provided by the honeypot. For example, an emulated FTP service listening on a particular port may only emulate an FTP login, or it may further support a variety of additional FTP commands. 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.

The advantages of low-interaction honeypots are that they are simple and easy to deploy and maintain. In addition, the limited emulation available and/or allowed on low-interaction honeypots reduces the potential risks brought about using them in the field. However, with low-interaction honeypots, only limited information can be obtained, and it is possible that experienced attackers will easily recognise a honeypot when they come across one. Some examples of low interaction honeypots are honeyd, specter, BOF. Honeyd is an open source 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 large network on a single host [2, 8].

Example: Façades

A façade is a software emulation of a target service or application that provides a false image of a target host. When a façade is probed or attacked, it gathers information about the attacker. Some façades only provide partial application-level behaviour (e.g. banner presentation), while others will actually simulate the target service down to the network stack behaviour. The value of a façade is defined primarily by what systems and applications it can simulate, and how easy it is to deploy and administer.

Medium-interaction Honey pots

Like low interaction honeypots these also do not provide OS access to attacker but chances to be probed are more than low interaction honeypots [9] .Some examples of medium interaction honeypots are Napenthes , Dioneae , honeytrap ,mwcollect .These honeypots also provide facad services to the attackers .Mwcollect and napenthes can be used to collect the spreading malwares. High-interaction honeypots are more complex, as they involve real operating systems and applications. For example, a real FTP server will be built if the aim is to collect information about attacks on a particular FTP server or service. 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

These are the most sophisticated honeypots .These are difficult to design and implementation .These honeypots are very time consuming to develop and have highest risks involved with this as they involve actual OS with them .In high Interaction Honeypots nothing is simulated or restricted [10]. High interaction Honey pots are more complex and involve highest risk because they involve an actual operating system. Some example of High interaction honeypots are Sebek, Argos. As these honeypots involves real operating system the level of risk is increased by many extents, but to capture large amount of information by allowing an attacker to interact with the real operating system, it is a kind of trade off [13]. By giving attackers real systems to interact with, no restrictions are imposed on attack behaviour, and this allows administrators to capture extensive details about the full extent of an attacker's methods. However, it is not impossible that attackers might take over a high-interaction honeypot system and use it as a stepping-stone to attack other systems within the organisation. Therefore, sufficient protection measures need to be implemented accordingly. In the worst case, the network connection to the honeypot may need to be disconnected to prevent attackers from further penetrating

the network and machines beyond the honeypot system itself.

Attacks against Network Security

We know that there are many possible security threats today those are spread over the Internet. The most common include are listed below [2].

1. Viruses, worms, and Trojan horses
2. Spyware and adware
3. Denial of service attacks
4. Data interception and theft
5. Zero-day attacks, also called zero-hour attacks
6. Hacker attacks
7. Identity theft

Networks are subject to attacks from different types of malicious sources. There are two types of attacks.

A. Active attacks

In passive attacks intruder generally observers the data travelled through network and do the activities which disturb the normal behavior of network by running different commands. Some examples of active attacks are wiretapping, port scanning or idle scanning [5].

B. Passive attacks

Passive attacks have a nature of monitoring, without destroying the actual data. There are 2 types of passive attacks. In passive attacks intruder generally observers the data travelled through network by wiretapping or by another ways. He can also do port scanning to scan the entire network. Sometimes intruder do idle scanning means he just observe the network activities but do nothing. Some examples of passive attacks are denial of service, spoofing, man in the middle, ARP poisoning, Smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, cyber attack etc.

Table 1:

Various Factors Associated with Honey pots				Sr. no	Honey pots	Types of Honey pots	Example
	Low interaction honey pot	**Mid interaction honey pots**	**High interaction honey pots**				
Degree of involvement	Low	Mid	High	1	On the basis of interaction	1) Low interaction honey pots.	Honeyd, Kippo
Real operating system	-	-	x			2)Medium interaction honey pots	Dionea, Napenthes
Risk	Low	Mid	High			3) High Interaction honey pots	Specter
Information Gathering	Connections	Requests	All				
Compromised wished	-	-	x	2	On the basis of purpose	1) Research honey pots.	A standalone PC having any operating System installed like Linux.
Knowledge to run	Low	Low	High				
						2) Production Honey pots.	kF sensor, specter, Dioneae, Napenthes
Knowledge to Develop	Low	High	High				
Maintenance time	Low	Low	Very High				

Honey pot 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

For the security conscious, there is always room for another weapon against attackers. Firewalls, intrusion detection systems, packet sniffers — all are important pieces of the puzzle. So too is Honeyd the "honeypot daemon." Honeyd simulates the existence of an array of server and client machines on your network, including typical traffic between them.

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. Z to simulate multiple operating systems 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 1 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. 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 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 go through the personality engine to match the characteristics of the configured operation system (Vusal Aliyev, 2010). In practice, Honeyd trips up attackers in two ways. First, it slows them down by vastly increasing the amount of work they must do to correctly identify the real target machines on your network. The Nmap scans and traffic logs will be much larger, and take much longer to sort through. Think of this as akin to the way medieval castles were built with multiple rings of walls, with the gates at different positions around the perimeter. The more you slow down the attacker, the better your chances of catching him or her through your other methods.

Second, each of the Honeyd virtual servers is a "honeypot" in the sense that it attracts real attacks even though it is not a real machine. No legitimate user on your network will ever need to probe a Honeyd virtual server, because they do not offer real services. Therefore any probes or connection attempts are automatic red flags. Obviously, a misconfigured program on another machine could generate false positives (as could an uninformed-but-curious new admin), but by and large the honey attracts ne'er-do-wells.

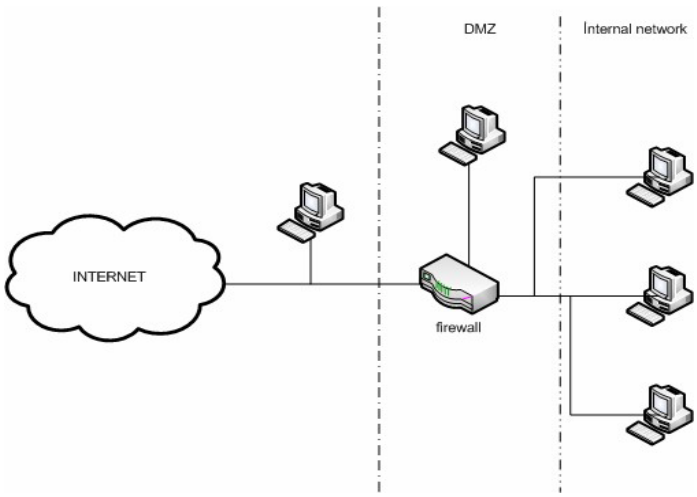

Figure 1: The architecture of honeyed system

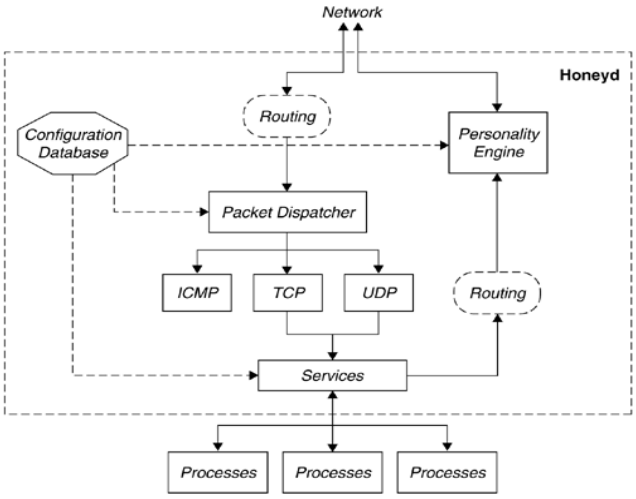

Figure 2: Process of honeyed system

Honey tokens

Honey tokens are the small sized honeypots. Unlike honeypots the standalone machines, honey token are the digital entities such as digital data created and solely analyzed which are used to capture digital thefts. They can be fake data sets which can't exist in real world, at least within a specific enterprise. These are used to track malicious outsiders and insiders engaging in unauthorized activity. Honey tokens may be a URL address, an excel sheet or sometimes a fake record in the organization's database. For instance, a number of companies use honey tokens like fake email address, user account, database data and sometime s executables or false programs. Fake email accounts are used for early warning for spammers. The basic idea is that the fake email address is never used and thus would have no valid reason for receiving spasm.

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.

Examples of freeware honeypots include

1. Deception Toolkit 6: DTK was the first Open Source honeypot released in 1997. It is a collection of Perl scripts and C source code that emulates a variety of listening services. Its primary purpose is to deceive human attackers.

2. La Brea 7: This is designed to slow down or stop attacks by acting as a sticky honeypot to detect and trap worms and other malicious codes. It can run on Windows or UNIX.

3. Honey wall CDROM 8: The Honeywell CDROM is a bootable CD with a collection of open source software. It makes honey net deployments simple and effective by automating the process of deploying a honey net gateway.

4. Honeyd 9: This is a powerful, low-interaction Open Source honeypot, and can be run on both UNIX-like and Windows platforms. It can monitor unused IPs, simulate operating systems at the TCP/IP stack level, simulate thousands of virtual hosts at the same time, and monitor all UDP and TCP based ports.

5. Honey trap 10: This is a low-interactive honeypot developed to observe attacks against network services. It helps administrators to collect information regarding known or unknown network-based attacks.

6. Honey C 11: This is an example of a client honeypot that initiates connections to a server, aiming to find malicious servers on a network. It aims to identify malicious web servers by using emulated clients that are able to solicit the type of response from a server that is necessary for analysis of malicious content.

7. Honey Mole 12: This is a tool for the deployment of honeypot farms, or distributed honeypots, and transport network traffic to a central honeypot point where data collection and analysis can be undertaken.

Advantages

Being a part of network security mechanism honeypots has many advantages. Here we will highlight some specialties of honeypots.

A. Small data sets:

Any connection made with the honeypot is considered as malicious. So the thousands of alerts logged by organizations can be reduced to hundreds of entries.

B. Reduced False Positives

Honeypots help in reducing false positives. The larger the probability that a security resource produce false positives or false alerts the less likely the technology will be deployed. Any activity with the honeypot is considered dangerous and making it efficient in detecting attacks.

C. Catching False negatives:

Catching false negatives with the help of honeypots is quiet easy because every connection made to honeypot is considered un-authorized. Traditional attack detecting tools becomes fail in detecting new attacks like signature based detection tools.

D. Encryption:

Honeypots have the capability to capture the malicious activity if it is in encrypted form. Encrypted probes and attacks interact with the honeypots as end point where the activity is decrypted by the honeypot.

E. Working with IPv6:

Honey pots work in any IP environment, including IPv6. IPv6 is the new version of IPv4 and actively used by the countries like Japan and the department of defence. Many current technologies like firewalls and Ids sensors do not work on IPv6.

F. Flexible

Honeypots are extremely adaptable in variety of environments. From a social security number embedded into a database, to an entire network of computers designed to be broken into.

G. Minimal Resources:

Honeypot require minimal resources. A simple Pentium computer can monitor millions of IP addresses.

Disadvantages

Single Data Point: Honeypots all share one huge drawback; they are worthless if no one attacks them. Yes, they can accomplish wonderful things, but if the attacker does not send any packets to the honeypot, the honeypot will be blissfully unaware of any unauthorized activity.

Risk: Honeypots can introduce risk to your environment. Different honeypots have different levels of risk. Some introduce very little risk, while others give the attacker entire platforms from which to launch new attacks. Risk is variable, depending on how one builds and deploys the honeypot. Some of them are:

- A poorly contained honeypot puts the rest of your network at risk.
- There is also the temptation to retaliate. One should be careful and stay within legal means. Returning tit for tat only gets one in trouble. The goal is to increase ones own security, not go to war with the script kiddies.
- Honeypots won't fulfill their promise unless one has the time to administer them correctly. Companies concerned about security threats are "better off using an intrusion-detection system" if they don't have a dedicated team of highly trained administrators.

Thus though honeypots can add value, the time and resources involved may best focus on greater priorities. It is because of these disadvantages that honeypots do not replace any security mechanisms. They can only add value by working with existing security mechanisms.

Legal Issues with Honeypots

A. Entrapment

A person is entrapped when he is induced by law enforcement officers or their agents to commit a crime that he had not any previous intent to commit. Truly, entrapment is not an issue. There are some reasons like firstly, most individuals in the organization are not law enforced and they do not act under the control of law and they don't have procecution as intent. So, entrapment doesn't apply here. Also, for law enforcement honeypots do not represent entrapment, as honeypots ae not used to persuade or induce attackers.

B. Privacy

The next considerable issue is the privacy .It could be considered in two ways. Either in the files placed on compromised systems by intruders or the interception of communication relayed through the honey nets. There is less case law surrounding interception of communication that is relayed through a compromised host.

Conclusion and Future Scope

The trend of using honeypot is very traditional in network security. It has become necessity of the security for information to lure attackers to some other fake sites in the network than the actual site, where real resources of information are available. Even these honeypots could be extended to honey nets, where attacker deals with the bunch of honeypots. The log files analyzed through these honeypots and honey nets could be used to enhance the Intrusion detection system to make it smarter in catching intrusions. 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.

REFERENCES:

1. Spitzner, L. Open Source Honeypots: Learning with honeyd, Security Focus, 2003.
2. Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).
3. Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 2004.
4. Know your enemy Honeynets, http://www.honeynet.org/papers/key.html SANS institute GIEC certification GSEC Assignments#1.4:Honeypots Stretegic Considera-tions,2002.
5. Kreibich, C. and Crowcroft, J. Honeycomb – Creating Intrusion Detection Signatures Using Honeypots

Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II), Boston, 2003, 51-56.

6. Martin, W.W. Honeypots and Honeynets – Security through Deception. http://www.sans.org/reading_ room/whitepapers/attackin g/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room.
7. John Carroll, Computer Security, 3rd ed., Butterworth-Heinemann, 1997.
8. Provos, Honeypot Background. http://www.honeyd. org/background.php.
9. Baumann, R. and Plattner, C. White Paper: Honeypots, Swiss Federal Institute of Technology, Zurich, 2002.
10. Sutton Jr., R.E. DTEC 6873 Section 01: How to Build and Use a Honeypot.
11. Craig Valli, Honeyd-OS artifice Australian Computer, Network & Information Forensics Conference 2003.
12. Netsec. (2012, 15th March). Specter. Available: http://www.specter.com/default50.htm
13. N. Singh and R. Joshi, "A honeypot system for efficient capture and analysis of network attack traffic," in International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011, 2011, pp. 514-519.
14. Honeypots catching the insider threat lans spitzner.
15. http://www.infoworld.com/d/security/
16. http://honeytrap.mwcollect.org/
17. https://www.client
18. http://www.honeynet.org.pt/index.php/HoneyMole
19. http://www.symantec.com/business/support/documentation.jsp?language=english&view=manuals&pid=51899