International Journal of Advance Research and Innovation
Vol. 1(2), Apr-Jun 2013, pp. 5-11
Doi: 10.51976/ijari.121302

Article Info
Received: 01 Aug 2012 | Revised Submission: 22 Aug 2013 | Accepted: 28 Aug 2013 | Available Online: 20 Sept 2013

Distributed Honeypots System

Sachin Chaudhary and Kanchan Chaudhary***

ABSTRACT

Honeypot is a supplemented active defence system for network security. It traps attacks, records intrusion information about tools and activities of the hacking process, and prevents attacks outbound the compromised system. Integrated with other security solutions, Honeypot can solve many traditional dilemmas. It has emerged as a prominent technology that helps learn new hacking techniques from attackers and intruders. Honeypots can initiatively lure hackers to attack the internet, take the record of the ways and means of their invasion, and then analyze and study them.

Keywords: *Honeypots; Types of Honeypots; Legal Issues.*

1.0 Introduction

Due to rapid growth of internet technology, people easily retrieve their information and quickly transfer messages. However, due to such a swift internet growth, if we don't concurrently attach value to basic network security, it will lead hackers to control the network by using some malicious code, system vulnerabilities and program weakness. Then the attack, devastation and stealing, tampering of information by the hackers may lead to great damages and loss of data. Traditionally we use IDS (Intrusion Detection System) and Firewall System in network to prevent our damages and to provide network defense against the intruders. But IDS and firewall cannot avail all the subsequent information to know the intruders attack and reduce loss caused by attacks.

Infected or malicious code: According to PeiShengHuang et al [4] "Any malicious, unauthorized access, the program is not in line with expectations". Such as computer virus, worm, Trojan or backdoor software, dangerous program (Risk ware) threats are malicious and malevolent codes. An attacker might use them to employ illegal activities, invasive of privacy, and cause individuals or businesses major financial loss.

By understanding these infected codes properly and knowing the target sites of attack in Network, we can provide support to security officials to detect and analyze infected code to guarantee network security.

This information is collected by Honeypot and offered to other gears that do not have this information. If we integrate this information together with an IDS and Firewall it may lead to reduction of false positive or false negative.

We have various open source command line interface Honeypots which show various complications during the implementation. Those collected information has some restrictions at various levels and these information's are not complete. Now we are presenting various problem statements and flaws which can be used for further research in this area to provide better security. Thus security officials can understand the information and can perform deep analysis to realize the patterns of attacks and risks attached with it. In 2002, Spitzner [1] defined Honeypot as "a security resource whose value lies in being probed, attacked or compromised". Further, Honeypots don't provide any solution to any problem, nor they "fix" anything, they are just a tool. It depends upon the user how and in which way they use this tool either for good or for bad.

A Honeypot is a computer system which is placed to get compromised to get the information about the black hats. A Honeypot is like any other computer system which contains directories, drives in it as real computer systems but, its motive is very specific and different. The use of real systems in this manner is famous among the white and blackhats only.

**Corresponding Author: Department of Computer Science & Engineering, TMU, Moradabad, Uttar Pradesh, India (E-mail: sachin.chaudhary126@gmail.com)*
***Department of Computer Science & Engineering, TMU, Moradabad, Uttar Pradesh, India*

One can never eliminate risk, but security helps reduce risk to an organization and protect its valuable resources [1].

Marty Roesch suggested Lance Spitzner in reference [1], the two types of honeypots are Research and Production. Further, according to Mokube I. & Adams M. (2007) we can group Honeypots according to their aims and level of interaction.

2.0 Related Works

Research in this area has resulted in a number of papers discussing specific topics concerning Honeypots and how Honeypots can be created and deployed. Several papers have explored the use of honey nets as an educational tool for IT students and academic institutions [8], [10].

This research indicates that honey nets can be an effective tool in security education. A significant amount of work is available that details the benefits of Honeypots [12], [6]. Other papers go into some detail about the strategic consideration involved when using Honeypots [12].

There are also papers that describe specific applications of Honeypots as building blocks for a system such as a honeycomb.

There are also papers that describe specific applications of Honeypots as building blocks for a system such as a honeycomb, which is used to create intrusion detection signatures [11].

A large amount of helpful information exists on the Honey net Project at [1]. This website documents lessons learned about security threats through the use of Honeypots.

Existing work looks at specific areas concerning Honeypots; however it is difficult to find information from a single source that provides an overall picture of Honeypots including their benefits, the concepts behind Honeypots, the approach to using Honeypots, and the challenges involved when implementing Honeypots.

The purpose of this paper is to do a survey of honeypots, and provide a reasonable overview and starting point for persons who are interested in this technology.

3.0 Types of Honeypots

Honeypots can be classified based on their purpose (production, research, and honeytokens) and level of interaction (low, medium, and high). We include honeytokens as another type, because they do not belong to either of the categories mentioned above. We examine each type in more detail below.

3.1. Research honeypot

A research honeypot is designed to gain information about the black hat community and does not add any direct value to an organization [10]. They are used to gather intelligence on the general threats organizations may face, allowing the organization to better protect against those threats. Its primary function is to study the way in which the attackers progress and establish their lines of attack, it helps understand their motives, behavior and organization Research Honeypots are complex to both deploy and maintain and capture extensive amounts of data. They can be very time extensive.

Very little is contributed by a research honeypot to the direct security of an organization, although the lessons learned from one can be applied to improve attack prevention, detection, or response. They are typically used by organizations such as universities, governments, the military or large corporations interested in learning more about threats research. Research Honeypots add tremendous value to research by providing a platform to study cyber threats.

Attackers can be watched in action and recorded step by step as they attack and compromise the system. This intelligence gathering is one of the most unique and exciting characteristics of honeypots [15]. It is also a beneficial tool in aiding in the development of analysis and forensic skills. Sometimes they can even be instrumental in discovering new worms.

3.1.1. Production honeypot

This type of honeypot is used to protect company from malicious activities done by blackhats. This honeypot is placed under the production network to increase the overall security of the company.

Spitzner L. (2002) and Bruce Schneier model helps us to understand the honeypots. They divide the security issues into groups as: prevention, detection and response.

3.1.2. Prevention

In this type, as company's point of view they are solely concerned about their security and not much interested to know about blackhats. So, they put firewall, use strong passwords, even try encryption

techniques, digital signatures, digital certificates and provide well known security services. They do these just to keep away blackhats from their valuable resources.

3.1.3. Detection

Considering that the prevention doesn't work well, the other solution to overcome attacks is Intrusion Detection System. This technology will help us know whether the system has been compromised or not, but, it will not prevent hackers from attacking the system.

3.1.4. Response

We are unable to prevent the blackhats to infiltrate our system by the above two approaches. As our system has been compromised, in order to take down the attackers we have to backtrack them by the use of log files. Every system makes a log file, keeps information about everything happening in the system in it.

By studying and analyzing the log file we are able to find information about blackhats, the IP address they used, their network address from which they accessed and the available ports from which they accessed our system. This technique is known as forensic investigation. Based upon the level of interaction that we provide to the blackhats to access our systems, we can categorize honeypots as: low interaction and high interaction honeypots.

3.2. Level of interaction

In addition to being either production or research honeypots, honeypots can also be categorized based on the level of involvement allowed between the intruder and the system. These categories are: low-interaction, medium-interaction and high- interaction. What you want to do with your honeypot will determine the level of interaction that is right for you.

3.2.1. Low-interaction honeypots

In the low interaction honeypot, the interaction of the blackhats with the system is limited and is for small amount of time thus the blackhats can not intrude the system. This type of honeypot is made keeping in my mind that we are securing ourselves from the intruders.

But we get very little information about blackhats. So, this approach is widely used in companies where they are concerned about protecting their system from the outer world.

3.2.2. Prevention

In this type, as company's point of view they are solely concerned about their security and not much interested to know about blackhats. So, they put firewall, use strong passwords, even try encryption techniques, digital signatures, digital certificates and provide well known security services. They do these just to keep away blackhats from their valuable resources.

3.2.3. Detection

Considering that the prevention doesn't work well, the other solution to overcome attacks is Intrusion Detection System. This technology will help us know whether the system has been compromised or not, but, it will not prevent hackers from attacking the system.

3.2.4. Response

We are unable to prevent the blackhats to infiltrate our system by the above two approaches. As our system has been compromised, in order to take down the attackers we have to backtrack them by the use of log files. Every system makes a log file, keeps information about everything happening in the system in it. By studying and analyzing the log file we are able to find information about blackhats, the IP address they used, their network address from which they accessed and the available ports from which they accessed our system. This technique is known as forensic investigation.

Based upon the level of interaction that we provide to the blackhats to access our systems, we can categorize honeypots as: low interaction and high interaction honeypots

3.2.5. Medium-interaction honeypots

Medium-interaction honeypots are slightly more sophisticated than low interaction honeypots, but less sophisticated than high interaction honeypots [15]. Like low-interaction honeypots they do not have an operating system installed, but the simulated services are more complicated technically.

Although the probability that the attacker will find a security vulnerability increases, it is still unlikely that the system will be compromised [4] (pp. 20).

Medium-interaction honeypots provide the attacker with a better illusion of an operating system since there is more for the attacker to interact with. More complex attacks can therefore be logged and analyzed.

3.2.6. High-interaction honeypots

In high interaction honeypot, the main emphasis is to get the maximum information about the blackhats allowing them to access the whole system or even tamper it. This is solely research oriented, for those who want to discover new techniques used by the blackhats.

3.3. Honeytokens

Simply put, a honeytoken is a fake digital entity that can have many different applications. Although the term "honeytoken" was coined in 2003 by Augusto Paes de Barros [14], the concept of honeytokens is not new. For years dictionaries, encyclopedias, maps and directories have used fake entries or deliberately erroneous entries as copyright traps to facilitate detection of copyright infringement or plagiarism2.In computer security, Spitzner [14] defines a honeytoken as a honeypot that is not a computer, but a digital entity.

A honeytoken can exist in many forms such as a credit card number, an Excel spreadsheet, a PowerPoint presentation, a database entry, or even a fake login. Like other types of honeypots, no honeytoken has any authorized use.

This gives honeytokens the same power and advantages as traditional honeypots, but extends their capabilities beyond physical computers.

3.3.1. How honeytokens work

Whatever you choose as a honeytoken, no one should be interacting with it, therefore any interaction with it is suspicious, if not necessarily malicious. Honeytokens are flexible enough so that you can decide what you want to use as a honeytoken, and how you want to use it; in this regard you can be as creative as you choose. For example, fake credit card numbers can be inserted into a database, file server or some other kind of repository within a network. IDS's can be configured to watch the network so that if these numbers are accessed, you know the data has most likely been compromised.

Like traditional honeypots, honeytokens do not solve a specific security problem. They are a simple and flexible tool with applications in security that include ensuring data integrity, trapping malicious insiders, and detecting unauthorized access to a database. For example, to ensure data integrity, one could use a honeytoken in the form of a fake database entry that wouldn't normally be selected by authorised queries. The use of a honeytoken such as a fake login can help in tracking the activities, and determining the actions, capabilities and intentions of, a malicious intruder.

Honeytokens should not be used by themselves but should be used in addition to other security measures. In addition, the cost involved in the use of honeytokens is minimal because there is no new technology to deploy, no vendors to contact, and no licenses to deploy, which further increases their value. [16].

4.0 Honeypot Concepts and Approaches to Their Implementation

We now take a look at the main concepts of honeypots and a few different ways in which they can be implemented.

Honeypots are digital network bait and use deception to attract intruders [12], thereby distracting them from real production systems. A honeypot with several layers can slow down an attack, increasing the possibility of the attack being detected, and the possibility of countering the intrusion before it succeeds [2]. Intrusion detection and logging applications can be deployed within the honeypot to listen for and log unauthorized activity.

Since no interaction with a honeypot is authorized, there is no need to filter through the information collected by a honeypot for suspicious traffic. This information can then be used to learn how the intruders operate, and to come up with suitable countermeasures. In summary, the main concept of a honeypot is to learn from the intruder's actions [12].

4.1. Honeypot implementation

To implement a honeypot, some factors you need to consider include: Honeypot can be divided into physical honeypots and virtual honeypots according to their implementation:

4.1.1. Physiacl honeypot

A physical honeypot is a real computer with a complete software stack. The computer is connected into a network and has a dedicated network address. A physical honeypot is presumably the most plausible honeypot as almost everything is authentic and the environment does not have special restrictions. This allows practically the same level of interactivity as a real production system. However, outbound network connections aretypically restricted and carefully

monitored so that the honeypot cannot be used to launch further attacks.

4.1.2. Virtual honeypots

A virtual honeypot simulates the honeypot system in software. This has various advantages over a physical honeypot. A virtual honeypot is easier and safer to operate since only the necessary functionality needs to be implemented.In addition; simulation allows implementing even complex networks of honeypots with relatively few resources.

Virtual honeypots tend to be easier to monitor than physical honeypots. A virtual honeypot can be designed from the start to log every interaction. Although a honeypot based on a virtual machine is rather similar to its physical counterpart, the virtual machine itself can enforce monitoring. This allows capturing information even of attempts to exploit the actual operating system.

5.0 Legal Issues and Challenges

There are potential legal pitfalls that may turn your honeypot into a liability. There are many factors which determine whether or not the use of a honeypot is legal. We provide a brief overview of some of the issues. If deploying a honeypot in the United States, then there are at least three legal issues that you must consider:

- Entrapment - Attackers may argue entrapment
- Privacy – Laws exist that might restrict your right to monitor users on your system

5.1. Entrapment

Most articles written discussing legal issues and honeypots consider entrapment a concern for honeypot owners. The Supreme Court defines entrapment as "the conception and planning of an offense by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officers".

The defense is unlikely in a pure honeypot case where there was no government inducement and the private honeypot owner is acting independently from the government.

When commenting on whether "entrapment" is a concern for honeypot owners, Richard P. Salgado (senior counsel in the Computer Crime and Intellectual Property Section of the Criminal Division of the US Department of Justice) writes that "the issue is overstated" [14].

5.2. Privacy

Although as an owner of a network you have a responsibility to keep it secure, your rights to monitor all the activities of system users may have some limits. There are restrictions that limit monitoring. These restrictions may be in the form of state and federal statutes, privacy or employment policies, terms of service agreements, and other contracts. Depending on the restriction and its source, violating it may lead to civil liability or criminal sanctions. Following are some limitations found in the constitution and federal statutes.

- Fourth Amendment – If you are a government agency operating a honeypot, there is a potential that the Fourth Amendment could limit your monitoring. The Fourth Amendment limits the power of government agents to search for or seize evidence without first securing a search warrant from a judge. Monitoring a user's activities on a network could possibly constitute a "search and seizure". The test for this argument is if the attacker can expect "reasonable expectation of privacy". Hackers do not have this expectation, but other users on a honeypot may. A private organization, not acting at the government's direction can operate a honeypot without worrying about violating the Fourth Amendment.
- Wiretap Act – Essentially, the federal Wiretap Act forbids anyone from intercepting communications (which includes sniffing electronic communications) unless one of the exceptions listed in the act applies. Make sure your organization understands the statute's exceptions and meets their requirements. The exceptions that need to be considered are:

Computer Trespasser Exception – This exception states that the government may monitor a "trespasser". The operator must authorize the interception and the government must do the monitoring. Only the trespasser's communications may be intercepted and it must be relevant to an ongoing "investigation". Consent of a Party Exception – This exception permits an interception if a party to the communication has agreed to the monitoring.

It is recommended that you install a system banner to secure consent. Provider Exception (System Protection) – To apply, the monitoring must be done to protect the operator's rights or property. Some facts to take into consideration are to associate the honeypot with production servers and to separate system administration tasks from investigatory functions.

- Patriot Act – A part of the USA Patriot Act, the "computer trespasser" exception authorizes warrantless monitoring of hackers by the government in certain situations. In cases where honeypots are run under the direction of a government entity, this exception could be used. This exception allows someone acting as a government agent to sniff hacker communications if:
- The network's operator has authorized the interception
- The person sniffing the hacker's communications is engaged in a lawful investigation
- That person has a reasonable bias to believe that the communications that will be intercepted will be relevant to the investigation.

5.3. Liability

Liability implies you could be sued if your honeypot is used to harm others. For example, if it is used to attack other systems or resources, the owners of those may sue. Liability is not a criminal issue, but civil. The argument being that if you had taken proper precautions to keep your systems secure, the attacker would not have been able to harm my systems, so you share the fault for any damage occurred to me during the attack. The issue of liability is one of risk. If I deploy honeypots and they are compromised, what happens if they are used to attack someone else? First, anytime you deploy a security technology (even one without an IP stack), that technology comes with risk. For example, there have been numerous vulnerabilities discovered in firewalls, IDS systems, and network sniffers. Honeypots are no different.

However, just as in privacy, different honeypots have different levels of risk. Low-interaction honeypots have far less risk, as they do not give attackers a real operating system to interact with. Instead, they contain attackers within emulated services, controlling the actions of the attacker. High-interaction honeypots, such as Honeynets, are different; they provide actual operating systems for attackers to interact with. As a result, most high-interaction honeypots have greater risk. If liability is a concern for you, you most likely want to focus on honeypotwith less risk.

6.0 Disadvantages and Advantages

If knowledge is power to the attacker, so is it to the security practitioner. Knowing both the advantages and the disadvantages of honeypots is a must-know. By knowing the inherent risks in honeypots, we can use this knowledge to mitigate these risks and circumvent the disadvantages [20]. We highlight some of these disadvantages and advantages below:

6.1. Disadvantages

Honeypots have several risks and disadvantages. Although few in number, it is these disadvantages that prevent honeypots from completely replacing your current security mechanisms. A poorly contained honeypot puts the rest of your network at risk.

6. 2. Advantages

According to Mokube I. & Adams M (2007) some of the advantages of honeypot are [2]:

1. Honeypots are placed just to get information about the attacks as they are been recorded in the log files.
2. People who target the honeypot are the blackhats as they only know about it not the common people.
3. Honeypots are not bulky as they are placed just to capture a specific pattern of data i.e. malicious traffic.
4. Honeypots provide us the information about the newly generated attacks, newly defined technologies.
5. Honeypots are simple and easy to configure. They do not have complex algorithms.
6. As honeypots captures the malicious traffic, they also capture the new tools used by the blackhats.
7. Honeypot detects few false positive and false negative data also.

A honeypot can be placed in a network, with firewall, before firewall and after firewall. We are considering these places because these are the most frequent places from where the blackhats accesses the system and we can trap them to get maximum information about them. Our aim is to get maximum information about them by compromising our research data, so that they may not infiltrate the data

again in the future. We are here to know the tools used by the attackers.

7.0 Conclusions and Future Outlook

In this paper we have provided a brief overview of what honeypots are, and what they are useful for. We have discussed the different types of honeypots such as production honeypots, research honeypots, and honeytokens. We also looked at factors that should be considered when implementing a honeypot. For example, the level of interaction of your honeypot depends on what you want to use it for. The legal issues surrounding honeypots and their implementation were examined, and throughout we mentioned the advantages of honeypots. An important point to remember is that experts advise using honeypots together with some other form of security such as an ID.

References

[1] Spitzner, L. 2002. Honeypots: Tracking Hackers. 1st Ed Boston, MA, USA: Addison Wesley.

[2] Mokube, I. & Adams M. 2007 Honeypots: Concepts, Approaches, and Challenges. ACMSE 2007, WinstonSalem, North Carolina, USA, pp.321325

[3] Aaron Lanoy and Gordon W. Romney, Senior Member, IEEE [2006] A Virtual Honey Net as a Teaching Resource

[4] F.A. Shuja. (2005, November) Virtual Honeynet: Deploying Honeywall using VMware, Pakistan Honeynet Project [Online], Available: http://www.honeynet.org.pk/honeywall/roo/

[5] (2005, August). Know Your Enemy: Honeywall CDROM Roo3rd Generation Technology, Honeynet Project & Research Alliance, and [Online] Available: http://www.honeynet.org, Last Modified: 2005

[6] G. Romney, et al., "A Teaching Prototype for Educating IT Security Engineers in Emerging Environments," Presented at the IEEE ITHET 2004 Conference in Istanbul, Turkey, 2004.

[7] Cliaord Stoll. Stalking the Wily Hacker Communications of the ACM Pp 484497, 1988

[8] Ram Kumar Singh & Prof. T. Ramanujam. Intrusion DetectionSystem Using Advanced Honeypots, 2009

[9] Kabay, M.E. Honeypots, Part 2: Do honeypots constitute entrapment? *Network World*, 2003

[10] Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots *Journal of Computing Sciences in Colleges*, *20* (4)

[11] 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

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

[13] Spitzner, L. The Honeynet Project: Trapping the Hackers. *IEEE Security & Privacy*

[14] Spitzner, L. *Honeypots: Tracking Hackers*. Addison- Wesley Pearson Education, Boston, MA, 2002

[15] Spitzner, L. Honeytokens: The Other Honeypot. http://www.securityfocus.com/infocus /1713, Security Focus, 2003