Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review of Implementing a Working Honeypot System

Amandeep Singh*,
M.Tech Student
Department of Computer Engineering, Punjabi University
Punjab, India

Navdeep Singh
Assistant Professor
Department of Computer Engineering, Punjabi University
Punjab, India

Abstract— A honeypot is used in the area of computer and Internet security. It is a resource used to trap attacks, records intrusion information about tools and events of the hacking process, and avoids attacks outbound the compromised computer system. It can also be deployed to attract and divert an attacker from their real targets. The goal of our paper is to show the overview of honeypots and their use in a research as well as productive environment. A honeypot can be anything from Windows to UNIX. Compared to the other intrusion detection systems, honeypots have the big advantage that they do not generate incorrect alerts or large log files like other intrusion detection systems because no productive components are running on the system. Other big advantage of honeypot system is that we don't need to manage the data base of intrusions signature or definition. The honeypot system logs every byte that flows through the network. This log data helps the researcher to draw a picture of an attack and the attacker.

Keywords—Intrusion Detection System, Honeypot, Network security

I. INTRODUCTION

Global communication is getting more important every day. At the same time, computer wrongdoings are increasing. Countermeasures are developed to identify or prevent attacks- most of these measures are based on known facts, known attack patterns like in antivirus programs. As in the military, it is essential to know, who your enemy is, what thoughtful of strategy he uses, what tools he utilizes and what he is targeting for. Gathering this kind of information is not easy but important. By knowing attack tactics, countermeasures can be improved and vulnerabilities can be fixed. To collect as much information as possible is one main objective of a honeypot. Generally, such information gathering should be done silently, without worrying an attacker. All the gathered information leads to an advantage on the protecting side and can therefore be used on productive systems to prevent attacks. A honeypot is primarily an instrument for information gathering and knowledge. Its primary purpose is not to be an ambush for the blackhat community to catch them in action and to press charges against them. The attention lies on a silent collection of as considerable information as possible about their attack patterns, used programs, determination of attack and the blackhat community itself. All this information is used to know more about the blackhat actions and motives, as well as their technical knowledge and talents. This is just a primary purpose of a honeypot. There are a lot of other possibilities for a honeypot [4] divert hackers from productive systems or catch a hacker while conducting an attack are just two possible examples. Honeypots are not the perfect solution for solving or preventing computer crimes. Honeypots are hard to sustain and they need operators with good knowledge about operating systems and network security. In the other hands, a honeypot can be an effective tool for information gathering. In the wrong, inexpert hands, a honeypot can become another intruded machine and an instrument for the blackhat community.

This paper will introduce some basic terms, types as well as possibilities which can be used to implement a working honeypot.

II. History

The concept of Honeypots was first described by "Clifford Stoll" in 1990[2]. The book is a novel based on a true story which happened to Stoll. He discovered a hacked computer system and decided to learn how the intruder gained access to the computer system. To track the hacker back to his origin, Stoll created a faked environment with the determination to keep the attacker busy. The idea was to track the connection while the attacker was searching through prepared documents. Stoll did not call his trap a Honeypot; he just arranged a network drive with faked documents to keep the intruder on his machine. Then he used monitoring tools to track the hacker's origin and find out how he came in. In 1999 that idea was picked up again by the Honeynet project lead and founded by "Lance Spitzner". Unfortunately it is not clear who originated the term "Honeypot". Spitzner's book lists some early Honeypot results, but none of these had Honeypot in their name.

III. Honeypots

The buzz word "Honeypot"[3] is spooking around the world. Different vendors claim that they offer honeypot products, people are disagreeing about honeypots without having a clear image of what a honeypot is. To clarify this issue, a definition of what is meant when talking about honeypots is provided.

L. Spitzner defines the term honeypot as follows:

"A honeypot is a resource whose value is being in attacked or compromised. This means, that a honeypot is probable to get probed, attacked and potentially demoralized. Honeypots do not fix any particular problem. They provide us with additional, valued information".

Honeypots do not help directly in increasing a computer network's security. On the conflicting, they do attract intruders and can therefore attract some interest from the Blackhat community on the network where the honeypot is located.

There are two types of honeypots –

- **Production honeypots**
- **Research honeypots.**

A production honeypot is used to help transfer risk in an organization while the second category, research, is meant to collect as much information as possible. These honeypots do not add any extra security value to an organization, but they can help to recognize the blackhat community and their attacks as well as to build some better defences mechanism against security threats. A honeypot is a resource which is proposed to get compromised. All traffic from and to a honeypot is suspicious because no productive systems are located on this resource. In general, all traffic from and to a honeypot is illegal activity. All data collected by a honeypot [5] is therefore interesting data. A honeypot will in general not yield an awful lot of logs because no productive systems are running on that machine which makes analysing this data much easier. Data collected by a honeypot is of high value and can central to a better understanding and knowledge which in turn can help to increase complete network security. One can also argue that a honeypot can be used for prevention because it can prevent attackers from attacking other systems by occupying them long enough and bind their resources. Against most attacks nowadays a honeypot does not help lying individuals as there are no persons to deceive. If a honeypot does not get attacked, it is useless. Honeypots are normally located at a single point and the probability can be quite small that an attacker will "find" the honeypot. A honeypot does also introduce a certain risk - blackhats could get attracted to the whole network or a honeypot may get silently compromised.

IV. Levels of Involvement

One characteristic of a honeypot is its level of involvement. The level of involvement does measure the degree an attacker can interact with the computer system.

Low-Involvement Honeypot

A low-interaction Honeypot [9] emulates network services only to the point that an intruder can log in but perform no actions. Low-interaction Honeypots are used only for detection and function as production Honeypots. In comparison to IDS systems, low-interaction Honeypots are also logging and detecting attacks. Furthermore they are proficient of responding to certain login attempts, while an IDS stays passive. On a low-involvement honeypot there is no real operating system that an attacker can operate on. This will minimize the threat significantly because the complexity of an operating system is removed. On the other hand, this is also a disadvantage. It is impossible to watch an attacker interacting with the operating system, which could be certainly interesting. A low-involvement honeypot is like a one-way connection. We only listen, but we do not request questions ourselves. The role of this approach is very passive. A low-involvement honeypot can be compared to an passive IDS, as both do not alter any traffic or interact with the attacker or the traffic flow. They are used to produce logs and alerts if incoming packets match certain patterns.

Mid-Involvement Honeypot

Their primary purpose is detection and they are used as production Honeypots. A mid-involvement honeypot provides more to interact with, but still does not provide an actual underlying operating system. At the same moment, the risk increases. The probability that the attacker can find a security hole or susceptibility is getting bigger because the complexity of the honeypot increases. Through the higher level of interaction, more difficult attacks are possible and can therefore be logged and analyzed. The attacker gets an improved illusion of a real operating system. He has additional possibilities to interact and probe the system. Developing a mid-involvement honeypot is complex and time consuming. Extra Special care has to be taken for security checks as all developed fake daemons need to be as secure as possible. The knowledge for developing such a system is very high as each protocol and service has to be understood in detail.

High-Involvement Honeypot

These are the most explained Honeypots. A high-involvement honeypot has a real underlying operating system. This leads to a considerable higher risk as the complexity increases rapidly. At the same time, the possibilities to collect information, the possible attacks as well as the attractiveness increase a lot. High-interaction Honeypots are used primarily as research Honeypots but can also serve as production Honeypots. A high-involvement honeypot is very time consuming. The system should be constantly under observation. A honeypot which is not under control is not of much help and can even become a danger or security hole itself. It is very important to bound a honeypot's access to the local intranet, as the honeypot can be used by the intruders as if it was a real compromised system. Limiting outbound traffic is also an important point to reflect, as the danger once a system is fully compromised can be reduced. By providing a full operating system to the attacker, he has the potentials to upload and install new extra files. This is where a high-involvement honeypot can show its strength, as all actions can be recorded and analysed. Gathering new information

about the blackhat community is one main goal of a high-involvement honeypot and legitimates the higher risk. Each level of involvement has its advantages and disadvantages. The following table summarizes what has been seen so far.

	Low	Mid	High
Degree of involvement	Low	Mid	High
Real operating system	-	-	Yes
Risk	Low	Mid	High
Information Gathering	Connections	Requests	All
Compromise wished	-	-	High
Knowledge to run	Low	Low	Mid-high
Knowledge to develop	Low	High	Very-high

V. Network Topologies

Here we will discuss the placement of honeypots in a network as well as a special, more complex version of honeypots - a so called honeynet.

Honeypot Location

A honeypot does not need a certain surrounding environment as it is a standard server with no special needs. A honeypot can be located anywhere a server could be placed. But certainly, some places are well for certain methods as others. A honeypot can be used on the Internet as well as the intranet, based on the needed service. Assigning a honeypot on the intranet can be suitable if the detection of some bad guys inside a private network is wished. It is exclusively important to set the internal thrust for a honeypot as low as possible as this system could be compromised, probably without instant knowledge.

If the main concern is the Internet, a honeypot can be positioned at two locations:

- **In front of the firewall (Internet)**
- **Behind the firewall (intranet)**

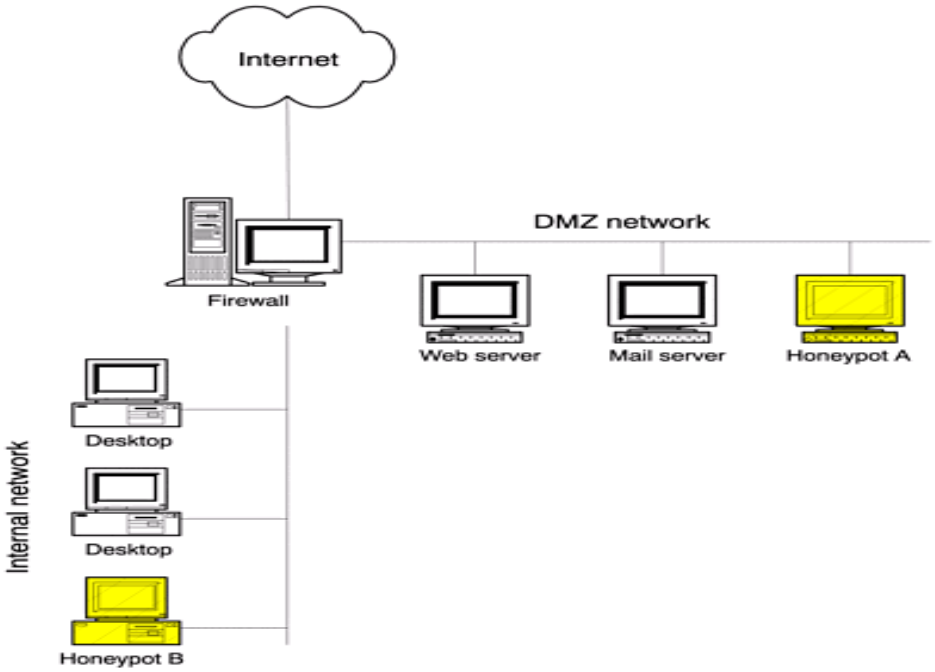

Fig.1 Locations of honeypot [12]

Each approach has its advantages as well as disadvantages. By placing the honeypot in front of a firewall the risk for the internal network does not increase. The risk of having a compromised system behind the firewall is eliminated. The disadvantage of placing a honeypot in front of the firewall is that internal attackers cannot be located or trapped that easy, especially if the firewall parameters outbound traffic and therefore limits the traffic to the honeypot. By placing a honeypot [7] outside the firewall, such events do not get listed by the firewall and an internal IDS system will not generate alerts. Otherwise, a large number of alerts would be generated on the firewall or IDS. Placing a honeypot inside a DMZ honeypot seems a good solution as long as the other systems inside the DMZ can be secured against the honeypot. A honeypot behind a firewall honeypot can introduce new security risks to the internal network, especially if the internal networks are not secured against the honeypot through additional firewalls. The main reason for placing a honeypot behind a firewall could be to detect internal attackers.

VI. Honeynets

Honeynets [1] are one of the most advanced and complex honeypots, their primary purposes is to capture extensive information on intimidations, both internal and external. Honeynets are complex in that they are entire networks of computers to be attacked. Nothing is outdone. The systems and applications within a Honeynet can be the same systems found in your organization. Within these systems you can place extra information, such as files, records in databases, log entries, any information you want the attacker to interact with. Honeynets [5] have this flexibility because they are not a standardized solution, instead a Honeynet is a specialized architecture that creates a fishbowl, you can then place any targets systems you want within this fishbowl. Just like a fishbowl, you can create your own virtual world; however instead of adding coral and sand, you add Solaris database servers or Cisco routers. Just like a fishbowl, you can watch everything that is going on, however with a Honeynet; the attacker never realizes you are watching them.

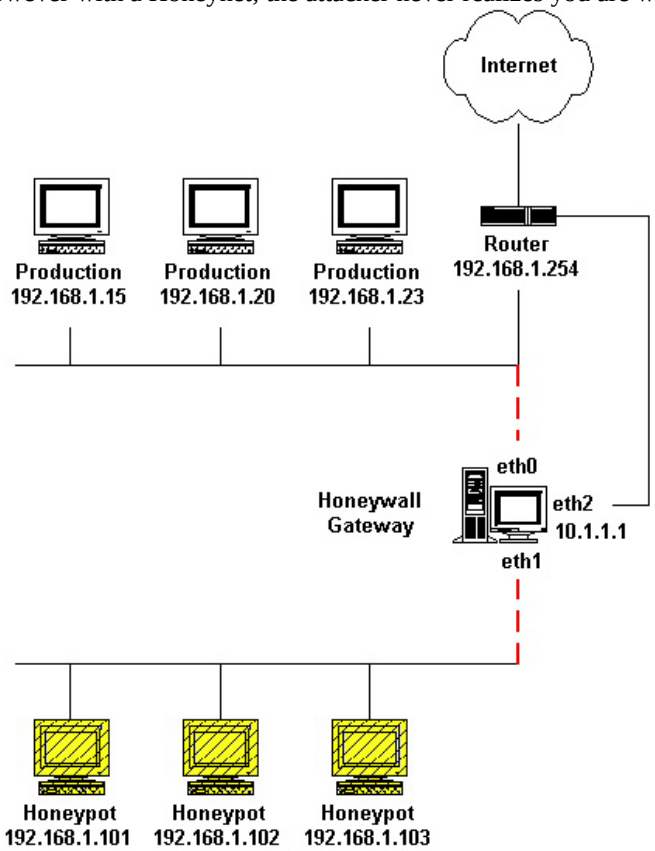

Fig. 2 Honeynet systems [11]

VII. CONCLUSION

Honeypots are an developing technology, with widespread potential. They have tremendous advantages that can be applied to a variety of different environments. They intensely reduce false positives, while providing an extra flexible tool that is easy to customize for different environments and threats. Traditionally, honeypots have been applied against external threats or common internal threats. The research on honeypot is still in the early stages, with the intent of greater testing and development in the future.

References

[1] Project Honeynet. http://www.project.honeynet.org.

[2] Provos, Niels. "A Virtual Honeypot Framework." In Proceedings of the 13th USENIX Security Symposium. 2004. 1-14

[3] Lance Spitzner. Honeypots – Definitions and Value of Honeypots. http://www.enteract.com/˜lspitz/honeypot.html
[4] The Honeynet Project "Know Your Enemy: http://www.honeynet.org/papers/profiles/cc-fraud.pdf
[5] The Honeynet Project "Know Your Enemy:http://www.honeynet.org/papers/honeynet.
[6] " HONEYPOT SECURITY"http:/www.infosec.gov.hk/english/technical/files/honeypots.pdf
[7 Old.honeynet.org/papers/individual/Mastersthesis_Doering.pdf.
[8] Reto Baumann, Christian Plattner" Honeypots"
[9] S.Mukkamala, K. Yendrapalli, R. Basnet **"**Detection of Virtual Environments and Low Interaction Honeypots**"**
[10] Reto Baumann" Honeyd – A low involvement Honeypot in Action",
[11] http://old.honeynet.org/papers/honeynet/
[12] http://advanced-network security.blogspot.in/2008/04/honey-pots.html

