Host Based Information Gathering Honeypots for Network Security

M. Purushotham Reddy[1], K. Subba Reddy[2], M. Indra Sena Reddy[3], G. Sreenivasulu Reddy[4]

[1,4]Dept. of Computer Science and Engineering, VBIT, Proddatur, Kadapa, A.P, India.

[2, 3]Dept. of Computer Science and Engineering CSE, RGMCET , Nandyal, Kurnool (Dt), A.P, India.

Abstract

Honeypots are an exciting new technology which is widely used in the areas of computer and Internet security that, allows us to turn the tables on the bad guys. It is a resource, which is intended to be attacked and computerized to gain more information about the attacker, and used tools. Compared to an intrusion detection system, honeypots have the big advantage that they do not generate false alerts as each observed traffic is suspicious, because no productive components are running in the system. The goal of *this* paper is to show the possibilities of honeypots and their use in research as well as productive environment.

Keywords: Levels of honeypots, Internet security, Network traffic, Firewall authentication.

1. Introduction

The concept of "honeypots" has been introduced in computing systems by Clifford Stoll in the late 80's. In the 'Cuckoo's Egg' [1], described the monitoring and tracking of an intruder. In the 90's, Cheswik implemented and deployed a real "honeypot" [2]. Bellovin discussed the very same year the advantages and problems related to its usage [3]. In 98, Grundschober and Dacier ([4, 5]) introduced the notion of "sniffer detector" , one of the various forms of what is called today a "honeytoken". Lance Spitzner, a senior security architect for Sun Microsystems is the author of "Honeypots, Tracking hackers" [6]. "A honeypot is security resource whose value lies in being probed, attacked or compromised." [6, page 40] .This is the most common definition and many papers refer to it [7, 8]. However its precise meaning is not so clear. If we take a deeper look at it, we see that the definition can be decomposed as follows:

- One term: « a security resource »
- A subordinate description: "its value which lies in being probed, attacked or compromised" .

This is the exact opposite of most production systems, which you do not want to be probed or attacked." [6, page 40] .In [6, page 42], the following example of a honeypot deployment is given: an old and unused server in the DMZ is closely watching any traffic to or from it. According to L.Spitzner, the server is here to "determine if there is any unauthorized activity happening within the DMZ". Can we reasonably call this machine a security resource? Furthermore, what happens if it logs nothing? According to lance Spitzner "if the system is never probed or attacked, then it has a little or no value". Reto Baumann, a Swiss engineer, discusses in [9] Lance Spitzner's interpretation. His definition slightly differs from the previous one: "A honeypot is a resource which pretends to be a real target. A honeypot is expected to be attacked or compromised. The main goals are the distraction of an attacker and the gain of information about an attack and the attacker." [9]

Many documents refer to Lance Spitzner's definition. Some of them adapt it to a more restrictive usage. This is the case of searchWebservices.com, a commercial portal on IT services. They suggest this one [10]: "A honeypot 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.) Maintaining a honey pot is said to require a considerable amount of attention and may offer as its highest value nothing more than a learning experience (that is, you may not catch any hackers)." [10] This definition is quite restrictive. First and foremost honeypots are not reserved to the Internet usage. They can be implemented to reveal internal attacks. In addition some of them are not 'expressively set up to attract'. One simple example consists in putting a basic Honeyd machine into the DMZ. It is likely to be scanned and attacked but it is not "expressly set op to attract people".

The niversity of Wisconsin-Platteville (http://www.uwplatt.edu/) as well as R.C. Barnett from the sourceforge.net web site ([11]) mentions the following definition:

"An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored." [11] .Last definition we propose is suggested by the SANS Institute [12]. It appears in an article written by Michael Sink in April 2001: "The use of Honeypots and Packet Sniffers for Intrusion Detection" [13]:

"Within the realm of computer security, a honeypot is a computer system designed to capture all traffic and activity directed to the system. While honeypots can be set up to perform simple network services in conjunction with capturing network traffic, most are designed strictly as a "lure" for would-be attackers. Honeypots differ from regular network systems in that considerably greater emphasis is placed on logging all activity to the site, either by the honeypot itself or through the use of a network/packet sniffer. A honeypot is designed to look like something an intruder can attack to gain access to a given system." [13]

The problem with this definition is that it is rather verbose and vague. It characterizes honeypots from “regular network systems” as those that place “considerably greater emphasis on logging all activity”. But many systems can be designed to capture traffic and activities. What does ‘greater’ exactly mean? A firewall which logs connections or an application that stores history may be considered as honeypot. The definition is very broad as many computer systems are collecting activities and traffic directed to them.

2. Honeypot Basics

A honeypot is a resource whose value is being in attacked and compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited.

Honeypot do not fix anything. They provide us additional, valuable information.

A honeypot is a resource, which pretends to be real target. A honeypot is expected to be attacked or compromised. The main goals are the distraction of an attacker and the gain of the information about the attack and the attacker.

Value of honeypots:

There are two categories of honeypots.

- Production honeypots
- Research honeypots

A production honeypot is used to help migrate risk in an organization while the second category, is meant to gather as much information as possible. These honeypots do not add any security value to an oraganition, but they can help to understand the blackhat community and their attacks as well as to build some better defenses against security threats. A properly constructed honeypot is put on a network, which closely monitors the traffic to and from the honeypot. This data can be used for a variety of purposes.

- Forensics: alyzing new attacks and exploits
- Trend analysis:look for changes over time of types of attacks,techniques,etc
- Identification: track the bad guys back to their home machines to figure out who they are.
- Sociology:learn about the bad guys as a group by snooping on email,IRC traffic,etc which happens to traverse the honeypot.

In general every traffic from and to a honeypot is unauthorized activity. All the data that is collected by a honeypot is therefore interested data. Data collected by the honeypot is of high value, and can lead to better understanding and knowledge which in turn can help to increase overall network security. One can also argue that a honeypot can be used for prevention because it can deter attackers from attacking other systems by occupying them long enough and bind their resources.

2.1 Low-involvement honey

A low-level involvement honeypot typically only provides certain fake services. In a basic form, these services could be implemented by having a listener on specific port.

In such a way, all incoming traffic can easily be recognized and stored. With such a simple solution it is not possible to catch communication of complex protocols. On a low-level honeypot there is no real operating system that attacker can operate on. This will minimize the risk significantly because the complexity of an operating system is eliminated. On the other hand, this is also disadvantage. It is not possible to watch an attacker interacting with operating system, which could be really interesting. A low-level honeypot is like one-way connection. We only listen, we do not ask any questions.

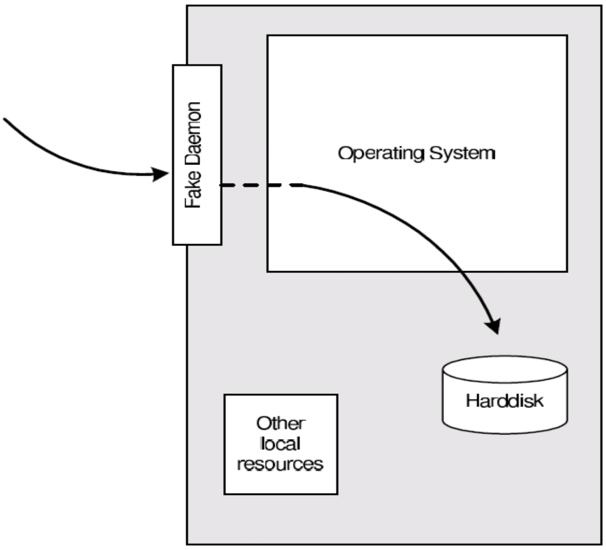


Figure 1. Low-involvement honeypot

2.2. Mid-involvement honeypot

A mid-involvement honeypot provides more to interact with but still does not provide a real underlying operating system. The fake daemons are more sophisticated and have deeper knowledge about the specific services they provide. At the same moment, the risk increases. The probability that attacker can find a security hole or vulnerability is getting bigger because the complexity of honeypot is increasing.

Through the higher level of interaction, more complexity attacks are possible and can therefore be logged and analysed. The attacker gets a better illusion of a real operating system. He has more possibilities to interact and probe the system. Developing a mid-involvement honeypot is complex and time consuming. Special care has to be taken for security check as all developed fake daemons need to be as secure as possible.

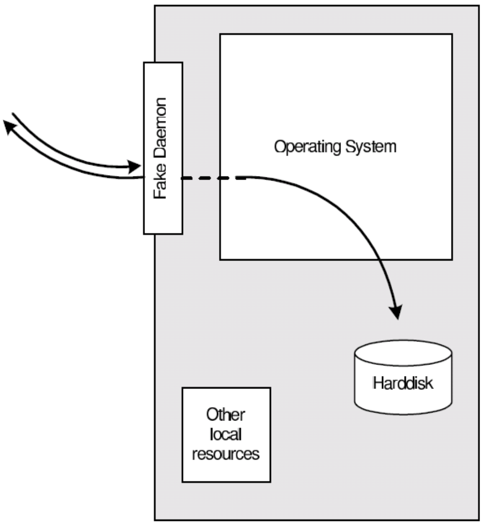


Figure 2. Middle level-involvement honeypot

2.3.High-involvement honeypot

A high-involvement honeypot has a real underlaying operating system. This leads to much higher risk as the complexity increases rapidly. At the same time, the possibilities to gather the information, the possible attacks as well as the attractiveness increase a lot. As soon as a hacker has gained access, his real work and therefore the interesting part begins.

A high-involvement honeypot is very time consuming. The system should be constantly under surveillance. A honeypot which is not under control is not of much help even become a danger or security hole itself. It is very important to limit a honeypot’s access to local intranet, as the honeypot can be used by blackhats as if it was a real compromised system. Limiting outbound traffic is also important point to consider, as the danger once a system is fully compromised can be reduced.

By providing a full operating system to attacker, he has the possibilities to upload and install new files. This is where the high-involvement honeypot can show its strength, as all its actions can be recorded and analyzed.

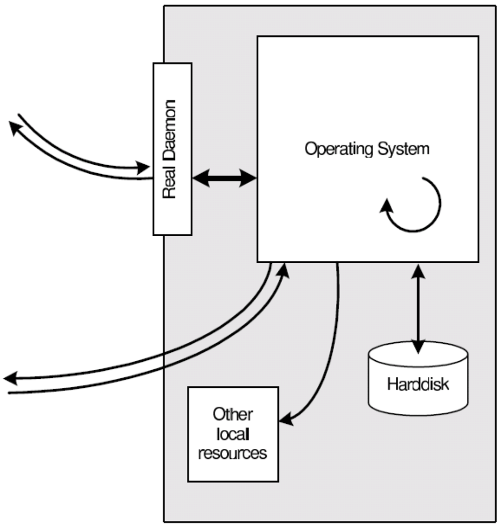
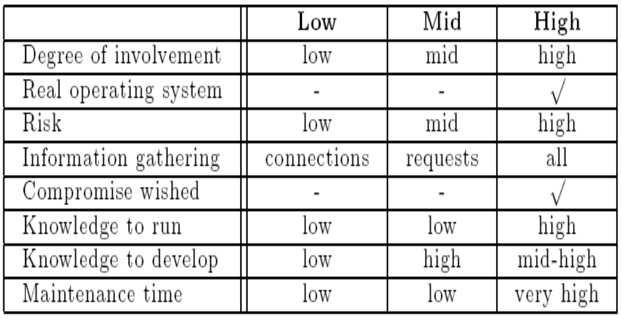


Figure 3. High level-involvement honeypot



	Low	Mid	High
Degree of involvement	low	mid	high
Real operating system	-	-	√
Risk	low	mid	high
Information gathering	connections	requests	all
Compromise wished	-	-	√
Knowledge to run	low	low	high
Knowledge to develop	low	high	mid-high
Maintenance time	low	low	very high

Figure 4. Details of honypot at different levels

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 placed anywhere a server could be placed. But certainly, some places are better for certain approaches as others.

A honeypot can be used on the Internet as well as the intranet, based on the needed service. placing a honeypot on the intranet can be useful if the detection of some bad guys inside a private network is wished. If the main concern is the Internet, a honeypot can be placed at two locations:

1. In front of firewalls(Internet)
2. DMZ
3. Behind the firewall(Intranet)

By placing the honeypot in front of firewall the risk for the internal works does not increases. A honeypot will attract and generate lot of unwished traffic like port scans or attack patterns. By placing a honeypot outside the firewall, such events do not get logged by the firewall and an internal IDS system will not generate alerts. Otherwise a lot of alerts would be generated on the firewall or IDS.

Probably the biggest advantage is that the firewall or IDS,as well as any other resources, have not to be adjusted as the honeypot is outside the firewall and viewed as any other machine on the external network. Running a honeypot does therefore not increase the dangers for the internal network nor does it introduce new risks.

The disadvantage of placing a honeypot in front of the firewall is that internal attackers cannot be located or trapped that easy. Placing a honeypot inside DMZ seems a good solution as long as the other systems inside the DMZ can be secured against the honeypot.Most DMZs are not fully accessible as only needed services are allowed to pass the firewall. In such a case, placing the honeypot in front of the firewall should be favored as opening all corresponding ports on the fire is too time consuming and risky.

A honeypot behind a firewall can introduce new security risks to the internal network, especially if the internal network is not secured against the honeypot through additional firewalls. This could be a special problem if the Ips are used for authentication. By placing the honeypot behind a firewall, it is inevitable to adjust the firewall rules if access from internet should be permitted. The biggest problem arises as soon as the internal honeypot is compromised by an external attacker. He gains the possibility to access the internal network through the honeypot.This traffic will be unstopped by the firewall as it is regarded as traffic to the honeypot only, which in turn is granted. Securing an internal honeypot is therefore mandatory, especially if it is a high-involvement honeypot. The main reason for placing a honeypot behind a firewall could be to detect internal attackers.

The best solution would be to run a honeypot in its own DMZ,therefore with a preliminary firewall. The firewall could be connected directly to the internet or intranet, depending on the goal. This attempt enables tight control as well as flexible environment with maximal security.

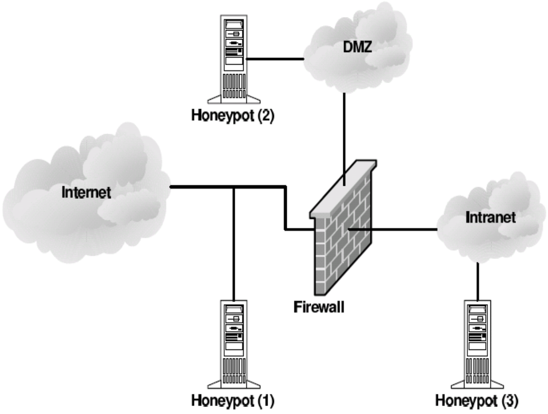


Figure 5. Firewalls involvement in honypot at different levels

3. HOST BASED INFORMATION GATHERING

This section will discussion possibilities that offer gain of information about ongoing on a honeypot by installing information gathering mechanisms on the honeypot itself.

Basic possibilities:

Information gathering facilities can basically be grouped into two categories; facilities that generates streams of information and facilities that offer the information to peek into the system and get the information about a certain state of the honeypot .

3.1. Microsoft windows

One could think the large amount of observed attacks on systems running ms windows operating system makes them ideal for the honeypot, but unfortunately the structure of these operating system makes the data gathering rather difficult. Until today the source code of the operating system of Microsoft is not freely available , which means that changes to the operating system are very hard to achieve.

B.Unix derivates:

Unix derivatives operating system offers interesting opportunities for deploying data gathering mechanisms since all of their components are available as source code.

Network based Information Gathering:Host based information gathering is always located at the host itself and is therefore vulnerable to detection and once detected it can also be disabled. Network based information gathering does not have to be located on the honeypot itself. It can also be implemented in an invisible way, as network traffic only gets analyzed but not manipulated. Network based information gathering is safer as it is harder to be detected and quiet impossible to disable.

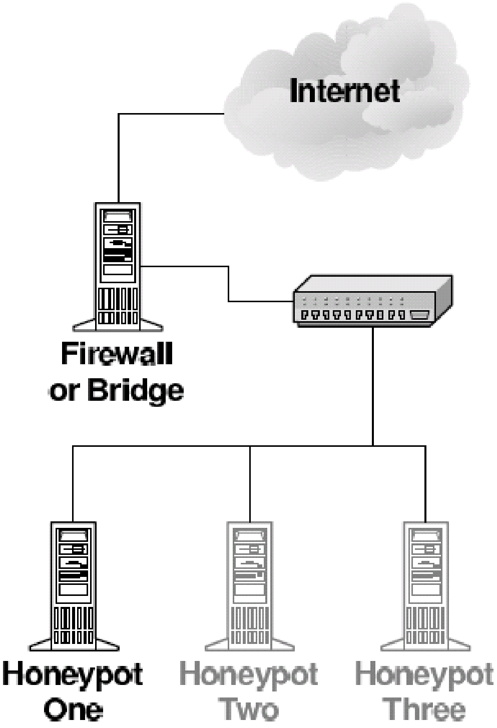


Figure 6. Firewall involvement in honypot

Dangers:

Running a honeypot or honeynet is not something that should be underestimated- there are some dangers one must be aware of which basically are:

1. Unnoticed takeover of the honeypot by an attacker
2. Lost control over the honey pot installation.
3. Damage done to third party.

Attractiveness:

Being the owner of a honeypot can be an interesting experience, but what if the members of the blackhat community do not find their way to the honeypot or, even more dramatically, are not interested in the honeyot at all. Another approach to lure attackers is the offering of the interesting services on the honeypot. Of course the question arises, what an interesting services is or what it should look like.

Advantages:

- Small Data sets→Honeypots only collect attack or unauthorized activity, dramatically reducing the amount of data they collect. Organizations that may log thousands of alerts a day may only log a hundred alerts with honeypots. This makes the data honeypots collect much easier to manage and analyze.
- Reduced False Positives→Honeypots dramatically reduce false alerts,as they only capture unauthorized activity.
- Catching False Negatives→Honeypots can easily identify and capture new attacks never seen before.
- Minimal Resources→Honeypots require minimal resources,even on the largest of networks.This makes them an extremely cost effective solution.
- Encryption→Honeypots can capture encrypted attacks.

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 sent any packets to the honeypot,the honeypot will be blissfully unware of any unauthorized activity.
- Risk→Honeypots can introduce risk to your environment.As we discuss later,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.

4. CONCLUSIONS

A honeypot is just a tool. How you use that tool is up to you. There are a variety of honeypot options, each having different value to organizations. We have categorized two types of honeypots, production and research. Production honeypots help reduce risk in an organization. Research honeypots are different in that they are not used to protect a specific oraganization. Instead they are used as a research tool to study and identify the threats in the Internet community. Regardless of what type of honeypot you use,keep in mind the 'level of interaction'. This means that the more your honeypot can do and the more you can learn from it, the more risk that potentially exists.You will have to determine what is the best relationship of risk to capabilities that exist for you.Honeypots will not solve an oraganization's security problems.Only best practices can do that.However,honeypots may be a tool to help contribute to those best practices.

5. References

1. C. Stoll, "Stalking the Wiley Hacker", Communications of the ACM, Vol. 31 No5. May 1988.
2. B. Cheswick, "An evening with Berferd in which a cracker is lured, endured and studied", Proc Winter USENIX Conference, San Francisco, Jan 20, 1992.
3. S. Bellovin, "There Be Dragons", Proc. of the Third Usenix Security Symphosium, Baltimore MD. Sept. 1992.
4. S. Grundschober, M. Dacier, "Design and Implementation of a Sniffer Detector", Recent Advances on Intrusion Detection Workshop (RAID98), 1998.www.raid-symposium.org/raid98/
5. S. Grundschober, "Sniffer Detector Report", Master Thesis, Eurecom Institute , June 1998, 50 pages, ref. Eurecom : CE-98/IBM/GRUN - Document number: 1914. Available on line: http://www.eurecom.fr/~nsteam/Papers/grundschober98.ps
6. L. Spitzner, "Honeypots: Tracking Hackers". Addislon-Wesley, ISBN from-321-10895-7, 2002.
7. E. Cole. Hackers Beware. New Riders Publishing 2001
8. R.Baumann. "White Paper: Honeypots". February 2002. Available on line: http://security.rbaumann.net/download/whitepaper.pdf
9. R. Baumann, C. Plattern. Honeypots, diploma thesis. Feb. 2002
10. Webservices commercial IT portal http://www.webservices.org/
11. Sourceforge home page: http://honeypots.sourceforge.net/
12. SANS Institute home page: http://ww.sans.org
13. M. Sink, « The Use of Honeypots and packet Sniffers for Intrusion Detection", Indiana University of Pennsylvania, April 2001. Available on line: http://www.lib.iup.edu/comscisec/SANSpapers/msink.htm