RESEARCH ARTICLE OPEN ACCESS

Intrusion Detection Using Honey pots in Network Security

Ahmad Shah[1], Manisha Dhongade[2]

Department of Computer science
BGSB University, Rajouri-185131 –India

Abstract:

Whether you arrange an intrusion detection system (IDS), or you gather and analyse the workstation and device logs on your association, Intrusion detection is a complex business, so it can be both complex and time consuming for identifying malicious traffic in a sea of legitimate commotion. An isolated collection of systems are Honey pots, the primary function of which is to elicit mistreatment from attackers either by the use of real or simulated vulnerabilities or by weaknesses in system configurations, like easily guessed passwords. In order to be able to better understand their attacks they attract attackers and log their movement.

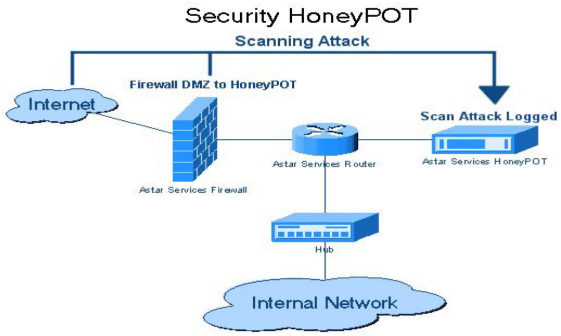
Identifying malicious traffic is dead simple by using honey pots. That's because any transfer to a honey pot, after some initial quick tuning to rule out false positives, is suspicious. To alert its owner if it is touched by using a fake computer asset that exists is called a honey pot. Nobody attempting to log or should be touching it. No analysis is required to tell good traffic from bad, because all activity is illegal.

Keywords — **Honeypot, hacking, security, Types of honeypots, network, intrusion detection (ID).**

1. Introduction

The ultimate goal of security is to reduce or eliminate risks to an organization's critical assets. Ideally, we prefer to do this by preventing attacks, but one of the key mottos of information security is, "Prevention is ideal, but detection is a must. "We must realize that an organization's key resources will be attacked, and we have to be ready to detect the attack as early in the cycle as possible and take advantage of this when it does occur. One way of doing this is with honey-x technology, such as honeypots.

Many of you might be familiar with the terms "honeypots" and "honey nets". While some may see them as a tool strictly for security researchers, when used properly, they can benefit enterprises as well.



2. HONEYPOTS AND THEIR AIMS

In this surrender, we will offer a brief overview of honeypots, common design consideration to take into relation when you are attempting to deploy one on your network, as well as launch you to a couple of their uses

2.1 What is a honeypot?

First of all, a honeypot is a computer method. There are collections, directory in it just like a real computer. However, the aim of the computer is to exert a pull on hackers to fall into it to stare at and follow their behaviour. So we can define it as a fake method which looks like a real system. They are different than other protection systems since they are not only finding one solution to a particular setback, but also they are eligible to apply variety of security problems and finding a number of approaches for them. For example, they can be used to log malicious behavior in a compromise system; they can be also used to learn new threats for users and creating ideas how to get rid of those troubles. We can divide honeypots according to their aims and level of exchanges. If we look at the aims of the honeypots, we will crack honeypots into two broad categories, as define by Snort, two types of honeypots.

2.2 Research honeypots

investigate honeypots are generally used by military, research and government organization. They are capturing a giant amount of information. Their aim is to notice new threats and find out more about the Black hat motives and techniques. The objective is to learn how to care for a system better; they do not bring any direct value to the security of an organization.

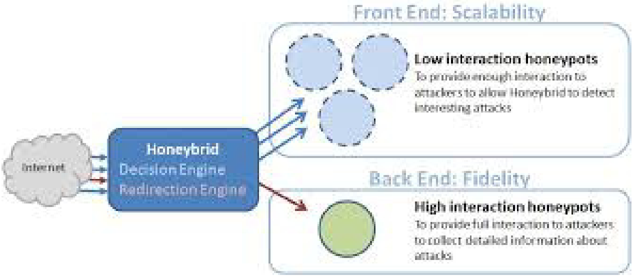
2.3 Production honeypots

creation honeypots are used to look after the company from attacks; they are implemented inside the production network to advance the overall protection. They are capturing a limited amount of information; generally low interaction honeypots are used. Thus, protection administrator watches the hacker's activities carefully and tries to lower the risks that may come from it towards the company. At this point, we will try to discuss and find out the risks of using invention honeypots. Because while testing the security of the systems existing in an organization, unexpected procedures may happen such as misusing other systems via honeypot features. If the network administrator is not aware of this trouble, they put organization in a big trouble.

2.4 Types of Honeypots

Pure honeypots are full-fledged creation systems. The behavior of the attacker are monitored by via a casual tap that has been installed on the honeypot's link to the system. No other software needs just before be installed. Even though a pure honeypot is useful, stealthiest of the defence mechanisms can be ensured by a more prohibited mechanism.

High-interaction honeypots are systems with a actual operating system (OS) (not emulated) that can be totally compromised. The attacker is interacting with a factual system with a complete examination stack. This system is designed to capture exhaustive detail on an attacker's activity on the system. Low-interaction honeypots only suggest portions of a real OS (e.g., the set of connections stack, processes and services), such as emulating an FTP service advertising a vulnerable version of code.


Front End: Scalability
Low interaction honeypots
To provide enough interaction to attackers to allow Honeybrid to detect interesting attacks
Internet
Honeybrid
Decision Engine
Redirection Engine
Back End: Fidelity
High interaction honeypots
To provide full interaction to attackers to collect detailed information about attacks

Low-interaction honeypot is easy to set up and preserve and is generally immune to conciliation by attackers. However, emulation capacity not be sophisticated sufficient and might cause the attacker to bypass the system, thereby rendering the honeypot unsuccessful in such scenarios. If the goal is to capture malware samples targeting specific vulnerable versions of services, a low-interaction honeypot would be sufficient.

2.5 History of Honeypots

In this part, we will give the record of honeypots so far:

1990-1991: It is the primary time that honeypot study released by Clifford Stoll (The Cuckoo's Egg) and Bill Cheswick (An Evening with Berferd).

1997: Deception Toolkit version 0.1 was introduced by Fred Cohen. After Clifford Stoll (The Cuckoo's Egg) and Bill Cheswick (An Evening with Berferd), Deception Toolkit gave an idea of primary honeypot structure.

1998: First commercial honeypot was unconfined which is known as Cyber Cop Sting.

1998: Back Officer Friendly honeypot be introduced. It was free and easy to configure. It is operational under Windows operating system. Most of the citizens tried this software and the concept of honeypot became more and extra known among people.

1999: After Back Officer Friendly, public were extra into this new technology. Honey net project ongoing at this year. Also, Know Your Enemy papers were also unconfined. Thanks to these releases, people understood the aim of the honeypots more.

2000-2001: Honeypots in progress to be used for capturing malicious software from internet and being aware of new terrorization. Companies began to exercise honeypots in their systems to look up protection and see the malicious traffic.

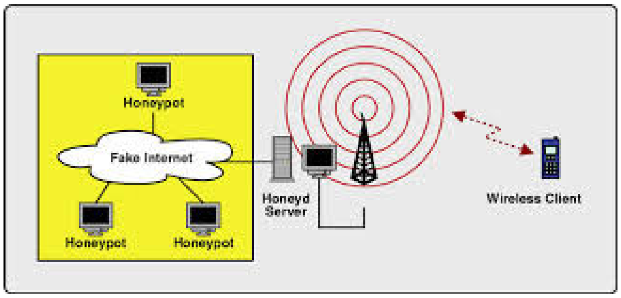
2002: Honeypot concept became all the rage and honeypots superior their functionalities, so they became more helpful and interesting for both researchers and companies.

2.6 Wireless Honeypots

In this part, we looked into a unusual kind of honeypot system which are wireless honeypots. The goal of deploying wireless honeypots is to capture behaviours of our organization in a wireless area and obtain some in sequence and statistics. IEEE 802.11 technology is covered, and also other technology are possible such as Bluetooth. We used Maggi F. & Zanero S., (2008) and Siles R., (2007) thoughts on this part.

3.6.1 Why Wi-Fi Honeypots?

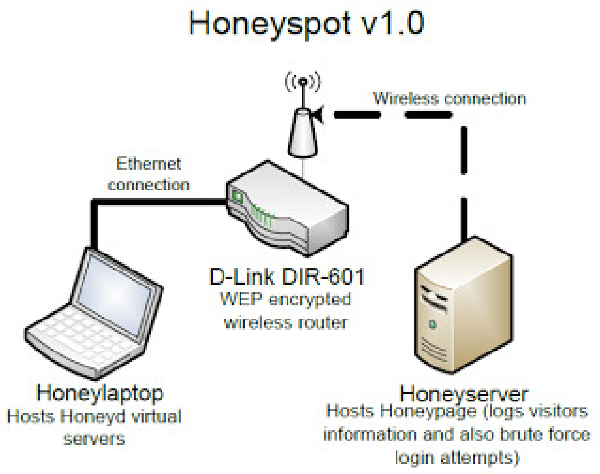
This Wi-Fi structure can be obtained with some right to use points, wired network and some open-to-attack Machines. Wi-Fi honeypots are used to capture unconstitutional traffic, and tries to answer questions if it is possible to catch war driving and hackers which are trying to concession wireless networks.



3.6.2 Wireless Honeypot History

i) First idea of wireless honeypots was unconfined by Kevin Poulsen in 2002. throughout his experiments, he realized that networks are not secure and confined. Intruders are trying to 7 monitor your structure, eavesdropping, hacking your system through your wireless system. Therefore, The Wireless in sequence safety Experiment started the work in 2002 in Washington USA. After that, the leader of this establishment Rob Lee continued the experiments and tried to answer questions related to wireless hacking, and understand the hackers' ideas and tools, especially the logic behind it.

ii) Late 2002, Tenebris organizations in Canada did the monitoring for malicious behavior, and understand that there was a huge malicious interchange going on through the network. They did the experiment use wireless honeypot. After that other experiments followed this proposal in 2003, 2004 and 2005.All the experiments proved that there had been always threats on wireless networks at that moment. Moreover, those kinds of threats still exist today.


Honeyspot v1.0
Wireless connection
Ethernet connection
D-Link DIR-601
WEP encrypted wireless router
Honeylaptop
Hosts Honeyd virtual servers
Honeyserver
Hosts Honeypage (logs visitors information and also brute force login attempts)

iii) In 2004, Laurent Oudot available "Wireless Honeypot Countermeasures" article about wireless honeypots. This article explains the wireless honeypots in feature, its aim and restrictions. In 2006, a new scheme was born named MAP Project. MAP was symbolize the triple suggestion for wireless honeypots: Measure, Analyse and guard. In this project, hacker was permitted to compromise the structure and after that the development members were capturing the malicious activities on the wireless honeypot. However, this project was not superior and it could not answer further questions about wireless honeypots and intruders.

3.6 Advantages of honeypots:

There are many protection solutions available in the market. Anyone can browse the variety of choices through internet and find the most suitable solution for their needs. Here are the reasons why we should choose honeypots:

Honeypots can capture attacks and give in sequence about the attack type and if looked-for, thanks to the logs, it is possible to see extra information about the attack.

New attacks can be seen and new protection solutions can be produced by looking at them.

More examinations can be obtained by looking at the type of the malicious behaviours. It helps to identify with more attacks that may happen.

Honeypots are not bulky in provisions of capturing data. They are only dealing with the incoming malicious traffic. Therefore, the in sequence that has been caught is not as much as the whole traffic. Focusing only on the malicious traffic makes the examination far easier. Therefore, this makes honeypots very helpful.

For the only malicious traffic, there is no need for huge data storage space. There is no need for new technology to maintain. Any computer can be used as a honeypot organization. Thus, it does not cost additional budget to generate such a method.

They are plain to value, to configure and to install. They do not have difficult algorithms. There is no need for updating or change some effects.

As honeypots can capture something malicious, it can also capture new tools for detecting attacks too. It gives more thoughts and deepness of the question proving that it is probable to discover unusual point of views and apply them for our protection solutions.

3.7 Disadvantages of honeypots:

As there are several significant advantages of by means of honeypots, there are also some disadvantages of them as well.

We can only capture data when the hacker is offensive the method actively. If he does not attack the method, it is not possible to catch in sequence. If there is an attack going on in another system, our honeypot will not be able to identify it. So, attacks not towards our honeypot system may dent other system and cause big problems.

There is fingerprinting disadvantage of honeypots. It is easy for an qualified hacker to value if he is attacking a honeypot system or a real system. Fingerprinting allows us to make out between these two. It is a not a wanted result of our testing.

The honeypot may be used as a zombie to reach other systems and conciliation them. This can be very dangerous.

4. LOOKING AT THE SECURITY PROBLEMS CLOSER

At this chapter, we will cover the security problems in honeypots and related issues. We will state the today’s situations and emphasize the solutions based on our experiments throughout the thesis.

4.1 Legal issues with honeypots

4.1.1 Using honeypots are illegal or not?

While deploying and start using a honeypot, present are some legal issues that a person should know about. each country has special laws regarding to honeypot usage and in sequence capturing. These regulations are connected to data security, collection of data and finally how to use honeypots. All these special laws are based on the excellence of the statistics that a honeypot can capture and a individual who is deploying it. In here, the type of the data and its stuffing are significant. It is not easy to say that if using honeypots are banned or not. As we stated before, it depends on the intention and the practice of the information that has been collect. Therefore, there are several steps to think about before doing this job.

4.1.1.1 Privacy

Let us start with privacy issue. As the type of data we are get-together is important, privacy and data leads us to confidentiality term in network security. Our example is being a network supervisor in a corporation. Does he have a right to collect in sequence from other people in the corporation? Consequently, it is the same logic with the hacker. Does the hacker have a right to do so? If we combine both of these situations, then we come up with these: Does honeypot have a correctly to collect in sequence from the hacker and his/her friends? Confidentiality is relative here. As there are more than a few levels of relations honeypots, the information that is gained is also relative. Higher level of communication means more protection risks but more data we can capture.

4.1.1.2 Entrapment

The designation of setup is "a law-enforcement officer" or supervision agent's encouragement of a someone to commend a crime, by means of fraud or undue arguments, in an attempt to later bring a criminal prosecution against that personality."(Spitzner L. (2002) taken from Campbell H.B.) Therefore, honeypot can be setup issue.

4.1.1.3 Civil liability

Civil liability is another official trouble in honeypots. The explanation can be defined with an case in point considering a hacked organism. When a system is hacked, it can be use to hack and misuse other systems. Misused honeypot may transport troubles as it is being used by hacker to contact other systems to hack as well. It should be noted that there is not anything to do with centralized or law in this problem. When that kind of problem occurs, you should consult state which means you should talk about this problem with legal recommend.

4.2 Security risks

As we started our experiment with low communication honeypot Honeyd, we exposed its safety risks. It is somewhat easy to detect Honeyd as a trap method Without configuring our own honeypot with our settings, it is even easier to identify Honeyd. It is because Honeyd is dropping the associations until it cannot deal with them anymore as Maggi F. and Zanero S. (2008) stating. Honeyd is terminating the relationship when SYN put together is not high-quality also. Using this information, any tool which can help to check associations through honeypot can help hackers to understand it is a honeypot method. Intruder will just look at the output of the tool and see dropped associations.

5. INTRUSION DETECTION USING HONEYPOT

Internally, the achievement of the IDS section of protected Direct is very simple. The IDS method runs as a separate TCP server, and listens for client requirements on a specified port.

When a relation is made, the IDS fork a child method when receives the content of the packet, and then checks it against a list of known attacks.

It then returns the effect of this check to the load balancer method, which makes the decision on whether to forward the request to the creation server cluster, or the Honeypot.

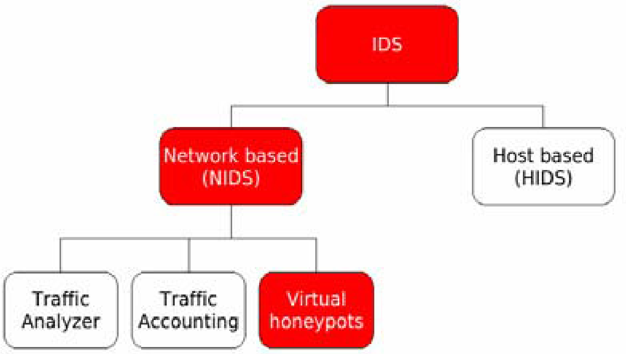


fig: Intrusion Detection System hierarchy 1

The multithreaded propose of the load balance ensures that several requests from a client will not get 'mixed up'; however, it is possible that an assault would occur from a single IP at the same time as a valid application. In this case, the initial, harmless packets may be undamaged forwarded to the real servers until the IDS process finds the attack packet and detects the signs of intrusion. At this point, it directly informs the load balancer development to discontinue forwarding packets to the real server, and to send an RST packet to the resultant server to end the connection. Thus, the server will never receive the attack. In the attacker side, observing silence from the server side causes it to imagine the server has crashed and probably causes it to try to re-connect. However from this point, after detect the infringement, all the incoming traffic from the attacker's IP will be forwarded to the Honeypot.

One of the key points in maintaining speed of this method is that, once an IP is recognized as an Attacker IP, packets coming from that source are not approved to the IDS process any more. The load balancer process directs the incoming travel from attackers to the Honeypot.

6. PRACTICAL IMPLEMENTATION

In this chapter we are present our practical work. We are starting with low communication honeypot and then maintain on a middle level of interaction to to finish conclude with a high level of interaction.

6.1 Starting with low level interaction honeypots: Honeyd

Low interaction honeypots are emulating the services of a real in service system. We started with deploying Honeyd. It is the most well-known low level communication honeypot.

6.2 Continuing with medium level of interaction honeypots: Nepenthes

After deploying Honeyd, we understood how it is operational and examined its problems. Now, we are moving on to medium level of communication honeypots. Medium level of interaction honeypots are frequently used on learning new pressure for the users that is on internet such as worms and new viruses and being aware of them. Nepenthes are residential with Mwcollectd.

6.3 High level of interaction honeypots: Honeywall

Our last experiment will be based on high level of communication honeypots. As we examined two types of interface honeypots, we will move on further on implementation. Now, with high level of interaction honeypots, we will realize more on honeypots and with real in commission system we will be able to catch more helpful and interesting findings. Hackers will be freer with a real system without restrictions. realization will be time consuming and convoluted.

7. FUTURE WORK:

Honeypots are a new field in the sector of system security. Currently there is a lot of ongoing research and negotiations all more or less the world. more than a few companies have already launched commercial products. A comparison of available harvest showed that there are some usable low- to elevated involvement honeypots on the market. In the sector of research honeypots, self-made solutions have to be residential as only these solutions can provide a certain amount of freedom and elasticity which is needed to cover a wide range of possible attacks and attackers. every research honeypot usually has its own goals or unusual emphasis on the question. Developing a self-made explanation needs a good technical understanding as well as a time intensive improvement phase.

8. CONCLUSION

As with any technology, there is no great solution. A honeypot can grant value to an organization if it is deployed correctly. However, it can also cause a decrease in an organization's defense by being more attractive to worms or attacks. Therefore, an association must clearly define the risks it wants to condense with a honeypot and the rations for accomplishing this. Then, any operation can be tested to make sure it benefits the association.

Network safety is not a path many students are pleasing but we see it as one of the most significant topics when we speak about computing. We were curious about this subject and certain to write this on that field. New threats are revealed every day and the best way to stay confined is to always stay up to date. By doing this simple task, most attacks will not have any outcome on the method. The problem nowadays is that people using pirated version of an working system are causal to botnets. Their system does not support critical updates and they are more sensitive to automated attacks. currently, the implementation and growth of honeypots are under control by network safety expert. The weakness of this system is that it is not backed up by a clear legislation. Most of the work in the future should be about humanizing the laws about honeypots. The current laws about honeypots in most of the country are not clear. There is a gap between the lawyers and the IT professionals. They should learn to collaborate with each other in order to clarify the legislation and give a clear retort about the legality of this technology. A lot of work should be done in the future to develop this situation. On a procedural aspect, the main obscurity is to keep up with the new attacks. These days, it is not hard to detect a honeypot coordination; most of the work should focus on making this machinery stealthier.

REFERENCES

[1] Anand Sastry: http://searchsecurity.techtarget.com/tip/Honeypots-for-network-security

[2] http://www.diva-portal.org/

[3] The Honeynet Project. Know Your Enemy : Honeynets (May 2005) http://www.honeynet .org/papers/honeynet/.

[4]http://www.infoworld.com/article/2624430/intrusion-detection/intrusion-detection-honeypots-simplify-network

[5] http://www.sans.edu/research/security-laboratory/article/honeypots-guide

[6]https://en.wikipedia.org/wiki/Honeypot_(computing)