International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015
ISSN 2229-5518

Second Generation: - Approach and Futures of Honeypots

Surendranadh Koundinya
M.Tech Student
SHOBHIT UNIVERSITY

Pankaj Kumar
System Administrator
SHOBHIT UNIVERSITY, MEERUT

Bambam kumar
M.Tech Student
SHOBHIT UNIVERSITY, MEERUT

ABSTRACT

Now a day's information security is increasing day by day. Intruders probe and attempt to gain access to your systems. 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. In this paper we
discuss different kinds of honeypots and approaches.

Keywords

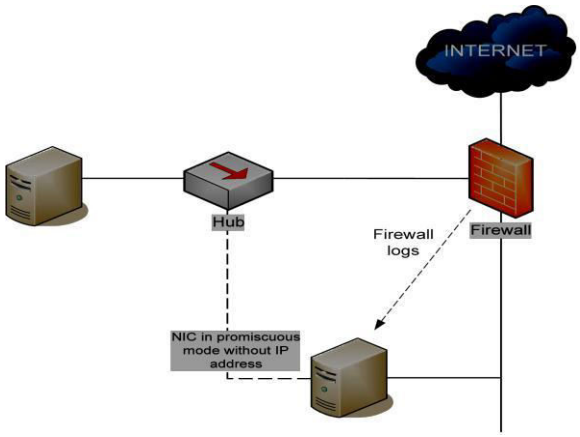
Honeypot,network security,IDS,types of honeypots,Virtual Machine. Kernel

1.Introduction

Honeypots are any security resource whose value lies in being probed, attacked, or compromised. They can be real operating systems or virtual environments mimicking production systems. Honeypots are often the best computer security defense tool for the job. They can be used as an adjunct tool and to log and prevent hacking.

Honeypots are currently in the second formal stage of development, known as GenII. GenII honeypots use inline IDSs to change outgoing malicious packets into harmless traffic and use keystroke logging software built into the kernel. Hacking attacks can be manual, automated, or blended.

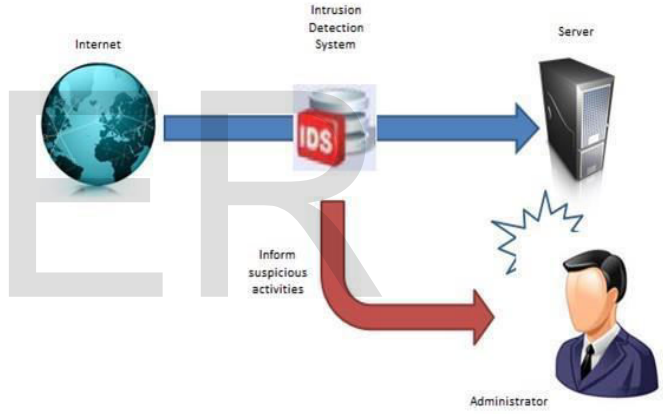
Honeypots are not "install and forget it" systems. There are several steps you can take to minimize the legal risks from using a honeypot. Honeypots can be classified according to their usage Production honeypots are usually deployed within organizations with the main purpose of decreasing the overall risk. As the main role of production honeypots is in detecting malicious activities and alerting the security administrator, they are simpler to setup as in this case the interaction with the attacker can be low level. Services that these honeypots offer are usually simulated as they should only lure the attackers into thinking that they are trying to compromise a real, production machine. In this setup, the honeypot administrator has only limited possibilities to analyze attackers' behavior and activities, which will be restricted due to the fact that the service is simulated; however, as the main purpose is just to detect potential threats, this will be sufficient



1.1 Related Work

In this research paper how honeypots are created and deployed in the virtual machine .Honeypots is an educational tool for CS & IT students 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 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

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



2. Different types of Honeypots

Honeypot are describe on the basis of their purpose i.e.:- Honeytokens, production and research

Level of interaction i.e.:-Low, medium and high

2.1 Purpose of Honeypots

(i).Honey tokens
(ii).Production
(ii)Research

2.1.1 Honey tokens

The term "honey Token" was introduced in 2003 by Augusto Paes It is fake digital entry that can have many different applications.

He idea is similar to that of a honeypot, which he defines as "an information system resource whose value lies in unauthorized or illicit use of that resource". Rather than having a computer that's designed to be broken into, however, you have say, a record in a database or a file has no legitimate use; ergo, if anyone uses it, it must be illegitimate Honeypots tell you who's attacking. But to catch individuals Honey tokens contain digital data created and monitored solely as indicators of digital theft. They can be real data containing a "marker" -- fake data that simply doesn't exist in the real world, at least within a given enterprise

2.1.2 Production

They are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do.

2.1.3 Research Honeypot

They are run to gather information about the motives and tactics of the Black hat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats.Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

How honey tokens Work?

A honey token is just like a honeypot, you put it out there and no one should interact with it. Another example is bogus Social Security or credit card numbers. We have read numerous stories of large databases compromised, with thousands of SSNs or millions of credit card numbers compromised. Even worse, often these compromises are not detected for weeks if not months later. This gives attackers extensive amounts of time to use or sell the information. Honey tokens can once again be used to simplify this problem. Bogus numbers can be embedded in a database. If the numbers are accessed, you know someone is violating system security. A university could put SSN honey tokens in their student database. If someone attempted to steal the entire database (as has happened at several universities) the attackers would also be grabbing the honey tokens mixed with the valid SSNs. The same could be done for credit card numbers embedded into a vendor's on-line ecommerce site. These honey tokens would be unique numbers, so attackers would not know what the honey token was and what valid numbers were. Databases could watch for whenever someone attempted to access the records and generate an alert. Or, IDS sensors could be configured to watch the local networks. If these honey token numbers are detected on the wire, then the databases have most likely been compromised.

For example, the credit card number 4356974837584710 could be embedded into database, file server, or some other type of repository. The number is unique enough that there will be minimal, if any, false positives. An IDS signature, such as Snort, could be used to detect when that honey token is accessed. Such a simple signature could look as follows.

```
alert ip any any -> any any (msg:"Honeytoken Access - Potential Unauthorized Activity";
```

3. Level of interaction

(i) Low Level of interaction
(ii) Medium Level of interaction
(iii) High Level of interaction

3.1.1 Low Level of interaction

We already know that low-interaction honeypots do not provide a complete operating system environment to adversaries. So, clearly, one way to detect them is the fact they cannot be broken into or that they do not provide interesting or complicated services. For low-interaction honeypots, it is also possible to create configurations that are completely unrealistic, such as running a Windows web server and a Unix FTP server. However, low-interaction honeypots are most often used as network sensors and not really meant to withstand targeted attempts at detecting them.

The main level of interaction with a low-interaction honeypot is via the network. In practice, this means that there is a physical machine with a real operating system in which the low-interaction honeypot is running. Resources are shared by the operating system between all processes that run on it. If we can find a way to take resources away from the honeypot process, we will notice that the honeypots are slowing down or have higher response latencies than before. If we could log into the operating system, we could start a CPU-intensive process to create this effect. However, as we usually don't have this level of access, we have to find ways to create the extra load via the network. For example, if the low-interaction honeypot system was collocated with a web server, expensive HTTP requests to the web server could slow down the low-interaction honeypots.

A very simple experiment to demonstrate this interaction is the following. Machine A runs the Net BSD operating system at IP address 192.168.1.10. On A, we deploy Honeyed to create a low-interaction virtual honeypot B at IP address 192.168.1.90. We run two different measurements. The first measurement uses the ping tool to send 100 ICMP ping requests to B.

```
$ ping -c 100 192.168.1.90| tee ping.noload PING 192.168.1.90 (192.168.1.90): 56 data bytes 64 bytes from 192.168.1.90: icmp_seq=0 ttl=255 time=0.443 ms
64 bytes from 192.168.1.90: icmp_seq=1 ttl=255 time=0.430 ms
64 bytes from 192.168.1.90: icmp_seq=2 ttl=255 time=0.434 ms
64 bytes from 192.168.1.90: icmp_seq=3 ttl=255 time=0.421 ms
...
```

3.1.2 Medium Level of interaction

Medium-interaction honeypots are slightly more sophisticated than low interaction honeypots, but less sophisticated than high interaction honeypots 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 some examples of medium-interaction honeypots include collect, nepenthes and honey trap. Collect and nepenthes can be used to collect autonomously spreading malware These daemons can log automated attacks, and extract information on how to obtain the malware binaries so that they can automatically download the malware. Honey trap dynamically

Creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks.

3.1.3 High Level of interaction

These are the most advanced honeypots. They are the most Complex and time-consuming to design, and involve the highest Amount of risk because they involve an actual operating system The goal of a high-interaction honeypot is to Provide the attacker with a real operating system to interact with, where nothing is simulated or restricted .The possibilities for collecting large amounts of information are therefore greater with this type of honeypot, as all actions can be logged and analyzed. Because the attacker has more resources at his disposal, a high interaction honeypot should be constantly monitored to ensure that it does not become a danger or a security hole honey net is an example of a high-interaction honeypot, and it is typically used for research purposes.

4. Legal Issues and Challenges

Honeypots are a new and emerging technology for the security community. Many security professionals are just now beginning to understand what honeypots are, their different types, how they work, and their value. As with many new technologies, not only are the professionals attempting to learn about them but so is the legal community. As honeypots and their concepts have grown more popular, people have begun to ask what legal issues could apply. The purpose of this paper is to address the most commonly asked issues. The concepts covered here will be focusing on US statutes, not international, mainly because I'm only familiar with US law. However, these concepts most likely also play some role in the international community. Also, this paper assumes you are familiar with the definition of a honeypot. If you are new to honeypots

4.1 Precedents

In the past there has been some confusion on what are the legal issues with honeypots. There are several reasons for this. First, honeypots are relatively new. If security professionals are still learning about them, how do you think the legal community feels? Second, honeypots come in many different shapes and sizes and accomplish different goals. We will attempt to identify the different uses of honeypots and how they apply to legal issues. Last, there are no precedents for honeypots. There are no legal cases recorded on the issues. The law in the US is developed through cases. Without cases directly on point, we are left trying to predict, based on cases in other contexts, how courts will treat honeypots. Until a judge gives a court order, we will really never know.

4.2 Entrapment

Honeypots are not a form of entrapment. For some reason, many people have this misconception that if they deploy honeypots, they can be prosecuted for entrapping the bad guys. Nothing could be further from the truth. Entrapment, by definition is "a law-enforcement officers or government agent's inducement of a person to commit a crime, by means of fraud or undue persuasion, in an attempt to later bring a criminal prosecution against that person."

What this means is that entrapment can only be used as a defense to avoid a conviction. You will not be prosecuted for 'entrapment.' Rather, entrapment is a defense to a criminal prosecution. Second, you have to be law enforcement, or an agent of law enforcement, and prosecute the attacker before entrapment becomes an issue. If you are not law enforcement or not an agent of the law, and you do not intend on prosecuting, then entrapment is not an issue. Last, even if you are law enforcement, and even if you do want to prosecute the attacker, honeypots still are most likely not a form of entrapment. Entrapment is when you coerce or induce someone to do something they would not normally do. Honeypots do not induce anyone. Attackers find and break into honeypots on their own initiative.

4.3 Privacy

The first challenge we run into is there is no single statute that covers privacy. Instead there are many different legal statues, including the Federal Wiretap Act and the Electronic Communication Privacy Act. To make the issue of privacy more challenging, which legal statutes do you apply? In the United States, often state law concerning privacy can supplement Federal law, as it is in the state of California. So if your honeypot is in Chicago, but the attacker is coming in from California, which privacy laws apply, Illinois, California, or Federal? To make matters even worse, what happens if the attacker(s) are coming from different countries, or bouncing through different countries? When different countries are involved, which privacy statutes do you apply? As you can see, things become exponentially confusing. Of all the privacy statutes, the one that most likely applies to honeypots deployed in the US is the Federal Wiretap Act. Under the Federal Wiretap Act it is illegal to capture the communications of an individual in real time without their knowledge or permission, as this violates their privacy. To determine if a honeypot does violate an individual's privacy, there are two major factors: what the honeypot is being used for and how much information it is collecting. These two factors influence the privacy legal implications.

5 .Advantages, Disadvantages and Risk

All traffic to a honeypot is deemed suspicious because it is designed so that it still has to be accessed using a near obvious "hole". Honeypots are generally based on a real server and operating system and with data that gives the impression of being real. The difference from real servers is its location, it is located in the DMZ (De-Militarized Zone: outside firewall but still accessible by internal computers) of a network. This ensures that the internal network is not exposed to the intruder. It should be placed close to the production servers in order to tempt intruders that are targeting them. The use of port redirection on an upstream router or firewall will give the impression that services are on the production server. This router will have to be capable of redirection and also have the ability to transparently handle the address translation of the honeypot so as to conceal its true IP. A good example of such use is an attempt to run a web server or telnet on a production server that normally does not accept such requests. Such connection requests could be then redirected to the honeypot, which will simulate response for the request

5.1 Advantages

The advantages of a honeypot outweigh the disadvantages is really specific to the designer. This is so because every individual has different resources and needs. The following is some of the advantages of setting up a honeypot. Firstly, one can learn about incident response; setting up a system that intruders can break into will provide knowledge on detecting hacker break-ins and cleaning-up after them. Secondly, knowledge of hacking techniques can protect the real system from similar attacks. Thirdly, the honeypot can be used as an early warning system; setting it up will alert administrators of any hostile intent long before the real system gets compromised. Another advantage of honeypots is its ability to deceive intruders easily. For example, the honeypot can be made to provide a banner that looks like a system that can easily be attacked. The banner may be a version of software where there is a well-known security flaw.

5.2 Disadvantages

The disadvantages of the system are as follows. First and foremost is that the honeypot may be used as a stepping stone to further compromise the network, may it be the user own internal network or some network on the internet. Secondly, honeypots add complexity to the network. Increased complexity may lead to increased exposure to exploits. Another disadvantage is that honeypots must be maintained just like any other networking equipment and services. Maintenance not only requires that the

system be shut off but also requires just as much use of resources as a real system. Lastly, building a honeypot requires that you have at least a whole system dedicated to it, and this may be an expensive resource for some corporations.

5.3 Risk

The third disadvantage of honeypots is risk: They can introduce risk to your environment. By risk, we mean that a honeypot, once attacked, can be used to attack, infiltrate, or harm other systems or organizations. 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. The simpler the honeypot, the less the risk. For example, a honeypot that merely emulates a few services is difficult to compromise and use to attack other systems. In contrast, a honeypot that creates a jail gives an attacker an actual operating system with which to interact. An attacker might be able to break out of such a cage and then use the honeypot to launch passive or active attacks against other systems or organizations. Risk is variable, depending on how one builds and deploys the honeypot.

Because of their disadvantages, honeypots cannot replace other security mechanisms such as firewalls and intrusion detection systems. Rather, they add value by working with existing security mechanisms. They play a part in your overall defenses.

5 .Conclusions

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.

Honeypots are a young and interesting solution for addressing today's security problems.Honeytokens are an interesting and viable way to detect insider threats Important is the right design which fits to a given environment, otherwise these solutions are pretty useless. These technologies alone won't help, important is the right mix with other technologies like IDS and Firewalls Information security isn't a question of ROI, more important is the ROSI aspect and a overall ESM solution and what could happen without suitable security solutions

No set of techniques will completely protect an address posted on the Internet from a resourceful spammer. Even with these techniques in place, you should still consider only posting alternative addresses that may be compromised. Whenever possible, keep your primary address off publically accessible websites entirely.

Honeypots do have their drawbacks. Because they only track and capture activity that directly interacts with them, they cannot detect attacks against other systems in the network. Furthermore, deploying honeypots without enough planning and consideration may introduce more risks to an existing network, because honeypots are designed to be exploited, and there is always a risk of them being taken over by attackers, using them as a stepping-stone to gain entry to other systems within the network. This is perhaps the most controversial drawback of honeypots.

Because honeypots only capture and archive data and requests coming in to them, they do not add extra burden to existing network bandwidth.

Acronyms

IDS Intrusion Detection System
DTK Deception Toolkit
ADS Anomaly Detection Systems
IDE Integrated Development Environment
FTP File Transfer Protocol
DOS Denial of Service [attack]

References:-

1.Martin, W.W. Honeypots and Honey nets – Security through Deception. http://www.sans.org/reading_room/whitepapers/attacking/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room.

2 Provo's, N. Honeypot Background. http://www.honeyd.org/background.php.

3. Spitzner,, L. The Honey net Project: Trapping the Hackers. *IEEE Security & Privacy*, *1* (2). 15-23.

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

5. Spritzer, L. Honey tokens: The Other Honeypot. http://www.securityfocus.com/infocus/1713, Security Focus, 2003.

6. Spitzner, L. Open Source Honeypots: Learning with Honeyed, Security Focus, 2003.

7. Spitzner, L. The Value of Honeypots, Part One: Definitions and Values of Honeypots, Security Focus,