HONEYPOTS DEPLOYMENT STRATEGIES AND LEGAL ISSUES

[1]Gagandeep Singh, [2]Pardeep kaur
[1]Deptt of Computer Science and IT, Lyallpur Khalsa College ,Jalandhar(India)
[2]Deptt of Computer Science and IT, DoabaCollege ,Jalandhar(India)

ABSTRACT

Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods involves the use of honeypots. A honeypot is a security resource whose value lies in being probed, attacked or compromised. In this paper we present an overview of honeypots and provide a starting point for persons who are interested in this technology. We examine different kinds of honeypots, honeypot concepts, and approaches to their implementation.

Keywords: ***Honeypots, Modes Of Honeypots, Deployment Strategies,And Legal Issues***

I. INTRODUCTION

Network IDS:An IDS (Intrusion Detection System) detects unwanted manipulation to the computer network in a network. An intrusion detection system is used to detect

all types of malicious network traffic and computer usage like network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malwares.

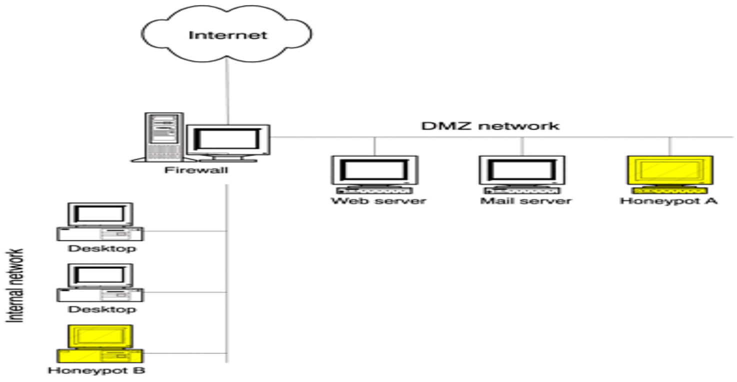
II. DEFINITION

It is a security resource used to detect, deflect or counter attacks attempts at unauthorized use of information system. It consist of a computer ,data or a network site that seems to be a part of network but actually it is not .It is an isolated ,protected and monitored terminal which seems to have valuable information for the attackers.

Honeypots can be defined in three layered networks:

- Prevention:Honeypots can be used to slow down or stop automated attacks
- Detection:It is used to detect unauthorized activity and capture unknown attacks. Generate very few alerts, but when they do you can almost be sure that something malicious has happened.
- Response:Production honeypots can be used to respond to an attack. Information gathered from the attacked system can be used to respond to the break-in.

Honeypot in a real network environment:



III. MODES OF HONEYPOT

3.1 Research mode: In this mode the Honeypot characterizes attack environment by collecting data on attacker motivations, attack trends and emerging threats.

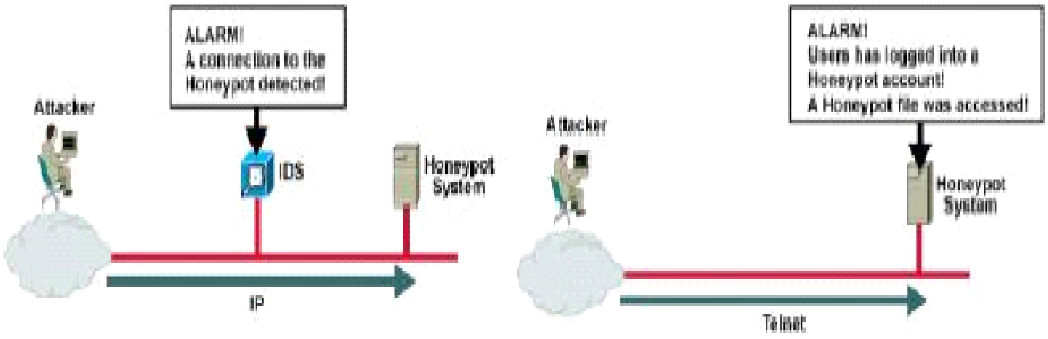
3.2 Production mode: The Honeypot is used to prevent, detect and respond to attacks. Prevention is accomplished through deterrence i.e. by impending scans initiated by attackers and diverting an attacker to interact with the Honeypot rather than critical files.

On the basis of level of interaction Honeypots are classified as:

- Low-Interaction Honeypots: Honeyd
- High Interaction Honeypots: HoneyNet

3.3 Honeyd:

Honeyd is an open-source solution which was created and maintained by NielsProvos. The primary purpose of Honeyd is intrusion detection; it does this by monitoring all the unused IPs in a network.


ALARM!
A connection to the Honeypot detected!
Attacker
IDS
Honeypot System
IP
ALARM!
Users has logged into a Honeypot account!
A Honeypot file was accessed!
Attacker
Honeypot System
Telnet

Any attempted connection to an unused IP address is assumed to be unauthorized or malicious activity. After all, if there is no system using that IP, why is someone or something attempting to connect to it? For example, if your network has a class C address, it is unlikely that every one of those 254 IP addresses is being used. Any connection attempted to one of those unused IP addresses is most likely a threat to the network.

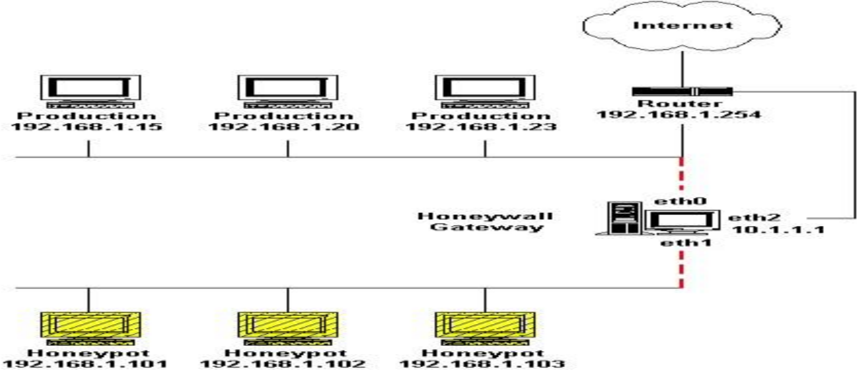
Honeyd can monitor all of these unused IPs at the same time. Whenever a connection is attempted to one of them, Honeyd automatically assumes the identity of the unused IP addresses and then interacts with the attacker. Honeyd can detect any activity on any UDP or TCP port, as well as some ICMP activity. The user doesn’t have to create a service or port listener on ports he wants to detect connections to, Honeyd does this all.

3.4 HoneyNet:

It is a high-interaction honeypot designed to capture extensive information on threats. High-interaction means a honeynet provides real systems, applications, and services for attackers to interact with, as opposed to low-interaction honeypots such as Honeyd which provide emulated services and operating systems. What makes a honeynet different from most honeypot is that it is a network of real computers for attackers to interact with. Conceptually honeynets are very simple; they are a network that contains one or more honeypots. Since honeypots are not production systems, the honeynet itself has no production activity, no authorized services. As a result, any interaction with a honeynet implies malicious or unauthorized activity. Any connections initiated inbound to your honeynet is most likely a threat. This makes analyzing activity within your honeynet very simple. With traditional security technologies, such as firewall logs or IDS sensors, you have to sift through gigabytes of data. A great deal of time and effort is spent looking through this information, attempting to eliminate false positives while identifying attacks or unauthorized activity.

IV. HONEYNET ARCHITECTURE

To successfully deploy a honeynet, you must correctly deploy the honeynet architecture. The key to the honeynet architecture is what we call a honeywall. This is a gateway device that separates your honeypots from the rest of the world. Any traffic going to or from the honeypots must go through the honeywall. This gateway is traditionally a layer 2 bridging device, meaning the device should be invisible to anyone interacting with the honeypots. Below we see a diagram of this architecture. Our honeywall has 3 interfaces. The first 2 interfaces (eth0 and eth1) are what separate our honeypots from everything else; these are bridged interfaces that have no IP stack. The 3rd interface (eth2, which is optional) has an IP stack allowing for remote administration.



There are several key requirements that a honeywall must implement; Data Control, Data Capture, Data Analysis, Data Collection.

1) **Data Control:** Our aim is to prevent the data from an attacker once he has entered the network.
2) **Data Capture:** is the monitoring and logging of all of the threat's activities within the honeynet.
3) **Data Analysis:** A honeynet is worthless if we have no means to analyze the data collected. Every organization has different means to apply this.
4) **Data Collection:** This only applies to organizations with multiple honeynets as it is necessary to collect data from all the sources.

V. WEB APPLICATION HONEYPOTS

Smart applications stay ahead by detecting attacks directed at them.Honeypots are sacrificial systems that we use to trap intruders. They were invented in the early 90s to study attackers in the real world. Dummy, unsecured systems were secretly placed on the web, and attackers were not stopped from breaking in. Once attackers broke in, however, their activity was monitored closely. That gave us a wealth of information about black hats during the last decade.

Honeypots are great for intrusion detection. They can be deployed on unused IP addresses in production networks. Since the honeypot has no legitimate purpose, any traffic to the honeypot is suspicious and signals the presence of an attacker. An intruder who triggers the honeypot can be tracked closely. Unlike traditional detection systems that had to spot attacks from the flood of normal traffic, all traffic honeypots receive are illegitimate.

We can adapt honeypots for web applications, lay traps that snare the attacker and give us an advantage. Let’s look at three strategies for web application honeypots:

- **Honeytokens:** Honeytokens are fake records that are inserted in the database. These fake records are not expected to be used by normal users. If any of these honeytokens are used, they alert us of the database having been compromised. An example of honeytokens are fake username/passwords in the user database. These users do not exist in the real world, and hence are not expected to be logging in to the application. If the application sees these credentials being used, it immediately recognizes that the user database has been compromised.
- **Honeypages:** These are obscure web pages sprinkled in the web site. They have no legitimate purpose, nay they are not even linked from any valid page. Normal users would never reach these pages. However, we drop hints about these pages by embedding their url as comments or hidden fields in valid pages. While normal users would never see this, an attacker who analyzes the source code, or a vulnerability scanner that spiders the site would see these and follow the link. When the page is accessed, it points us to the intruder.
- **Dummy domains:** A variant of honeypages use dummy domains that are published in the DNS. These domains do not have legitimate sites hosted on them, nor do they have URLs pointing to them. Any queries for these dummy domains indicate reconnaissance activity of intruders as they hunt for applications we host. This can give us an early warning of activity targeted at our sites.

VI. HONEYPOTDEPLOYMENT STRATEGIES

To maximise the strengths of honeypots, and minimise the risks involved, deployment should be carefully planned. The following is a set of common honeypot deployment strategies:

1. Install honeypots alongside regular production servers. The honeypot will likely need to mirror some real data and services from the production servers in order to attract attackers. The security of the honeypot can be loosened slightly so as to increase its chance of being compromised. The honeypot can then collect attackrelated information. However, if a successful attack takes place on the honeypot within the network, that compromised honeypot machine might be used to scan for other potential targets in the network. This is the main drawback of installing honeypots within the production system. In other honeypot deployment methods, this would not happen, as the whole honeynet can itself be a fictitious network.

2. Pair each server with a honeypot, and direct suspicious traffic destined for the server to the honeypot. For instance, traffic at TCP port 80 can be directed to a web server IP address as normal, while all other traffic to the web server will be directed towards the honeypot. To camouflage the honeypot, a certain amount of data, such as the website contents of a web server, may need to be replicated on the honeypot.

3. Build a honeynet, which is a network of honeypots that imitate and replicate an actual or fictitious network. This will appear to attackers as if many different types of applications are available on several different platforms. A honeynet offers an early warning system against attacks and provides an excellent way to analyse and understand an attacker’s intention, by looking at what kind of machines and Honeypot Security services have been attacked, and what type of attacks have been conducted..

VII. LEGAL ISSUES WITH HONEYPOTS

7.1 Using honeypots are illegal or not?

While deploying and start using a honeypot, there are some legal issues that a person should know about. Every country has different laws regarding to honeypot usage and information capturing. These regulations are related to data security, collection of data and finally how to use honeypots. All these different laws are based on the quality of the data that a honeypot can capture and a person who is deploying it. In here, the type of the data and its contents are significant. It is not easy to say that if using honeypots are illegal or not. As we stated before, it depends on the intention and the usage of the information that has been collected. Therefore, there are several steps to think about before doing this job. There are also several questions and approaches that you should ask yourself during the experiment. If it is for a company that you are deploying a honeypot rather than a homemade honeypot to use it at home, then as a network administrator you have other responsibilities as well. First thing is to think about the country laws regarding to these, and then company laws. Maybe the country is allowing you to experiment some things but what happens if there is a restriction on it in your company? Before taking any serious action, you should ask those questions to the responsible people to make sure that you are doing something without violating the laws of your country. We will look into three main legal issues now, which are privacy, entrapment and civil liability.

7.2 Privacy

Let us start with privacy issue. As the type of data we are gathering is important, privacy and data leads us to confidentiality term in network security. Our example is being a network administrator in a company. Does he have a right to collect information from other employees in the company? Accordingly, 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 right to collect information from the hacker and his/her friends?

Privacy is relative here. As there are several levels of interactions honeypots, the information that is gained is also relative. Higher level of interaction means more security risks but more data we can capture. The question is how much data can we take from the honeypot while not breaking the laws at the same time? Lance Spitzner (2001) is referring some useful points that is from the Department of Justice, mostly Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Here they are:

"The people breaking into these systems are NOT AUTHORIZED to use them, and if they place any files on them (when they have no legitimate accounts or use privileges), they have given up their privacy rights to that data by placing it on the honeypot.

- By using honeypots for communication, they have given up their right to privacy in that communication. Honeypots generally do not provide public accounts; therefore, they are not a service provider and are not bound by privacy requirements designed for service providers.
- Most organizations are not law enforcement, nor do they act under the control of law enforcement, so they are not bound by the evidence collection restrictions otherwise placed on law enforcement and their agents. Think about it, a honeypot is collecting the same information, in the same technical manner, as many of your other security devices are (system logs, IDS sensors, etc.)."
- Based on US constitutions, there are four main laws considering privacy on data communications. These four will be discussed in details under different laws in different countries US regulations part.

7.3 Entrapment

The definition of entrapment is "a law-enforcement officer" 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."(Spitzner L.(2002) taken from Campbell H.B.) Therefore, honeypot can be entrapment issue.

This issue is debatable as the concept of honeypots are new, there are not certain issues decided yet. There are also other aspects concerning entrapment issue of honeypots. According to Lance Spitzner's The Value of Honeypots, Part Two: Honeypot Solutions and Legal Issues article, honeypots cannot be entrapment issue. Here are his three reasons why entrapment is not an issue for honeypots:

- "Honeypots do not induce or persuade anyone, they are most often production systems, or emulate production systems.
- Attackers find and attack honeypots based on their own initiative.

- Most administrators are not law enforcement. They are not using honeypots to collect evidence and prosecute. Normally they are used as a means to detect, and possibly learn about, attacks."

7.4 Civil liability

Civil liability is another legal problem in honeypots. The explanation can be defined with an example considering a hacked system. When a system is hacked, it can be used to hack and misuse other systems. Misused honeypot may bring problems as it is being used by hacker to reach other systems to hack as well. It should be noted that there is nothing to do with federal or law in this issue. When that kind of problem occurs, you should consult state which means you should talk about this problem with legal counsel.

VIII. 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.

Honeypots are a relatively new technology that is becoming increasingly popular, and will become even more so as commercial solutions become available that are easy to use and administer. Because they can be used to collect information on attackers and other threats, we believe they can prove a useful tool in digital forensics investigation

REFERENCES

[1]Know Your Enemy: Honeynets. http://www.honeynet.org/papers/kye.html.

[2] SANS Instiitute GIAC Certification GSEC Assignment#1.4: Honey Pots-Strategic Considerations, 2002.

[3] Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).

[4] Baumann, R. and Plattner, C. White Paper: Honeypots, Swiss Federal Institute of Technology, Zurich, 2002.

[5] Gubbels, K. Hands in the Honeypot GIAC Security Essentials Certification (GSEC), 2002.