International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-1 Issue-2, June 2012

Use of Honeypots to Increase Awareness regarding Network Security

Bhumika, Vivek Sharma

Abstract: ***Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. Honeypots are a relatively new technique for achieving network security. While other techniques for securing networks e.g. IDS, Firewall etc are made to keep the attackers out, for the first time in the history of network security there is a technique which intends to keep the attackers 'in' thus allowing the researchers to gain more insight into the workings of an attacker. With the rapid development of Internet and the advent of the network socialization, network security has been more concerned in the technologies. Among the main network security technologies are firewall, intrusion detection techniques, access control, etc., which are based on the known facts and attack mode and adopt passive defensive approach. The current commonly-used intrusion detection technology of passive defense, based on model matching, needs to update the intrusion detection rule library, otherwise omission of the latest attack will occur in the process. To eliminate the shortcomings of detection system being unable to update feature library, the users should adopt a proactive defense honeypot technology to automatically update its att ack signature to reduce the miss probability of int rusion detection system. Honeypot is a newly-developing area of network security. It lures the intruder to attack it by constructing a system with security vulnerability and then record the intrusion methods, motives, and tools of the intruder in the intruding process. By analyzing the intrusion information, we can get the content of the newest techniques of the intruder and find the system vulnerability. And the virtual honeypot can prevent the host computer from attacking.***

Index Terms: Honeypots, Honeyd, Honeynets, IDS, Network Security

I. INTRODUCTION

Almost all security technologies being used today are made to keep the bad guys out. For example firewalls are made to keep systems secure by keeping bad guys from outside out of the network and keeping internal bad guys reaching out of the network, similarly IDS are designed to keep harmful attacks out of network/system.

Revised Manuscript Received on 30 June 2012.
* Correspondence Author
Bhumika*, Department of CSE., Kurukshetra University, India.
Vivek Sharma, Department of CSE., Kurukshetra University, India.

However, honeypot is a technology which is designed specifically to make the bad guys come inside the network so that their behavior can be studied and which will be used to further strengthen systems. Thus one can say that firewalls and IDS used defensive security whereas honeypots work as offensive security measure.

They entice the bad guys to attack the system in order to study them.The exact definition of a honeypot is contentious, however most definitions are some form of the following:

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

What this definition means is honeypots derive their value from threats using them. If the enemy does not interact or use the honeypot, then it has little value. This is very different from most security mechanisms. For example, the last thing one wants an attacker to do is interact with the firewall, IDS sensor, or PKI certificate authority..

II. HONEYPOTS: AN OFFENSIVE SECURITY MEASURE

A more practical, but more limiting, definition of Honeypot is given by pcmag.com:

A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server doing work, but all the data and transactions are phony. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system.

In practice, honeypots are computers which masquerade as unprotected. The honeypot records all actions and interactions with users. Since honeypots don't provide any legitimate services, all activity is unauthorized (and possibly malicious). Honeypots are analogous to the use of wet cement for detecting human intruders.[1]

In practice, honeypots are computers which masquerade as unprotected. The honeypot records all actions and interactions with users. Since honeypots don't provide any legitimate services, all activity is unauthorized (and possibly malicious). Honeypots are analogous to the use of wet cement for detecting human intruders.[2] First, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that has many applications to security. They can be used everything from slowing down or stopping automated attacks, capturing new exploits to gathering intelligence on

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

emerging threats or early warning and prediction. Second, honeypots come in many different shapes and sizes. They can be everything from a Windows program that emulates common services, such as the Windows honeypot KFSensor3, to entire networks of real computers to be attacked, such as Honeynets. In fact, honeypots don't even have to be a computer, instead they can be a credit card number, Excel spread sheet, or login and password (commonly called honeytokens)

All honeypots share the concept; they are a resource or entity with no production value. By definition, a honeypot should not see any activity. Anything or anyone interacting with the honeypot is an anomaly, it should not be happening. Most likely, it implies an unauthorized or malicious activity. For example, a honeypot could be nothing more than a webserver deployed in a DMZ network. The webserver is not used for production purposes, its does not even have an entry in DNS, its merely physically located with other webservers.

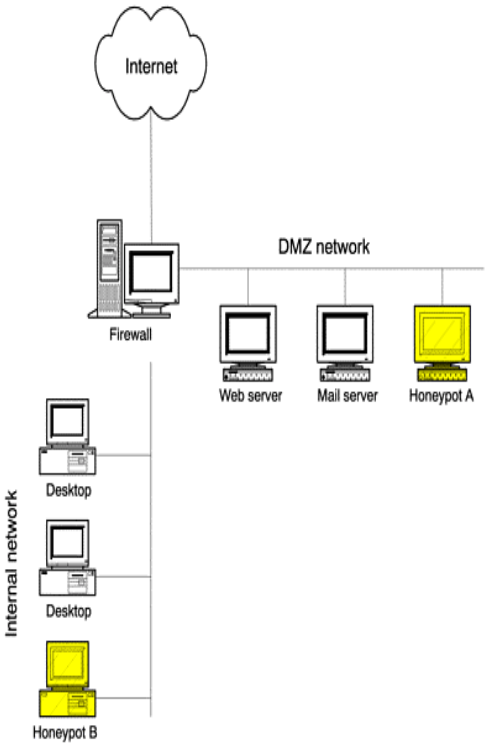

Figure 1 Two Honeypots

Any interaction with the honeypot is assumed unauthorized and most likely malicious. If the webserver honeypot is probed by external systems from the Internet, it means a probe or attack, most likely the same one other production webservers are facing. If the honeypot is probed by one of the production webservers on the DMZ, that can imply that the production webserver has been compromised by an attacker, and is now being used as a launching pad to compromise other systems on the DMZ

The Figure 1 shows two honeypots (Honeypot A and B) deployed by an orga-nization. Honeypot A is running on a DMZ network along with other servers of the organization. Honeypot B is running on the internal network along with other systems of the users. The intent of Honeypot A is to determine if there is any unauthorized activity happening within the DMZ. Since this system is not functioning as a normal server, no one should be connecting to it. Now, if anyone from the Internet connects to the honeypot, he is most likely probing or potentially attacking the system, perhaps looking for vulnerable Exchange servers. If any of the production servers on the DMZ, such as the new mail server or the Web server, make a connection to the honeypot, these servers may have been compromised, and now the attacker is probing for other vulnerable systems, including probing the honeypot. The system A is a honeypot by definition.

Lets suppose La Brea tarpit is installed on Honeypot B. La Brea Tarpit is a honeypot solution that detects connection attempts to a system that does not exist and then forges replies to the attacker on behalf of the system that does exist. Since the honeypot is monitoring IP address space that has no live systems, it knows that any packets sent to these non existing systems is most likely a probe or an attack. The forged replies sent by the honeypot are crafted to maintain an open connection with the attacker, slowing down or even stopping the automated attack. Honeypot B responds on behalf of systems that do not exist, so it knows anything sent to these systems is most likely an attack. Honeypot B's primary goal is not to detect attacks but slow them down, potentially even stopping them. This can give an organization critical time in responding to worms once they have been infected.

III. ADVANTAGES

Following are the advantages of honeypots:[3]

1. **Small Data Sets:** Honeypots only collect data when someone or something is interacting with them. Organizations that may log thousands of alerts a day with traditional technologies will only log a hundred alerts with honeypots. This makes the data honeypots collect much higher value, easier to manage and simpler to analyze.
2. **Reduced False Positives:** One of the greatest challenges with most detection technologies is the generation of false positives or false alerts. It's similar to the story of the 'boy who cried wolf'. The larger the probability that a security technology produces a false positive the less likely the technology will be deployed. Honeypots dramatically reduce false positives. Any activity with honeypots is by definition unauthorized, making it extremely efficient at detecting attacks.
3. **Catching False Negatives:** Another challenge of traditional technologies is failing to detect unknown attacks. This is a critical difference between honeypots and traditional computer security technologies

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

which rely upon known signatures or upon statistical detection. Signature-based security technologies by definition imply that "someone is going to get hurt" before the new attack is discovered and a signature is distributed. Statistical detection also suffers from probabilistic failures – there is some non-zero probability that a new kind of attack is going to go undetected. Honeypots on the other hand can easily identify and capture new attacks against them. Any activity with the honeypot is an anomaly, making new or unseen attacks easily stand out.

4. **Encryption:** It does not matter if an attack or malicious activity is encrypted, the honeypot will capture the activity. As more and more organizations adopt encryption within their environments (such as SSH, IPsec, and SSL) this becomes a major issue. Honeypots can do this because the encrypted probes and attacks interact with the honeypot as an end point, where the activity is decrypted by the honeypot.
5. **IPv6:** Honeypots work in any IP environment, regardless of the IP protocol, including IPv6. IPv6 is the new IP standard that many organizations, such as the Department of Defense, and many countries, such as Japan, are actively adopting. Many current technologies, such as firewalls or IDS sensors, cannot handle IPv6.
6. **Highly Flexible:** Honeypots are extremely adaptable, with the ability to be used in a variety of environments, everything from a Social Security Number embedded into a database, to an entire network of computers designed to be broken into.
7. **Minimal Resources**: Honeypots require minimal resources, even on the largest of networks. A simple, aging Pentium computer can monitor literally millions of IP addresses.

I. DISADVANTAGES

Apart from all the advantages, honeypots also have some disadvantages. Disadvantages of honeypots are listed below:[3]

1. **Risk :**Honeypots are a security resource the bad guys to interact with, there is a risk that an attacker could use a honeypot to attack or harm other non-honeypot systems. This risk varies with the type of honeypot used. For example, simple honeypots**n** such as KFSensor have very little risk. Honeynets, a more complex solution, have a great deal of risk. The risk levels are variable for different kinds of honeypot deployments. The usual rule is that the more complicated the deception, the greater the risk. Honeypots that are high-interaction such as Gen I Honeynets are inherently more risky because there is an actual computer involved.
2. **Limited Field of View:** Honeypots only see or capture that which interacts with them. They are not a passive device that captures activity to all other systems. Instead, they only have value when
3. directly interacted with. In many ways honeypots are like a microscope. They have a limited field of view, but a field of view that gives them great detail of information.
4. **Discovery and Fingerprinting:** Though risk of discovery of a honeypot is small for script kiddies and worms, there is always a chance that advanced blackhats would be able to discover the honeypot. A simple mistake in the deception is all a savvy attacker needs to "fingerprint" the honeypot. This could be a misspelled word in one service emulation or even a suspicious looking content in the honeypot. The hacker would be able to flag the honeypot as "dangerous" and in his next attacks, he would most certainly bypass the honeypot. In fact, armed with the knowledge, an advanced blackhat could even spoof attacks to the honeypot thus redirecting attention while he attacks other vulnerable systems in the network.

Table 1: Advantages and Disadvantages of honeypots

Degree Of Involvement	Low	Medium	High
Real Operating Systems	No	No	Yes
Risk	Low	Mid	High
Information Gathering	Connections	Requ-est	All
Compromised Wished	No	No	Yes
Knowledge To Run	Low	Low	High
Knowledge Develop	Low	High	Mid -High
Maintenance Time	Low	Low	Very High

IV. CLASSIFICATION OF HONEYPOTS

Honeypots can be classified into various categories depending on their purpose i.e. either they are being setup for research or production (as a security measure in a corporation). Depending on the level of interaction they provided to the attacker – can the attack get full control of thehoneypot or can it only connect to it and depending on how they are implemented i.e. are they implemented on a real environment or they are running on a virtual environment as a fake system.[4]

A. Classification according to Purpose

Honeypots can be used for production or research. Production honeypots protect an organization, while research honeypots are used to learn.

Production Honeypots Production honeypots are what most people typically think of as a honeypot. They add value to the security of a specific organization and help mitigate risk. These honeypots are implemented within the organization because they help secure its environment, such as detecting attacks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Production honeypots are the law enforcement of honeypot technologies. Their job is to deal with the bad guys. Commercial organizations often use production honeypots to mitigate the risk of attackers. Production honeypots usually are easier to build and deploy than research honeypots because they require less functionality. Because of their relative simplicity, they generally have less risk. It's much more difficult to use a production honeypot to attack and harm other systems. However, they also generally give us less information about the attacks or the attackers than research honeypots do. One may learn which systems attackers are coming from or what exploits they launch, but he will most likely not learn how they communicate among each other or how they develop their tools. e.g. Specter

Research honeypots Research honeypots are designed to gain information about the blackhat community. These honeypots do not add direct value to a specific organization. Their primary mission is to research the threats organizations may face, such as who the attackers are, how the are organized, what kind of tools they use to attack other systems, and where they obtained those tools. If production honeypots are similar to law enforcement, then one can think of research honeypots as counterintelligence, used to gain information on the bad guys. This information helps in understanding who the threats are and how they operate. Research honeypots are far more involved than production honeypots. To learn about attackers, one need to give them real operating systems and applications with which to interact. This gives the researchers far more information than simply what applications are being probed. One can potentially learn who the attackers are, how they communicate, or how they develop or acquire their tools. However, this increased functionality has its disadvantages. Research honeypots are more complex, have greater risk, and require more time and effort to administer. In fact, research honeypots could potentially reduce the security of an organization, since they require extensive resources and maintenance. e.g. Honeyd

B. Classification according to Interaction

According to level of involvement between the attacker and the honeypots, the honeypots can be divided into three categories

Low-interaction honeypots: These types are limited in their extent of interaction; they are actually emulators of services and operating systems, whereby attacker activity is limited to the level of emulation by the honeypot. An example of an emulated service is FTP service; listening on port 21 may just emulate an FTP login, or it may support a variety of additional FTP commands. The deployment and maintenance of such systems is fairly simple and does not involve much risk.

In addition the emulated services mitigate risk by containing the attacker's activity. Unfortunately these systems log only limited information and are designed to capture known activity. Moreover, an attacker can detect a low-interaction honeypot by executing a command that the emulation does not support. Examples of low-interaction honeypots include Specter, Honeyd and KFSensor.

Medium-interaction honeypots: In terms of interaction, this is a little more advanced than low-interaction honeypots, but a little less advanced than high interaction honeypots. Medium-Interaction honeypots still do not have a real operating system, but the bogus services provided are more sophisticated technically. Here the levels of honeypots get complicated; the risk also increases especially with regards to vulnerability. These honeypots will give a certain feedback when it is queried upon.

High-interaction honeypots: These are different, whereby they are a complex solution and involve the deployment of real operating systems and applications. The advantages include the capture of extensive amounts of information and allowing attackers to interact with real systems where the full extent of their behavior can be studied and recorded. Examples of high-interaction honeypots include Honeynets Sebek. These kinds of honeypots are really time consuming to design, manage and maintain Among the three types of honeypots, this honeypot possess a huge risk. But, the information and evidence gathered for analysis are bountiful. With these we can learn what are the kind of tools hackers' use, what kind of exploits they use, what kind of vulnerabilities they normally look for, their knowledge in hacking and surfing their way through operating systems and how or what the hackers interact about.

IV. COMPARISON OF VARIOUS HONEYPOTS

Each available honeypot has different strengths. BOF can be specified as a very simple solution, a toy with very limited services and limited logging functionality. But it is easy to install and quite interesting to watch and play. Especially on a cable modem or dial-up, there should be lots of attacks (these networks often get scanned by people).Specter is easy to install and even easier to run due to the nice graphical user interface. Unfortunately, its value is not that high, as no real operating system is provided. But this fact does also help in reducing the risk significantly[5]. ManTrap and DTK honeypots are highly customizable. Their value can be very high, as well as their risk. Therefore their cost of ownership, which represents the outlay of the routine maintenance, is higher. ManTrap's main advantage over DTK is the provided GUI. It is very comfortable to configure, analyze and manage this commercial solution.[6][7]

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Honeypot	Interaction Level	OS	Emulation	Free Source
HoneyBOT	Low	No	Yes	Closed
BackOfficer Friendly	Low	No	No	Closed
Specter	High	Yes	No	Closed
Honeyd	Low	Yes	Yes	Open
Deception Toolkit	Low	No	Yes	Open
Cybercop Sting	Low	Yes	No	Closed
NetFacade	Low	Yes	No	Closed
ManTrap	High	Yes	No	Closed
Homemade	Depends	Depends	Yes	Open
Honeynets	High	Yes	Yes	Open

Table 2: Comparison of various honeypots

II. CONCLUSION

Honeypot technologies has changed the traditional passive defense of the network security, is an important expansion to the existing security system . From passive defense to active defense is the inevitable trend of network security technology development. Therefore, the research of Honeypot technology will have broad development and application prospects. In this paper, on the basis of the research on Honeypot technology, in view of the many problems in current traditional security resource applications, the Honeypot technology is used in network security defense, and a Honeypot-based distributed intrusion prevention model is presented. The experimental results show that the program can successfully remedy the deficiencies of existing monitoring system and improve the performance of the safety defense systems.

REFERENCES

1. Lance Spitzner, Honeypots: Tracking Hackers. Addison Wesley, September 13,2002
2. Eric Peter et al., A Practical Guide to Honeypots. http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html, Fetched 20/06/2011.
3. Ryan Talabis, Honeypots 101: Risks and Disadvantages. http://www.philippinehoneynet.org/index.php?option=com_docman&task=doc_download&gid=4&Itemid=29. 2007, Fetched 21/06/2011
4. HoneynetProject.KnowYourEnemy:Honeynets.http://www.honeynet.org/papers/honeynet/
5. Neils Provos, A Virtual Honeypot Framework. SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium, Volume 13, 2004
6. Neils Provos,Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison Wesley Professional, July 16, 2007
7. Ryan Talabis, Honeypots 101: What's in it for me?. http://www.philippinehoneynet.org/index.php?option=com_docman&task=doc_download&gid=3&Itemid=29, 2007, Fetched 21/06/2011

AUTHOR PROFILE

Miss.BhumikaLall, B.Tech in Information Technology from Kurukshetra University, Kurukshetra; M.teh In Computer Science & Engineering from Kurukshetra University, Kurukshetra; Research work in **Design and Implementation of Honeyd to Simulate Virtual Honeypots**

Assistant Prof. Vivek Sharma, B.Tech (Gold Medalist) in Computer Science & Engineering from Kurukshetra University, Kurukshetra,; M.tech in Computer Science & Engineering from Kurukshetra University, Kurukshetra; Publicatios in **WIFI protocols** and **Mobile Sensor Networks in Health Care**, Specialization in **Object Oriented Programing Languages(OOPL)**, Research work **In Mobile Networks.**, Member of **CSI(Computer Society Of India).**

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)