IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

Honeypot in Information System Security

N. Shoba[1*], V. Sathya[2]

[1]Govt. Arts College for Women- Krishnagiri
[2]MGR Arts and Science College- Hosur

Available online at: www.ijcseonline.org

Abstract—This days security in information system is very challenging , so security for network security plays a vital role in all fields. A honeypot is a network-attached system set up as a decoy to lure cyberattackers and to detect, deflect or study hacking attempts in order to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers -- usually a server or other high-value target -- and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users. Honeypot is a well designed system that attracts hackers into it. By luring the hacker into the system, it is possible to monitor the processes that are started and running on the system by hacker. In other words, honeypot is a trap machine which looks like a real system in order to attract the attacker. The aim of the honeypot is analyzing, understanding, watching and tracking hacker's behaviours in order to create more secure systems. Honeypot is great way to improve network security administrators' knowledge and learn how to get information from a victim system using forensic tools. Honeypot is also very useful for future threats to keep track of new technology attacks.

Keywords— Honeypot, hacking, security, forensic analysis of honeypots, network.

I. HONEYPOT

Honeypot is a security mechanism for network security. It detects, deflects and counteracts the unauthorized use of information systems. It consists of data which is isolated and monitored but appears as if it is a part of the site. Honeypots are classified into two categories production honeypot and research honeypot. Production honeypots capture only limited information and are easy to use whereas research honeypots collect information about the black hat communities who are trying to attack the network.

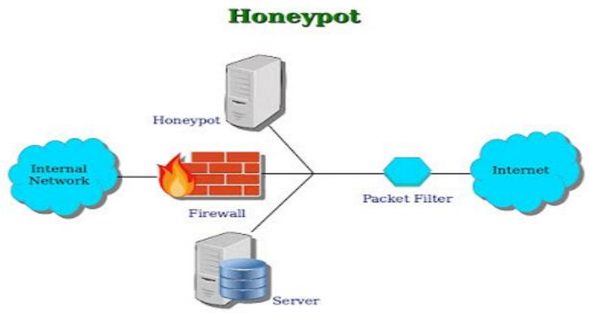

Fig. 1

II. WHAT ARE HONEYPOTS AND HOW CAN THEY SECURE COMPUTER SYSTEMS

Honeypots are traps which are set to detect attempts at any unauthorized use of information systems, with a view to learning from the attacks to further improve computer security.

Traditionally, sustaining network security has involved acting vigilantly, using network-based defense techniques like firewalls, intrusion detection systems, and encryption. But the current situation demands more proactive techniques to detect, deflect and counteract attempts at illegal use of information systems. In such scenario, the use of honeypots is a proactive and promising approach to fight off network security threats.

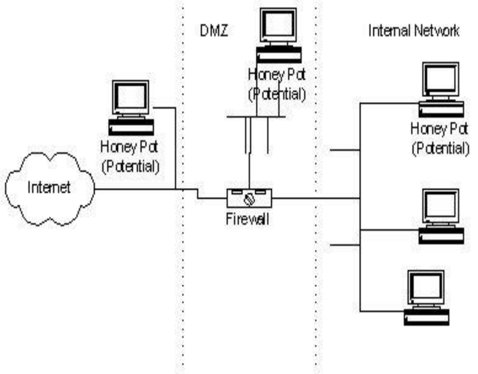

Fig. 2

Considering the classical field of computer security, a computer needs to be secure, but in the domain of **Honeypots**, the security holes are set to open on purpose.

Honeypots can be defined as a trap which is set to detect attempts at any unauthorized use of information systems. Honeypots essentially turn on the tables for Hackers and computer security experts. The main purpose of a Honeypot is to detect and learn from the attacks and further use the information to improve security. Honeypots have long been used to track attackers' activity and defend against coming threats. There are two types of honeypots:

III. Research Honeypot

A Research Honeypot is used to study about the tactics and techniques of the intruders. It is used as a watch post to see how an attacker is working when compromising a system.

IV. Production Honeypot

These are primarily used for detection and to protect organizations. The main purpose of a production honeypot is to help mitigate risk in an organization.

1) *Why set up Honeypots*

The worth of a honeypot is weighed by the information that can be obtained from it. Monitoring the data that enters and leaves a honeypot lets the user gather information that is not otherwise available. Generally, there are two popular reasons for setting up a Honeypot:

i. Gain Understanding

Understand how hackers probe and attempt to gain access to your systems. The overall idea is that since a record of the culprit's activities is kept, one can gain understanding into the attack methodologies to better protect their real production systems.

ii. Gather Information

Gather forensic information that is needed to aid in the apprehension or prosecution of hackers. This is the sort of information which is often needed to provide law enforcement officials with the details needed to prosecute.

2) *How Honeypots secure Computer Systems*

A Honeypot is a computer connected to a network. These can be used to examine the vulnerabilities of the operating system or the network. Depending on the kind of setup, one can study security holes in general or in particular. These can be used to observe activities of an individual which gained access to the Honeypot.

Honeypots are generally based on a real server, real operating system, along with data that looks like real. One of the chief differences is the location of the machine in relation to the actual servers. The most vital activity of a honeypot is to capture the data, the ability to log, alert, and capture everything the intruder is doing. The gathered information can prove to be quite critical against the attacker.

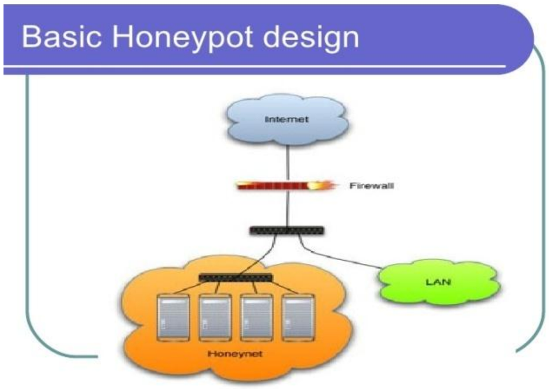

Fig. 3

3) *Advantages of using Honeypots*

A. Collect Real Data

While Honeypots collect a small volume of data but almost all of this data is a real attack or unauthorized activity.

B. Reduced False Positive

With most detection technologies (IDS, IPS) a large fraction of alerts is false warnings, while with Honeypots this doesn't hold true.

C. Cost Effective

Honeypot just interacts with malicious activity and does not require high-performance resource.

D. Encryption

With a honeypot, it doesn't matter if an attacker is using encryption; the activity will still be captured.

E. Simple

Honeypots are very simple to understand, deploy and maintain.

A Honeypot is a concept and not a tool which can be simply deployed. One needs to know well in advance what they intend to learn, and then the honeypot can be customized based on their specific needs. There is some useful information on sans.org if you need to read more on the subject.

Honeypots can be classified based on their deployment (use/action) and based on their level of involvement. Based on deployment, honeypots may be classified as

- ➢ production honeypots
- ➢ research honeypots

Production honeypots are easy to use, capture only limited information, and are used primarily by 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.

Research honeypots 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.[2] Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.[3]

Based on design criteria, honeypots can be classified as:

- pure honeypots
- high-interaction honeypots
- low-interaction honeypots

Pure honeypots are full-fledged production systems. The activities of the attacker are monitored by using a bug tap that has been installed on the honeypot's link to the network. No other software needs to be installed. Even though a pure honeypot is useful, stealthiness of the defense mechanisms can be ensured by a more controlled mechanism.

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste their time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly. In general, high-interaction honeypots provide more security by being difficult to detect, but they are expensive to maintain. If virtual machines are not available, one physical computer must be maintained for each honeypot, which can be exorbitantly expensive. Example: Honeynet.

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyd.

V. HIGH-INTERACTION VS. LOW-INTERACTION HONEYPOTS

High-interaction honeypots can be compromised entirely, permitting an enemy to gain full access to the system and use it to launch further network attacks. With the help such honeypots, users can learn more about targeted attacks against their systems or even about insider attacks.

In contrast, the low-interaction honeypots put on only services which cannot be exploited to get complete access to the honeypot. These are more limited but are useful for gathering information at a higher level.

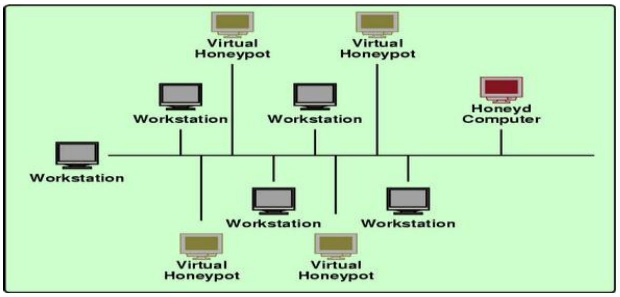

FIG. 4

VI. CONCLUSION

The future is becoming more and more difficult to predict with each passing year. So we should always expect an increasing pace of technological change. In this paper, the main importance of security in information system through honeypot . and also how honeypot secure the system ,types of honeypot, Why Honeypots set up, advantages of honeypot .With all of these wonderful advantages, you would think honeypots would be the ultimate security solution. Unfortunately, that is not the case. They have several disadvantages. It is because of these disadvantages that honeypots do not replace any security mechanisms; they only work with and enhance your overall security architecture. 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. 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. Honeypots have tremendous potential for the security community, and they can accomplish goals few other technologies can. Like any new technology, they have some challenges to overcome. Most likely none of these problems will ever be completely solved or eliminated.

REFERENCES

[1]. Spitzner L.2001.The Value of Honeypots, Part Two: Honeypot Solutions and Legal Issues [Online] (Updated 23 October 2001) Available at : http://www.symantec.com/connect/articles/value-honeypots-part-two-honeypot-solutionsand-legal-issues [Accessed 13 March 2010].

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

[3]. Sutton Jr.,R.E DTEC 6873 Section 01:How to build and use a honeypot.

[4]. https://searchsecurity.techtarget.com/definition/honey-pot

[5]. Lakhani A.D., A dissertation on deception techniques using honeypots.Information Security Group Royal Holloway, University of London,UK.

[6]. Shuja F.A.,2005. Pakistan Honeynet Project Virtual Honeynet: Deploying Honeywall using Vmware [Online](Updated November 2005) Available at: http://www.honeynet.pk/Honeywall/roo/index.htm [Accessed 7 May 2010].

[7]. https://www.symantec.com/connect/articles/problems-and-challenges-honeypots

[8]. http://www.informit.com/articles/article.aspx?p=30489&seqNum=2