Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

Honeypots
“Luring the Hackers”

Mr. Konark T Dave[1]

[1]*Computer Engineering Department, C U Shah University*

Abstract— A common problem with people dealing with the internet and using many facilities on it is, “Attack of Hackers”. One eye of hackers may be on you while working on internet. The problem is how to trace the hackers. This task is much similar to catch the person red-handed for criminal or unauthorized activity. A tricky system referred as “Honeypot” can be used to achieve the same. So, how Honeypots are used and how you can entrap hackers are covered in this.

Keywords— Honeypot, Honeytrap, network security, honeypot implementation, honeypot trends, honeyd

I. INTRODUCTION

In this era, many people are thinking about the systems that track the hackers and in this way a loot can be shunned. There are many tools available to spot and find the hackers. Many ways are also available that do the same but the most popular and economical way is to use “Honeypot”.

II. HISTORY OF HONEYPOTS

There is a unique history of Honeypots. The idea of honeypots originated in 1991 with two publications, First “The Cuckoos Egg” and the second is “An Evening with Breford”. “The Cuckoos Egg” by Clifford Stoll was about his experience catching a computer hacker that was in his corporation searching for secrets.

The other publication “An Evening with Berferd” by Bill Chewick was about a computer hacker’s move through traps that he and his colleagues used to catch him. Based on the idea of these two publications, the first type of honeypot was released in 1997 called the Deceptive Toolkit.

The point of this kit was to use deception to attack back. In 1998 the first commercial honeypot came out. This was called Cybercop Sting. Since 2002, honeypot technology has been improved significantly.

Third-order headings, as in this paragraph, are discouraged. However, if you must use them, use 12-point Times, boldface, initially capitalized, flush left, preceded by one blank line, followed by a period and your text on the same line.

III. WHAT THE HONEYPOT IS

"Honeypot is 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 spurious. It is located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques.”Saying practically, 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 activities are unauthorized. In another way Honeypot can be defined as a computer system on the Internet that is deliberately set up to attract and trap hackers who attempt to penetrate other computer systems.

IV. ROLE OF HONEYPOTS IN NETWORK SECURITY

Honeypot is a trap. Moreover it is an electronic bait. In most cases, Honeypots are installed with firewalls. Honeypots and firewalls work in opposite to each other. They allow all the traffic to come in but block all outgoing traffic whereas the firewall does the reverse of it. Most honeypots are installed inside network firewalls that monitor and track the hackers. Honeypot is a unique tool to learn about the tactics of hackers.

Now thinking in the other direction, Honeypot is often a computer but it can also be in other forms like data records, idle IP address spaces. It must be handled carefully.

These systems can only react to or prevent attacks but they are not able to give us information about the attacker. Hence, Honeypots are a narrative approach to network security. Honeypots are closely monitored decoy systems that are employed in a network to study the trail of hackers and to alert network administrators. Honeypots provide a cost-effective solution. Now a day, these systems are also used by the research groups to study problems in network security.

V. HOW DO HONEYPOTS WORK

As expressed, Honeypots are generally based on a real server, real operating system, and with data that appears to be real. One of the main differences is the location of the machine in relation to the actual servers.

A critical element to any honeypot is data capture, the ability to record, alert, and confine everything the hacker is doing.

It is highly recommend deploying Snort with any honeypot deployment. Snort is an Open Source IDS system that will not only detect and alert any attacks against your honeypot, but it can capture the packets involved in the attack.

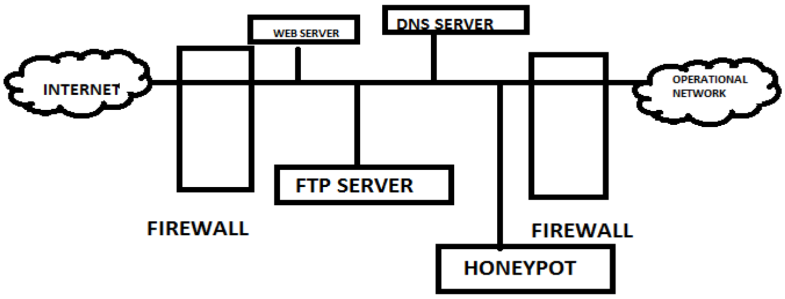

Figure-1 Working Mechanism of Honeypot

VI. TYPES OF HONEYPOT

There are two wide categories of honeypots available today. These categories are defined based on the services, or interaction level, provided by the honeypot to potential hackers.

1. High-interaction honeypots
2. Low-interaction honeypots

High-interaction honeypots

High Interaction Honeypots make use of the real susceptible service or software. High-interaction honeypots are typically complex solutions as they include real operating systems and applications.

In High Interaction Honeypots everything is genuine. They provide a lot more detailed picture of how an attack or how a particular malware execute in real-time. Since there is no emulated service, High Interaction Honeypots help in identifying unknown vulnerabilities.

But High Interaction Honeypots are more even to infections and increases the risk because attackers can use these real honeypot operating systems to attack and compromise systems.

They permit the hacker to relate with the system with the goal of capturing the maximum amount of information on the attacker's techniques.

A very famous example of High-interaction honeypots is Honeynet.

Low-interaction honeypots

Unlike High-interaction honeypots, Low-Interaction Honeypots allow only limited interaction for an attacker or malware. All services offered by a Low Interaction Honeypots are emulated. Thus Low Interaction Honeypots are not themselves vulnerable and will not become infected by the exploit attempts against the emulated vulnerability.

They replicate 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.

A good example of High-interaction honeypots is Honeyd.

VII. EXISTING HONEYPOT PRODUCTS

There are some products or tools of Honeypots available like Honeyd, HoneyBOT, Specter etc. These tools are to be installed on the computer across network and used in such type of environment in which hackers are activate.

VIII. HOW DOES HONEYPOT COLLECT THE INFORMATION

Honeypots must capture the data in such a way that hackers are not able to access them. There are some levels on which the information can be gathered. The first and simplest way is to store the data in Log of firewall and the other is to use packet sniffer. This system should be configured to examine network traffic.

IX. GHH

GHH stands for “Google Hack Honeypot”. Google Hack Honeypot is the response to a new type of malicious web traffic. It is deliberated to offer inspection against attackers that use search engines as a hacking tool against the different resources. It implements honeypot theory to provide extra security to your web presence. This has been developed by Google.

X. FOOTNOTES

Honeypots must be employed at the places which include sensitive work as well as information. One has to always keep in mind that someone is continuously watching you to steal the information. In such places, Honeypots are used to catch the hacker red handed by alluring him/her.

REFERENCES

[1] http://ghh.sourceforge.net/
[2] https//my.safaribooksonline.com
[3] https://Wikipedia.org
[4] https://pcmag.com