International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 13 • Issue 2 pp. 1-3 Jan 2020 - June 2020 www.csjournals.com

HONEYPOT-A Security Measure

Alstyne Victor Kuraty
Lecturer, Dept of Computer Science, KLE's J.G.College of Commerce
Vidyanagar, Hubli.

Abstract: Honeypot is used in the area Information Technology and Internet security. It is a security resource, whose value lies in being probed, attacked or compromised. They are special decoy servers used to catch the Blackhats (people with evil and illegal intents). With the help of a security team they attract the hackers to attack a vulnerable computer system, which is under observation, and then the information about the attackers is logged and monitored. It's a relatively new concept in network security and researchers all over the world are making it more independent and secure. Compared to an Intrusion Detection System (IDS) or Firewalls, Honeypots have the big advantage i.e they do not generate false alerts as each observed traffic is suspicious because of non productive components running on the system.

Introduction:

As communication is getting is globalized day by day, so are the crimes related to computers and countermeasures are developed to detect or prevent attacks as such, most of these measures are based on known facts and known attack patterns. Countermeasures can be formed by knowing what kind of strategy an attacker uses, what tools he utilizes and his intention. To gather such information is one main goal of a honeypot.

A honeypot is primarily an instrument used to gather information. Its purpose is not to be an ambush for the blackhat community to catch them in action, rather prevent them from intruding.

The focus lies on a silent collection of information about their attack patterns, programs used, purpose of attack and the blackhat community itself. All this information is used to learn more about the blackhat proceedings and motives, as well as their technical knowledge and abilities. There are a lot of other possibilities for a honeypot divert hackers from productive systems or catch a hacker while conducting an attack.

Types of Honeypots:

1) Low-Involvement Honeypot

A low-involvement honeypot typically only provides certain fake services. Basically these services can be implemented by having a listener on a specific port. In such a way all the incoming traffic can easily be recognized and stored. On a low involvement honeypot the real operating system does not exist thus disabling the attacker to operate upon which will minimize the risk significantly because the complexity of an operating system is eliminated. On the other hand this is also a disadvantage because it is not possible to watch an attacker interacting with the operating system, which could be really interesting.

2) Mid-Involvement Honeypot

A mid-involvement honeypot provides more interaction but does not provide a real underlying operating system. The fake background processes are more sophisticated and have deeper knowledge about the specific services they provide. At the same time the risk increases. Through

the higher level of interaction more complex attacks are possible and can therefore be logged and analyzed.
The attacker gets a better illusion of a real operating system. He has more possibilities to interact and probe the system. Developing mid-involvement honeypot is complex and time-consuming. Special care has to be taken for security checks as all developed fake background processes need to be as secure as possible.

3) High-Involvement Honeypot
A high-involvement honeypot has a real underlying operating system which leads to a much higher risk as the complexity increases rapidly. At the same time, the possibilities to gather information, the possible attacks as well as the attractiveness increase a lot. A high involvement honeypot does offer such an environment. It is very time-consuming and hence the system should be constantly under surveillance.
The goal of a hacker is to gain root and to have access to the machine which is connected to the Internet. By providing a full operating system to the attacker we make it possible to upload and install new files. This is where a high-involvement honeypot can show its strength, as all actions can be recorded and analyzed. Unfortunately, the attacker has to compromise with the system to get this level of freedom. He will then have root rights on the system and can do everything at any moment on the compromised system thus making this system unsecure.

Honeypot working:
A honeypot works by being an intentionally vulnerable gap in the security. These devices will typically take the form of a virtual machine (VM) that has been deliberately weakened and placed in an accessible area of the network. These VM's will often have critical security updates missing, along with open ports and unnecessary services enabled for a hacker to exploit.
Additionally, a honeypot device will usually have administrator accounts with weak passwords or no password at all, making it easy for an attacker to escalate their privileges without difficulty.
All of these security weaknesses will cause an attacker to think that they've found an easy target to infiltrate, when in reality their time is being wasted as the administrator monitors their activity and shuts down access to the rest of the network. The end result is an attacker being caught in a trap with nothing to show for it in terms of valuable data or systems access. By the time the hacker has realized what's going on, the administrator has gathered sufficient information to further reinforce the network or report the activity to authorities.
Overall, a honeypot can be an effective tool for securing the personal network by diverting hackers' attention away from the sensitive data. Implementing this tool carefully helps the user in adding an effective layer of defense to the home network.

Advantages of Honeypots
a) Small Data Sets: Honeypots only collect data when someone or something is interacting with them. Organizations that may log thousands of alerts a day may only log a hundred alerts with honeypots thus making the honeypots collect the data in a much easier manner and to analyze.

b) Reduced False Positives : Honeypots dramatically reduce false positives. Any activity with honeypots is defined as unauthorized, thus making it extremely effective at detecting attacks. This allows the organizations to quickly and easily reduce or eliminate the false alerts further allowing organizations to focus on other security priorities, such as patching.

c) Catching False Negatives : Honeypots can easily identify and capture new attacks or actions against them. Any activity with the honeypot is an anomaly, making new or unseen attacks to easily stand out.

d) Minimal Resources

Even on the largest of networks honeypots require minimal resources. A simple Pentium computer can monitor literally millions of Internet Protocol addresses on an OC-12 network.

e) Encryption

Any attack thus encrypted makes no difference as the honeypot will capture the activity.

f) Protocol Independent

Usage of any IP protocol by the attacker makes no difference at all, as the honeypots will detect, capture and log all the IP activities.

g) Intelligence Gathering

Honeypots can gather a wealth of valuable information about the attackers, and also the nature of their attacks, which can be used to take appropriate action against them. It is a valuable resource, especially to collect information about the proceedings of the attackers as well as their deployed tools.

Conclusion:

Honeypots are a new field in the sector of network security. Currently, there is a lot of ongoing research and discussions all around the world. No other mechanism is comparable in the efficiency of a honeypot wheras gathering the information is considered as a primary goal, especially if the tools an attacker uses are of wide interest. As honeypots are getting more advanced, hackers will also develop methods to detect such systems thus leading to a regular arms race between the good people and the blackhat community.

References

1. *hide.me › blog › honeypot*
2. *cybersecurity.att.com*
3. *us.norton.com › honeypot*