DOI: http://dx.doi.org/10.26483/ijarcs.v10i3.6420

ISSN No. 0976-5697

Volume 10, No. 3, May-June 2019

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

STUDY ON HONEYPOT BASED SECURE NETWORK SYSTEM

Katkam Rushikesh
Department of Computer Science
Sreenidhi Institute of Science and Technology
Hyderabad.Telangana, India

***Abstract*:** In this modern world the use of computers are increasing day by day. As the result of this computer revolution the use of internet and computer networks also increases. People are so habituated to Internet as they do all kinds of work like food orders, online shopping, job assignments, online education by just one click. By sitting in home we can know what is happening around the world. Though it has several advantages, it has its own risks and vulnerabilities too. The private industries and government organizations which uses internet must adopt some security measures to safe guard their networks from cyber attacks. This paper explains the concept of honeypot an intrusion detection system that provide security to networks. This model runs as a virtual machine with small vulnerability which is created on purpose to lure the attackers so that the intruder can gain company's content. This model is used to capture patterns and various techniques used by intruders and create list activities. By using this list the network system can be protected from cuber attacks. Honeypots can capture any kind of unauthorized access, record and report it to the admin to prevent those attacks and go further with legal actions. Group of honeypots are combined to form honeynet that provide security to several networks.

Keywords:Honeypot, honeynet, intrusion detection system, cyber attacks.

I. INTRODUCTION

The internet is collection of networks. Internet is vast and it is used by almost everyone throughout the world. Apart from its benefits it has many defects. Many cyber threats have been reported and increasing day by day. In internet, security is minimized due to some functionality. Attacks against computer networks cost industries and government organizations millions of money to recover from those attacks. Some of the attacks are DoS (Denial of Service), identity spoofing, password based attacks, data breaches, eavesdropping. To overcome these attacks the organizations must adopt intrusion based detection system to protect the sensitive data. The criteria are not only to detect the attacks but also react quickly to prevent those attacks. One such technology is Honeypot. Honeypot is a security mechanism runs on a virtual machine and act as a real production system. Honeypot put attractive information about the company which is fake information in their network to lure the intruders to attack them so that honeypots can record information about intruders and their attacking patterns. As shown the fig.1 how bees are attracted to the honey in the same way honeypot servers try to lure the attackers with the attractive information.

Fig 1 honeypot

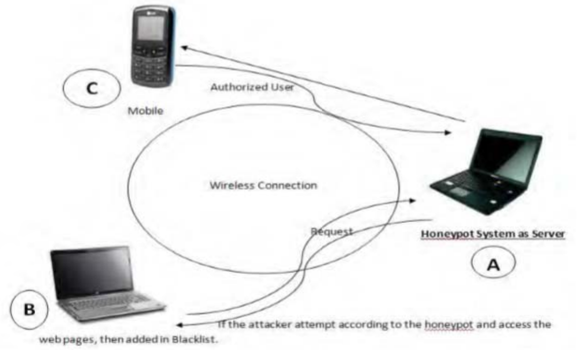
C
Mobile
Authorized User
Wireless Connection
Request
Honeypot System as Server
A
B
If the attacker attempt according to the honeypot and access the web pages, then added in Blacklist.

Fig 1.1 Network with honeypot

.

II. TYPES OF HONEYPOT

Honeypot is type of intrusion detection system that runs on a virtual machine or system put on network as bait for attackers .Depending on deployment and design honeypots are of two types.

RESEARCH HONEYPOTS

This honeypot is used for research purpose to understand the techniques that are used by intruders to compromise network security. Research honeypots are used to learn about the method attackers. They can trace the patterns of their attacks. Research honeypots help the researchers to detect the new techniques that can compromise the security of network. This study is used to improve existing security system.

PRODUCTION HONEYPOTS

Organizations use production honeypots as the part of security mechanisms. Production honeypots increase the security of network. They collect partial information about the attackers. These honeypots gives warning to the administrator if the system is under attack so that admin can take precautions to prevent any loss. Production honeypots can be set up to behave like real production system. This will allow discovering the vulnerabilities in the network. Attackers try to compromise the honeypots by directly dealing with real systems. So as to prevent this some necessary steps has to be taken like firewall enhancement.

Based on the interaction honeypots are divided into 3 types

1. Low interaction honeypot
2. Medium interaction honeypot
3. High interaction honeypot

LOW INTERACTION HONEYPOT

These honeypots collect little information about the attacks. It can be available at low cost and easily maintained. Only a part of application and operating system are emulated by low interaction honeypots. It is easy to deploy and they does not give access to production system.A low interaction honeypot will only give an attacker very limited access to the operating system.When a highly skilled hacker tries to attack an organization network he can easily detect this low interaction honeypot and can compromise it. Low interaction honeypots are also called as honeyed.

HIGH INTERACTION HONEYPOT

High interaction honeypots have complete access to operating system. These honeypots can get complete information about the attack and the person who triggered it. In high interaction honeypot nothing is emulated everything is real. It involves high level of risk as it directly exposes the real system. High interaction honeypot provide more security and it is difficult to detect by the intruder. Compared to low interaction honeypots high interaction honeypots are more expensive and difficult to maintain.

WORKING OF HONEYPOT

In this paper I proposed that honeypot will collect information about the attacks and now we will see how it will do it. The two goals are

1. How attacker gets into the network
2. How honeypot collects information about the attacker and their techniques to submit to law enforcement officer for legal actions

In order to do this first we need to make ensure that

- Honeypot computer is similar to production system
- What is the attractive information that is used to lure the attacker
- How it will restrict the traffic from and to the internet

Honeypot is one of the Intrusion detection systems that enhance the security of the network but due to wide usage of honeypots attackers found a way to bypass the honeypot. In this situation firewall play a major role in addition to honeypot. Some other tools like Sniffer tool that controls the flow of packets between the internet and firewall. Sniffer tool collects more information about the intruder

HONEYPOT ARCHITECTURE

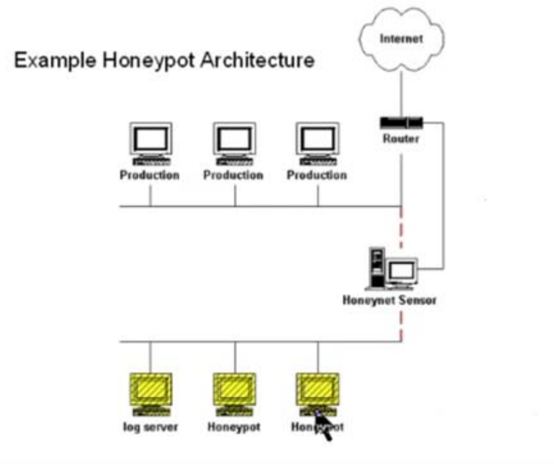

Fig 1.2: honeypot architecture

As shown in the fig honeynet is a collection of honeypots that provide security to various networks and lie in between real production system and honeypots that behave like real system. The honeypots maintain more attractive information so that whenever an attacker perform reconnaissance on the network thinks that the honeypots are the real system and tries to attack them. When a intruder attack the honeypot, a log server which is connected to honeypot collects the information about the attacker and attacking techniques. Honeynet sensor which lies in between real production system and honeypots controls the flow of packets between router and system and it has intrusion detection system.

III. FUTURE WORK

In future honeypots can be enhanced with techniques and algorithms like connection trackers, protocol analysis and pattern detection in flow control etc. Honeypot can also be used in cloud computing as security is the worst nightmare of cloud.

IV. CONCLUSION

Honeypot play a major role that provides security to networks honeypots as one of the intrusion detection system that collects information about the attacker and the patterns they use. Depend upon their usage different kind of honeypots can be deployed by the organization. Now a day's cyber crimes are increasing enormously and there is no doubt that the number is going to increase. I think there must be a need for security and honeypots will play a major role in it

V. REFERENCES

[1] Akshay A.Somwanshi, "Implementation of Honeypots for Server Security" Mar. 03, 2016. [Online]. Available: https://www.irjet.net/archives/V3/i3/IRJET-V3I358.

[2] Yogendra Kumar Jain, "Honeypot based secure Network System" Feb.02,2011.[online]. Available: https://www.researchgate.net/publication/50247428_Honeypot_based_Secure_Network_System/.