Method for Honeypot Technology

Mariadas Ronnie C.P
Asst. Professor, Dept. of MCA
SCMS School of Technology and Management,
SSTM, Muttom, Aluva.

Devika Prakash
P G Scholar, Dept. of MCA
SCMS School of Technology and Management,
SSTM, Muttom, Aluva.

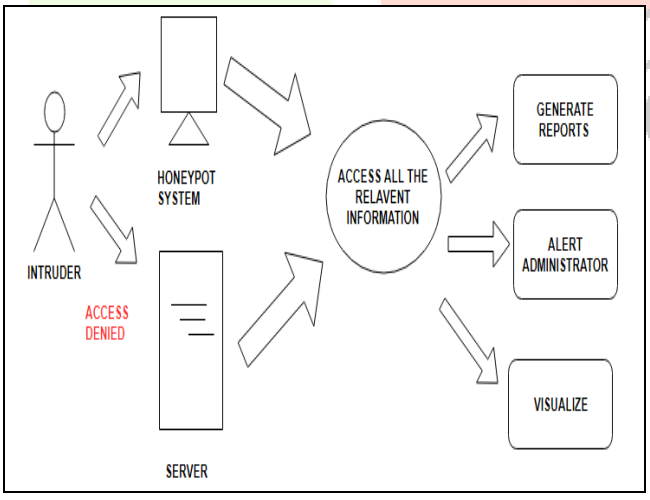
Abstract—Internet attacks have been increasing in a day to day basis and it causes greatest challenge in the data security. Security of data has to be improved and also it must have the power to detect zero-day attack and deploy them. Firewall is one tool that is used to protect the organization from attacks. Intrusion Detection System (IDS) is another tool that is used to discover attacks in an organization. The main disadvantage of these tools is that it produces false alarms; it gathers only less information about the attacker and fails to identify zero-day attacks. Honeypot is a trap for the one who try to attack the system. Honeypot is designed in such a way that it hooks the attacker who tries to attack the system of any organization. In a honeypot network, attacker may not be aware that they are been tracing by gathering all the relevant information.

Keywords: Honeypot, Honeynet, Network security, HoneyTokens, IDS

1. INTRODUCTION

Network security is one problem faced by many of the industries in today's world. The confidential information in industries can be protected and secured by the use of honeypots. Network administrator is responsible for providing security for unauthorized access, modification of message, and misuse of the data. For example: Each user in the network has been provided with some authentication process for accessing the relevant data or information.

Honeypot is a system that attracts the attacker and traps the attacker who tries to access critical information. Security of data involves authentication, confidentiality, encryption of data that are transmitted. Honeypot is a security system that can detect zero-day attacks and solve them. Honeypot systems will look as it is a real host with main applications. When the attacker get accessed into the honeypot system, they are been observed completely. In honeypot systems online hackers are investigated. The information related to the attacker pattern and log analysis, attack methods has been stored in order to learn and improve security.



1.1 HONEYPOT

Honeypot is a kind of modern technology which can be simply detect the threats and identifies the attack and mode or kind of attack to control and optimize the network security. It actually creates a kind of artificial network which contain all the data which is similar to another or same kind of network in which an attacker attempts to attacks the network which unauthorized damage or steal the DMZ (De militarized zone) in which attacker can easily capture the necessary details which can be properly managed and controlled by the administrator in real time. The main aim is to focus on a collection of as much information as possible about their attack patterns, the mode or way by which they steal information and their used programs.

All the accessed information about the attacker is used to learn more about the importance of their patterns and motives, as well as their technical knowledge about the following network and to understand the abilities. It is difficult to find information from a single source that provides an overall picture of honeypot including their benefits, the concepts behind honeypots, the approach to using honeypots and the challenges involved when implementing honeypots.

Honeypot have evolved in diverse directions to cope with various new security threats against not only security defenders but also novice users in the internet today. The recent changes including those in hardware, software and even user demography, have been rapid enough to require a new survey especially on the recent challenges and evolutions in honeypots. Honeypot is a term that is frequently used where honeypots are concerned. A honeypot is simply a network that contains one or more honeypots.

Honeypot is designed to capture extensive information on threats and provides real systems, application and services for the attackers to interact with in a high interaction honeypot. Hackers exploit more tricky and obscure methods when access the system. The traditional approach to security has been largely defensive so far, but interest is increasingly being paid to more aggressive forms of defense.

One purpose of honeypot is to study what the hackers are doing and from which address they are attacking. Honeypots are generally useless and it does not matter whether they attack or hack the honeypots. While they are busy doing it, we can see what kind of methods they use to hack the network as we will be snorting the network traffic all the time and we can locate the source of the attacker. It is just a primary purpose of a honeypot.

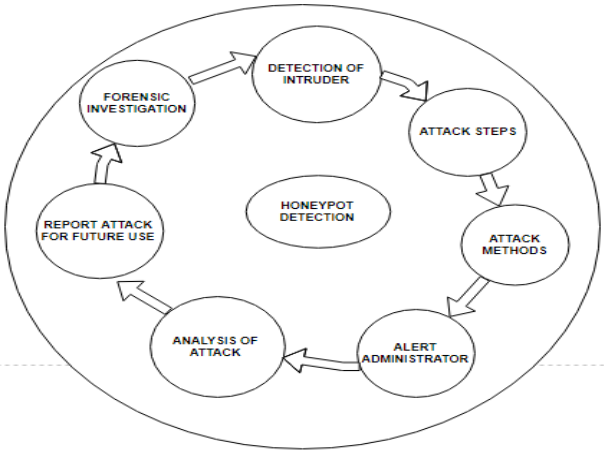
There are a lot of other possibilities for honeypot divert hackers from productive systems or seize a hacker while conducting an attack are just two possible examples. Honeypots can be classified based on their deployment and based on their level of involvement.

Web server, mail server, client etc are forwarded to the legitimate destination and honeypot fulfill the task of luring the attacker. Standard mechanisms are used for protection of web and mail servers.

Honeypot can be implemented internally to the intranet as well as external to the internet. When we place honeypot in front of firewall, the internal network will be secured and reduces risk. While we place honeypot behind the firewall then the activities of attacker can be recorded meanwhile risk will be higher.

The Activities include:

1. Detect unsuspicious traffic in the network.
2. Divert the attacker to a honeypot system which looks like a real host.
3. Identifies the motives of the attacker.
4. Access all the relevant information related to the attacker includes new tools, methods, attacking patterns, log etc. and trap the attacker.



2. CLASSIFICATION OF HONEYPOT

2.1 Production Honeypot

Production honeypot is a honeypot that is used inside the organization to protect and provide more security for the information's within an organization. In production honeypot, when attacker interacts with this system it alerts the administrator about the attack and inform early warning of attack and reduce the risk of losing information. Production honeypots are easy to built and implement in an organization. Even though production honeypot help in reducing the risk and identify the attack but it does not provide detailed information about the attackers.

2.2 Research Honeypot

Research Honeypot does not have any direct advantage to the organization but it provides detailed information about the attacker. This technology is used to learn new tools and methods used by the hacker. It will access the information such as who the attacker is, what method they used, purpose of attack, new techniques used for attack and patterns used. In research honeypots, it provides real operating system for the attacker to interact because of that the risk is higher.

2.3 Low Interaction Honeypot

In low interaction honeypot system, it does not provide any actual system to interact with the attacker. It will be provided some fake services and application to interact with attacker. In this type of honeypot system, the information regarding the attacker will be limited and also the risk is less. The services emulated on low interaction systems are FTP, Telnet, and SQL, SSH etc. The aim of low interaction honeypot is to detect unauthorized activities and unsuspicious login attempts. Example of low interaction system is Honeyd.

Honeyd

Honeyd is a low interaction honeypot it is used for connecting virtual honeypots. Honeypot provides multiple virtual honeypots can be implemented in a single machine. Virtual machine can be can be implemented easily and deploy them. Honeyd can be maintained easily.

2.4 Medium Interaction Honeypot

In Medium Interaction honeypot does not provide a real operating system for the interaction of the attackers. The application is installed in the host system and only provides some services for the public. It will gather much information so that the risk will be increased than low interaction honeypot. Implementation of Medium Interaction honeypot is easy and it can be easily maintained. The failure of this type of honeypot is that the attacker can quickly identify that the system is not behaving as it normally. Example of medium interaction honeypot is Nepenthes.

Nepenthes

Nepenthes are one of the techniques used in medium interaction honeypots. In Nepenthes, it access all the information regarding the attacker and also it informs about the new tools and techniques used for attacking.

2.5 High Interaction Honeypot

High Interaction Honeypot system provides a real operating system for interacting with the attacker. It will gather all the detailed information and behavior can be studied and recorded. In this system, risk is increased and we get more details than the above systems. It is mainly used in production and research honeypots. An Example for high interaction honeypot is Honeynet.

Honeynet

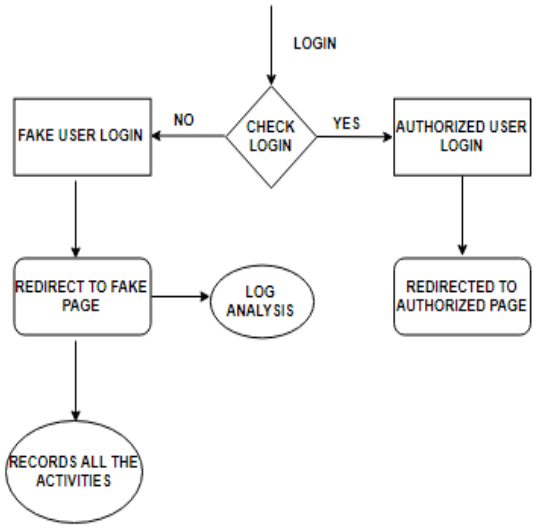
The Honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot". Honeynet is a high-interaction honeypot. High interaction honeypot means that it will give full access to the real operating system for attacking.

Honeynet is a system in which two or more honeypots connected in a network. Each of the system in honeynet is designed as a honeypot which are to be attacked. If a system is attacked, all the details will be collected by the honeynet.

2.6 HONEYTOKENS

Honeytokens are the fake entity that is not a computer but it is a honeypot. Honeytokens can be any database entry, excel sheet etc. The use of honeytoken is based on particular user. Honeytoken can help in knowing the patterns, methods and actions of the attacker.

3. HONEYPOT ARCHITECTURE



- Identify the attacker when accessing the system in the network.
- It will identify the when a normal user and fake user login
- If it is a normal user it will redirect to the genuine page and valuable information's.
- But if it is fake login, then redirect to fake page.

- When it identified as a fake id, it will record all the activities and log details for further learning.
- The details that are recorded can be used for security purpose thereafter and know about the new techniques and tools.

4. APPLICATIONS OF HONEYPOT

Honeypot is used in different areas. It includes:

4.1 Network Security

Honeypot provides more advantage in the network security by tracking the attackers and accessing the detailed information regarding the attack. Network has been provided with the security mechanism and authentication process for detailed data and information.

4.2 Protected Environment

In a protected environment a firewall is placed between in honeypot and the internet. Firewall helps in protecting the honeypot system.

4.3 Unsafe Environment

Honeypot has to be implemented in a safe environment. If it is implemented in an unsafe environment then the IP address and Port number of the system will be accessible so easily and it make the attacker more reliable to access the system and gain the information. So the Honeypot must implement in a safe environment so that the information must be safe and secure.

5. ADVANTAGES OF HONEYPOT

When comparing current security mechanism with honeypot technology, the advantage

- Flexible: Honeypot systems are flexible. It does not have any complicated algorithms or signature to update.
- Resource: Honeypot system access only unauthorized activities so they need minimal recourses.
- Discover new tools: The new tools and patterns that are used for accessing the record is recorded for further learning.
- Reduce false alarms: Honeypot reduces false alarms.
- Simplicity: Honeypot have simple design, no complicated architecture, easy to implement which is more useful for the companies or organizations.

6. DISADVANTAGES OF HONEYPOT

- When an attacker directly interacts with the honeypot systems are been observed and tracked but they does not have vision for the other parts of the system.
- There is huge risk in high level interaction system as it gives access to the real operating system for attacking.

7. FUTURE SCOPE

In the following days network security concerns are high because of the attacks those who want to steal or damage the information regarding the necessary details which can be costly effect the organization or companies.

Honeypot can be used to detect the attacker in real time basis and can be easily findable, which will give a effective network security.

This approach in honeypot works in a way that when an attacker go for an attack it alerts the administrator which basically give a maximum possible details of that particular attacker and also by using honeypot we can easily trace the attacker and its kind or mode of attack and simply managed in a way to deal with the security issues. Honeypot is bitterly design and comes with hybrid solution to detect the enemy in real time basis and trap. Although a many times attacker may know that a honeypot is used in a system to lure him. So further refinement can be done in such a way that attacker does not feels he is being trapped. The attacker by knowing the mode of attacking it actually interpreters the exact details of the following community through they come with their purpose which will clear the problems and effective necessary concerns which provides better relation in network security.

8. CONCLUSION

Honeypot technology as said it is technically designed to control the security threat in the day to day basis. Honeypot gives detailed information of the incidents that how the attacks take place, which time, what mode of attacks is it internal or external. When honeypot has been implemented it makes easy to detect crime and easy to identify the unauthorized access. It also provides better network security also give reliable effect and makes network more secure and safe environment to use.

REFERENCES

[1] Sandeep Chaware, "Banking Security using Honeypot", IJSIA Vol.5, No.1, 2011.
[2] Savita Paliwal, "Honeypot: A Trap for Attackers", IJARCCE Vol.6, March 2017.
[3] Georg Wicherski "Medium Interaction Honepots", in April 7, 2006.
[4] Abhilash Verma, "Production Honeypots: An Organization's view", October 2003.
[5] M.Balamurugan,BSri ChitraPoornima,"Honeypot as a Service in Cloud".
[6] A. Barfar and S. Mohammad. "Honeypots: Intrusion Deception," ISSA Journal, USA; 2007.
[7] Navita Sharma and Gurpreet Singh, "Intrusion Detection System Using Shadow Honeypot", International Journal of Emerging Technology and Advanced Engineering, Volume 2, No 8, 498-00, 2012.
[8] L.Spitzner, "Honeypots: Traking Hackers", 2002.
[9] Akshay A. Somwanshi, "Implementation of Honeypots for Server Security", IRJET Vol.03, Issue: 03 March 2016.
[10] Navnveet Kambow, Lavleen Kaur Passi, "Honeypots: The Need of Network Security", Vol.5 (5), 6098-6101, 2014.
[11] Christian Doring, "Improving networking security with Honeypot".
[12] Aaditya Jain, Bhuwnesh Sharma, Pawan Gupta, "Honeypot: An External Layer of Security against Advance Attacks On Networks", IJIRSE, Vol.No2, Issue 04, April 2016.
[13] Nithin Chandra, S.R, Madhuri, "Cloud Security using HoneypotSystems", International Journal of Scientific and Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518
[14] L. Spitzer, "Honeypots: catching the inside threat", Proceeding of 19th Annual Computer Security Applications Conference, 2003, pp.170-179.
[15] Muhammet Baykara, Resul Das, "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems", International Journal Of Computer Networks and Applications, Volume 2, Issue 5, September-October (2015).

AUTHORS

Mariadas Ronnie C.P received M.Phil Information Technology (IT) in 2012, M.Tech Computer and Information Technology (CIT) in 2011 from M.S University, Tirunelveli, India, MCA Degree from Bharathiar University, and Coimbatore, India in 2001. Currently he is working as Asst. Professor at SCMS School of Technology and Management (SSTM), Muttom. His Research interest lies in the areas of Image
Processing and Network Security.

Devika Prakash is currently pursing Post Graduation in MCA at SCMS School of Technology and Management (SSTM), Muttom, Alwaye, Cochin. Her keen interest lies in the areas of Database Management System and Network Security.