A Study on Honeypot System for Web Based Network

Deepali Jawale
AISSMS IOIT

Abstract- *Honeypots are a new approach for network security. A honeypot is a computer security mechanism set to detect, deflect, and tract t attempts at unauthorized use of information systems. A honeypot is used in the area of internet security and cryptography. This we can use to find attacks that are attempting on the network. It will divert the attacker from the location so that the attacker cannot get actual data. It can used in IDS because it will not generate an false alarm because no productive components are running on the system.. This paper would first give a brief introduction to honeypots the types and its uses. This paper will give the brief detail about what is honey pot its type and the structure and component of honeypot.*

Keywords- Honeypot, IDS(intrusion detection system)

I. INTRODUCTION

Now a days due to World Wide Web communication and accessing or getting data is become very easy. It also improves the cyber crime. Counter various systems are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. But it is not mandatory that each time the attack type will be match to well known patterns day by day hacks and attackers are implementing new strategies to attempt attacks. Honey pot will collect data about attacker and this data we can used against the attacker for securing the system. Then we can prevent attacker from the system.

A honeypot is basically a tool to gather information. A honeypot is resource that is trap set or to divert or discover attempts at unauthorized use of information systems. Honeypots do not have any administration system on network. Its primary purpose is not to be an perform a surprise attack with some attackers but to catch them while doing attack. In this technique we are collecting the every movement of attackers so that later on we can create a database of multiple attacks. This patterns will help use to understand the pattern of attacks and even we can use the patterns for further improvement in system. This is actual purpose of a honeypot. There are a lot other possibilities for a honeypot- divert hackers from systems or seize a hacker while conducting an attack are just two possible examples.

What is after honeypot is Honeynet: - A combination of two or more honeypots on a network is called as a honeynet. A honey net is used to keep track on network in which small system cannot work or single honey pot system cannot work. It can Honeynets can be used as a part of IDs system.

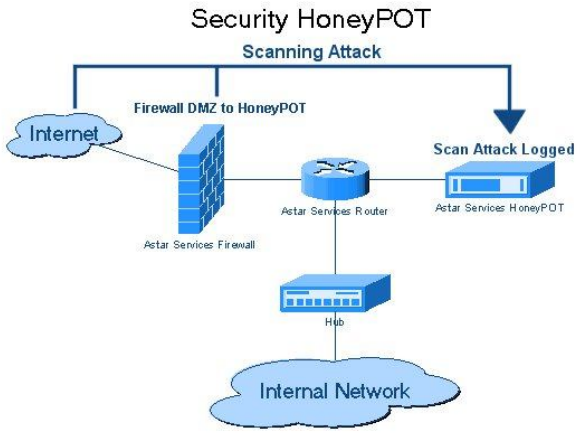

Fig 1. Honeypot

II. MORE DETAIL INTRODUCTION ABOUT SYSTEM

The major objective behind development of honeypot is

1. To keep track on intruder and collect many sample against it. The patterns which are collected used for analysis of how he is attempting the attacks, which methods he used to take access of data. All this useful for developing more secure system.
2. To collect information to form more rules and regulation for forensic so that cyber crimes can be avoided.

There are 3 type of honeypot:
1. Low interaction
2. Middle interaction
3. High interaction

Interaction between intruder and system marks multiple activity and we can learn to prevent the attacks that an intruder may have with honeypot. The honeypots can be used prevent spam. Spammers are searching for webs with vulnerable open relays or less secure webs to forward spam on the other networks. Honeypots can allow intruder to use web so that it can catch all activities. It attracts the intruder with fake servers so that it can observe the activity. The snort is a tool which is usually used for Intrusion detection system and honeypots or honeynets as well. By implementation we can

implement honeypots like virtual and physical. There are two categories of honeypots based on the deployment they are having and the categories are

1. Production honeypots:

This kind of systems are easy, and limited used by only small scale industries where security is not a major issue. Which will look after towards production servers only these are having low interaction, and also having very less information about attackers.

2. Research honeypots

This kind of system are complicated for development, for maintenance and deployment. The main motive about it is to collect samples of attacks it pattern for accessing the information on the secured system and use this information for research purpose.Various organizations are now a days using Intrusion detection system using honeypots.

III. HONEYPOT ARCHITECTURE

LOW-INTERACTION HONEYPOT:-

The low-interaction honeypot is also known as GEN-I honeypot. This system is used for automated attacks and is also used for simple beginner level attack. Honeyd is commmon example and also called as GEN-I honeypot which introduce a device on a network just for testing the system services and their responses for typical network function, on same time system will be act like multiple operating system and this act by honeypot is false kind. This honeypot system will calculate the actual the interaction done between attackers and the dummy server that we have created to be act like server. examples of low interaction honeypots are honeyd, specter, BOF [1]

DRAWBACKS:

1. This kind of architecture provides a limited structure using this we can add more device and enhance structure of system.
2. A single defect or single activity can make attacker alert because of less security.
3. There will be always chance to rebuilt honeypot system because there will be always a huge scope of better system for security.

4. MEDIUM LEVEL INTERACTION:

It is similar to low interaction honeypots because it do not provide OS access to attacker but thre are more chance to capture the attempt than low interaction honeypots . examples like honeypots are Nepenthes.[1]

DRAWBACKS:

Same as low interaction ststem.

5. HIGH INTERACTION HONEYPOT :-

It consists of the following elements: resource of interest, data control, data capture and external logs. High-interaction honeypots are complicated to develop because these kind of systems require real operating systems and application on networks. To capture the attacker's activity they attract attacker to use the web which is of system. Honeynets and Sebek are the examples of high interaction honeypots .As it is used for Research purpose this kind of system is take time to for implementation and design so there could not be any error by this system we can understand what technique, and tacks the attackers are using for attempting an attack.

DRAWBACKS:

1. It is for limited no of honeypots on the network.
2. This is very complex to implement.

APPLICATION

a) It can be used for Cyber Crime Investigation and Network Forensic System .
b) It is used in security system used for e-banking
c) It is used to Prevent DDos Attacks on Cloud.
d) It is used to make cloud system secure
e) It is used for research of new attacks and patterns
f) It is used as structure of large security system.

IV. CONCLUSION AND FUTURE WORK

Now a day's globe is using web for all kind of things like e banking n all so while doing this there should be a secure system which can detect attacks and lock the intruder to access the actual data or traffic on the network the honey pot is talking care of the network traffic could not be read by intruder and prevent attack also secure the data. There are some honeypot software that can be used directly. It is comparatively more efficient than firewall and IDS because it is even detect the attacks and vulnerabilities that we do not know. this can be a part of IDS system to make it more secure.

REFERENCES

[1] Snehal B Rase, Pranjali Deshmukh "Summarization of Honeypot- A Evolutionary Technology for Securing Data over Network, And Comparison with some Security Techniques" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[2] Srivathsa S Rao,Vinay Hegde, Boruthalupula Maneesh, Jyothi Prasad N M, Suhas Suresh"Web based honeypots network" International Journal of Scientific and Research Publications, Volume 3, Issue 8, August 2013 1 ISSN 2250-3153

[3] Ashish Girdhar1, Sanmeet Kaur "Comparative Study of Different Honeypots System" International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 2, Issue 10 (August 2012), PP. 23-27

[4] Muhammet Baykara, Resul Daş, " A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems" International Journal of Computer Networks and Applications (IJCNA) Volume 2, Issue 5, September – October (2015)

[5] Cristine Hoepers, Klaus Steding-Jessen, Luiz E. R. Cordeiro, Marcelo H. P. C. Chaves "A National Early Warning Capability Based on a Network of Distributed Honeypots"

[6] http://www.honeyd.org/

[7] www.wikipedia.com

[8] Janardhan Reddy Kondra , Santosh Kumar Bharti Sambit Kumar Mishra, Korra Sathya Babu "Honeypot-Based Intrusion Detection System: A Performance Analysis" Proceedings of the 10th INDIACom; INDIACom-2016; IEEE Conference ID: 37465 2016 3rd International Conference on "Computing for Sustainable Global Development", 16th - 18th March, 2016 Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)