MAT JOURNALS

Journal of Android and IOS Applications and Testing
Volume 1 Issue 2

Role of Honeypot in Computer Security

Rohini Degaonkar, Savita Khatode

Department of CSE, JNEC, Aurangabad, India

E-mail: sk503921@gmail.com

Abstract

A honeypot could be a deception entice, designed to tempt an offender into trying to compromise the data systems in a corporation. If deployed properly, a honeypot will function an early-warning and advanced security police investigation tool, minimizing the risks from attacks on that systems and networks. Additionally, it offers valuable insight into potential system loopholes. Information assortment is that the major task of network forensics and honeypots are utilized in network forensics to gather helpful information. Honeypot is an exciting new technology with huge potential for security communities. This paper would first provide a temporary introduction to honeypots the categories and its uses, their importance in network security.

Keywords*: Honeypot, network forensics, information, network security, attackers*

INTRODUCTION

In the era of knowledge and technology network security has become the core issue in each structure network. Honeypots are outlined as "a data system resource whose worth lies in unauthorized or illicit use of that resource". Honeypots are integrated in network with firewall and Intrusion detection systems to supply solid secure platform to a corporation. Honeypots introduced within the network to utilize the network's unused IPs and also the attacker's behavior is analyzed on these honeypots.

WHAT IS HONEYPOT?

A honeypot is largely associate in nursing instrument for military operation and learning. A lot of typically a honeypot could be a entice set to divert or discover tries at unauthorized use of knowledge systems. Honeypots do not have any unprotected, unused digital computer on a network being closely watched by administrators.

Honeypots square measure usually virtual machines, designed to emulate real machines, feigning or making the looks of running full services and applications, with open ports that may be found on a typical system or server on a network [1]. A honeypot works by casual attackers into basic cognitive process it is a legitimate system; they attack the system while not knowing that they are being determined covertly. Once associate in nursing assaulter makes an attempt to compromise a honeypot, attack-related info, admire the IP address of the assaulter, are going to be collected. Its primary purpose is not to be associate in nursing ambush for the black hat community to catch them in action and to press charges against them [2].

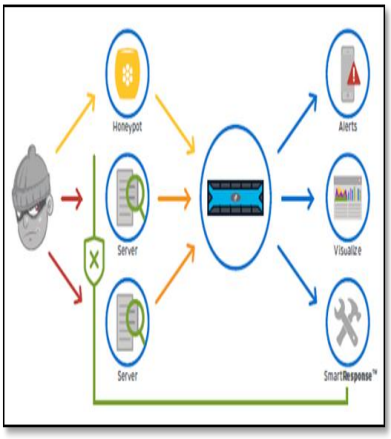

Fig. 1: *Honeypot Diagram.*

TYPES OF HONEYPOTS

Honeypots can be classified into categories:

Low-Interaction Honeypots

Low-interaction honeypots work by emulating bound services and operative systems and have restricted interaction. The attacker's activities area unit restricted to the amount of emulation provided by the honeypot. For instance, associate degree emulated FTP service listening on a selected port could solely emulate associate degree FTP login, or it should additional support a spread of further FTP commands. The advantages of low-interaction honeypots are that they are simple and easy to deploy and maintain [3].

Example: Façades.

Medium Interaction Honeypots

Like low interaction honeypots these also do not provide OS access to attacker but chances to be probed are more than low interaction honeypots. Some examples of medium interaction honeypots are Nepenthes, Dioneae, honey trap, mwcollect. These honeypots also provide facade services to the attackers. Mwcollect and nepenthes can be used to collect the spreading malwares.

High-Interaction Honeypots

High-interaction honeypots are a lot of complicated, as they involve real operative systems and applications. As an instance, a

true FTP server is designed if the aim is to gather data regarding attacks on a specific FTP server or service. By giving attackers real systems to move with, no restrictions are obligatory on attack behavior, associated this permits directors to capture in depth details regarding the complete extent of an attacker's ways [4].

Examples: Sacrificial Lambs, Instrumented Systems [4].

BUILDING HONEYPOTS

To build a honeypot, a collection of virtual machines are created. They are then setup on a non-public network with the host software package. To facilitate information management, a stateful firewall adore science tables is wont to log connections. This firewall would generally be designed in Layer a pair of bridging mode, rendering it clear to aggressor. The ultimate step is information capture that tools adore Sebeka and Term Log is used. Once information has been captured, analysis on the information is performed victimization tools adore Honey Inspector, PrivMsg and Sleuth Kit. Honeypot technology below development can eventually give an oversized scale honeypot readying that redirects suspected attack traffic to honeypot.

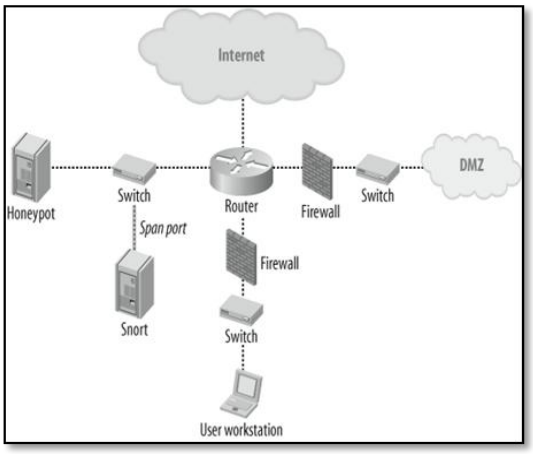

Fig. 2: *Building of Honeypot.*

PURPOSE OF HONEYPOTS

Research Honeypots

Research honeypots area unit primarily accustomed attain info concerning the new ways that of attacks, new attacks, viruses, worms that do not seem to be detected by IDS. These honeypots area unit used for analysis purpose. Principally, academic entities, military or government organizations, these types of honeypots area unit accustomed gathers info concerning motives and new ways concerning the black hat community. Its primary operate is to follow the footprints of offender and gain data concerning the new ways that of attacks performed threats [5].

Production Honeypots

Production honeypots area unit straight forward to deploy, use and capture less data and area unit primarily employed by

firms or firms. These honeypots area unit placed alongside the assembly server within the assembly network of the organization to enhance overall security. It provides immediate security to production resources. Production honeypot tend to duplicate the assembly network or give some services equivalent to FTP, HTTP, SMTP to the attackers [6].

ADVATAGES OF HONEYPOTS

Small Data Sets

Any affiliation created with the honeypot is taken into account as malicious. Therefore, the thousands of alerts logged by organizations will be reduced to many entries.

Reduced False Positives

Honeypots facilitate in reducing false positives. The larger the chance that a security resource turns out false positives or false alerts the less probably the technology is deployed. Any activity with the honeypot is taken into account dangerous and creating it economical in police investigation attacks.

Catching False Negatives

Catching false negatives with the assistance of honeypot is quiet simple as a result of each association created to honeypot is taken into account unauthorized. Ancient attack sleuthing tools becomes fail in sleuthing new attacks like signature primarily based detection tools. These tools discover solely those attacks whose signatures square measure already in their information. As per honeypot's approach, there is no want of predefined information.

Encryption

Honeypots have the aptitude to capture the malicious activity if it is in encrypted kind. Encrypted probes and attacks act with the honeypots as finish purpose wherever the activity is decrypted by the honeypot.

DISADVANTAGES OF HONEYPOTS

1. Honeypots add complexness to the network. Inflated complexness might cause inflated exposure to exploitation.
2. There is additionally level of risk to think about, since a honeypot is also comprised and used as a platform to attack another network. But this risk is often satisfied by dominant the amount of interaction that attackers have with the honeypot [5].

EXAMPLES OF HONEYPOT SYSTEMS

Examples of freeware honeypots include:

Deception Toolkit6

DTK was the first Open Source honeypot released in 1997. It is a set of Perl scripts and C ASCII text file that emulates a spread of listening services. Its primary purpose is to deceive human attackers

LaBrea7

This is designed to prevent or stop attacks by acting as a sticky Honeypot to sight and entice worms and different malicious codes. It will run on Windows or operating system.

Honeywall CDROM8

The Honeywall CDROM could be a bootable CD with a set of open supply computer code. It makes honeynet deployments straightforward and effective by automating the method of deploying a honeynet entry referred to as a Honeywall. It will capture, management and analyze all inward and outward-bound honeynet activity.

Honeyd9

This is a strong, low-interaction Open Source honeypot, and might be run on each UNIX-like and Windows platforms. It will monitor unused IPs, simulate operational systems at the TCP/IP stack level, simulate thousands of virtual hosts at an equivalent time, and monitor all UDP and protocol based mostly ports.

SOME COMMERCIAL HONEYPOTS AND HELPFUL SOFTWARE

Back Officer Friendly by NFR

This product is intended to emulate a back officer server. BOF (as it is ordinarily called) could be a terribly easy, however, extremely helpful honeypot developed by Marcus Ranum and crew at NFR. It is a superb example of low interaction honeypot.

Tripwire by Tripwire

This product is for use on NT and UNIX machines and is intended to match binaries, and inform the service operator, that has been altered. This helps to shield machines from hackers and is wonderful thanks to verify if a system has been compromised.

Mantrap

Mantrap could be a honeypot. Rather than emulating services, Mantrap creates up to four sub-systems, typically known as ‘jails’. These ‘jails’ are logically separate OSs separated from a mother in operation system. Security directors will modify these jails even as they ordinarily would with the other OS, to incorporate putting in applications of their alternative,

resembling Oracle info or Apache internet server, therefore, creating the honeypots much more versatile.

CONCLUSION

Honeypots have their blessings and drawbacks. They are clearly a useful gizmo for luring and housings attackers, capturing info and generating alerts once somebody is interacting with them. The activities of attackers provide valuable info for analyzing their assaultive techniques and ways. However, honeypots do have their drawbacks. As a result of the solely track and capture activity that directly interacts with them, they cannot discover attacks against different systems within the network.

REFERENCES

1. Maximillian Dornseif, Thorsten Holz, Sven M. Uller. Honeypots and limitations of deception.
2. Xiaoyan Sun, Yang Wang, Jie Ren, et al. Collecting internet malware based on client-side honeypot. *9th IEEE International Conference for Young Computer Scientists (ICVCS 2008)*. 2008; 1493–1498p.
3. C. H. Nick Jap, P. Blanchfield, K. S. Daniel Su. The use of honeypot approach in software-based application protection for shareware programs. *IEEE International Conference on Computing & Informatics, (ICOCI '06)*. 2006; 1– 7p.
4. Spitzner, L. Open source honeypots: Learning with honeyed. *Security Focus*; 2003.
5. Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).
6. Karthik, S., Samudrala, B., Yang, A.T. Design of network security projects using honeypots. *Journal of Computing Sciences in Colleges*; 2004.