Honeypot: Concepts, Types and Working

[1]Sneha Padhiar
[1]Assistant Professor [1]Department of Computer Engineering,
[1]Charusat Unniersity,
Changa, India

Abstract:
The Number of attacks on IT system has increased extremely during the last few years. Among the multitude of attack vectors, particularly sophisticated attacks have increased dramatically, which now also increasingly affect small and medium-sized companies. In comparison to other attacks, these attacks comprise some special features like involvement of professional attackers as well as a high knowledge of the offender about the target itself. Attackers use SQL injection and XSS type of attacks to exploit the vulnerability of the system or the organization. A mechanism which is created to learn about the attackers' method of attack and pattern and also used to get useful information about the intrusive activity is Honeypot. Honeypots can be classified according to the level of interaction as low-interaction, medium-interaction, high-interaction and the purposed for which it is used as research honeypot and production honeypot. Detailed study about the types of honeypot is included in this paper

Key words - Network security, Honeypot, Intrusion-detection, Types of Honeypot, Honeynet

I. Introduction:

With the development of Internet, the network of information exchange has been rapid development, to the people's daily lives brings great convenience. With the development of network attack techniques, every host on the internet has become the target of attacks. Therefore, the security of network information can not be ignored as a problem. There are few features of these sophisticated attacks which involve high skilled attackers, also knowledge about the targets etc. So there must be some system to detect those attacks on the databases. Honeypot technology as a new type of active defense theory was invented. The honeypot lures attackers in a pre-arranged manner, analyzes and audits various attacking behavior, tracks the attack source, obtains evidence, and finds effective solutions. A honeypot system can detect attack behavior and redirect such attacks to a strictly controlled environment to protect the practical running system[1]. This system collects intrusion information to observe and record the behavior of the attacker and examine the level, purpose, tools, and intrusion methods of the attack such that evidence can be obtained and possible legal action can be taken..

II. honeypot definition and development

A honeypot system is designed to attract hackers. Thus after an intrusion, network administrators and security specialists an be determine how the attacker succeed, prevent subsequent attacks, and identify security gaps[4]. In addition to identifying the various tools used by hackers, honeypot technology can also identifying the social networks of intruders by determining the relationships among hackers(fig 1).

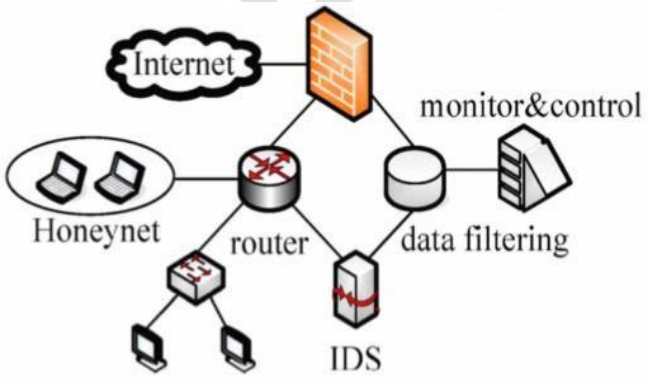

Fig.1 Honey Pot System Design

Honeypot technology is a security resource whose values lies in being scanned, attacked, and captured. This characteristics indic

ates that honeypot technology does not have other actual effects. Therefore, all network traffic that flows into or out of the honeypot may prefigure being scanned, attacked, and captured. The core value of this technology lies in monitoring, detecting, and analyzing intrusive activities. The most popular honeypot tools are the deception tool kit and honeyed[5].

B.Working

Honeypot is a system to collect intelligence. Honeypots are usually located behind the firewall. Honeypot mainly used to simulate a variety of services and holes, to induced the occurrence of various attacks, attack data. When an intruder tries to enter the system with a fake identity, the administrator system will be notified. According to Open Web Application Security Project (OWASP) some top attacks recorded were SQL injection and XSS.[9] When someone tries to enter the system, a log is generated about all the entries. Even though the intruder succeed in entering the system and captures the data from the database, we can fool them by providing fake data, this is done by honeypot, but intruder will not be aware bout this fake information. So by this we can save our system and fool intruders. At the same time the logs will be created, so that all the data about attacker are recorded like system IP, attack type, attack pattern, available footprints etc., and attack method for the evidence which can be used for further actions.

III. HONEYPOT CLASSIFICATION

Based on level of interaction:

Honeypots can be classified based on the level of interaction between intruder and system. These are Low-interaction, high- interaction and medium-interaction honeypot.

Low-interaction honeypot: These types of honeypots have the limited extend of interaction with external system. FTP is the example of this type of honeypot. There is no operation system for attackers to interact with, but they implement targets to attract or detect attackers by using software to emulate features of a particular operating system and network services on a host operation system. Main advantage of this type of honeypot is that, it is very easy to deploy and maintain and it does not involve any complex architecture. With this advantage there is also some drawback of this system. That is, it will not respond accurately to exploits. This creates the limitation in ability to aid in discovering new vulnerabilities or new attack patterns. Low-interactive honeypots are a safer and easy way to gather info about the frequently occurred attacks and their sources. [2][5][6][7]

High-interaction honeypot: this is the most advanced honeypot.[7] This type of honeypot have very higher level of interaction with the intrusive system. It gives more realistic experience to the attackers and gathers more information about intended attacks; this also involves very high risk of capturing of whole honeypot. High-interaction honeypot are most complex and time consuming to design and manage. High- interactive honeypots are more useful in the cases, where we want to capture the details of vulnerabilities or exploits that are not yet known to the outside world. This honeypots are best in the case of "0-Day attacks". Ex: Honeynets: which are typically used for research purpose. [2][5][6]

Medium-interaction honeypot: these are also known as mixed-interactive honeypots.[3] Medium-interaction honeypots are slightly more sophisticated than low-interaction honeypots, but are less sophisticated than high-interaction honeypots. It provides the attacker with a batter illusion of the operation system so that more complex attacks can be logged and analysed. Ex: Honeytrap: it dynamically creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks. [7]

Based on the purpose

Honeypots can be classified based on the purpose as Research honeypot and Production honeypot.

Research honeypot: Research honeypots are basically used for learning new methods and tools of attacks.[8] Research honeypots are used to gather intelligence on the general threats organizations may face, which gives the organization a better protection against those threats. Its main goal is to gain info about the way in which the attackers progress and performs lines of attacks. Research honeypots are complex to build, deploy and manage. They are basically used by organizations like universities, governments, the military and intelligence systems to learn more about threats.

Research honeypots provides a strong platform to study cyber-threats and forensic skills. [7]

Production honeypot: production honeypots are simply aimed to protect the network.[8] Production honeypots are easy to build and deploy, as they require very less functionalities. They protect the system by detecting attacks and giving alerts to administrators. It is typically used within an organization environment to protect the organization. [7][8].

IV. CONCLUSION

Honeypot is a useful tool for luring and trapping attackers, capturing information. Honeypot technologies has changed the traditional passive defense of the network security, is an important expansion to the existing security system[7]. Among all these types of Honeypot low-interaction Honeypot is the mostly used Honeypot, because it is easy to implement and manage. But the most secure and efficient Honeypot type is High-interaction Honeypot. These honeypots provide security as well as generates a log about all entries in the system which is very helpful to find the intrusive activity in the system.

But the honeypot must need to upgrade to new methods and attacks at some interval of time to provide security against new type to attacks. It can't be said as a solution but it is a good supplement for the security system.

REFERENCES

[1] Supeno Djanali, FX Arunanto, Baskoro Adi Pratomo, Abdurrazak Baihaq Hudan Studiawan, Ary Mazharuddin Shiddiqi, "Aggressive Web Application Honeypot for Exposing Attacker's Identity" , 2014 1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE).
[2] Iyad Kuwatly, Malek Sraj, Zaid AI Masri, and Hassan Artail, "A Dynamic Honeypot Design for Intrusion Detection", ©2004 IEEE.
[3] Song LI, Qian Zou, Wei Huang, "A New Type of Intrusion Prevention System", ©2014 IEEE.
[4] Jian Bao,Chang-peng Ji and Mo Gao,"Research on network security of defense based on Honeypot", 2010 international Conference on Computer Application and System Modeling (ICCASM 2010).
[5] Mr. Kartik Chawda ,Mr. Ankit D. Patel ,"Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring", ©2014 IEEE.
[6] Robert McGrew, Rayford B. Vaughn, JR, PhD," Experiences With Honeypot Systems: Development, Deployment, and Analysis", Proceedings of the 39th Hawaii International Conference on System Sciences – 2006.
[7] Iyatiti Mokube , Michele Adams, "Honeypots: Concepts, Approaches, and Challenges".
[8] Feng Zhang, Shijie Zhou. Zhiguang Qin, Jinde Liu, "Honeypot: a Supplemented Active Defense System for Network Security", ©2003 IEEE
[9] https://www.owasp.org/index.php/Top_10_2013-Top_10
[10] Yun Yang, Jia Mi," Design and Implementation of Distributed Intrusion Detection System based on Honeypot", ©2010 IEEE