Honeypot: Concepts, Types and Working

[1]Maitri Shukla, [2]Pranav Verma,
[1] ME Research Scholar, [2]Assistant Professor
[1]Department of Computer Engineering,
[1]SOCET, Ahmedabad, India

***Abstract* - In couple of decades number of attacks on IT organization has increased. Among them small and medium sized organization's risk is higher because of lower security architecture in their system. 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. Various honeypot results are enlisted in this paper to show that how honeypot works in real-time environment and how it responds when any unwanted activity occurs in the network.**

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

IJEDR

I. INTRODUCTION

Attacks on websites and databases are increasing day by day rapidly. Among all of them sophisticated attacks are being increased drastically, which affects small and medium sized companies also. 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. To use honeypot for these systems special care should be given like after applying honeypot the system must look realistic and is capable for generate logs for all suspicious entries. From the basis on this idea we have formed this architecture which is useful to detect attacks and also create logs for all entries in the database, from which we can find if there is any suspicious entry is occurred with wrong purpose.[1] Though hardware based honeypots are very expensive and complex to install for medium and small sized companies, software based low-interaction honeypot are more suitable for that.

According to the Lance Spitzner, Founder of Honeypot Technology, "A honeypot is an information system resources whose value lies in unauthorized of illicit use of that resources".[2]

A honeypot can detect the behaviour of the attacker or the intrusion information to observe and record the details of the attacker and create a log of malicious entries and examines level, purpose, tools and methods used by the attacker so that evidence can be obtained and further actions can be taken. [3]

Honeypot technology and traditional security system combined can build an active network security protection system.[4]

II. HONEYPOT CLASSIFICATION

A. 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]

B. 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]

III. SYSTEM DESIGN OF HONEYPOT

A. System architecture

General system design of honeypot architecture is shown in Fig-1. Entire network is firstly protected by a firewall, then by a router and compartmented data layers are separated from network inside the organization and outside customers' or operations' network. Organization network is then protected by a mechanism called as honeynet, which is a network of computers participation in honeypot architecture. For extra security and detection IDS is implemented in the system. Monitoring control system supports to manage the logs created by the honeynet and also monitors all the incoming entries in the network.

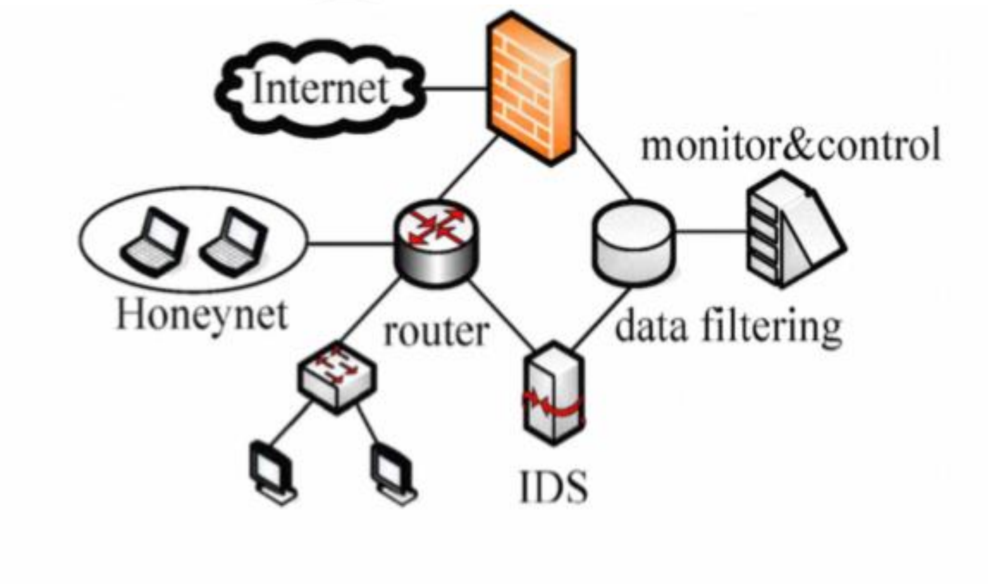

Figure 1: system design of the honeypot architecture. [4]

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.

IV. SURVEY RESULTS

Table1 shows the experimental results of various recent honeypot.

Table 1: Result analysis of different honeypots

Sr No.	Title	Type of honeypot	Result	Remarks
1.	Aggressive Web Application Honeypot for Exposing Attacker's Identity [1]	Web based low-interaction honeypot	SQL-injection test is done using SQLMap, and this honey pot successfully handled it. Likejacking test several Facebook accounts were successfully caught.	Machine generated attacks can also be handled, social media accounts can be helpful to get more information like location and

				personal details of the attacker.
2.	Research on Network Security of Defense based on Honeypot [4]	Low-interaction honeypot (Honeyd)	Honeypot simulation system exposure to worm holes and then capture and analyse details about the features of the worm, which limit the spread of warm in the network.	Low-interactive honeypots can also be used to give security against the worm in the network.
3.	Design and Implementation of Distributed Intrusion Detection System Based on Honeypot [10]	Low-interaction honeypot (Honeyd)	The highest detection rate of the intrusion is 88.32% at threshold value 30 which is for probing type of attack. The lowest detection rate is 61.12% for R2L at threshold value 50. The missing rate of the honeypot varies between 1.43% to 7.11%.	This honeypot is more efficient for probing type of attacks. Missing rate is lower when the threshold value is 40-50, but it is higher when the threshold is low. Less efficient for R2L.

V. CONCLUSION

Honeypot is a useful tool for luring and trapping attackers, capturing information. Security is the essential element of any organization web sites, but though the security provided by the honeypots based on hardware setups are very expensive for small and medium scaled organization; a software based honeypot may be proven as a very effective security solution for these organizations. 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.

VI. FUTURE SCOPE

From the above conclusion it is clear that low-interaction Honeypot is most popular and widely used because of its ease of deployment but there are some disadvantage like it may not detect all the attacks and gathers limited information only. Whereas high-interaction honeypot is complex to manage and deploy but gathers more precise details. Future challenge will be combining both types of Honeypot and design a hybrid kind of Honeypot which will have advantages of both the approaches. This can have moderate complexity and it should obtain more precise information of the intruder.

VII. 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