Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 3, March -2017

A Survey on Honeypot Technology : Concepts, Types and Working

Binal S. Naik[1], Harshal Shah[2]

[1] *Department of Computer Engineering, PIET, Parul University, Vadodara*
[2] *Department of Computer Science and Engineering, PIET, Parul University, Vadodara*

Abstract — *Information security is a rising concern today in this era of the internet. HoneyPots are fake computer Systems which appears vulnerable to attack though it actually prevents access to valuable sensitive data and administrative controls. A well designed and developed Honeypot provide data to the research community to study issues in network security like Internet worms, Zero-day attacks, spam control, DoS attacks, etc. In this paper we present a detailed overview on Honeypot technology.We examine different Types of Honeypots, Honeypot concepts and approaches in order to determine how we can intend measures to enhance security using these technologies*.

Keywords- *Honeypot; Types of honeypots; IDS; intrusion detection/prevention system; network security*

I. INTRODUCTION

In recent years, with the development of internet network has extended to every social corner. People have been led into the era of information technology. In this process the network environment becomes more and more complicated. The threat is becoming the multi-source and dynamic [1]. Security mechanisms such as routing security, identity authentication, encryptions and firewall are static, passive security mechanisms. The static security technologies play an important role to prevent illegal intrusion but from the management perspective, the only passive defense is not sufficient.

IDS can't give alert when intrusion occurred using new signature. Even worse, we can't down the service system to check it completely because there still many online users making their deals [2]. Intrusion detection system is divided into two categories : anomaly detection and signature detection (misuse detection). Anomaly detection based on protocol can verify the unknown attacks effectively, but cannot detect attack violating an agreement [3]. Misuse detection system matched attack action with stored attack signature in intrusion rule databases. This method achieves a high detection rate and required less time. However, signature detection system is unable to distinguish new type of attacks or a large number of complicated attacks [3]. Traditional security technologies cannot solve the problem.

II. HONEYPOT TECHNOLOGY

The Honeypot technology is an attempt to conquer the shortcomings of the intrusion detection systems.
Definition :
"A Honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource [6]."

A. What is Honeypot

A Honeypot is a decoy, put out on a network to attract attackers. Honeypots are designed as the emulation of the real machines, creating the appearance of running full services and applications, with open ports that might be found on a typical system or server on a network. This way honeypot mimic the real system,create confusion for attackers and monitor the intruder without risk to production servers or data. Honeypot technology is not to replace the traditional security mechanisms and defense technologies, but it's supporting and complementary. Honeypot technology proactively detect and respond to network intrusion and attacks [4]. A honeypot system can detect attack behavior and redirect such attacks to a strictly controlled environment to protect the practical running system [5]. This system collects intrusion information to examine and record the behavior of the attacker. It also examines the level, tools, purpose, and intrusion methods of the attack such that evidence can be obtained and possible legal actions can be taken.

Carefully set by the Honeypot system to attract hackers, and hackers to track, the intruder can be observed record system [4]. Honeypot can be a computer simulation of a known hole or a service computer, also can simulate a variety of operating system and its corresponding features, or just a normal standard operating system, and only through special processing can be a complete record of the attacker's attack.

B. Honeypot Work Principle

A honeypot works by fooling attackers into believing it is a legitimate system.So attackers attack the system without knowing that they are being observed completely. Honeypot looks like a really host provided important service, so it has more attraction to hacker. through its attraction to hackers and being attacked, the related information of the attackers such as the IP address, motives of the attackers entering the system and attack behavior of the attacker will be collected. Which is done generally through the implementation of the background software [7]. Which monitors and records the network communication data between the attackers and honeypot host, and uses some analytical tools to interpret and analyze these data. Data capture is a difficult section to any honeypot which have the ability to capture everything the attacker is doing. It can also capture the packets and packet payloads involved in the attack. This information can prove important in analyzing the attackers' activities.

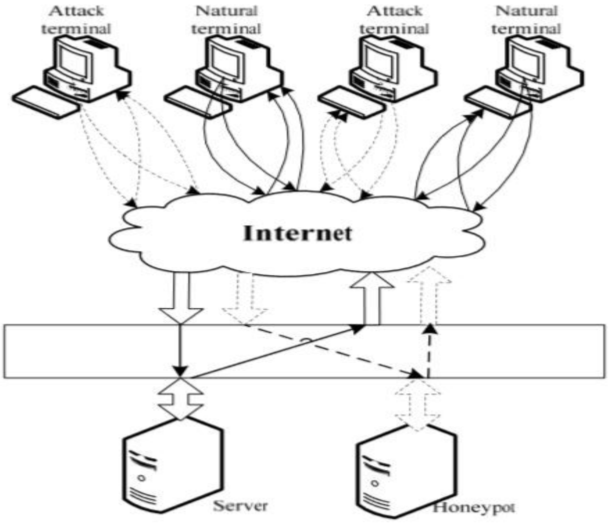

Figure 1. Honeypot Work principle

Honeypot system has generally three modules which are induced, deceive and analysis. The induced module is used to attract the attackers to attack on the Honeypot system. The deceived module calls the simulation information from the database for the deceived host to generate false information which will be sent to the attackers [7]. All the induction and deception events of the system are recorded in the remote log server, and analyzed by the analysis module for adjusting the induction and deception strategy.

III. CLASSIFICATION OF HONEYPOT

According to the Design Deployment honeypot can be classified into Production and Research honeypot.

A. Production Honeypot

A production honeypot is one used within an organization's environment to protect the organization and help mitigate risk [8].Production honeypots emulate the production network of the company. Attackers interact with them in order to expose vulnerabilities of the production network. Uncovering these vulnerabilities and alerting administrators of attacks can provide early warning of attacks and help reduce the risk of intrusion[9].It is placed inside the production network with other production servers like firewall to improve their security. Production honeypot helps to reduce the risks of intrusion and add values to the security measures of an organization.

Production honeypot require less functionality then a research honeypot. They are easier to build and deploy. Although they identify attack patterns, they does not give much information about the attackers than research honeypots. You may learn from which system attackers are coming from and what exploits are being launched, but maybe not who they are, how they are organized, or what tools they are using [10].

B. Research Honeypot

Research honeypots are real operating systems and services that attackers can interact with. Generally It is designed to get knowledge about the blackhat community. They involve higher risk, collect extensive information and intelligence on new attack techniques and methods. So it provides a more accurate picture of the types of attacks. It is used to research the threats organizations face and helps to provide better protection against those threats. Research Honeypot is more complex to deploy and maintain. They are used primarily by research, military, or government organizations.

Research honeypots add tremendous value to research by providing a platform to study cyber threats. Attackers can be watched in action and recorded step by step as they attack and compromise the system. This intelligence gathering is one of the most unique and exciting characteristics of honeypots [11].

According to the Honeypot with Different Attacker Interaction Level, we may divide honeypots into three major classes: low-interaction, medium interaction, and high-interaction.

C. Low- interaction Honeypot

Low-interaction honeypot systems do not provide intruders with the actual operating system for remote login [5]. They are used for simulating the specific function or service which is running in the existing system, attackers can only have movement in this controlled range. A low-interaction honeypot provides specific analog services that can be conducted by monitoring a specific port [12]. Low interaction honeypots emulate network services on preconfigured port, such as FTP, SQL, Web, SSH, etc. Example: Honeyd, Specter

D. Medium–interaction Honeypots

Medium-interaction honeypots provide the attacker with a better illusion of an operating system since there is more for the attacker to interact with. More complex attacks can therefore be logged and analyzed [10]. They can capture more information, and have stronger concealment than low interactive honeypots. They more efficiently interact with intruder than do low-interaction honeypots but less functionality than high-interaction honeypots.

This type of honeypot system emulate a specific service which causes intruders to think that they are attacking the real operating system. It enables the system to collect high amounts of data but increases the risk of intrusion.
Example: mwcollect, nepenthes and honeytrap

E. High-interaction Honeypots

High interactive honeypots are configured with real operating system and provide a real operating system for attackers. They are a complex solution and involve the deployment of real operating systems and applications [13]. High interactive honeypot allows attackers running all the instructions in the real operating system. So there are high chances for collecting large amounts of information, as all actions can be logged and analyzed. Any error in the system may allow a hacker to control the full operating system, attack other systems, or intercept messages in the application system [14].

High-interactive honeypots are more useful to capture the details of vulnerabilities or exploits that are unknown to the outside world. This honeypots are best in the case of Zero Day attacks.
Exampls: Honeynets Sebek

IV. ADVANTAGES AND DISADVANTAGES OF HONEYPOT

A. Advantages

- Honeypot creates confusion for attackers by giving them bogus data.
- It can provide forensic evidence that is admissible in a court of law. it can be used as legal evidence As long as it is deployed correctly and is not advertised,
- Honeypots can be used to intruder attacks. Knowing that a system is set up to capture and log all activities may scare away would be intruders.
- The properly designed and configured Honey Pot provides data such as the IP address, motives of the attackers entering the system and attack behavior of the attacker will be collected.
- Honeypots divert intruders from the production system making them use all of their efforts in a harmless manner.
- Honeypots are fairly not expensive.Some simple versions are free to download.
- Honeypots can detect insider attacks by providing valuable information on the patterns used by insiders.

B. Disadvantages

- Honeypots can only track activity that interacts with it. They have a narrow field of view. They only see what activity is directed against them.
- Honeypots are also at risk because attackers may misuse honeypot to harm other systems [16]
- Another disadvantage of honeypots is fingerprinting. Fingerprinting is when an attacker can identify the true identity of a honeypot because it has certain expected characteristics or behaviors [17].
- Another disadvantage is that honeypots must be maintained like any other networking equipment and services.

- Building a honeypot requires that you have at least a whole system dedicated to it and this may be an expensive resource for some corporations.

V. LITERATURE SURVEY

Table 1. Literature Survey

Title	Type of Honeypot	Results	Remarks
Aggressive Web Application Honeypot for Exposing Attacker's Identity [18].	Web based low-interaction honeypot	Detects cross site scripting and SQL injection	SQL-injection test is done using SQLMap, and this honey pot successfully handled it. Like jacking test several facebook accounts were successfully cached.
Research on Network Security of Defense based on Honeypot [4].	Low-interaction honeypot (Honeyd)	Gives security against the worm in the network	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.
Design and Implementation of Distributed Intrusion Detection System based on Honeypot [3].	Low-interaction honeypot (Honeyd)	This honeypot is more efficient for probing type of attacks	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.
Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring [13]. .	Low interaction (front-end) High-interaction(Back-end)	Track Internet threats such as worms or automated attacks	Design includes a dynamic & hybrid honeypot engine that integrates data collected from passive fingerprinting tools such as POf and active probing tools such as Nmap to dynamically configure Honeyds
Detecting and Analyzing Zero-day Attacks using Honeypots [19].	Low -interaction and High - interaction Honeypot	Provides security against zero-day attack	As this paper shows, it is easier to use and implement a detecting method for Honeyd as it offers logging capabilities. On the other hand, we can get more valuable information by using a high-interaction honeypot.

VI. CONCLUSION

Honeypot is not a solution or replacement to network security but a good tool supplements other security technologies to form an alternative active defense system for network security. This paper presents detail concept of Honeypots, how they are designed to attract intruders so that their activities can be monitored without risk to production systems or data. Honeypot must need to upgrade to new methods and attacks at some interval of time to provide security against new type to attacks. Honeypots can be used for production or research purposes. Compared with other security mechanisms honeypot is simple to configure. Honeypots occupies less resource and working effectively in a complex environment. Well desiged and configured honeypot can also detect unknown attacks.

REFERENCES

[1] Suo, Xiangfeng, Xue Han, and Yunhui Gao. "Research on the application of honeypot technology in intrusion detection system." Advanced Research and Technology in Industry Applications (WARTIA), 2014 IEEE Workshop on. IEEE, 2014.

[2] Zhang, Feng, et al. "Honeypot: a supplemented active defense system for network security." Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003. Proceedings of the Fourth International Conference on. IEEE, 2003.

[3] Yang, Yun, and Jia Mi. "Design and implementation of distributed intrusion detection system based on honeypot." Computer Engineering and Technology (ICCET), 2010 2nd International Conference on. Vol. 6. IEEE, 2010.

[4] Bao, Jian, 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). Vol. 10. IEEE, 2010.

[5] Koch, Robert, Mario Golling, and Gabi Dreo. "Attracting sophisticated attacks to secure systems: A new honeypot architecture." Communications and Network Security (CNS), 2013 IEEE Conference on. IEEE, 2013.

[6] Martin, William W. "Honey pots and honey nets-security through deception." SANS Institute Paper (2001).

[7] Li-Juan, Zhang. "Honeypot-based defense system research and design." Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on. IEEE, 2009.

[8] Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 20 (4).

[9] Gubbels, Kecia. "Hands in the Honeypot." GIAC Security Essentials Certification (GSEC) (2002).

[10] Mokube, Iyatiti, and Michele Adams. "Honeypots: concepts, approaches, and challenges." Proceedings of the 45th annual southeast regional conference. ACM, 2007.

[11] Spitzner, Lance. "The value of honeypots, part one: Definitions and values of honeypots." Security Focus (2001).

[12] R. Berthier, D. Korman, M. Cukier, M. Hiltunen, G. Vesonder, and D. Sheleheda,ĀOn the Comparison of Network Attack Datasets: An Empirical Analysis," 11th IEEE High Assurance Systems Engineering Symposium, 2008. HASE 2008, 2008,pp. 39-48.

[13] Chawda, Kartik, and Ankit D. Patel. "Dynamic & hybrid honeypot model for scalable network monitoring." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014.

[14] E. Cooke, M. Bailey, Z.M. Mao, D. Watson, F. Jahanian, and D. McPherson,ĀToward understanding distributed blackhole placement," Proceedings of the 2004ACM workshop on Rapid malcode, ACM New York, NY, USA, 2004, pp. 54-64.

[15] Baumann, Reto, and Christian Plattner. "Honeypots." White Paper, Swiss Federal Institute of Technology (2002).

[16] Spitzner, Lance. "The honeynet project: Trapping the hackers." IEEE Security & Privacy 99.2 (2003): 15-23.

[17] Spitzner, Lance. Honeypots: tracking hackers. Vol. 1. Reading: Addison-Wesley, 2003.

[18] Djanali, Supeno, et al. "Aggressive web application honeypot for exposing attacker's identity." Information Technology, Computer and Electrical Engineering (ICITACEE), 2014 1st International Conference on. IEEE, 2014

[19] Musca, Constantin, Emma Mirica, and Razvan Deaconescu. "Detecting and analyzing zero-day attacks using honeypots." Control Systems and Computer Science (CSCS), 2013 19th International Conference on. IEEE, 2013