IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

An Overview of Honeypot Systems

Neha Titarmare[1*], Nayankumar Hargule[2], Anand Gupta[3]

[1]Department of Computer Science & Engineering, Rajiv Gandhi College of Engineering & Research, Nagpur, India
[2]Department of Computer Engineering, Suryodaya College of Engineering & Technology, Nagpur, India
[3]Department of Computer Technology, KDK College of Engineering, Nagpur, India

[*]Corresponding Author: nehatitarmare@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i2.394397 | Available online at: www.ijcseonline.org

Accepted: 17/Feb/2019, Published: 28/Feb/2019

Abstract— In today's world, network security is a very crucial issue. Providing security to the network, services is a major concern these days. Therefore, in this paper we study the concept of Honeypots. A Honeypot is a fake system which lures the attackers. The attackers give in to the temptation and launch attacks. Such attacks help the researchers and organization to study the attack patterns and gain vital information about the attackers. A honeypot is only meant to tantalize the intruders, attackers to perform the malicious activity which results in revealing information about attacks. Thereby, honeypots are quite useful in preventing and counter attacking various types of attacks. We can build Honeynet, Honeywalls using the concept of Honeypots. In this paper, we focus on the concept of Honeypot systems and represent the various aspects of honeypots. We also discuss the various types of honeypots along with its advantages and disadvantages. We also focus on the concepts of Honeynet and Honeywalls.

Keywords— Honeypot, Honeynet, Honeywalls, Intruders

I. INTRODUCTION

Honeypot systems are extensively used in Intrusion Detection technology. Honeypots can be defined as systems used to entice attackers, intruders, malicious users away from the main systems [1]. Honeypots have been designed with the aim to distract the attackers from critical systems and to gain vital information about their malicious activity. Honeypot systems are developed with fake information so that it appears important. The system is often equipped with monitors and event loggers. This equipment monitor, keep an eye on all the accesses and activity carried on honeypot. In this way, who so ever accesses honeypot becomes a suspect. Honeypot can be said to be a trap, as it is set for trapping the adversary. All the data from honeypot is recorded. These records are analyzed to learn about new attack patterns which pose a threat to vital resources. The value of honeypots and the problems they help solve depend on how you build, deploy, and use them [2]. Honeypots are of no use if they are not attacked [3]. Fig. 1 gives an idea of honeypot systems.

Characteristics of Honeypot Systems:

1) Honeypot plays a significant role in preventing the attacks and malicious activities.
2) It improves the attack detection time, response time [4].
3) It extracts the intrusion behaviour profiles, system behaviour and methods used to launch attacks.
4) It intercepts the behaviour patterns of adversary.
5) It records all the activities of Intruder [5].
6) They can be physically deployed or can be virtually set up [6].
7) Honeypots are expected to have zero false alarms [7].

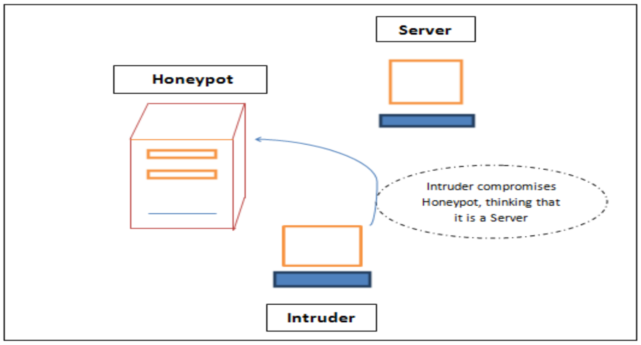

Figure.1 Honeypot Systems

The figure 1. illustrates the honeypot system. Here the attacker gets attracted to honeypot and attacks it.

The rest of the paper is organized as follows: in the next section we will discuss the various advantages of the honeypot systems. In section 3, discusses the disadvantages of the honeypot systems. In section 4, we present the various categories of Honeypot systems. The section 5, gives presents the concept of Honeynet and section 6, describes the concept of Honeywalls. In the last section that is 7, conclusion is illustrated**.**

II. ADVANTAGES OF HONEYPOT

1) Data Value
Honeypots collect data which is of great value. It gathers precise data which is easy to understand. This facilitates easy analysis of data.

2) Resources
Honeypots do not face the problem of resource exhaustion unlike other security mechanisms. This is so because they capture data directed to them only. Thereby, less money needs to be spent on hardware for installing Honeypots. They are much cheaper as they do not require current technologies, RAM with huge capacity or disk drives.

3) Simplicity
They are simple as they do not require high end algorithms, configurations. Also they are much easy to use. Simply deploy them and monitor is what we require to do.

4) Return on Investment
Honeypots are quite valuable as it quickly captures the malicious activities. It reflects the security mechanism level of the system.

5) Reduce false positives
Various security mechanisms provide a potential amount of false positive alert messages but honeypots do not provide false positives as it is mostly accessed by the intruders.

Also, additionally honeypots help to understand various new vulnerabilities, threats and attack patterns [8].

III. DISADVANTAGES OF HONEYPOT

1) Narrow Field of View
One of the disadvantages of Honeypots is that they are narrow in their perspective. They only capture that malicious activity which is launched against them.

2) Fingerprinting
Another demerit is Fingerprinting. It means that an attacker can identify the true identity of a honeypot because it has certain expected characteristics or behaviours.

3) Risk
The last disadvantage of honeypots is risk. They pose a risk to the overall system. It means that honeypots can be used as a platform to launch attacks and infiltrate. The risk depends upon the complexity of honeypot systems. Simple honeypots pose less risk.

Due these disadvantages, honeypots cannot take place of Intrusion detection systems (IDS) and firewalls. They give an added advantage to these systems and play a vital role in defence mechanisms.

IV. TYPES OF HONEYPOT

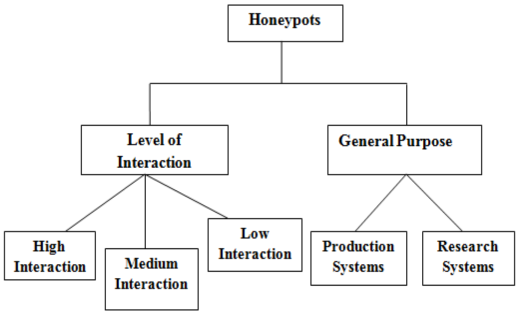

Figure. 2 Classifications of Honeypots

Honeypots can be classified in two categories based on their level of interaction with the intruders and on the basis of their purpose. Figure 2 shows the classification of Honeypots systems.

Productive honeypots
Production honeypots are used to protect an organization or a corporation. They are implemented so as to protect and secure the environment. They also mitigate the attacks and risks. Production honeypots are the law enforcement of honeypot technologies [2]. Production honeypots are used by commercial organizations to reduce the risk of attackers. These systems are easy to deploy, implement and maintain. They are simple, have less functionality and thereby involve less risk. Production honeypots provide a limited amount of information because of their functionality [2]. They can only provide data about the compromised systems, what exploits intruders launch. They do not give details about the attack profiles or tools used. They are generally low interaction honeypots and provide less information than research honeypots.

Research honeypots
Research honeypots are used by research, military or government agencies. They are specifically used for research purposes, so as to learn about the potential threats posed to the organization. They provide details about the attack

patterns, profiles, who the attacker are, tools used to launch the attacks, motive of the attacker, communication patterns and so on. Research honeypots penetrate into the system deeply to extract the information about intruders. They create the real environment of the operating system to learn about the attackers. These systems are quite complex and involves a great risk. Also, it requires more efforts and time of an administrator [2].

Honeypots are also categorized on the basis of design criteria or level of interaction [6]:

1) High Interaction Honeypot
2) Medium Interaction Honeypot
3) Low Interaction Honeypot
4) Pure Honeypots

Level of interaction stands for how much the hacker will be able to interact with the system [8]. The interaction level determines the amount of data gathered from the adversaries.

1) High Interaction Honeypots

.

High Interaction Honeypots usually collects a large amount of data as they interact more. However, such systems are more risky as they allow the intruders to penetrate into the system and access it to a great deal. They are complex and difficult to build and maintain. The purpose of a high-interaction honeypots is to give the attacker access to a real operating system where nothing is emulated or restricted. This system provides a great deal of opportunities to identify various threats and vulnerabilities and thus is the most powerful [2]. Argos is an example of this type of honeypot [8, 9].

2) Medium Interaction Honeypots

Medium Interaction honeypots are less capable than High interaction but more than Low interaction honeypots. They do not contain operating system. They are less advanced than the high interaction ones but have certain level of security holes. This causes the intruder to attack the system. Mwcollect, honeytrap and Nepenthes are some of the examples of medium interaction honeypots [8].

3) Low Interaction Honeypots

The low interaction honeypots systems provide the minimal amount of information. It is only use for the sake of capturing malicious information. The amount of risk is less as the data is less. These systems are easy to install and configure as compared to the other two. It does not contain the real operating system. They only mimic the services of Operating systems [10]. Honeyd is an example of this category of Honeypots.

4) Pure Honeypots

Pure Honeypots are nothing but a well established production system. A bug tap is installed on honeypot’s link through which the malicious activities are monitored.

V. HONEYNET

A honeynet is collection of various honeypots. They are special networks developed to lure the attackers. The aim of a Honeynet is to collect information about malicious activity. This recorded data is later studied by the investigators to extract the useful information [11]. Honeynet are high interaction honeypots [2]. They are very flexible and act like any honeypot. They can easily fool any blackhats as they will require sufficient amount of time to determine the fake system. A Honeynet can run almost any conceivable operating system and application [2].

The honeynet is made up of core elements [12, 13]:

- Data Control - It refers to capturing and recording malicious activity of the intruder.
- Data capture - It refers to controlling the activity of attacker.
- Data Collection - It refers to storing and preserving data at a central location.
- Data Analysis - It refers to investigation of all the collected data.

VI. HONEYWALLS

The honeywall can be said to be a transparent bridge that restricts the malign data to leave the honeynet. This prevents other systems on honeynet from being harmed. Thus, honeywall provides data control and keeps a check on outbound traffic [6].

VII CONCLUSION

Honeypots are a potential tool in the world of security. They provide an added benefit if they are used with firewalls or intrusion detection systems. They are available for commercial as well as research purposes and are quite flexible to fulfill our requirements. Honeypots have been used in various deception techniques like Honey farms, Simple port listener, honeypots as mobile code throttlers, Random Servers, digital breadcrumbs [14, 15]. Thorough care must be taken while deploying honeypots as it involves substantial amount of risk. Hence, a tight risk analysis needs to be done prior to deployment. Also strict rules must be framed for the maintenance purpose. They are cheaper, flexible, provide low false positive rate, can extract encrypted data. Laws and legal issues must be considered for deploying honeypot systems. Honeypots can reap great benefits if they are used in a smart way by using various new technology trends.

REFERENCES

[1] William Stallings "Cryptography and Network Security Principles and Practices" Prentice Hall Publication, pp. 581, 2005.

[2] Lance Spitnzer "Honeypots: Tracking Hackers" Addison Wisley Longman Publishing Co.in, 2002.

[3] Liu Dongxia, Zhang Yongbo, *"An Intrusion Detection System Based on Honeypot Technology"* , In the Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE2012), Hangzhou, pp. 451-454.

[4] Tao, Jing. Immune-based intrusion prevention model [J]. Network and Information, 200907

[5] Peng Hong, Wang Cong, Guan Xin *"Intrusion Prevention System in the Network of Digital Mine"* 2nd International Conference on Computer Engineering and Technology, Volume 6, pp. 296-299, 2010.

[6] M. Sqalli, R. AlShaikh, E. Ahmed *"Towards Simulating a Virtual Distributed Honeynet at KFUPM: A Case Study"* UKSim Fourth European Modeling Symposium on Computer Modelling and Simulation.pp. 316-321, 2010

[7] Ariel Bar, Bracha Shapira, Lior Rokach and Moshe Unger, *"Identifying Attack Propagation Patterns in Honeypots using Markov Chains Modeling and Complex Networks Analysis"* IEEE International Conference on Software Science, Technology and Engineering , pp. 28-36, 2016.

[8] Thesis on "Honeypots in Network Security" by Deniz Akkaya-Fabien Thalgott, School of Computer Science, Physics and Mathematics, Linnaeus University, 29th June 2010.

[9] Gérard Wagener. "Self-Adaptive Honeypots Coercing and Assessing Attacker Behaviour" Computer Science [cs]. Institut National Polytechnique de Lorraine - INPL, 2011. English.

[10] Jules Pagna Disso, Kevin Jones, Steven Bailey, *"A Plausible Solution SCADA Security: Honeypot Systems"*Eighth International Conference on Broadband, Wireless Computing, Communication and Applications,pp. 443-448, 2013.

[11] Mohammed H. Sqalli, Shoieb Arshad, Mohammad Khalaf, Khaled Salah, *"Identifying Scanning Activities in Honeynet Data using Data Mining"* Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 178-183, 2011.

[12] A. Mairh, et al., Honeypot in network security: a survey, In: Proceedings of the 2011 International Conference on Communication, Computing & Security. ACM, 2011. p. 600-605.

[13] L. Spitzner, Honeypots: Catching the insider threat, In: Computer Security Applications Conference 2003, Proceedings. 19th Annual. IEEE, 2003. p. 170-179, 2003

[14] Dissertation on "Deception Techniques Using Honeypots" by Amit D. Lakhani, Information Security Group Royal Holloway, University of London, UK.

[15] Keith Harrison, James R. Rutherford, and Gregory B. White *"The Honey Community: Use of Combined Organizational Data for Community Protection"* 48th Hawaii International Conference on System Sciences, pp. 2288-2297, 2015.