International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June -2018 www.irjet.net p-ISSN: 2395-0072

Detecting Hacker activities using Honeypot

Vijay Singh[1], Vaishali Gatty[2]

[1]*Student, Master of Computer Applications, VES Institute of Technology, Mumbai university, Maharashtra, India*
[2]*Professor, Master of Computer Applications, VES Institute of Technology, Mumbai university, Maharashtra, India*

Abstract - *From past couple of decade many types of attacks have increased day by day in IT sector. The major reason behind this is, due to lower security architecture, Organization which are small and medium in size are more prone to such threats. To exploit the vulnerability of the system or the organization attackers use SQL injection and XSS type of attacks. A Honeypot is a computer security mechanism which is designed to track the attackers, pattern of attack, detect attempts at any unauthorized use of information systems so it can learn from the attacks and further use this information to improve security. Based on deployment there are two types of honeypots research honeypot and production honeypot. On the basis of implementation of honeypots, they can be classified as low-interaction, medium-interaction, high-interaction. A detailed study about all these types of honeypot and some most popular honeypots is included in this paper.*

Key Words: **Honeypot, Types of Honeypot, Honeynet, Intrusion-detection, Network Security**

1.INTRODUCTION

Definition of honeypot 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". A honeypot is a nearly monitored computing resource that we want to intruded, probed, attacked, or compromised. A honeypot can catch each activity of an attacker or intruder make inside the honeypot. A honeypot can catch keystrokes, can recognize the files accessed and modified, can log access attempts, can identify the programs executed inside honeypot [4]. If an attacker is uninformed that he/she's inside a honeypot we can even distinguish his ultimate intentions. The gathered information can prove to be quite critical against the attacker. Honeypots are not generally designed to recognize hacker. Developers of honeypots are more interest on getting into the brains of hackers so they can design more secure systems as well as to educate others experts about the lessons learned through their effort [7]. In general, honeypots are considered an effective strategy to track hacker behavior.

2. Types of Honeypots

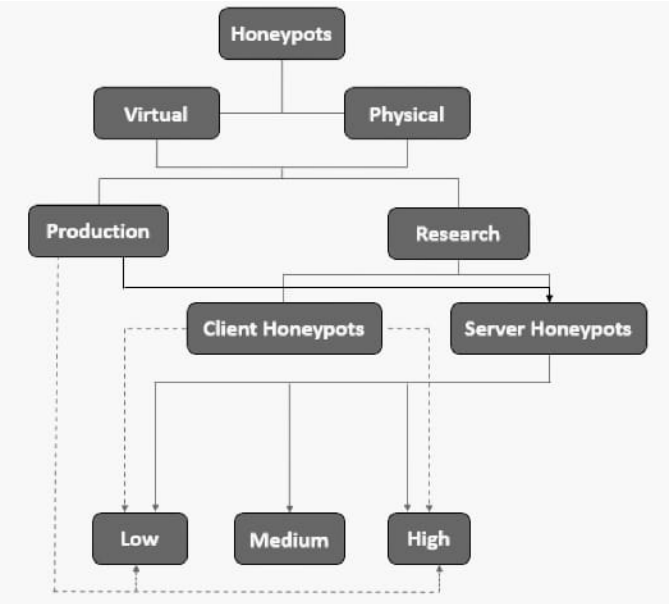

Fig -1: Honeypot taxonomy [5]

2.1 Purpose of Honeypot

According to usage, honeypot may be classified as Production honeypots and research honeypots

2.1.1 Production Honeypot

Production honeypots is used in business/production environment they are easy to use thus are largely deployed in organizations. It is used to reduce the risk of companies or corporations. Production honeypots are easier to build and deploy it require less functionality [2], it is a low-interaction honeypot it captures only limited information, the collected information is very useful because it relates only to unauthorized or illegitimate activity. The gathered data can be used to the way intruders use to probe and gain access to the systems, existing vulnerabilities and to learn about the attack.

2.1.2 Research Honeypot

This Honeypot is utilized to find out the strategies and methods of the Black hat community [3] (In the computer security community, a Black hat is a talented programmer who utilizes his or her capacity to seek his

interest illegally The Honeypot administrator picks up information about the Black hats tools and strategies. When an attacker attacks the systems, a tool used by them is find out by administrators but there is no knowledge on how they were used. A honeypot gives a genuine knowledge on how the attack was happened

2.2 Level of Interaction

Honeypots can also be categorized based on the level of involvement allowed between the intruder and the system. These categories are: low-interaction, medium-interaction and high-interaction.

2.2.1 Low-interactive honeypots

Low-interactive honeypots are more secure and simple approach to gather information about the frequently occurred attacks and their sources. On a low-interaction honeypot, the attackers have no operating system to interact with, but they implement targets to attract or detect attackers by using software to emulate features of a specific operating systems and network service on a host operating system. These type of honeypot does not involve any complex structure, it is very easy to deploy and maintain [2]. Example of low-interaction honeypot is honeyd

2.2.2 Medium-interactive honeypots

Medium-interaction honeypots are slightly more complex than low-interaction honeypots but are less complex than high-interaction honeypots [2]. It is also called as Mixed-interactive honeypots. Medium-interaction honeypots provide 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. It provides forensics in detailed how the attackers target. Medium-interaction honeypots provide additional time for manual responses if automated responses are not possible. Medium-interaction honeypots cost more than low-interaction honeypot

2.2.3 High-interactive honeypots

These are the most developed honeypots. The intention of a high-interactive honeypots is to hold the attacker in the illusion indefinitely while the developers gather every information about the attackers. High-interactive honeypots can hold the attackers for longest possible timeframe. The possibility of collection larger amount of information and all action can be logged and analyzed. It is more complex and time consuming to design and manage. High-interaction honeypots provide more security it is hard to detect [8]. Honeynet is an example of high-interaction honeypots

3. Most popular Honeypots

3.1 Back officer friendly (BOF)

It is an example of a low involvement honeypot. It copies some essential administrations like telnet, ftp, http. Someone connects one of these ports, back officer friendly tuning in and log the attempt. It also works on windows platform. The incentive in BOF is in detection. It can monitor only a predetermined number of ports; however, these ports regularly speak to the most generally scanned and targeted services [6].

3.2 Specter

It is also an example of a low involvement honeypot. It works on different operating system as well [1]. It is similar to BOF is also Emulates services like telnet, ftp, http. It is easy to implement like BOF. There is no real operating system for the attacker to interact with so the risk is reduced. It has automated ability to gather more knowledge about the attacker.

3.3 Homemade honeypots

It is also an example of a low involvement honeypot, there purpose is to capture specific activity, such as worms or scanning activity. Depending on there purpose it can be used as production or research honeypots. Example of a homemade honeypot is to create a service that listen on port80(http), capturing all the traffic from the port. It captures worm attacks using netcat, as: netcat -l -p 80 > c:\honeypot\worm In this command a worm will connected to listening on port [6]. The attacking worm make a successful TCP connection which can be further analyzed by the administrator.

3.4 Mantrap

It is an example of highly involved honeypot. It emulates services like Telnet, Http and Ftp [1]. This honeypot is more flexible, attacker has a full operating system to interact with and a variety of applications to attack. It gives more in-depth knowledge on malicious attackers

4. Honeynets

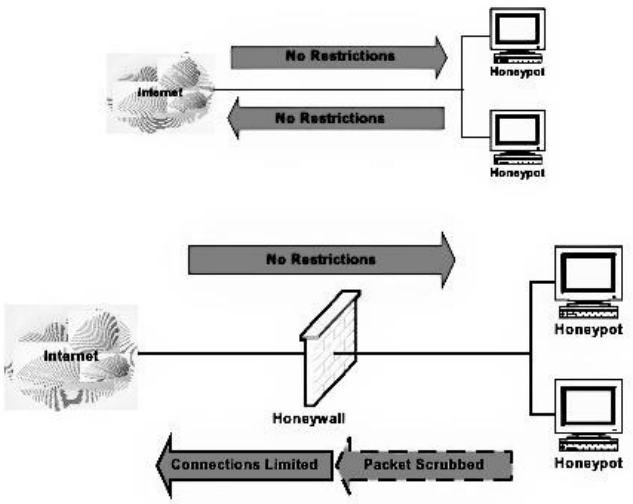

Fig -2: Data Control of the honeypot

To create a single honeynet a collection of honeypots is joined together. Honeynets extend to concept of single honeypots to a network of honeypots. Honeypot and honeywall at least these two devices is needed to deploy a honeynet. A honeypot with a real operating system is given to attacker the attacker can fully access it and easily attack other system or launch a denial-of-services attack [6]. A firewall is configured on the honeywall to reduce the risk. Honeywall monitors and records every packet going to and from the honeypot.

5. Advantages of honeypots

Honeypots have many advantages. Here we will highlight some specialties of honeypots.

- Minimal Resources: honeypots require minimal resources they only gathered information about bad activities
- New tools and tactics: honeypots can also capture new tools and tactics that have been never seen before
- Encryption: A malicious activity which is in encrypted form thrown at honeypot it will be detected and captured by honeypot
- Simplicity: honeypots are conceptually very simple

6. Disadvantages of honeypots

- It will not capture attacks against other system it can only track and capture activity that interacts with them.
- Attacker can used it to attack other systems
- Honeypots can introduce risk to organization environment.

7. CONCLUSIONS

In this paper a brief overview of what honeypots are, and what they are useful for. The different types of honeypots such as production honeypots, research honeypots are also discussed. Honeypots is becoming increasingly popular and will become even more so as commercial solutions become available that are easy to use and administer. Because they can be used to collect information on attackers and other threats, they can prove a useful tool in digital forensics investigations.

REFERENCES

[1] https://www.scribd.com/doc/66498955/abstract-on-honey-pots

[2] Maitri Shukla, Pranav Verma "Honeypot: Concepts, Types and Working" © 2015 IJEDR

[3] http://catchupdates.com/honeypots/

[4] http://www.omnisecu.com/security/infrastructure-and-email-security/honeypots.php

[5] https://www.certsi.es/en/blog/industrial-honeypots

[6] https://www.symantec.com/connect/articles/value-honeypots-part-two-honeypot-solutions-and-legal-issues

[7] https://www.techopedia.com/definition/10278/honeypot

[8] https://en.wikipedia.org/wiki/Honeypot_(computing)