International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Honeypots: Sweet OR Sour spot in Network Security?

Aman Sachan†* and Renuka Panchagavi‡

†Computer Engineering Department, Bharati Vidyapeeth Deemed University, College of Engineering Pune-43, Maharashtra, India

Accepted 25 May 2016, Available online 02 June 2016, **Vol.6, No.3 (June 2016)**

Abstract

In the past few years, there has been a dramatic escalation of cyber and network attacks. In the next generation of attacks, attackers are more likely to use less malware and instead find valid credentials online. A lot of traditional defensive technologies like intrusion detection, firewalls and prevention systems, anti-malware scanners, fail to detect such breaches. Therefore, there is a need for sophisticated anomaly detection or a deception trap, designed to entice an attacker and when deployed correctly can serve as an early warning and security surveillance tool. The deception trap can be in the form of a server attached to the internet which acts as a decoy, luring in potential hackers and monitoring their activities. Such a system is called a honeypot. Honeypots are designed to mimic the actual systems that the intruder wants to break into but limiting the intruder from accessing the entire network. Despite of several advantages, Honeypots cannot be the ultimate security solution for networks. This paper discusses about the pros and cons of using honeypots as a network security solution for overcoming breaches of information security.

Keywords: *Honeypots, Production Honeypot, Research Honeypot, Honeynets, Specter, BackOfficer friendly, Honeyd, ManTrap.*

1. Introduction

Today, securing our valuable information and data from the attackers has become a major concern. Honeypots are the computer systems deployed in the network to lure the attacker [LanceSpitzner, 2003a]. Honeypots can be data, applications and computer systems which seems useful and legitimate, but are mainly designed to mimic the actual systems that the intruder wants to break which are being closely monitored for any potential attacker and threats, so that an early warning can be provided. The primary use is to gain direct, observable knowledge of how intruders operate [RyanMohammed, 2001]. Despite of several advantages, Honeypots cannot prove to be the ultimate security solution for networks. This paper discusses about the pros and cons of using honeypots as a network security solution for overcoming breaches of information security.

2. Working of Honeypots

Honeypot is a web server deployed in the DMZ network. The deployed dummy web server is not even registered in domain name system (DNS), it's just physically located with other web servers. Any communication or interaction with the deployed honeypot is assumed to be unauthorized and attack-related information, such as the IP address, MAC address etc. of the attacker are collected. Honeypots capture everything the attacker is doing and also have the ability to keep log, alert the administrator. The captured packets and packet payloads involved in the attack, proves valuable in analyzing the attackers' activities. The firewall can hence be described as a static defense mechanism and in comparison a honeypot is dynamic. The honeypot defends against attacks that the firewall is unable to see [Ryan Mohammed, 2001].

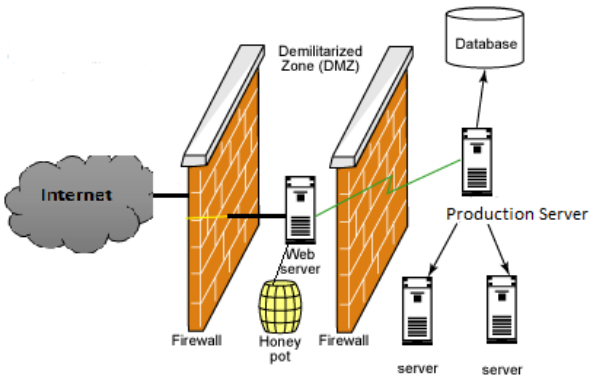

Fig. 1 Deployment of honeypot

2.1. Reasons behind setting up a Honeypot

1) To get to know about how intruders and attackers attempt to gain access to the system. As we very

*Corresponding author: **Aman Sachan; Renuka Panchagavi** is working as Assistant Professor (PG Section)

well know about attack methodologies we can easily protect the real system.
2) Providing the gather official information to law enforcement about the attacker, so that it will help in prosecution of attacker.

2.2. Myths about honeypots

Below are some common myths [LanceSpitzner, 2002] about using honeypots: -

1) Honeypots negatively affects network services and applications.
2) People feel that if an attacker is trapped into a honeypot, the attacker will get furious by the deception and get revenge against the organization.
3) Honeypots require a large amount of work like constructing a fake but similar kind of environment, recoding binaries, or developing a robust kernel module.
4) Attackers will have access to resources, if the honeypot is misconfigured or maintained properly.

3. Classification of Honeypots

Security experts like Mr. Lance Spitzner classified the honeypot into:

1) Production and Research honeypot according to the design deployment.
2) Low interaction, medium interaction, and high-interaction according to attacker interaction level.

3.1. Production honeypot

Production honeypots [IyatitiMokube, 2007] are simple and easy to configure. These honeypots recognize attacks from external intruders and are used to protect the organization network. Production honeypots perhaps delay or stop the intrusion or malicious attack on the production servers to reduce the risks. It captures only limited information and is placed beside the other production servers like firewall to improve the security of production network. The purpose of a production honeypot is to add values to the security measures and to reduce risks of an organization. Examples of production honeypot is Specter.

3.2. Research honeypot

Research honeypot [NehaSahu, 2012] is more complex to deploy and maintain. Research honeypot is run by a volunteer who gathers important information about, who the attackers are and what kind of tools they used in order to attack systems. In other words, research honeypots are deployed by the organizations and to learn how to provide improved protection against threats and attackers. It is used mainly for research purposes by universities, military and government organizations.

3.3. Low interaction honeypot

It is easier to deploy and maintain a low interaction honeypot. It does not contain any operating system for the attacker to interact with and hence, a low interaction honeypot can be compared to a passive intrusion detection system (IDS) since it neither modifies network traffic nor interact with the attacker. It is very difficult to hide low interaction honeypots, but they can be used as preventive measure against worms. Examples of low interaction honeypot are honeyd, Specter and BackOfficer Friendly.

3.4. Medium interaction honeypot

Medium interaction [AteeqAhmad, 2011] honeypot is better than a low interaction honeypot, but not so better than a high interaction honeypot. Medium interaction honeypot gives attacker a better decoy of an operating system or small application program. Hence, it provides more for the attacker to interact with, so complex attacks and malicious work can therefore, be logged and analyzed easily. Examples of medium interaction honeypots are mwcollect, nepenthes and honeytrap.

3.5. High interaction honeypot

High interactive honeypots are the most advanced honeypots and it is difficult to develop this kinds of honeypots. It provides attacker a real operating system, which allows attacker to run all kind of instructions and commands. Hence, the chances of collecting large amounts of information about the attacker is very high in this type of honeypot, as all actions are being logged and monitored. Example of high interaction honeypots is honeynet.

4. Overview of Different Types Honeypots

This section provides a comprehensive review about different types of honeypot technologies.

4.1. BackOfficer friendly

BackOfficer [LanceSpitzner, 2003b] Friendly, or BOF is a simple, free honeypot solution developed by Marcus Ranum and the group at Network Flight Recorder. BOF is a low interaction honeypot.

Pros of backofficer friendly

- It can almost secure every Windows platform.
- Installation and configuring of BOF is easy compared to other honeypots.
- Deploying cost of BOF is zero as it is open source software.

Cons of backofficer friendly

- Limited identification of threats.

- Not suitable for enterprise level as it does not function like remote logging and alerting.
- It can monitor only 7 ports.

4.2 Specter

Specter [Network Security Software, 2012] is developed and sold by NetSec. It is a production and low-interaction honeypot. It has alerting and logging capabilities.

Pros of specter

- It can detect unauthorized activity in the networks immediately.
- Easy to deploy and has low risk.
- It stores detailed logs of attacker activities and can identify any malicious activity.
- Suitable for enterprise level as it has function like remote logging and alerting.

Cons of specter

- Provides no real operating system.
- Can't create a record of attacker's activity.
- Monitor at max 14 ports.

4.3 Honeyd

Honeyd [JunWang, 2003] was developed by Niels Provos in April 2002 and is a free low-interaction honeypot.

Pros of honeyd: -

- Honeyd is relatively easy to install and has a command line interface.
- It monitors entire networks instead of a single IP.
- It automatically interacts with the attacker and increases the ability to capture and detect malicious activities.

Cons of honeyd

- Designed only for the Unix background.
- Can't create a record of attacker's activity.

4.4 Homemade

To suit a specific need Homemade [Lance Spitzner, 2002] honeypots are developed. Generally, homemade honeypots have properties of medium interaction honeypots.

Table 1 Comparison of different type honeypots

	Interaction Level	OS Deployment	Creating Records	Graphical Interaction	Software Type
BackOfficer Friendly	Low	No	No	Yes	Freeware
Homemade	Generally Medium	Yes	Yes	Yes	Proprietary software
Honeyd	Low	No	Yes	Yes	Freeware
Honeynets	High	Yes	Yes	Yes	Open source software
ManTrap	High	Yes	Yes	Yes	Retail software
Specter	Low	No	Yes	Yes	Retail software

Pros of homemade

- Can be developed depending on the system requirements.
- Used mainly for research purposes.

Cons of homemade

- Can't be deployed two systems as the two systems have different requirements.

4.5 ManTrap

ManTrap [LanceSpitzner,2002] is a commercial honeypot developed and sold by Recourse. It can be a medium to high interaction honeypot.

Pros of mantrap

- Provides the administrator control and to capture attacker's activity.
- Dummy operating systems has exact the same functionality as the production systems.
- Automatically detects and scans unauthorized connections to collect attacker's information.

Cons of mantrap

- Increases Risk as the same honeypot can be used to attack production systems.

4.6 Honeynets

Honeynets [Honeynet Project, 2006] are high-interaction honeypots. Honeynets are different types of systems implemented with an extremely controlled network.

Pros of honeynets

- Provide the attacker a complete operating system to attack and interact with.

- The developed controlled network captures all the attacker's activity which happens within the Honeynet.
- Capture the information on almost any platform.

Cons of honeynets

- It is complex to design a Honeynet as it is difficult to build controlled network to control and capture all the attacker's activity.
- Honeynets have the highest risk.

Conclusions and Future Work

Though there have been many research contributions to make honeypots technologies more secure, reliable and risk free, there are various legal and ethical issues which can make you to be liable if a honeypot is compromised and used as a launching pad for other unauthorized intrusions. Therefore, honeypots do not replace other traditional internet security systems but are an additional level or system. In this paper, we have given an overview of classification of honeypots technologies, and their advantages and disadvantages. We have examined different types honeypots depending on design deployment and interaction level with the production server. We have also suggested the use of appropriate kind of honeypots for certain specific applications depending on the interaction and design of the system. A combination of traditional network security monitoring and recent advancements in honeypots and active defense tools is a key to detecting today's threats. In future, honeypots can be combined with Rogue Access Point Detection systems and IDS to get a detailed log of attacker's activity.

References

Ateeq Ahmad, Muhammad Ali, Jamshed Mustafa (2011) Benefits of Honeypots in Education Sector. *IJCSNS 11.10:24.*

Brazillian Honeynet Project (2008) honeydsum.pl, Available: http://www.honeynet.org.br/tools/.

JanGerritGöbel (2006) Advanced Honeynet Based Intrusion Detection, Department of Computer Science, Diploma Thesis.

KarlHable (2003) HoneyView a honeyd Logfile Analyzer, available: http://www.honeyview. sourceforge.net/.

Honeynet Project (2006), Know Your Enemy: Honeynets, available: www.project.honeynet.org/paper/honeynet.

John Harrison (2003). Honeypots: The sweet spot in network security,*Symantec Corp*.

Martin (2001). Honeypots and Honeynets – Security through Deception, available: http://www.sans.org/reading_room/whitepapers/attacking/41.php, SANS Institute.

IyatitiMokube, Adams Michele (2007) Honeypots: concepts, approaches, and challenges, Proceedings of the 45th annual southeast regional conference, *ACM*.

Network Security Software (*NETSEC*) (2012), Available: www.specter.com.

Roesch Marty, Spitzner Lance (2001) The value of honeypots, Part One: Definitions and Values of Honeypots, Security Focus.

Ryan Mohammed (2001). Network Deception Systems: Honeypots,http://imps.mcmaster.ca/courses/SE-4C03-01/papers/Mohammed-honeypots.html

NehaSahu, VineetRichhariya (2012) Honeypot: A Survey, *IJCST* Vol. 3, Issue 4, Oct - Dec 2012.

Lance Spitzner (2002) Honeypots: Tracking hackers,*Addison Wesley Professional.*

Lance Spitzner (2003a) Honeypots: Catching the Insider Threat, Computer Security Applications Conference, Proceedings. 19th Annual, *IEEE*.

LanceSpitzner (2003b) Honeypots: Definitions and Value of Honeypots, Available: http://www.trackinghackers.com/papers/honeypots.html

JunWang, Jing Zeng (2003) Construction of large-scale honeynet Based on Honeyd, *Procedia Engineering*, Vol. 15, pp.3260-3264.