Survey of Honey pot system for the Network Security

Prof Sulakshana B Mane
(Computer Engineering Department),
BVCOE, kharghar , Navi Mumbai
sulumane@gmail.com

Prof. Khiarnar V .D
H.O.D (Information technology Department)
TPCT COE, Nerul, Navi Mumbai
khairnar.vaishali3@gmail.com

Abstract— In **this Paper, I presented basic concept of honey pot system. In this paper it is defined what is honey pot, and different types of honey pot, history of honey pot, what are different ways to implement the honey pot if according to the consideration of level of attack there are low interactions and high interactions .there are so many drawbacks of low interaction and high interaction that is resolved in hybrid honey pot system**

Keywords— VMware, honey pot, Low-interaction honey pot, High-interaction honey pot, Proxy etc

I. Introduction

Now a day's lot of people penetrating the network. Sometimes threatening is done by the open ports also. The purposes of honey pot are to detected and learn from attacks and use that information provides network security. Honey pots are analyzed by their role of application, which is meant it can be used for production and research.

II. Definition of honey pot

"A honey pot is security resource whose value lies in being probed, attacked, or compromised".

The main functions of a honey pot are

1. To divert the attention of the attacker from concept of the real network, in a way that the main information resources are not compromised.
2. To capture new viruses or worms for future study
3. To build attacker profiles in order to identify their preferred attack methods, similar to criminal profiles used by law enforcement agencies in order to identify a criminal's modus Operandi.

III. Advantages

1. Fewer false positives since no legitimate traffic uses honey pot
2. Collect smaller, higher-value, datasets since they only log illegitimate activity
3. Work in encrypted environments
4. Do not require known attack signatures, unlike IDS

IV. Disadvantages

1. Can be used by attacker to attack other systems.
2. Only monitor interactions made directly with the honey pot - the honey pot cannot detect attacks against other systems
3. Can potentially be detected by the attacker

V .Existing Honey pot Products

V.1 Honeyed (practical tool)

- Honeyed is a honey pot for Linux/Unix developed by security researcher Niels Provos. Honeyed was ground- breaking in that it could create multiple virtual hosts on the network (as opposed to just using a single physical host). The honey pot can emulate various operating systems (which differ in how they respond to certain messages) and services. Since Honeyed emulates operating systems at the TCP/IP stack level, it can fool even sophistic network analysis tools such as

nmap. Upon attack, Honeyed can passively attempt to identify the remote host.

V.2 HoneyBOT (Practical tools)

It is a Windows medium-interaction honey pot by Atomic Software Solutions

(It originally began as an attempt to detect by the Code Red and Nimda worms in 2001 and has been released for free public use since 2005. HoneyBOT allows attackers to upload files to a quarantined area in order to detect Trojans and root kits. HoneyBOT's user interface

V.3 Specter (Practical tools)

Spectre's authors describe Specter as a "honey pot-based intrusion detection system". However, the product is primarily a honey pot designed to lure attackers away from production systems and collect evidence against the attackers. Specter has a few interesting features not found in other solutions: Specter makes decoy data available for attackers to access and download. These data files leave marks on the attacker's computer as evidence

Specter can emulate machines in different states: a badly configured system, a secured system, a failing system (with hardware or software failures), or an unpredictable system. Specter actively attempts to collect information about each attacker

VI. Type of Honey pots

VI.A. Production

Production honey pots are usually used by commercial organizations to help mitigate risks. This kind of honey pots adds value to the security measures of an organization.

VI.B Research

Research honey pots are designed to gather information about the attackers. They do not provide any direct value to a specific organization but are used to collect information about what threats

VII. Level of interaction

The level of interaction is defined as the range of attack Possibilities that a honey pot allow an attacker to have, where as it can be classified as high- interaction honey pot and low interaction honeypot there are two types of honey pots

1. Low interaction honey pot
2. High interaction honey pot

VII.1 High- Interaction Honey pot

In high- interaction honey pot, attacker interaction with real operating systems, services and programs and it can be used to observe the attackers behavior, their tools, and motivation and Explored vulnerabilities. This kind of honey pot must have a robust containment mechanism in order to prevent, once compromised, its use to attack other networks. One goal of a hacker is to gain root and to have access to a machine, which Tools like Sebek can help high-interaction honey pot to instrument to log and/or System calls.

VII.2. Low- Interaction Honey pot

In low- interaction honey pot, there is no operating system is involed that an attacker can operate on. Tools are installed in order to emulate operating systems and services. And they interact with the attackers and malicious code. This will minimize the risk significantly. This kind of honey pot has a small chance of being compromised. It is production honey pot. Typical use of low-interaction honey pot includes port scans identification, generation of attack signatures, trend analysis and malware collection. On the other hand, this is also a disadvantage It is not possible to watch an attacker interacting with the operating system, which could be really interacting. Example of low interaction honey pot is honeyed. Honeyed is an open source low-interactivity honey pot system that creates virtual hosts that can be configured to run arbitrary services and their personality can be adapted so that they appear to be running certain operating systems. Honeyed, enables a single host to claim multiple

addresses. Honeyed improves cyber security by providing mechanism for threat detection and assessment. It also deters adversaries by hiding systems in the middle of virtual systems.

VII.3. Comparison between low- interaction honey pot and high interaction honey pot

Each level has advantages and disadvantage as mention below;

	Low interaction honey pot	High interaction honey pot
Degree of involvement	Low	high
Real Operating System	No	Yes
Risk	Low	high
Information gathering	Connections	all
Compromised Wished	No	yes
Knowledge to run	Low	high
Knowledge to develop	Low	Mid high

Table 1 comparison between low interaction and high interaction

VIII **Hybrid honey pot system**

Low-interaction honey pot is more secure than high- interaction honey pot because of running real service; it lacks the ability to provide a good level of realism. However, high-interaction honey pot provides the best possible level of realism but it has more risk.

. In this system, low- interaction honey pot act as lightweight proxy. We want high-interaction honey pot to process all traffic destined to black IP address space. We need to offload them as front end to high-interaction honey pot because it is instrumented machines. Honeyed has the appropriate properties to play the role of the front end and acts as a filtering component. The lightweight proxy responds only to TCP/SYN requests to ports that are open. For any other ports, it just absorbs and records the packets received. When the three-way handshake has completed properly between the attacker and

The low- interaction honey pot, the connection must be handoff to the appropriate high-interaction honey pot . At this point, also referred as zero point, the low-interaction honey pot set as a connection with the high- interaction honey pot. The low interaction honey pot sets as like relay agent. Any application level data coming from attacker is forwarded to the high interaction honey pot and vice versa, until the connection is terminated. This behavior is embedded to the honeyed implementation, know as proxy mode. The proxy mode is instrumented to record the message exchanges, for further analysis purposes. Hand-off is useful in case of port scanning, where low-interaction honey pot will absorb all incoming connections without disturbing high-interaction honey pot.

IX. Value of honey pots

The value of honey pots depends closely on what kind of honey pot we are dealing with. Production honey pots are used to help organizations protecting themselves against attackers, which include preventing, detecting and responding to attacks. Research honey pots are used to collect information that will be analyzed to develop better protection methods.

IX.1. Prevention

Prevention means keeping the threat out of the productions systems. This can be done by several means such as firewalls, authentication and encryption. However, honey pots add a little value to prevention. While honey pots can prevent the spreading of a worm across the network (sticky honey pots), they also prevent from human attackers. Two concepts are involved in human prevention: deception and deterrence. Deception is making the attacker waste his time and resources attacking honey pots. The deterrence is when the attacker doesn't want to attack some network because

he knows that there are honey pots in that n/w fearing to be logged n caught.

IX .2. Detection

Detection is to identify a failure or a breakdown in the prevention. This can be also done by several means such as IDS but honey pots address effectively some weaknesses of such prevention systems: false positives, false negatives and value of data gathered. Because honey pots have no productions purposes, they generate very few false positives. Because all the traffic to and from the honey pots is suspicious, they also address the false negative issue. Because of their simplicity and design, honey pots gather little amount of data with very high value.

IX.3. Response

The challenge that organizations face when they want to react to an attack is evidence collection. This is an important issue when the organization wants to prosecute the attacker as well as when they want to defend themselves against this threat. Honey pots address these problems in 2 ways. First, the only traffic on the honey pot is the attacker traffic and it makes it easier to analyze the attacker behaviors in honey pots than in production systems since the only data retrieved from the honey pot is malicious data. Second, it is much simpler to pull offline the honey pot for further analysis without affecting other business activities of the organizations

Conclusion:

In this way, I conclude honeypot, is used to detect an attack. So many works is done on the honey pot through the hardware, some software tools and attacks detected. There is forensic analysis that daily 60% attack is happen on sites that's why so many tools are there like Nikto and Nmap, nesses with the help of that tools attacks are detected.

References:

[1]
"Hybrid Honey pot System for Network Security"
By Kyi Lin Lin Kyaw, Department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay.vol World Academy of Science, Engineering and Technology 48 2008

[2] Improving network security with Honey pots.

[3]"Taxonomy of Hybrid Honey pots"
Hamid Mohammadzadeh.e.n 1, Masood Mansoori 2 and Roza Honarbakhsh 3
1 Faculty of computer Science & Technology, University of Malaya, Kuala Lumpur
2 Faculty of Computer Science and Software Engineering, University of Canterbury, New Zealand
IPCSIT vol.11 (2011)

[4] "A Technique for Detecting New Attacks in Low-Interaction Honey pot Traffic"
S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann
Information Security Institute, Queensland University of Technology
Brisbane, Queensland, Australia
{s.almotairi, a. lark, g.mohay, j.zimmerm}@isi.qut.edu.au
2009 Fourth International Conference on Internet Monitoring and Protection

Bibliography

Author1
Name: Mrs. Sulakshana B Mane
Designation: Assistant Professor (BVCOE), kharghar, Navi Mumbai
Teaching Exp: 10 years
No of Published Papers 05

Author2
Name: Prof Vaishali D. Khairnar
Designation: H.O.D (information technology) TEC, Nerul, Navi Mumbai.
Teaching Exp: 12 years
No of Published Papers 12