WEB BASED HONEYPOTS NETWORK

Srivathsa S Rao[#1],Vinay Hegde[#2] , Boruthalupula Maneesh[#3], Jyothi Prasad N M[#4], Suhas Suresh[#5]

Abstract -- Honeypots are a modern approach to network security. A honeypot is used in the area of internet security and cryptography. It is a resource, which is intended to be attacked and compromised to gain more information about the attacker and the used implementations. It can be deployed to attract and divert an attacker from their real targets. Honeypots have the big advantage that they do not generate false alerts as each observed traffic is doubtful, because no productive components are running on the system. This fact enables the system to log every byte that flows through the network through and from the honeypot, and to relate this data with other sources to draw a picture of an attack and the attacker.

This paper would first give a brief introduction to honeypots- the types and its uses. We will then look at the other components of honeypots and the way to put them together. Finally we shall conclude by looking at what the future holds for honeypots.’

I. Introduction

Global communication is getting more significant every day. At the same time, computer crimes are growing rapidly. Counter measures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. As in the military, it is important to know, who your enemy is, what kind of strategy and plan he uses, what tools he utilizes and what he is aiming for. Gathering this kind of information is arduous but important. By knowing attack strategies, countermeasures can be improved and anomalies can be fixed. To gather as much information as possible is one main target of honeypot.

Generally, such information gathering should be done without the attacker’s knowledge. All the gathered information provides an advantage to the defending side and can therefore be used on productive systems to prevent attacks.

II.WHAT IS A HONEYPOT?

A honeypot is basically an instrument for information gathering and learning. A honeypot is an information system resource whose value lies in the unauthorized or illicit use of that resource. More generally a honeypot is a trap set to divert or discover attempts at unauthorized use of information systems. Essentially, honeypots are resources that allow anyone or anything to access it and add production value. Honeypots do not have any unprotected, unused workstation on a network being closely watched by administrators.

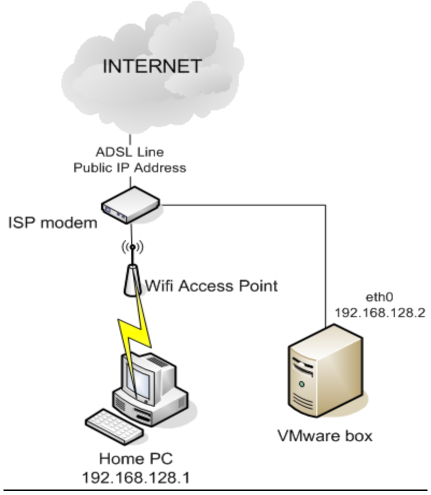

Fig.1 Honeypot

Its primary purpose is not to be an ambush for the black hat community to catch them in action and to press charges against them. The focus lies on a silent collection of as much information as possible about their attack patterns, used programs, and the black hat community itself. All this information is used to learn more about the black hat proceedings and motives, as well as their technical knowledge and abilities. This is just a primary purpose of a honeypot. There are a lot other possibilities for a honeypot- divert hackers from productive systems or seize a hacker while conducting an attack are just two possible examples.

III. WHAT IS A HONEYNET?

Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring and/or more diverse network in which one honeypot may not be sufficient. Honeynets are usually implemented as parts of larger network intrusion-detection systems. Honeynet is a network of production systems. Honeynets represent the extreme of research honeypots. Their primary value lies in research, gaining information on threats that exists in the Internet community today.

The two main reasons why honeypots are deployed are:

1. To learn how intruders probe and attempt to gain access to your systems and gain insight into attack methodologies to better protect real production systems.

2. To gather forensic information required to aid in the apprehension or prosecution of intruders,

IV.TYPES OF HONEYPOTS

Honeypots came in two flavors:

1. Low interaction 2. High interaction.

Interaction measures the amount of activity that an intruder may have with honeypot. In addition, honeypots can be used to combat spam. Spammers are constantly searching for sites with vulnerable open relays to forward spam on the other networks. Honeypots can be set up as open proxies or relays to allow spammers to use their sites.

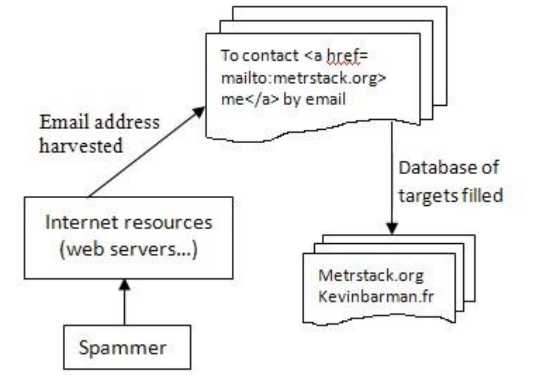
To contact <a href= mailto:metrstack.org> me</a> by email
Email address harvested
Database of targets filled
Internet resources (web servers...)
Metrstack.org
Kevinbarman.fr
Spammer

Fig.2 Spammer detection

This in turn allows for identification of spammers.

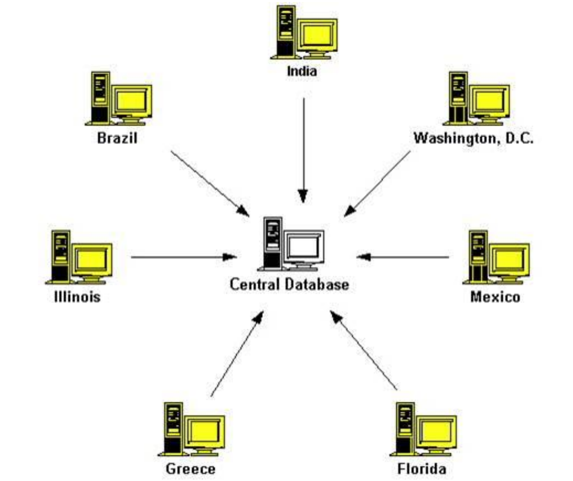

Fig.3

We will break honeypots into two broad categories, as defined by Snort, namely:

- Production honeypots
- Research honeypots

The purpose of a production honeypot is to help alleviate risk in an organization. The honeypot adds value to the security measures of an organization. Think of them as 'law enforcement', their job is to detect and deal with intruders.

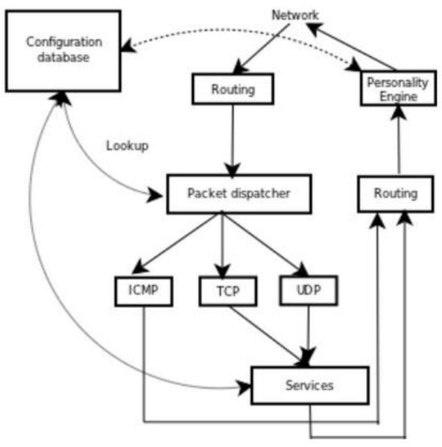

Fig.4 Honeyd architecture

Traditionally, commercial organizations use production honeypots to help protect their networks. The second category, research, is honeypots designed to gain information on the black hat community. These honeypots do not add direct value to a specific organization. Instead they are used to research the threats organizations face, and how to better protect against those threats.

V.HONEYPOT ARCHITECTURE:

1. *Structure of a LOW-INTERACTION HONEYPOT (GEN-I)*:- A typical low-interaction honeypot is also known GEN-I honeypot. This is a simple system which is very effective against automated attacks or beginner level attacks Honeyd is one such GEN-I honeypot which emulates services and their responses for typical network functions from a single machine, while at the same time making the intruder believe that there are numerous different operating systems. It also allows the simulation of virtual network topologies using a routing mechanism that mimics various network parameters such as delay, latency and ICMP error messages. The primary architecture consists of a routing mechanism, a personality engine, a packet dispatcher and the service simulators. The most important of these is the personality engine, which gives services a different 'avatar' for every operating system that they emulate.

   DRAWBACKS:

   - This architecture provides a restricted framework within which emulation is carried out. Due to the limited number of services and functionality that it emulates, it is very easy to fingerprint.
   - A flawed implementation also leads to reduce itself to alerting the attacker.
   - It has constrained applications in research, since every service which is to be studied will have to be re-built for the honeypot.

2. *Structure of a HIGH INTERACTION HONEYPOT (GEN-II)*:- A typical high-interaction honeypot consists of the following elements: resource of interest, data control, data capture and external logs ("known your enemy: Learning with Vmware, Honeypot project");

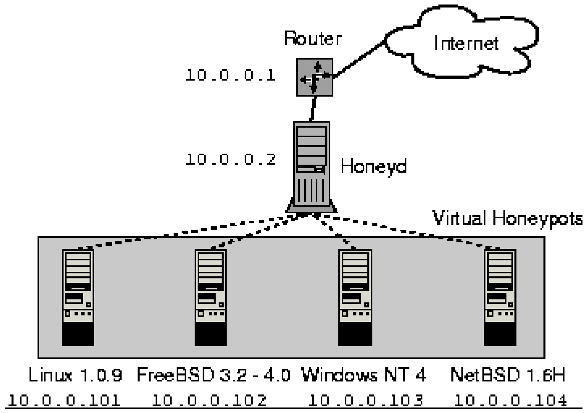

Fig.5 how Honeyd works

These are also known as GEN-II honeypots and started development in 2002. They provide better data capture and control mechanisms. This makes them more complex to deploy and maintain in comparison to low-interaction honeypots.
High interaction honeypots are very useful in their ability to identify vulnerable services and applications for a particular target operating system. Since the honeypots have full-fledged operating systems, attackers attempt numerous attacks providing administrators with very detailed information on attackers and their methodologies. This is essential for researchers to identify fresh and unknown attack, by studying patterns generated by these honeypots.

DRAWBACKS:

- The number of honeypots in the network is limited.
- The risk associated with GEN-II honeypots is higher because they can be used easily as launch pads for attacks.

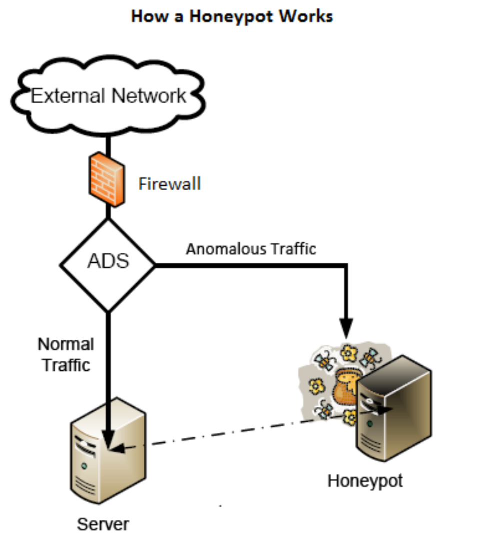

Fig.5 how Honeypot works

VI.BUILDING a HONEYPOT:

To build a honeypot, a set of Virtual Machines are created. They are then setup on a private network with the host operating system. To facilitate data control, a stateful firewall such as IP tables can be used to log connections. This firewall would typically be configured in Layer 2 bridging mode, rendering it transparent to attacker. The final step is data capture, for which tools such as Sebek and Term Log can be used. Once data has been captured, analysis on the data can be performed using tools such as Honey Inspector, PrivMsg and SleuthKit.

Honeypot technology under development will eventually allow for a large scale honeypot deployment that redirects suspected attack traffic to honeypot. In the figure an external attacker

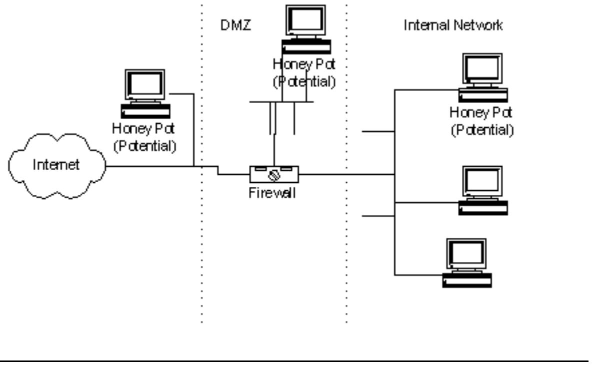

Fig.6 Building a Honeypot

- Penetrates DMZ and scans the network IP address.
- The redirection appliance.
- Monitors all unused addresses, and uses layer 2 VPN technologies to enable firewall.
- TO redirect the intruder to honeypot.
- This may have honeypot computers monitoring all types of real network devices.
- Scanning the network for vulnerable systems is redirected.

By the honeypot appliance when he probes unused IP addresses.

VII.RESEARCH USING HONEYPOTS:

Honeypots are also used for research purposes to gain extensive information on threats, information few other technologies are capable of gathering. One of the greatest problems security professionals face is lack of information or intelligence on cyber threats. How can your organization defend itself against an enemy when you do not know who the enemy is? Research honeypots address this problem by collecting information on threats. Organizations can use this information for variety of purposes including analyzing trends, identifying the attackers and their community, ensuing early warning and prediction or understanding attacker's motivation.

ADVATAGES OF HONEYPOTS:

1. They collect small amounts of information that have great value. This captured information provides an in-depth look at attacks that very few other technologies offer.
2. Honeypots are designed to capture any activity and can work in encrypted networks.
3. Honeypots are relatively simple to create and maintain.

DISADVANTAGES OF HONEYPOTS:

1. Honeypots add complexity to the network. Increased complexity may lead to increased exposure to exploitation.
2. There is also level of risk to consider, since a honeypot may be comprised and used as a platform to attack another network. However this risk can be mitigated by controlling the level of interaction that attackers have with the honeypot.

VIII.LEGAL ISSUES PERTAINING TO HONEYPOT:

Most of the research found in this area concluded that there are two major legal spectrums considering honeypots:

1. *ENTRAPMENT*: Entrapment is when somebody includes the criminal to do something he was not otherwise supposed to do. Honeypots should generally be used as defensive detective tool, not an offensive approach to luring intruders.

2. *PRIVACY*: The second major concern is what information is being tracked: operational data and transactional data. Operational data includes things like addresses of user, header information etc while transactional data includes key strokes, pages visited, information downloaded, chat records, e-mails etc. Operational data is safe to track without threats of security concern because IDS system routers and firewalls already track it. The major concern is transactional data.

IX.SOME COMMERCIAL HONEYPOTS AND HELPFUL SOFTWARE:

1. *BACK OFFICER FRIENDLY BY NFR*: This product is designed to emulate a back officer server. BOF (as it is commonly called) is a very simple but highly useful honeypot developed by Marcus Ranum and crew at NFR. It is an excellent example of low interaction honeypot.

2. *TRIPWIRE BY TRIPWIRE*: This product is for use on NT and UNIX machines and is designed to compare binaries, and inform the service operator, which has been altered. This helps to protect machines from hackers and is an excellent way to determine if a system has been compromised.

3. *SPECTER*: Specter is a commercial product and low interaction production honeypot. It is similar to BOF, but it can emulate a far greater range of services and a wide variety of operating systems. Similar to BOF, it is easy to implement and has low risk. Specter works by installing on a Windows system. The risk is reduced as there is no real operating system for the attacker to interact with. Specters value lies in the detection. As a honeypot, it reduces both false positives and false negatives, simplifying the detection process, supporting a variety of altering and logging mechanisms. One of the unique features of specter is that it also allows for information gathering, or the automated ability to gather more information about the attacker.

4. ***MANTRAP***: Mantrap is a commercial honeypot. Instead of emulating services, Mantrap creates up to four sub-systems, often called 'jails'. These 'jails' are logically discrete operating systems separated from a mater operating system. Security administrators can modify these jails just as they normally would with any other operating system, to include installing applications of their choice, such as Oracle database or Apache web server, thus making the honeypot operating system far more flexible. The attacker has a full operating system to interact with, and a variety of applications to attack. Currently, Mantrap only exists on Solaris operating system.

X.CONCLUSION:

Honeypots are positioned to become a key tool to defend the corporate enterprise from hacker attacks it's a way to spy on your enemy; it might even be a form of camouflage. Hackers could be fooled into thinking they have accessed a corporate network, when they are actually hanging around in a honeypot-- While the real network remains safe and sound.

Honeypots have gained a significant place in the overall intrusion protection strategy of enterprise. Security experts do not recommend that these systems replace existing intrusion detection security technologies; they see honeypots as complementary technology to network-and host – based intrusion protection.

The advantages that honeypots bring to intrusion protection strategies are hard to ignore. In time, as security managers understand the benefits, honeypots will become an essential ingredient in an enterprise –level security operation.

We do believe that although honeypots have legal issues now, they do provide beneficial information regarding the security of a network. It is formulated to foster and support research in this area. This will help to solve the current challenges and make it possible to use honeypots for the benefit of the broader internet community.

REFERENCES

[1]] Maximillian Dornseif, Thorsten Holz, and Sven M□uller. *Honeypots and limitations of deception.*

[2] Xiaoyan Sun, Yang Wang, Jie Ren, Yuefei Zhu and Shengli Liu, "Collecting Internet Malware Based on Client-side Honeypot", 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2008.

[3] C. H. Nick Jap, P. Blanchfield, and K. S. Daniel Su, "The use of honeypot approach in software-based application protection for shareware programs", IEEE International Conference on Computing & Informatics, (ICOCI '06), pp. 1-7, 2006.

[4] Jian Bao and Chang-peng Ji, and Mo Gao, "Research on network security of defense based on Honeypot", IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302, 2010.

[5] Anjali Sardana, R. C. Joshi, "Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level", IEEE International Symposiums on Information Processing (ISIP), pp. 505-509, 2008.

[6] Guanlin Chen, Hui Yao and Zebing Wang, "Research of Wireless Intrusion Prevention Systems based on Plan Recognition and Honeypot", IEEE International Conference on Wireless Communications & Signal Processing (WCSP), pp. 1-5, 2009.

[7] Chao-Hsi Yeh and Chung-Huang Yang, "Design and Implementation of Honeypot Systems Based on Open-Source Software", IEEE International Conference on Intelligence and Security Informatics (ISI), 265-266, 2008.

[8] Babak Khosravifar, Maziar Gomrokchi, Jamal Bentahar, "A Multi-Agent-based Approach to Improve Intrusion Detection Systems False Alarm Ratio by Using Honeypot", IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 97 – 102, 2009.

[9] Wei Li-feng, Wang Xiao-bin, "Research on Honeypot Information Fusion Based on Game Theory", Second IEEE International Conference on Computer Research and Development, pp. 803 – 806, 2010,

[10] Marc Dacier, Fabien Pouget, and Herve Debar. Honeypots: practical means to validate malicious fault assumptions. In Dependable Computing, 2004. Proceedings. 10th IEEE Pacific Rim International Symposium on, pages 383 - 388, march 2004.

[11] David Dagon, Xinzhou Qin, Guofei Gu, Wenke Lee, Julian Grizzard, John Levine, and Henry Owen. *Honeystat: Local worm detection using honeypots*. [12] Reto Baumann and Christian Plattner. Honeypots, 2002.

[13] Jeremy Bri
aut, Jean-Francois Lalande, and Christian Toinard. Security and results of a large-scale high-interaction honeypot. Journal of Computers, 4(5):395-404, 2009.

[14] Bill Cheswick. An evening with berferd in which a cracker is lured, endured, and studied. In Proc. Winter USENIX Conference, pages 163{174, 1992.

[15] Sabharwal. *Opaqueness characteristic of a context honeypot system*. Information Security Journal: A Global Perspective, 19(3):142-152, 2010.