HONEYPOT – tracking hackers

Vaibhav kumar gupta[1]

[1]Department of Computer Science Engineering

[1]Saveetha School of Engineering

Abstract— For every consumer and business that is on the Internet, viruses, worms and crackers are a few security threats. There are the obvious tools that aid information security professionals against these problems such as anti-virus software, firewalls and intrusion detection systems, but these systems can only react to or prevent attacks-they cannot give us information about the attacker, the tools used or even the methods employed. Given all of these security questions, honeypots are a novel approach to network security and security research alike.

A honeypot is used in the area of computer and Internet security. It is a resource, which is intended to be attacked and compromised to gain more information about the attacker and the used tools. It can also be deployed to attract and divert an attacker from their real targets. Compared to an intrusion detection system, honeypots have the big advantage that they do not generate false alerts as each observed traffic is suspicious, because no productive components are running on the system. This fact enables the system to log every byte that flows through the network to and from the honeypot, and to correlate this data with other sources to draw a picture of an attack and the attacker.

This paper will first give an introduction to honeypots-the types and uses. We will then look at the nuts and bolts of honeypots and how to put them together. Finally we shall conclude by looking at what the future holds for the honeypots and honey nets.

I. INTRODUCTION

Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures 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 he uses, what tools he utilizes and what he is aiming for. Gathering this kind of information is not easy but important. By knowing attack strategies, countermeasures can be improved and vulnerabilities can be fixed. To gather as much information as possible is one main goal of a honeypot.

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

II. HONEYPOT

A honeypot is primarily an instrument for information gathering and learning. A honeypot is an information system resource whose value lies in the unauthorized zed or illicit use of that resource. More generally a honeypot is a trap set to deflect or detect attempts at unauthorized use of information systems. Essentially; honeypots are resources that allow anyone or anything to access it and al production value. More often than not, a honeypot is more importantly, honeypots do not have any resample and unprotected, unpatched, unused workstation on a network being closely watched by administrators. 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, purpose of attack 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 catch 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 (and honeypots) 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 exist 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:

- Low-interaction
- High-interaction.

Interaction measures the amount of activity that an intruder may have with honeypot.In addition,

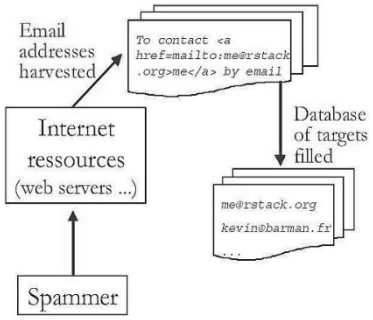


Fig.1: Honeypot

Categories, as defined by Snort, two types of

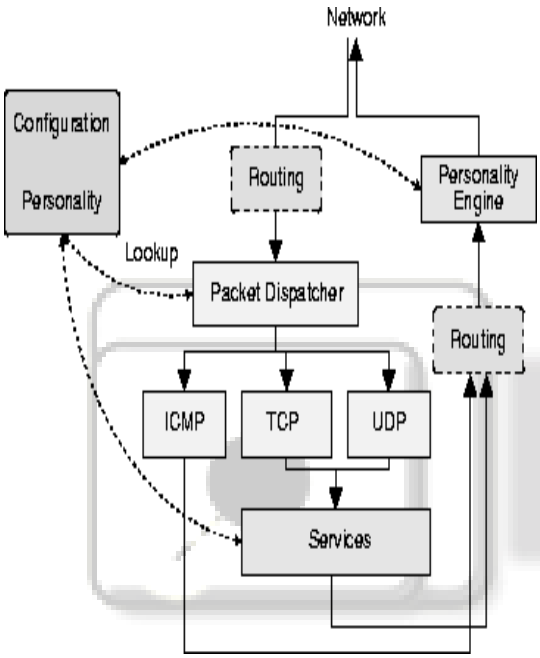


Fig.2: Network

honeypots are:

– Pro duction honeypots

– Res earch honeypots

The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot 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 .This in turn allows for identification of spammers.

We will break honeypots into two broa

V. HONEYPOT ARCHITECTURE

A. Structure of a LOW-INTERACTION HONEYPOT(GEN-I):-

A typical low-interaction honeypot is also known

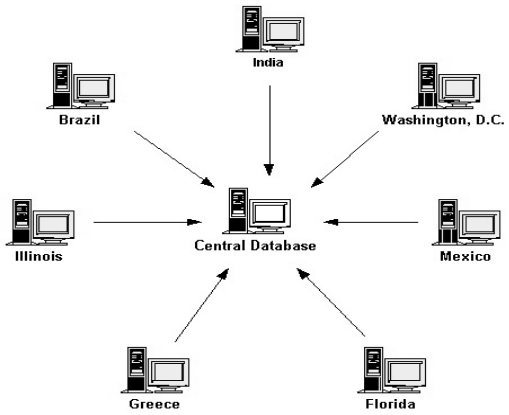


Fig.3: Structure of a LOW-INTERACTION HONEYPOT(GEN-I)

as GEN-I honeypot. This is a simple system which is very effective against automated attacks or beginner level atacks.

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.

VI. DRAWBACKS

(1) 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.

(2) A flawed implementation (a behavior not shown by a real service) can also render itself to alerting the attacker.

(3) It has constrained applications in research, since every service which is to be studied will have to be re-built for the honeypot.

B. Structure of a HIGH INTERACTION HONEYPOT(GEN-II):-

A typical high-interaction honeypot consists of the following elements: resource of interest, data control, data captur e and extern al log

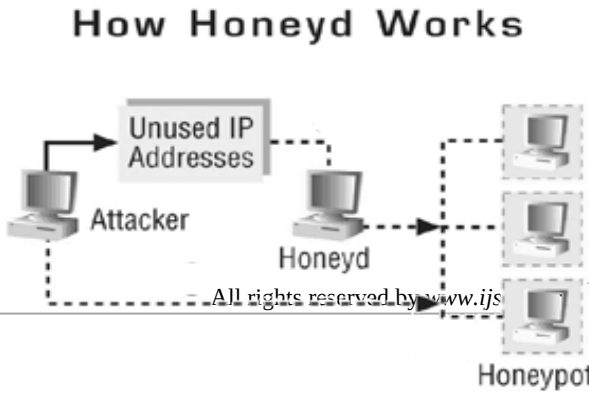


Fig.4: Struct ure of

a HIGH INTERACTION HONEYPOT (GEN-II)

known your enemy: Learning with VMware, Honeynet project"); 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 various attacks providing administrators with very detailed information on attackers and their methodologies. This is essential for researchers to identify new and unknown attack, by studying patterns generated by these honeypots

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

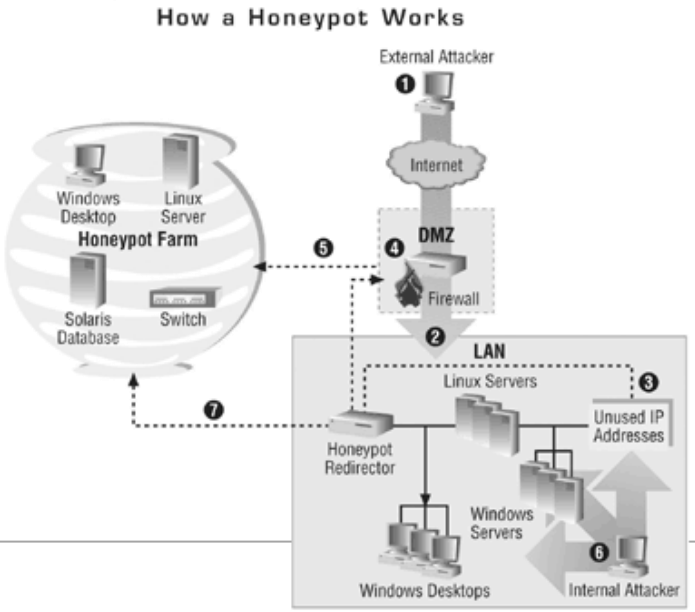
VII. BUILDING A HONEYPOT:

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 the 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:

- Penetrates DMZ and scans the network IP address.
- The redirection appliance.
- Monitors all unused addresses, and uses Layer 2 VPN technology to enable firewall.
- To redirect the intruder to honeypot.



- Which may have honeypot computers

Fig.5:How a Honeypot Work

mirroring all types of real network devices?

- Scanning the network for vulnerable systems is redirected.
- By the honeypot appliance when he probes unused IP addresses.

VIII. 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 then use this information for a variety of purposes including analyzing trends, identifying new methods or tools, identifying the attackers and their communities, ensuring early warning and prediction or understanding attacker's motivation.

IX. ADVANTAGES 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) They can lure the intruders very easily.
(4) Honeypots are relatively simple to create and maintain.

X. DISADVANTAGES OF HONEYPOTS:

(1) Honeypots add complexity to the network. Increased complexity may lead to increased exposure to exploitation.
(2) There is also a 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.
(3) It is an expensive resource for some corporations. Since building honeypots requires that you have at least a whole system dedicated to it and this may be expensive.

XI. 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've accessed a corporate network, when actually they're just banging 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 the 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 important that new legal policies be 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.

BIBLIOGRAPHY

[1] Loras R. Even. What is a Honeypot? SANS Institute. July 12, 2000
URL:
http://www.sans.org/newlook/resources/IDFAQ/honrypot3.htm

[2] Michael Sink. The Use of Honeypots and Packet Sniffers for Intrusion Detection. SANS Institute. April 15, 2001.
URL: http://rr.sans.org/intrusion/honey_pack.php

[3] Computer Security: A Practical Definition.
URL: http://www.albion.com/security/intro-4.html

[4] Mark Merkow. CCP, CISSP. Playing With Fire: Not So Sweet Honeypots. January 12,2001.
URL:
http://ecommerce.internet.com/news/insights/outlook/article/0,,7761_559431,00.html

[5] Mathew Schwartz. Networks use 'honeypots' to catch an online thief. Computerworld.April 4, 2001.
URL:
http://www.cs.nmt.edu/~cs491_02/IA/honeypot.htm

[6] Lance Spitzner. Honeypots: Definitions and Value of Honeypots. May 17, 2002.
URL: http://www.eneract.com/~1spitz/honeypot.html

[7] Honeynet Project. Know Your Enemy: Honeynets. May 11, 2002.
URL: http://www.honeynet.org/papers/honeynet/

[8] Douglas B. Moran. Vice President, Research & Development. Recourse Technologies,
Inc. Trapping and Tracking Hackers: Collective security for survival in the Internet age.
URL: http://www.recourse.com/
Global Integrity Corporation (an SAIC company). Honeypot Effectiveness Study. Study conducted for Recourse Technologies, Inc. September 22, 2000.

[9] The 'Lectric Law Library's Lexicon On Entrapment.
URL: http://wwwlectlaw.com/def/e024.html
The Evolution of Deception Technologies as a Means for Network Defense. Recourse Technologies.

