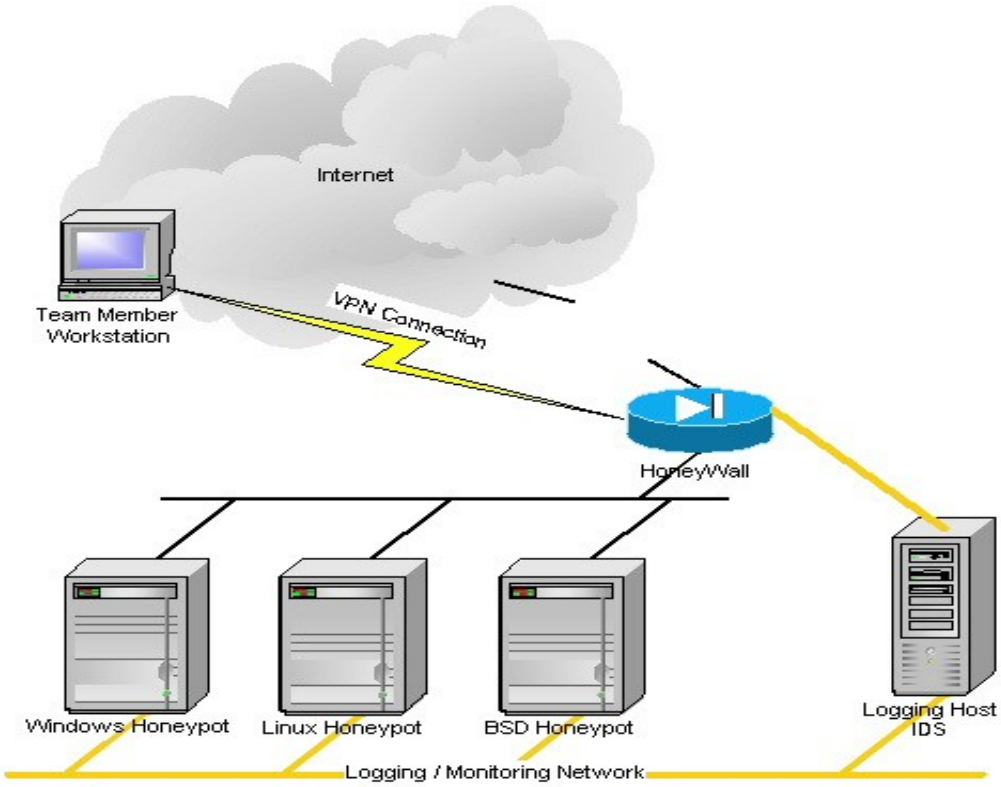
HONEYPOTS

(NETWORK SECURITY AND CRYPTOGRAPHY)



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. One goal of this paper is to show the possibilities of honeypots and their use in a research as well as productive environment.

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. With a more advanced idea of how honeypots work, we will then look at the possible legal ramifications for those who deploy them. Finally we shall conclude by looking at what the future holds for the honeypots and honeynets.

1. INTRODUCTION

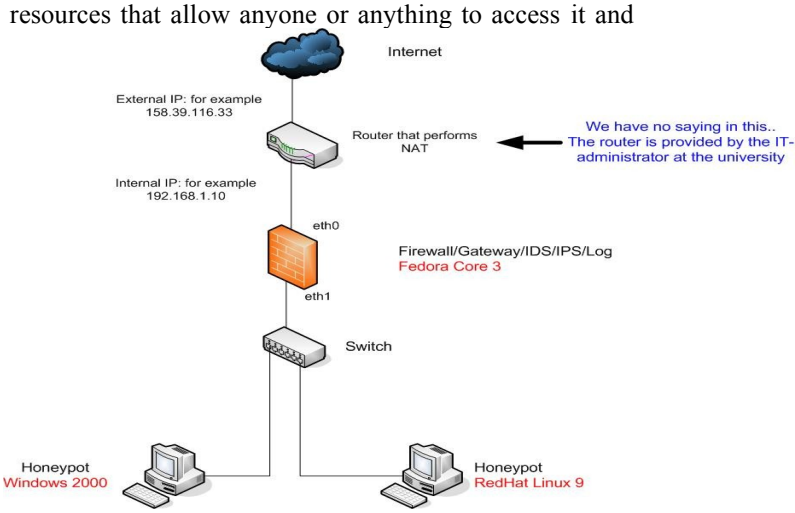
Global communication is getting more important every day. At the same time, computer crimes are increasing.

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.

WHAT IS A 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 resimply an unprotected, unpatched, unused workstation on a network being closely watched by administrators.

Its primary purpose is not to be an ambush for the blackhat 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 blackhat community itself. All this information is used to learn more about the blackhat 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.

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.

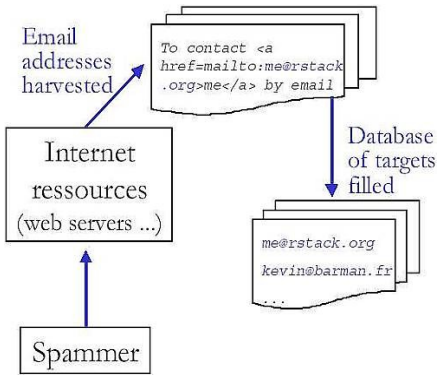
TYPES OF HONEYPOTS:

Honeypots came in two flavors:

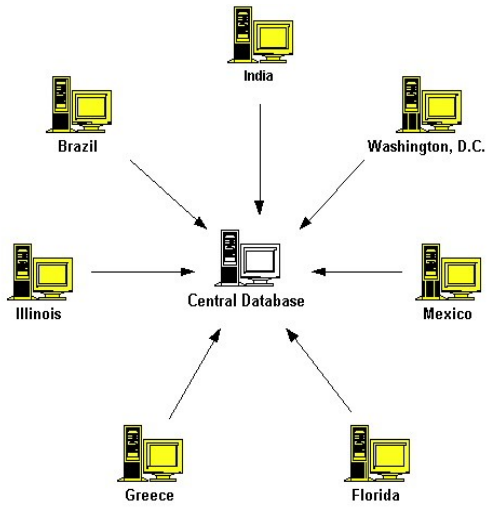
- Low-interaction
- High-interaction.

Interaction measures the amount of activity that an intruder may have with honeypot.In addition, 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 broad categories, as defined by Snort ,two types of honeypots are:

- Production honeypots
- Research honeypots

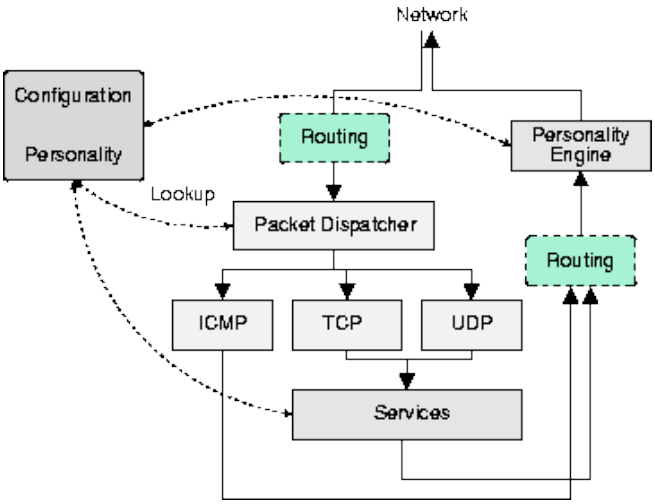
The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot adds value to the security measures of an organization. Think of them as 'law enforcement', their job is to detect and deal with bad guys. Traditionally, commercial organizations use production honeypots to help protect their networks. The second category, research, is honeypots designed to gain information on the blackhat 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.

HONEYPOT ARCHITECTURE:

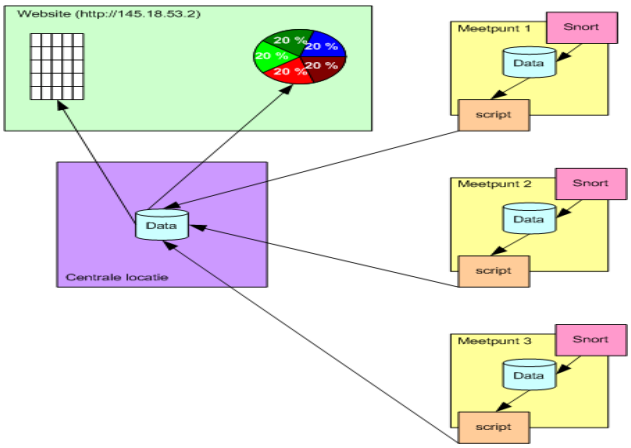
1. Structure of a LOW-INTERACTION HONEYPOT (GEN-I):-

A typical low-interaction honeypot is also known as 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:

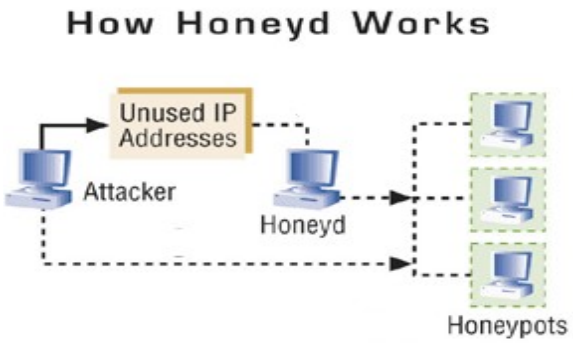
1. This architecture provides a restricted framework within which emulation is carried out. Due to the limited number of services and functionality that it emulates, it is very easy to fingerprint.

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

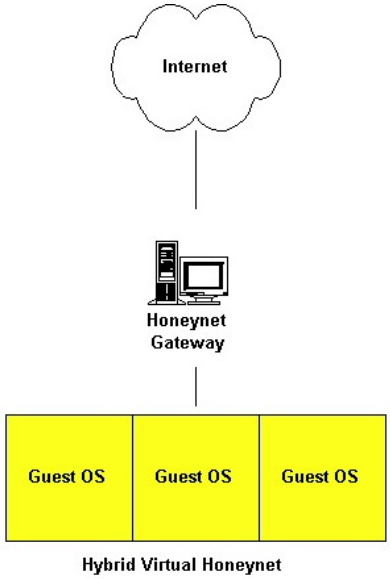
3. It has constrained applications in research, since every service which is to be studied will have to be re-built for the honeypot.

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

A typical high-interaction honeypot consists of the following elements: resource of interest, data control,

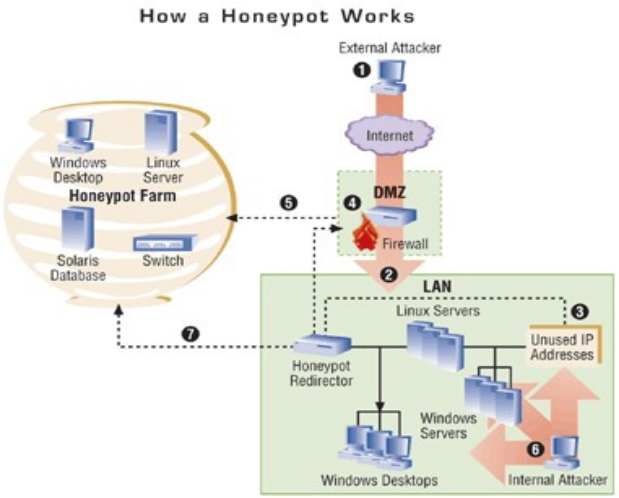


data capture and external logs



your ("known 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

DRAWBACKS:

However, GEN-II honeypots do have their drawbacks as well.

1. To simulate an entire network, with routers and gateways, would require an extensive computing infrastructure, since each virtual element would have to be installed in it entirely. In addition this setup is comprehensive: the attacker can know that the network he is on is not the real one. This is one primary drawback of GEN-II.

2. The number of honeypots in the network is limited.

3. The risk associated with GEN-II honeypots is higher because they can be used easily as launch pads for attacks.

COMPARISON:

FEATURE	GEN-I	GEN-II
Number of virtual systems/ services that can be deployed	Large	Small
Data Control	Limited	Extensive
Level of Interaction	Low	High
Ability to discover new attacks	Low	High
Risk	Low	High

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: **1.**penetrates DMZ and scans the network IP address **2**.the redirection appliance **3**.monitors all unused addresses, and uses Layer 2 VPN technology to enable firewall **4.**to redirect the intruder to honeypot **5**.which may have honeypot computers mirroring all types of real network devices. **6**. Scanning the network for vulnerable systems is redirected **7.** By the honeypot appliance when he probes unused IP addresses

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 attackers motivation.

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.

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.

LEGAL ISSUES PERTAINING HONEYPOTS:

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

- Entrapment,
- Liability
- Privacy.

1. ENTRAPMENT:

Entrapment is when somebody induces the criminal to do something he was not otherwise supposed to do.Honeypots should generally be used as defensive detection tools, 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. The more contents a honeypot tracks, more privacy concerns get generated.

3. LIABILITY:

Is the owner of the honeypot liable for any damage done by that honeypot? They will be safe as long as honeypots are used for directly securing the network.

SOME COMMERCIAL HONEYPOTS AND HELPFUL SOFTWARE:

1. CYBERCOP STING BY NETWORK ASSOCIATES:

This product is designed to run on Windows NT and is able to emulate several different systems including LINUX, SOLARIS, CISCO IOS and NT. It is made to appeal to hackers for looking as if it has several well-known vulnerabilities.

2. BACK OFFICER FRIENDLY BY NFR:

This product is designed to emulate a Back Orifice 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 a low interaction honeypot. . It is a great way to introduce a beginner to the concepts and value of honeypots. BOF is a program that runs on most Windows based operating system. All it can do is emulate some basic services, such as http, ftp, telnet, mail, or BackOrrifice.

3**. TRIPWIRE BY TRIPWIRE**:

This product is for use on NT and UNIX machines and is designed to compare binaries, and inform the server operator, which has been altered. This helps to protect machines from would be hackers and is an excellent way to determine if a system has been compromised.

4. **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 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 detection. It can quickly and easily

determine who is looking for what. As a honeypot, it reduces both

false positives and false negatives, simplifying the detection process, supporting a variety of alerting 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

5. 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 master operating system. Security administrators can modify these jails just as they normally would with any operating system, to include installing applications of their choice, such as an Oracle database or Apache web server, thus making the honeypot far more flexible. The attacker has a full operating system to interact with, and a variety of applications to attack. All of this activity is then captured and recorded. Currently, Mantrap only exists on Solaris operating system.

RELATED WORK:

Much work has been performed using the concept of honeypots i.e., an illicit resource to which any and all traffic or access is deemed to be suspect.

1. TARPITS:

One of the easiest ways to identify vulnerable systems is by using a tool called a scanner or a spider .This brute forces attacks on a whole range of IP addresses, attempting to find vulnerable hosts. This is where a tarpit comes handy. A tarpit blocks a scanner by responding to its first TCP setup message, but ignoring the rest .This simple approach causes the scanner to allocate buffers, start timers and retry, since it believes it has found a valid host .This process repeats until the scanner exhausts its memory and CPU resources and crashes or slows down to an almost unproductive speed.

2. HONEY TOKENS:

It is a data entity whose value lies in the inherent use of data. Honey tokens are entities such as false medical records, incorrect credit card numbers and invalid social security numbers. The very act of accessing these numbers, even by legitimate entities is suspect. This concept is especially useful in preventing larger classes of attacks.

FUTURE WORK:

Honeypots are a new field in the sector of network security. Currently there is a lot of ongoing research and discussions all around the world. Several companies have already launched commercial products. A comparison of available products showed that there are some usable low- to high-involvement honeypots on the market. In the sector of research honeypots, self-made solutions have to be developed as only these solutions can provide a certain amount of freedom and flexibility which is needed to cover a wide range of possible attacks and attackers. Each research honeypot normally has its own goals or different emphasis on the subject. Developing a self-made solution needs a good technical understanding as well as a time intensive development phase.

There is an inherent scope for the research community to be misled by script kiddies, while sophisticated attackers plan more devastating attacks on computer systems across the globe. Although fingerprinting a honeypot is easier said than done, most attackers worth their salt would stay away from any computer system that they deem to be monitoring their activities. Thus in reality, for honeypots to be truly effective, they require to be residing very close to a legitimate resource, probably even on the same network.

This would definitely serve as a precursor to any attacks on the production system making honeypots a true window to the future.

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)<http://www.macom.com/

2)<http://www.enteract.com/honepot.html

3)<http://project.honeypot.org/