

# ***An Investigation of Honeypots and Honeynets***

Network Security  
June 7<sup>th</sup> 2004

Shyh-Sen Huang  
ECE 578

Nathan McReynolds  
ECE 478

# Table of Contents

<b>0. OVERVIEW .....</b>	<b>3</b>
0.1 ABSTRACT .....	3
0.2 INTRODUCTION .....	3
<b>1. HONEYPOTS .....</b>	<b>4</b>
1.1 WHAT IS A HONEYPOT? .....	4
1.2 WHO USES THEM? .....	5
1.3 SUMMARY OF ADVANTAGES AND DISADVANTAGES .....	5
<b>2. DEPLOYMENT.....</b>	<b>6</b>
2.1 ARCHITECTURE .....	6
2.2 DATA CONTROL .....	6
2.3 DATA CAPTURE.....	7
<b>3. BENEFITS AND DRAWBACKS.....</b>	<b>7</b>
3.1 THE BENEFITS .....	7
3.2 THE DRAWBACKS.....	9
<b>4. EXISTING HONEYPOT SOLUTIONS.....</b>	<b>10</b>
4.1 BAIT N SWITCH .....	10
4.2 HONEYD.....	10
4.3 NETBAIT.....	11
4.4 SPECTER .....	11
<b>5. CONCLUSION .....</b>	<b>11</b>
<b>6. RESOURCES.....</b>	<b>12</b>
<b>7. BIBLIOGRAPHY .....</b>	<b>12</b>

## **0. Overview**

### ***0.1 Abstract***

In this generation, the network has become the important part of everyone's life. People use email to contact with friends, to send messages to students at school or employees in a company. They also use the network for web commerce, paying a bill, or transferring funds between bank accounts. Nowadays, more and more people know they should pay attention to their network security. Most of them use some traditional mechanisms to protect their information, including a firewalls, Intrusion Detection Systems, and anti-hack software, which are designed to defensively protect sensitive information. In this project, we will study HoneyNet, which is a deception-based mechanism and different from standard defensive mechanisms. It gathers information about security threats on the system, analyzes the data, then gives users information about the tools, methods, or motivations of the hacker. In this project, we will discuss the properties and differences of honeynets in different architectures. We will also analyze the advantages and drawbacks of honeynets as security solutions.

### ***0.2 Introduction***

A classic means of ensuring network security is to prevent viruses and worms from penetrating the network with the use of patches and security update software. But no network is impenetrable and in time, the network security shall be compromised. Network administrators respond by determining the how the security was breached and implementing the necessary steps to prevent such an occurrence from happening again.

This is a standard approach to network security. Unfortunately, nothing about the hacker or the methods used to penetrate the network is learned. Those who integrate honeypots into their network take a different approach. Instead of only responding to security violations, they watch and learn from the hackers. And from the data collected from the intrusion, better defense mechanisms can be developed to prevent security breaches in the future,

This document shall define the honeypot, describe how they operate, the benefits and drawbacks they provide, and why they are becoming more commonly used by security professionals.

## 1. Honeypots

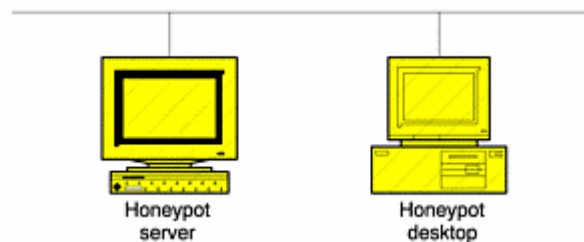
### 1.1 What is a Honeypot?

According to Lance Spitzner, author of **Honeypots, Tracking Hackers**,

*A honeypot is security resource whose value lies in being probed, attacked, or compromised.*<sup>1</sup>

This is counter-intuitive to traditional security measures. Typically, one wants to build stronger and taller walls to prevent unauthorized access to valuable possessions, and in this case, sensitive data held on a computer network. As a network administrator, it is necessary to understand that in time, a hacker (or often referred to in this paper as a *blackhat*) shall successfully infiltrate a network and steal information. Instead of only reacting to these attacks, a well designed honeypot can provide administrators with valuable information about the blackhat.

A simple honeypot can be a single computer connected to a network that runs client software designed to log the actions of a blackhat connected to that system. The honeypot computer otherwise looks like any other production computer on the network. But as the name implies, it is essential to lure the blackhat to the honeypot system in order to record and analyze their actions.



**Figure 1. A Simple Honeypot Configuration**

As the name suggests, a Honeynet is a network of multiple systems. The network can include routers, switches, and machines running different operating systems to resemble of real network environment. Also, nothing is emulated or made to make the network less secure. The idea is to create a network that looks like a real production system used in organizations.

*Honeynets can collect in-depth information about attackers, such as their keystrokes when they compromise a system, their chat sessions with fellow blackhats, or the tools they use to probe and exploit vulnerable systems. This data can provide incredible insight on the attackers themselves. The advantage with Honeynets is that they collect information based on the attackers' actions in the wild.*<sup>2</sup>

Common elements of a Honey net include:

- A firewall computer that logs all incoming and outgoing connections,
- An intrusion detection computer than can see and log all network traffic,
- A remote system log computer so that all commands that a blackhat would use are sent to this computer
- And finally, the honeypot itself. It can run the client software on anything from Windows 2000 to Redhat.

### **1.2 Who uses them?**

There are two main groups that utilize Honey nets: production and research. The production honeypot adds value to the security measures of an organization. They detect intruders, both from outside and within the network, and use the information to enforce their security policies and implement better ones. Research facilities do not use the Honey net as a means of protection. Instead, they research and gather information of security threats that organizations face and determine better ways to protect them.

### **1.3 Summary of Advantages and Disadvantages**

Honey pots have certain advantages and disadvantages as a security tool.

Advantages include:

- **Data Collection.** Remember, computers *should not* be communicating with the honeypot. Any communication that occurs is highly likely to be a blackhat performing a port scan on the system. So normally, the data it collects is of high value, including network activity and what the blackhat does on the system.
- **Detection.** Honey pots have the unique ability to detect and capture unknown attacks otherwise not detected on systems which look for a particular known signature.
- **Resources.** The honeypot does not need to be a top of the line system to simply capture the events that occur on them. They do not have to monitor all the traffic that occurs on the network. Only the traffic that enters the honeypot.

Disadvantages include:

- **Single data point.** The honeypot is essentially of no use to the researcher or the organization if it is not attacked. If the blackhat doesn't send packet to it, then it can't serve any useful purpose.
- **Risk.** Honey pots can be designed with varying levels of risk. Essentially, the more functionality and freedom that is given to the blackhat using the system, the more resources they have to launch new attacks.

A further discussion on the benefits and drawbacks of incorporating a Honey pot into a network are described in Section Three.

## **2. Deployment**

### **2.1 Architecture**

Conceptually, honeypots are uncomplicated. They are the resources that do not produce value, and have no authorized activity. Whenever there is any interaction with a honeypot, it may mean that there are malicious activities. For example, if someone scans your vulnerable desktops on the internal network, and the attacker scans your internal honeypot, your honeypot will detect and log this unauthorized activity effortlessly as no one should be interacting with it.

Therefore, any interaction with a honeynet implies the malicious or unauthorized activity. The connections initiated inbound to the honeynet may be a probe, scan, or attack. We can analyze the activities within the honeynet easily because almost any outbound connections from the honeynet imply someone has compromised a system and has initiated outbound activity. We need to sift through gigabytes of data, or thousands of alerts by traditional security technologies, like the firewall logs. However, we can save a lot of work by using honeynet. A honeynet is built by a network of honeypots, and all captured activity is assumed to be unauthorized or malicious. All we are doing is capturing needles. It's up to the administrator to prioritize which of those needles has the greatest value to us, and then analyze them in detail.

Honeynets are not a product, they are an architecture. This architecture creates a highly controlled network, and we can control and monitor all activities that happen within it. Then we build target systems within the architecture. We create the environment where we can watch everything questionable happening inside it, i.e. intruders interact within our honeynet.

To deploy a honeynet successfully, we must implement the honeynet architecture correctly. If not properly deployed, we may fail to capture the attacker's activities, or even worse, expose ourselves to great risk. To deploy a honeynet, there are two critical requirements: Data Control and Data Capture. All honeynet deployments should satisfy these two requirements. Data Control defines how activity is contained with the honeynet, without an attacker knowing it. Data Capture is capturing all of the attacker's activity, without the attacker knowing it.

### **2.2 Data Control**

Data Control is the containment of activity. It is what mitigates risk. There is always the potential of an attacker using a honeynet to attack non-honeynet systems. We would like to ensure even if an attacker is within the honeynet, he can not accidentally or purposefully harm other non-honeynet systems. First, we have to allow the attackers some degree of freedom to act. The more activities we allow the attackers to own, the more information we can learn about them. However, the more freedom means the more risk that they will circumvent Data Control and harm other non-honeynet systems. Second, we have to control the attacker's activities but do not let them know their actions are being controlled.

One of the best ways to approach Data Control is not to rely on a single mechanism which to implement it. The best approach is to implement Data Control by using layers, i.e. counting outbound connections, intrusion prevention gateways, or bandwidth restrictions. The combination of several different mechanisms will help us to protect a single point of failure, especially while we deal with new or unknown attacks. Data Control should also operate in a fail closed manner. This means if there is a failure in the mechanisms; the honeynet should block all outbound activities, without allowing them.

### **2.3 Data Capture**

Data Capture is the monitoring and logging of all of the attacker's activities within the honeynet. The captured data is analyzed to learn the tools, tactics, and motives of blackhats. The challenge is to capture as much data as possible, without the blackhat detecting the process.

Just like Data Control, one of the primary lessons learned for Data Capture is to use the layers. It is critical to use multiple mechanisms for capturing activity. Not only the combination of layers will help piece together all the attacker's actions, but it prevents to have a single point of failure. The more layers of information that are captured, the more information that can be obtained at the network and host levels.

However, one of the challenges in Data Capture is that a large portion of attacker activities happens over encrypted channels. Data Capture mechanisms must take encryption into consideration. Besides, just like Data Control, we have to minimize the ability of attackers to detect the capture mechanisms.

One of the rules is to make as few modifications to the honeypots as possible. The more modifications we make, the greater the chance of detection. Besides, it is better that we do not store the captured data locally on the honeypots themselves. It is because not only this data could be detected by the attackers, but it could also be modified or deleted. Therefore, the captured data should be logged on a separate and secured system.

## **3. Benefits and Drawbacks**

### **3.1 The Benefits**

#### **Prevention**

The area of using honeypots as a means of prevention is somewhat limited. They are not firewalls. Some organizations may use them under the guiles of deception with the reasoning that they would rather have blackhats attack the honeypots rather than production machines. So they really do little as far as preventing further attacks.

But others use them as a means to discourage blackhats from attacking their network. For example, the honeypot LaBrea Tarpit is used to "tarpit" or slow down automated TCP attacks, such as worms.

## **Detection**

Some organizations have an enormous amounts of data routed through their networks. Despite their use of Intrusion Detection Systems (IDS) used for detecting and alerting administrators of possible attacks, the number of falsely identified attacks recorded by the system can be overwhelming. And over time, the alerts could be simply ignored all together because of the impossibility of organizing and filtering the large amounts of data into true and false attacks.

In addition, counter-IDS methodologies are being developed. For instance, it is possible to use a known attack methodology that might not be detected by an IDS, such as K2's ADM Mutate.

On the contrary, Honeypots do not have this problem. Surely there will be a few "false positives", but no where near the quantities reported by an overwhelmed IDS. The reason is that *any* network activity with a honeypot is immediately regarded as suspicious because no one has any legitimate reason to be communicating with that machine!

Also, the Honeypot can detect intrusions otherwise undetectable when intrusion signatures are new, or have not been updated into the IDS.

But obviously, this detection enhancement to a network should never replace the IDS and its role of intrusion detection and prevention. The honeypot should be used to complement all other security measures implemented on the network.

## **Reaction**

Many times a system that has been compromised (data was stolen or altered) can not be taken offline to determine what exactly is effected or to complete a thorough evaluation of the attack. But, if the system that had been compromised was a honeypot, then it would not have been a problem to simply replace the effected honeypot computer with another one. Afterwards, the administrator has the opportunity to perform diagnostics on the effected system to accurately evaluate the problem.

Otherwise, dedicated systems may not be allowed to be taken offline because of their importance to the organization, if for instance, it was an e-commerce server. Time offline could result in lost revenue. And being unable to perform a detailed evaluation of the attack, determining the root cause of the problem could become nearly impossible.

## **Research**

Throughout history, every successful military has studied, analyzed, and even mimicked the capabilities of their enemy in order to shore up their own defenses and strategize effective means of countering their attacks. Honeypot research facilities do nothing different.

What better way to learn about the bad guys then to watch them in action, to record step-by-step as they attack and compromise a system. Of even more value is watching what they do after they compromise a system, such as communicating with other blackhats or uploading a new tool kit. It is this potential of research that is one of the most unique

characteristics of honeypots. Also, research honeypots are excellent tools for capturing automated attacks, such as auto-rooters or Worms. Since these attacks target entire network blocks, research honeypots can quickly capture these attacks for analysis.<sup>3</sup>

Techniques learned from researchers are then implemented into organization's honeypots. Keep in mind that research honeypots are designed to watch and observe the techniques of blackhats, whereas organization honeypots are designed primarily for the detection of and reaction to intrusions.

### **3.2 The Drawbacks**

Generally speaking, honeypots have some disadvantages. That is the reason that they do not replace any existing technologies. Honeynets allow us to collect extensive information on a variety of threats. However, to obtain this information, we have to allow attackers access to our system and application. Therefore, the price we pay for this capability is risk. In this section, we list the drawbacks and risks of honeypots.

#### **Harm**

Harm is when a honeynet is used to attack or harm other non-honeynet systems. For example, an attacker may break into a honeynet, then launch an outbound attack never seen before, successfully harming its intended victim. Data Control is the primary means of mitigating this risk. Multiple layers of Data Control are put in place to make it more difficult for the attacker to cause damage. However, there is no guaranteed method to ensure that a honeynet can not be used to attack or harm someone else. No matter what mechanisms are put in place, an attacker can eventually bypass them. For low risk organizations, we may want to minimize the activity allowed outbound. For greater risk organizations, we may decide to allow greater outbound activity.

#### **Risk of detection**

Once the true identity of a honeynet has been identified, its value will be reduced dramatically. Attackers can ignore or bypass the honeynet, eliminating its capability for capturing information. Perhaps even more dangerous is the threat that once identified, an attacker can introduce false or bogus information into a honeynet, misleading the data analysis. For example, with local access to the honeynet, an advanced attacker, or an attacker armed with proper tools, can potentially identify that a honeynet is in place and may even identify the Honeynet Data Control and/or Data Capture mechanisms themselves. If we are simply blocking after 10 outbound connection attempts, the attacker simply needs to try 20 outbound connections and watch the 11th one consistently fail. If we modify the packets as they pass through the honeynet, the attacker simply needs to send packets with a known payload to systems that they control and see if they are modified in transit. If we are tunneling traffic to a "honey farm", the added latency may give away the fact that a honeynet is in place. Or the attacker may simply use methods to detect the presence of local Data Capture capabilities on the honeypot itself.

**Risk of disabling Honeynet functionality**

This part could be an attack against either Data Control or Data Capture routines. Attackers may want not only to detect a honeynet's identity, but disable its Data Control or Data Capture capabilities, potentially without the honeynet administrator knowing that functionality has been disabled. For example, an attacker may gain access to a honeypot within the honeynet, then disable Data Capture functionality on the honeypot. The attacker could then feed the honeypot with fake activity, making administrators think Data Capture is still functioning and recording activity. Having multiple layers of Data Control and Data Capture helps to mitigate this risk, as there is no single point of failure.

These risks can also be mitigated by utilizing human monitoring. With human monitoring, a trained professional monitors and analyzes the honeynet in real time. Anytime a suspected blackhat has successfully gained (or is attempting to gain) access to one of the honeypots (such as detection of outbound connections, frequent established inbound connections, increased inbound traffic, transfer of files, unusual system activity, etc) a security professional should be monitoring and analyzing all captured data. This helps prevent the risk of an attacker detecting or disabling a honeynet, and attempting to harm other non-honeynet systems. In a worse case scenario, the honeynet can always be shut down if the attacker has exceeded the organizations threshold for risk. Although the honeynet can help to mitigate risk, the best tool is to have human beings involved in monitoring, analyzing, and reacting to honeynet activity.

**4. Existing Honeypot Solutions**

In this section, we list some available products for honeypots. They include some freeware and commercial software.

**4.1 Bait n Switch**

The Bait and Switch Honeypot is a multifaceted attempt to take honeypots out of the shadows of the network security model and to make them an active participant in system defense. To do this, it creates a system that reacts to hostile intrusion attempts by redirecting all hostile traffic to a honeypot that is partially mirroring your production system. Once switched, the would-be hacker is unknowingly attacking your honeypot instead of the real data and your clients and/or users still safely accessing the real system.

**4.2 HoneyD**

Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses on a LAN for network simulation. Honeyd improves cyber security by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems.

### **4.3 NetBait**

NetBait is a network security solution that foils intruders and attackers on an organization's network through deception and disinformation. Its key features include dynamic behavior configuration, centralized remote management, and hack-proof operation

### **4.4 Specter**

Specter is a smart honeypot system. It simulates a complete machine, providing an interesting target to lure hackers away from the production machines. Specter offers common Internet services such as SMTP, FTP, POP3, HTTP and TELNET which appear perfectly normal to the attackers. Instead, they are traps for them to mess around and leave traces without even knowing that they are connected to a decoy system. Of course, the decoy does none of the things it appears to do, but instead logs everything and notifies the appropriate people. Furthermore, specter automatically investigates the attackers while they are still trying to break in. Specter provides massive amounts of decoy content and it generates decoy programs that will leave hidden marks on the attacker's computer. Automated weekly online updates of the honeypot's content and vulnerability databases allow the honeypot to change constantly without user interaction.

## **5. Conclusion**

The development of Honeypots as a network security device has increased over recent years as the demand for network connectivity has increased exponentially. As demonstrated, the Honeypot is not an alternative to Intrusion Detection Systems to secure a vulnerable network. Instead, they can be an effective supplement for detecting network intrusions, enabling reactions to those intrusions, and implementing more effective security policies.

Honeypots offer a unique perspective to defending networks by learning the habits and techniques of the blackhat at an additional cost of minimal network alert reporting and monitoring time. And honeypots are the result of taking a pro-active approach, rather than a defensive approach to network security.

## 6. Resources

### **Open Source Honeypots: Learning with Honeyd**

by Lance Spitzner, [www.tracking-hackers.com](http://www.tracking-hackers.com)

<http://www.honeynet.org>

<http://www.honeypots.net/>

<http://www.infosecwriters.com>

<http://www.securityfocus.com>

<http://www.techonline.com>

<http://www.tracking-hackers.com/>

<http://www.webtalkguys.com/>

## 7. Bibliography

---

<sup>1</sup> Spitzer, Lance. Honeypots, Tracking Hackers. PDF version. Addison Wesley, 2002. Pg 23.

<sup>2</sup> Same, Pg 124.

<sup>3</sup> Spitzer, Lance. Honeypots - Definitions and Value of Honeypots.

<http://www.infosecwriters.com>, March 6, 2003.