`

San Jose State University

Network Security

CMPE 209

Spring 2007

Prof. Richard Sinn

Presentation Report

Honeypots

Date: 03-13-2007

Submitted By:
Security Monkeys

Ankur Sharma
Ashish Agarwal
Elly Bornstein
Santak Bhadra
Srini Natarajan

Table of Contents

Honey Pots

Introduction

Network IDS:An IDS (Intrusion Detection System) detects unwanted manipulation to the computer network in a network. An intrusion detection system is used to detect all types of malicious network traffic and computer usage like network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malwares.

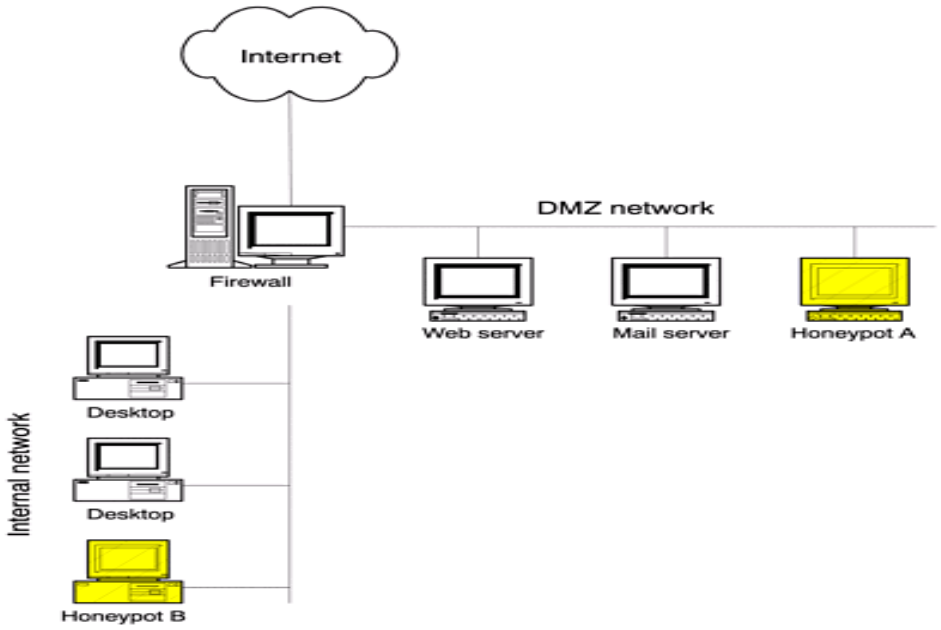
We all know that in today's society there are hackers and intruders attacking our computers from all directions. Moreover, most of these people feel as though the hackers will never fall victim to such a crime much less even be targeted by such an individual.

But, there are some new advances in technology that allow users to actually set traps for hackers and virtually fight back. This trap is known as the Honeypot. Honeypot is an advance technology which is used to trace and catch the hackers/attackers who intend to attack a secure system.

Definition: It is a security resource used to detect, deflect or counter attacks attempts at unauthorized use of information system. It consist of a computer ,data or a network site that seems to be a part of network but actually it is not .It is an isolated ,protected and monitored terminal which seems to have valuable information for the attackers.
Honeypots can be defined in three layered networks:

- Prevention: Honeypots can be used to slow down or stop automated attacks
- Detection: It is used to detect unauthorized activity and capture unknown attacks. Generate very few alerts, but when they do you can almost be sure that something malicious has happened.
- Response: Production honeypots can be used to respond to an attack. Information gathered from the attacked system can be used to respond to the break-in.

Honeypot in a real network environment:



Types of Honeypots

Honeypots can be classified on the basis of their deployment and on basis of their level of interaction/involvement in the network. On the basis of their deployment Honeypots can be classified in to two categories:

- Production Honeypots
- Research Honeypots

Production Honeypots:

The main purpose of this production honeypots is to mitigate the risk in an organization. Production Honeypots are placed under the production network with other production servers by the organization to improve their overall state of security .These are basically have a low level involvement with the network.

Research Honeypots:

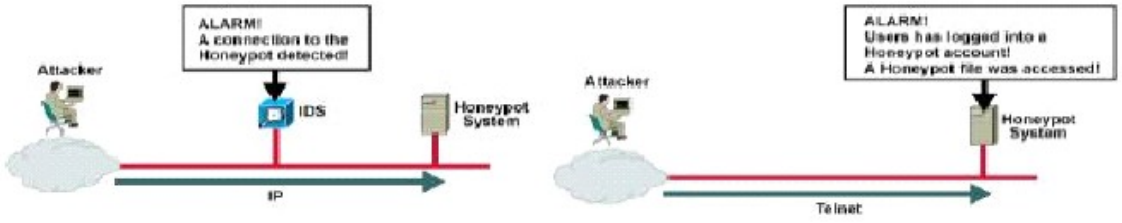
Research Honeypots are run by volunteer non profit organization whose aim is to gather information about the black hat community .These Honeypots do not add any value to any companies but work independently.

On the basis of level of interaction Honeypots are classified as:

- Low-Interaction Honeypots: Honeyd
- High Interaction Honeypots: HoneyNet

Honeyd:

Honeyd is an open-source solution which was created and maintained by NielsProvos. The primary purpose of Honeyd is intrusion detection; it does this by monitoring all the unused IPs in a network. Any attempted connection to an unused IP address is assumed to be unauthorized or malicious activity. After all, if there is no system using that IP, why is someone or something attempting to connect to it? For example, if your network has a class C address, it is unlikely that every one of those 254 IP addresses is being used. Any connection attempted to one of those unused IP addresses is most likely a threat to the network.



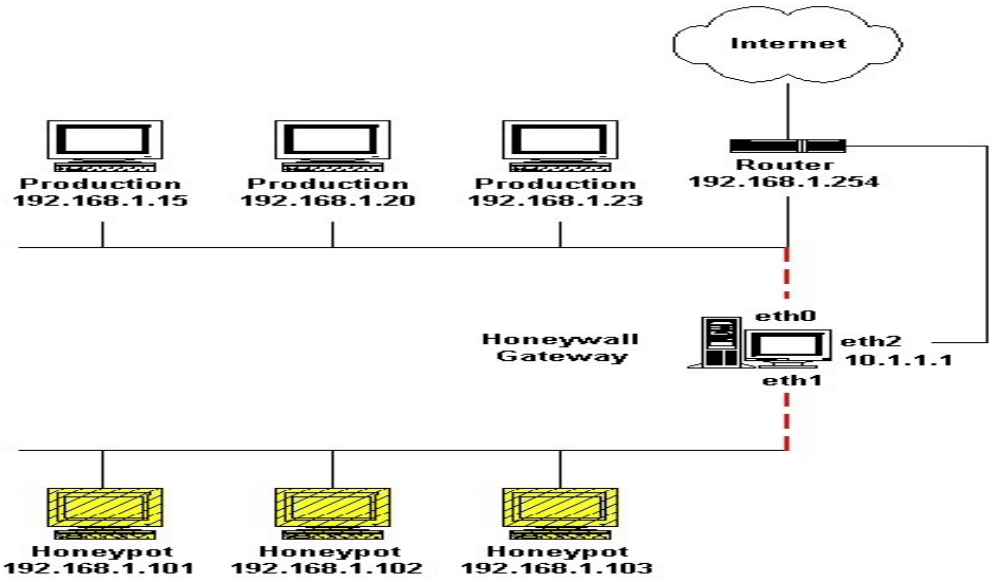
Honeyd can monitor all of these unused IPs at the same time. Whenever a connection is attempted to one of them, Honeyd automatically assumes the identity of the unused IP addresses and then interacts with the attacker.
Honeyd can detect any activity on any UDP or TCP port, as well as some ICMP activity. The user doesn't have to create a service or port listener on ports he wants to detect connections to, Honeyd does this all.

HoneyNet:

It is a high-interaction honeypot designed to capture extensive information on threats. High-interaction means a honeynet provides real systems, applications, and services for attackers to interact with, as opposed to low-interaction honeypots such as Honeyd which provide emulated services and operating systems. What makes a honeynet different from most honeypot is that it is a network of real computers for attackers to interact with.
Conceptually honeynets are very simple; they are a network that contains one or more honeypots. Since honeypots are not production systems, the honeynet itself has no production activity, no authorized services. As a result, any interaction with a honeynet implies malicious or unauthorized activity. Any connections initiated inbound to your honeynet is most likely a threat. This makes analyzing activity within your honeynet very simple. With traditional security technologies, such as firewall logs or IDS sensors, you have to sift through gigabytes of data. A great deal of time and effort is spent looking through this information, attempting to eliminate false positives while identifying attacks or unauthorized activity.

Honeynet Architecture:

To successfully deploy a honeynet, you must correctly deploy the honeynet architecture. The key to the honeynet architecture is what we call a honeywall. This is a gateway device that separates your honeypots from the rest of the world. Any traffic going to or from the honeypots must go through the honeywall. This gateway is traditionally a layer 2 bridging device, meaning the device should be invisible to anyone interacting with the honeypots. Below we see a diagram of this architecture. Our honeywall has 3 interfaces. The first 2 interfaces (eth0 and eth1) are what separate our honeypots from everything else; these are bridged interfaces that have no IP stack. The 3rd interface (eth2, which is optional) has an IP stack allowing for remote administration.



There are several key requirements that a honeywall must implement; Data Control, Data Capture, Data Analysis, Data Collection.

1) **Data Control:** Our aim is to prevent the data from an attacker once he has entered the network.
2) **Data Capture:** is the monitoring and logging of all of the threat's activities within the honeynet.
3) **Data Analysis:** A honeynet is worthless if we have no means to analyze he data collected. Every organization has different means to apply this.
4) **Data Collection:** This only applies to organizations with multiple honeynets as it is necessary to collect data from all the sources.

Advantages and Disadvantages of Honeypots

Advantages:

- Productive environment: It distracts the attention of attacker from the real target.
- We can peek in to the guest operating system at any time.
- We can reinstall the contaminated guest easily.
- It is really simple to implement and use honeypots.

Disadvantages:

- Sub-optimal utilization of computational resources.
- Reinstallation of polluted system is very difficult.
- Difficulty in monitoring of such system in a safe way.
- Detecting the honeypot is easy

References

1) http://www.securityfocus.com
2) http://www.honeypots.net/
3) http://en.wikipedia.org/wiki/Honeypot
4) http://www.tracking-hackers.com
5) http://www.governmentsecurity.org
6) http://www.securityforces.com