HONEYPOTS

COURSE PROJECT REPORT

SUBMITTEDBY

S. Pranav (RA2011030010212)
Y. Sree Santhosh (RA2011030010214)
K. Abhiram (RA2011030010218)

UNDERTHEGUIDANCEOF

Dr. Balasaraswathi R

(ASSOCIATE PROFESSOR,NETWORKING AND COMMUNICATIONS)

INPARTIALFULFILLMENTOFTHEREQUIREME NTS FORTHE DEGREEOF

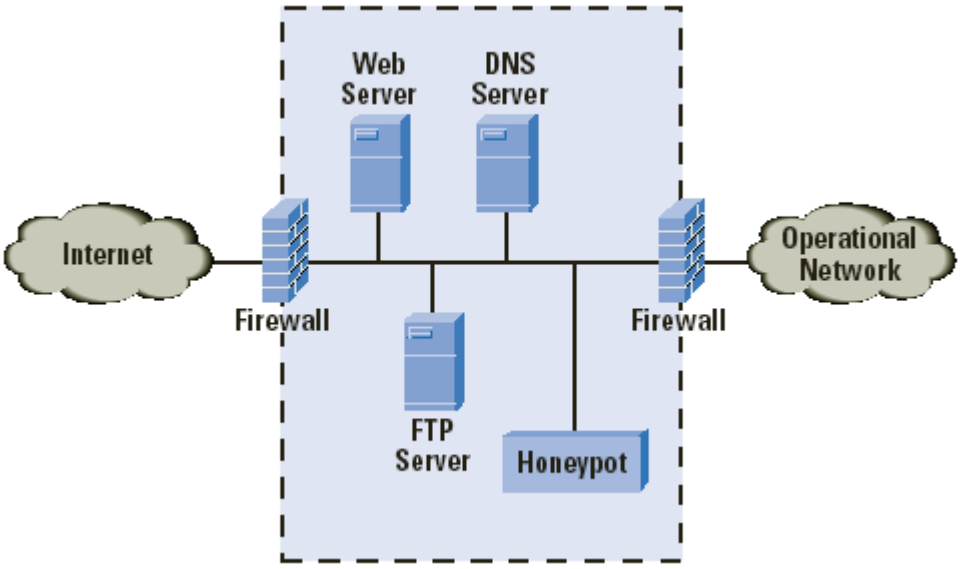
BACHELOROF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING
WITH SPECIALIZATION IN CYBER SECURITY

DEPARTMENT OF NETWORKING AND COMMUNICATIONS
COLLEGE OF ENGINEERING ANDTECHNOLOGY
SRMINSTITUTEOFSCIENCEANDTECHNOLOY
KATTANKULATHUR-603203

NOVEMBER 2022

TABEL OF CONTENTS

Abstract:
This paper introduces Honeypot, a new technology for Network Security. The paper deals with the basic aspects of Honeypots, their use in modern computer networks and their implementation in educational environments. It explains the different types i.e Production honeypot, Research honeypot, low level interaction honeypot, medium level interaction honeypot, high level interaction honeypot and functions of honeypots. The advantages & disadvantages related to honeypot are discussed further. Probable future work in the area of honeypot is discussed which includes enhancement in framework of honeypot.



Virtual machine that sits on a network or a client
Goals

- Should look as real as possible!
- Should be monitored to see if its being used to launch a massive attack on other systems
- Should include files that are of interest to the hacker

Introduction:

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. For example: users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Some other methods for securing the network are: Cryptography, Encryption-Decryption, Bio-metrics, Firewalls, Intrusion Detection System (IDS), Honeypots.

Encryption: It is a process of translating a message, called the Plaintext, into an encoded message, called the Ciphertext.

Decryption: It is the process of extracting the original information from the encrypted data.

Cryptography: Prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense.

Intrusion Detection System (IDS): It inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Firewall: It is a system which limits network access between two or more networks.

Biometrics: This technology measure a particular set of a person's vital statistics in order to determine identity.

HoneyPot: A honey pot is a computer security mechanism on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems.

Literature Survey:

A Honey pot is a computer system that is expressly set up to attract and "trap" people who attempt to penetrate other computer systems (This includes the hacker, cracker). It contains some interesting data or sometimes it behaves like a real operating system to the attacker to be probed or attacked. It is used as decoy. The intruder is intended to detect the Honeypot and try to break into it. The purpose of a Honeypot is to detect and learn from attacks and use that information to improve security. A network administrator obtains information about the current threats on his network. Honeypot can be used to examine vulnerabilities of the operating system or network. Moreover it can be used to observe activities of an individual which gained access to the Honeypot. Honeypots are a unique tool to learn about the tactics of hackers.

Classification:

By Level of Interaction:

- High
- Low

By Implementation:

- Virtual
- Physical

By Purpose:

- Production
- Research

Interaction:

Low interaction Honeypots

- They have limited interaction, they normally work by emulating services and operating systems
- They simulate only services that cannot be exploited to get complete access to the honeypot
- Attacker activity is limited to the level of emulation by the honeypot
- Examples of low-interaction honeypots include Specter, Honeyd, and KFsensor.

High interaction Honeypots:

- They are usually complex solutions as they involve real operating systems and applications.
- Nothing is emulated, the attackers are given the real thing.
- A high-interaction honeypot can be compromised completely, allowing an adversary to gain full access to the system and use it to launch further network attacks.
- Examples of high-interaction honeypots include Symantec Decoy Server and Honeynets.

Implementation:

- Physical
  - Real machines
  - Own IP Addresses
  - Often high-interactive
- Virtual
  - Simulated by other machines that:
    - Respond to the traffic sent to the honeypots
    - May simulate a lot of (different) virtual honeypots at the same time.

Production:

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations

- Prevention
    - To keep the bad elements out
    - There are no effective mechanisms
    - Deception, Deterrence, Decoys do NOT work against automated attacks: worms, auto-rooters, mass-rooters
- Detection
    - Detecting the burglar when he breaks in
- Response
    - Can easily be pulled offline

Research:

- Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.
- Collect compact amounts of high value information
- Discover new Tools and Tactics
- Understand Motives, Behavior, and Organization
- Develop Analysis and Forensic Skills

ADVANTAGES OF HONEYPOT:

Honeypots have several distinct advantages when compared to the current most commonly used security mechanisms.

• Small Data Sets - Honeypots only pay attention to the traffic that comes to them. They are not concerned with an overload of network traffic or determining whether packets are legitimate or not. Therefore they only collect small amounts of information – there are no huge data logs or thousands of alerts a day. The data set may be small, but the information is of high value.

• Minimal Resources – Since they only capture bad activity, they require minimal resources. A retired orlow end system may be used as a honeypot. • Simplicity – They are very simple and flexible. There are no complicated algorithms to develop, state tables or signatures to update and maintain.
• Discovery of new tools and tactics – Honeypots capture anything that is thrown at them, which can include tools and tactics not used previously.

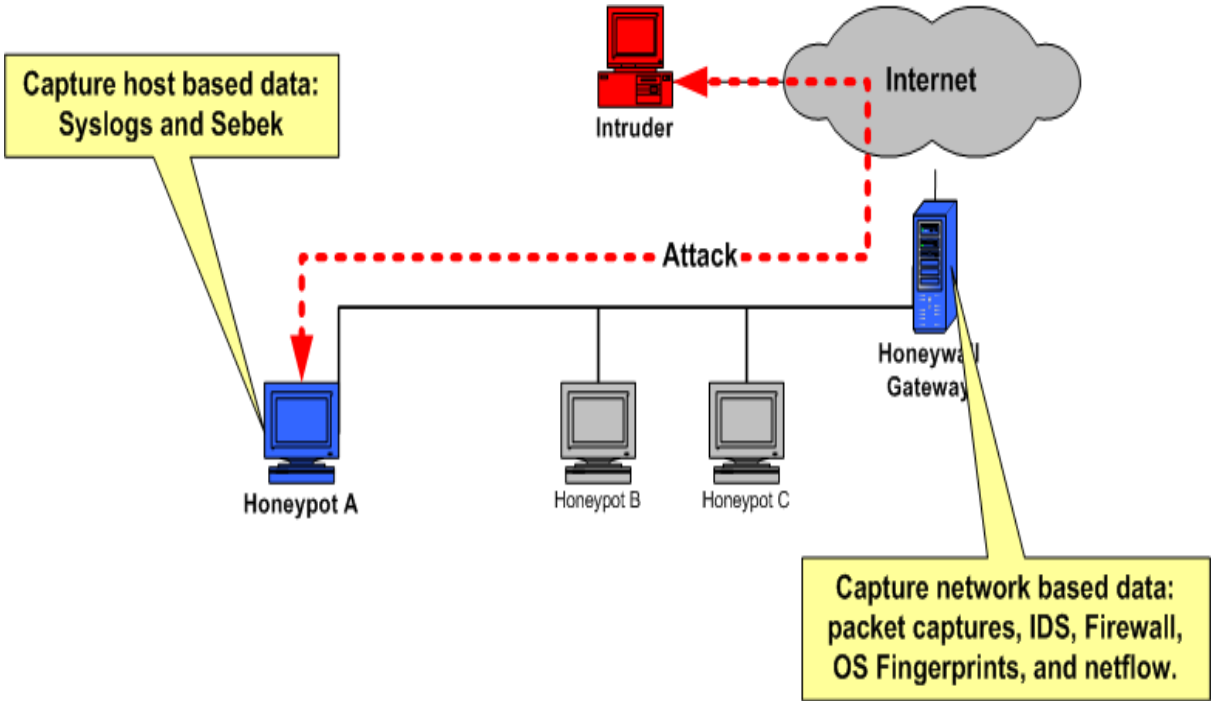
DISADVANTAGES OF HONEYPOT:

Honeypots have several risks and disadvantages. Although few in number, it is these disadvantages that prevent honeypots from completely replacing your current security mechanisms.
• Limited Vision – The only activity tracked and captured by a honeypot is when the attacker directly interacts with them. Attacks against other parts of the system will not be captured unless the honeypot is threatened also.
• Discovery and Fingerprinting – Fingerprinting is when an attacker can identify the true identity of a honeypot because it has certain expected characteristics or behaviours. A simple mistake such as a misspelled word in service emulation can act as a signature for a honeypot.
• High level of Risk- In case of Highlevel interaction honeypots there is huge risk as it provides real operating system to be probed or attacked.

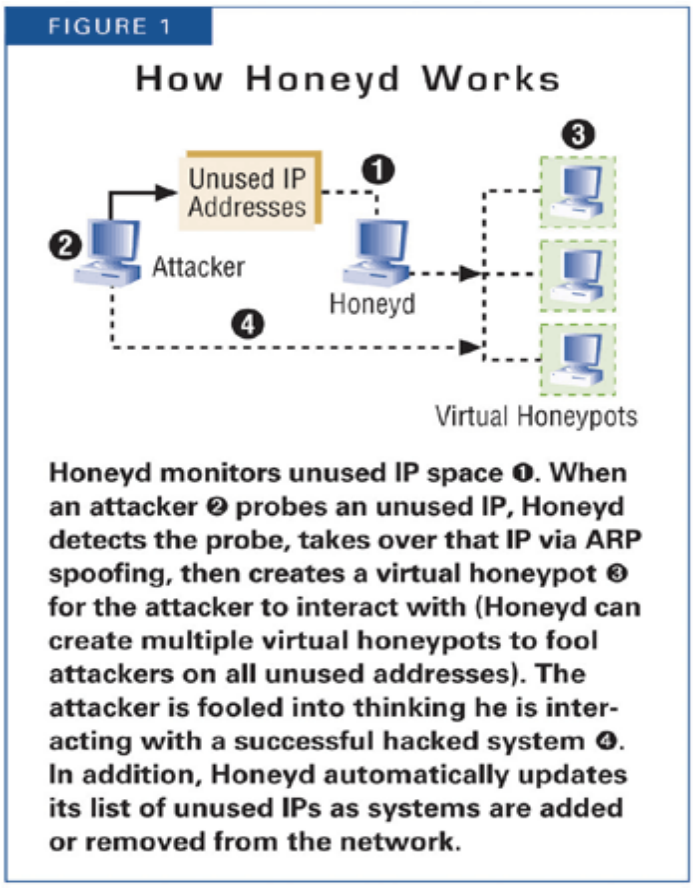
Working:

Working of Honeynet- High- Interaction Honeypot

- Honeynet has 3 components:
  - Data control
  - Data capture
  - Data analysis



Working of Honeyd- Low- Interaction Honeypot:



Conclusion:

The paper provides a brief overview of honeypot and their usage. Different types of honeypot such as production honeypot, research honeypot, low level Interaction honeypot, medium level Interaction honeypot and high level Interaction honeypots are discussed with examples. The honeypots is relatively a new technology and has good scope for future work. Honeypot can be used with other well established security tools such as IDS or Firewalls to make them more effective.

REFERENCES:

[1]. http://project.honeynet.org/papers/individual/Doering.pdf
[2]. http://security.rbaumann.net/download/honeyd.pdf
[3]. http://www.pixel-house.net/midinthp.pdf
[4]. http://www.honeypots.net/.
[5]. http://www.honeynet.org/papers/kye.html.
[6]. http://www.honeyd.org/background.php.