1. Introduction:

HoneyPot is a network trap or decoy system. It is a computer security mechanism (basically baiting a suspect). Virtual machine that sits on a network. HoneyPot is an intrusion detection technique used to study hacker's movement. The function of a honeypot is to represent itself on the internet as a potential target for attackers, usually a server or other high-value target and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

2. Types:

2.1 Based on purpose

- Production

1. Easy to use
2. Capture only limited information
3. Primarily used by companies and corporations
4. Prevention – Deception and decoys don't work against automated attacks like worms, auto rooters and mass-rooters

- Research

1. Complex to deploy and maintain
2. Capture extensive information

used primarily by research, military, or government organizations.

3. Discover new Tools and Tactics
4. Understand Motives, Behavior, and Organization

- Advantages of a Research Type HoneyPot

1. Easier and cheaper to analyze the data
2. Work fine in encrypted or IPv6 environments
3. Can collect in-depth information
4. Conceptually very simple

- Disadvantages of a Research Type HoneyPot

1. Building, configuring, deploying and maintaining a high-interaction honeypot is time consuming. Difficult to analyze a compromised honeypot

2.2 Based on Implementation

- Virtual

1. Respond to the traffic sent to the honeypots
2. May simulate a lot of (different) virtual honeypots at the same time

- Physical

1. Real machines

2. Own IP Addresses Often high-interactive

2.3 Based on interaction

- High level

They are usually complex solutions as they involve real operating systems and applications E.g. Symantec Decoy Server and Honeynets. 2-3 HoneyPOTs on a network form a honeynet which is an entire network of computers designed to be hacked. Key to the honeynet architecture is the honeywall.. Nothing is copied or cloned, the attackers are given the real system.

- Low level

They have limited interaction, they normally work by copying services and operating systems Attacker activity is limited to the copied system by the honeyPOT. E.g. Honeyd, Specter

3. Component diagram:

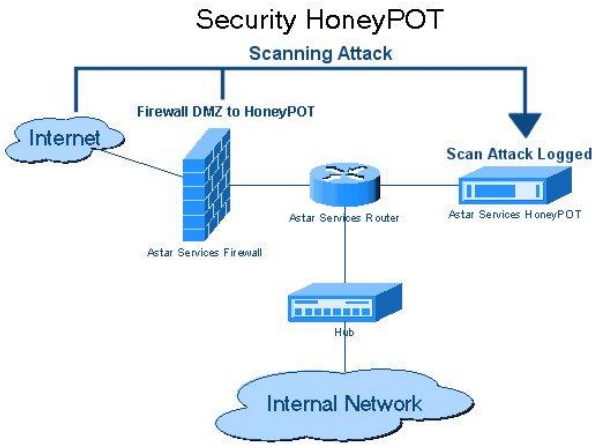

Fig.1. Information system of HoneyPOT

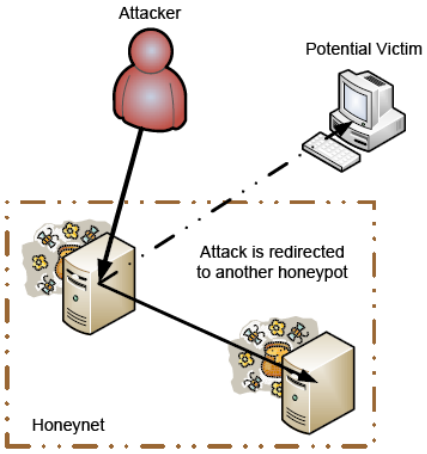

Fig.2. Generalized placement of HoneyPot

Terms:

1. Firewall – network security system that monitors and controls incoming and outgoing network traffic based on security rules. Basically, a barrier between trusted internal network and untrusted external network
2. DMZ (demilitarized zone) – physical / logical subnet that separates an internal local network (LAN) from other untrusted networks. It provides additional layer of security as it restricts the ability of hackers to directly access internal servers and data. A DMZ is made using one to two firewalls.
3. Hub – common connection point for devices in a network. It contains multiple ports internal network/ Local area network (LAN)

4. Honeyd – Low Interaction HoneyPOT

Concept – Monitoring unused IP Space

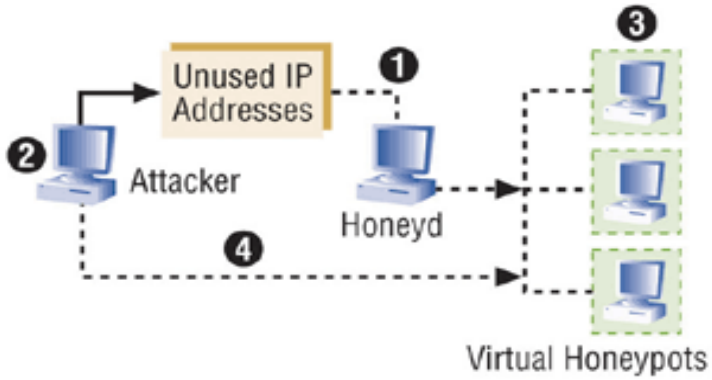

Fig.3. A low interaction honeyPot (Honeyd)

Working –

Honeyd monitors unused ip space. When an attacker probes an unused IP Honeyd detects that probe, takes over that IP using ARP Spoofing and then creates a virtual Honeypot (Honeyd can create multiple virtual honeypots) for the attacker to interact. The attacker is fooled into thinking he is interacting with a successful hacked system.

In addition, honeyd automatically updates its list of unused IPs as systems are added or removed from the network.

5. Honeynet – High Interaction Honeypot

Components – Data control, Data capture, Data analysis

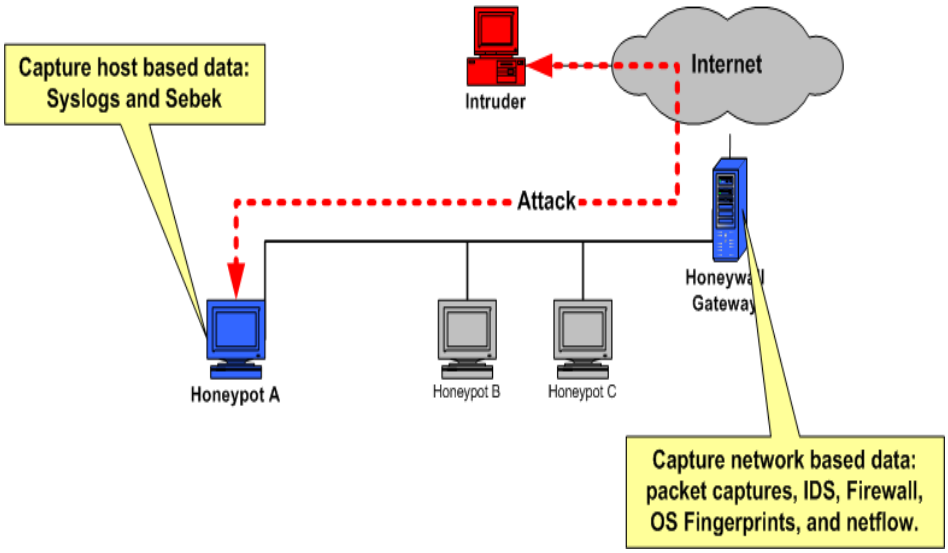

Fig.4. High Interaction honeyPot (Honeynet)

6. Application:

Worm signature generation using HoneyPOT Technology

Working of the system Architecture:

1. Gate translator will collect all traffic and will redirect them to the first inbound honeyPOT

2. Internal translator will redirect the malicious traffic to the second inbound honeyPOT

3. Stickey honeyPOT is adjusted between honeyPOT 1 and 2 to slow down the worm penetration rate. Different TCP tricks are there for stickey honeyPOT

4. HoneyPOT 3 consists of Antivirus Engine All the malicious traffic will go through the engine which consists of behavioural detection engine and corresponding signature will be generated and will further go through the low interaction honeyPOT

5. Low interaction honeyPOT will send the signature to a centralized storage system through which the IDS can get the information. So, analysing the signature IDS can protect any attack, as it will get its generated signature.

6. If the antivirus engine in honeynet 3 is unable to detect any signature then, that payload will be automatically redirected to internet through unused IP system.

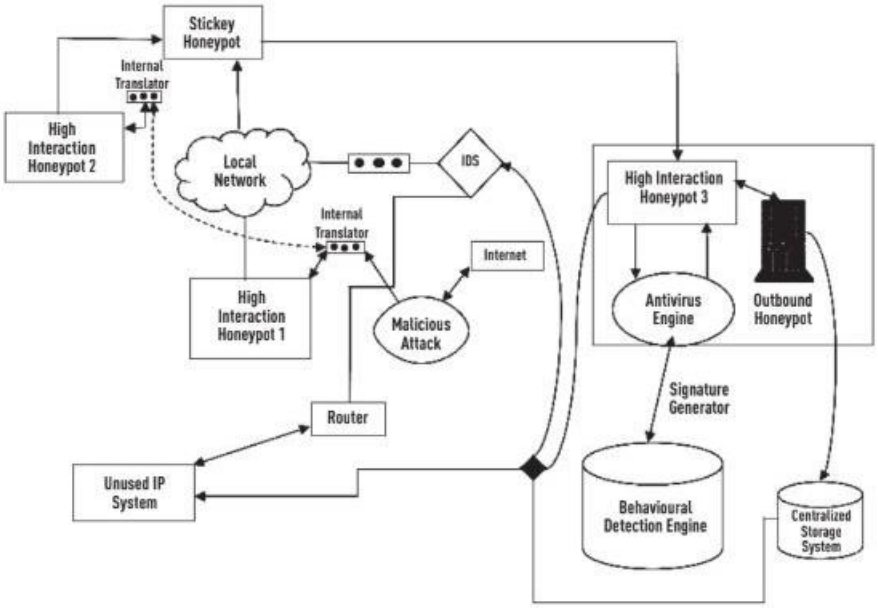

Fig.5. System Architecture

7. Conclusion:

HoneyPot can collect in depth data which no other technology can

Different from others – its value lies in being attacked, probed or compromised

Extremely useful in observing hacker movements and preparing the systems for future attacks

8. References:

- www.cnki.com.cn - HoneyPot - Network Trap
- Intrusion detection systems: possibilities for the future,
  By Karen A. Forchit
- CSI Communications: Volume No.43 |Issue no.5 | August 2019
- Honeypots : Tracking Hackers

  By Lance Spitzner