IMPLEMENTING HONEYPOT LAN DETECTION:
PORT DETECTION AND NETWORK MONITORING

AMRAN BIN SALLEH

**A thesis submitted in fulfillment of the
requirement for the award
of the degree of
Bachelor of Computer Science (Computer Systems and Network)**

**Faculty of Computer Systems & Software Engineering
University College of Engineering & Technology Malaysia**

OCTOBER 2005

ABSTRACT

Nowadays, most of attackers try to attack an unsecured network operating system and scanned a subnet by using a tool such as Nmap. The attacker then tried to attempt the server or important network parts through ports on the network. Regarding that situation, it will be cause some of the host on the network unusable. To overcome this problem, one system has been developed for network administrator and it be used in the area of computer and Internet security. It is a resource, which is it intended to be attacked and compromised to gain more information about the attacker and his attack techniques. By using this technique the administrator can gather more information about the attacker. The administrator will get the pop up message based on each suspicious traffic on the network. Honeypot used to save information from attacker such as IP address, Mac Address, time attack, local port and remote port that honeypot deal with. When honeypot was attacked, the administrator uses the information to learn about vulnerabilities of the current network and improve it for the future. The expected from this honeypot, it will help the administrator to detect and know what port that is use by the attacker in the network. Microsoft Visual Basic 6.0 and Microsoft Access 2003 will be used to develop interface and database of honeypot. The investigation on this system can be used in future and can be extensive.

ABSTRAK

Pada masa sekarang kebanyakan penceroboh lebih minat menyerang sistem operasi rangkaian yang kurang mempunyai keselamatan dengan menggunakan "*Nmap*" dan sebagainya. Kebanyakan mereka akan mendapatkan "*server*" atau mana-mana bahagian penting rangkaian melalui *"port"* yang digunakan dalam rangkaian. Ekoran dari situasi ini ia akan menyebabkan sesetengah *"host"* dalam rangkaian tidak berfungsi. Oleh hal yang demikian, satu sistem akan dibangunkan untuk mengatasi masalah tersebut. Sistem tersebut dinamakan sebagai *"Honeypot"* yang digunakan untuk keselamatan di dalam komputer rangkaian. Ia merupakan satu sumber untuk menarik penceroboh dan berkompromi dengan mereka. Ini adalah untuk membolehkan pentadbir rangkaian mengetahui semua maklumat tentang penceroboh. Pentadbir rangkaian akan mendapat satu mesej apabila berlakunya sebarang keraguan di dalam rangkaian. "*Honeypot"* ini juga akan menyimpan data dari penceroboh seperti *"IP Address", "MAC Address", "Time Attacked", "Local Port"* dan *"Remote Port"*. Sekiranya penceroboh memasuki *"Honeypot"*, pentadbir rangkaian akan mengetahui kelemahan rangkaiannya dan mencari penyelesian untuk meningkatkan kawalan pada masa hadapan. Dengan adanya *"Honeypot"* ini, ia akan dapat membantu pentadbir rangkaian dalam mengesan penceroboh dan mengetahui *"port"* yang digunakan. Untuk mambangunkan *"Honeypot"*, Microsoft Visual Basic 6.0 akan digunakan dalam membina antaramuka dan pengaturcaraan. Bagi menyimpan maklumat-maklumat penceroboh yang diperolehi, Microsoft Access 2003 akan digunakan sebagai pangkalan data. Dengan penghasilan *"Honeypot"* ini ia dapat digunakan pada masa hadapan dan secara meluas.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PC	-	Personal Computer
FTP	-	File Transfer Protocol
SMTP	-	Simple Mail Transfer Protocol
IP	-	Internet Protocol
IDS	-	Intrusion Detection System
MAC	-	Media Access Control
MX	-	Mail Exchange
DNS	-	Domain Name Service
NIC	-	Network Interface Card
UDP	-	User Datagram Protocol
TCP	-	Transmission Control Protocol
SDLC	-	System Development Life Cycle
LAN	-	Local Area Network
GUI	-	Graphical User Interface
RAID	-	Rapid Application Development
DAO	-	Data Access Object
RDO	-	Remote Data Object
ADO	-	ActiveX Data Object
VB	-	Visual Basic
KMC	-	Knowledge Management System
DNS	-	Domain Name System
CPU	-	Central Processing Unit

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

A honeypot is a security resource whose value lies in been probed, attacked, or compromised. That means, whatever administrator designate as a honeypot, it is our expectation and goal to have the system probed, attacked, and potentially exploited.

Honeypots do not help directly in increasing a computer network's security. On the contrary, they do attract attacker and can therefore attract some interest from the blackhat such as hackers, attacker community on the network, where the honeypot is located.

1.1 Problem Statement

As network and host-based security becomes more of an interest and concern for organizations, researchers and business people alike are looking for effective network security solutions. Therefore, the attacker try attack an unsecured network operating system. The attacker would have probably scanned a subnet with a tool such as *Nmap* to looking for open services and detect what operating systems individual machines were running on the scanned subnet. The attacker then tried to attempt the server or important network parts by using the port which is open and manipulate the whole of the network. This activity will cause that some of the host on the network unusable.

Currently the attackers almost exist in every network organization. They always try to hack server or other part of the network in order to get some confidential information about the organization or to break down the network. They will use scanning tool such as *Nmap* in order to discover vulnerabilities that able to help them to break into the server or other network part. Figure 1.1 shows how attackers use scanning tool to break into network.

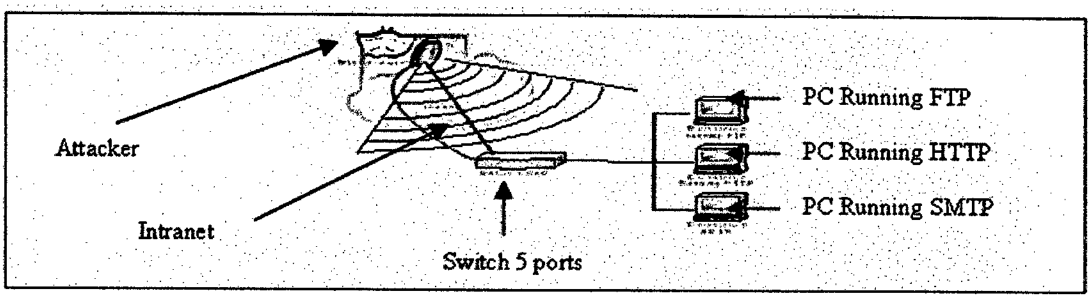


Figure 1.1: Attacker tries to attack the network by using scanning tool

As a network administrator, they need to know when and how the internal or external attacker attempt to break into the server and how to stop them. Therefore, to know that, honeypot will act as bait and log all the activities when they attempt to any Internet Protocol (IP), which bind with honeypot. After honeypot saved all the information about the attacker into database, it sends pop up message to the administrator to inform them. Figures 1.2 below shows how honeypot detect attacker.

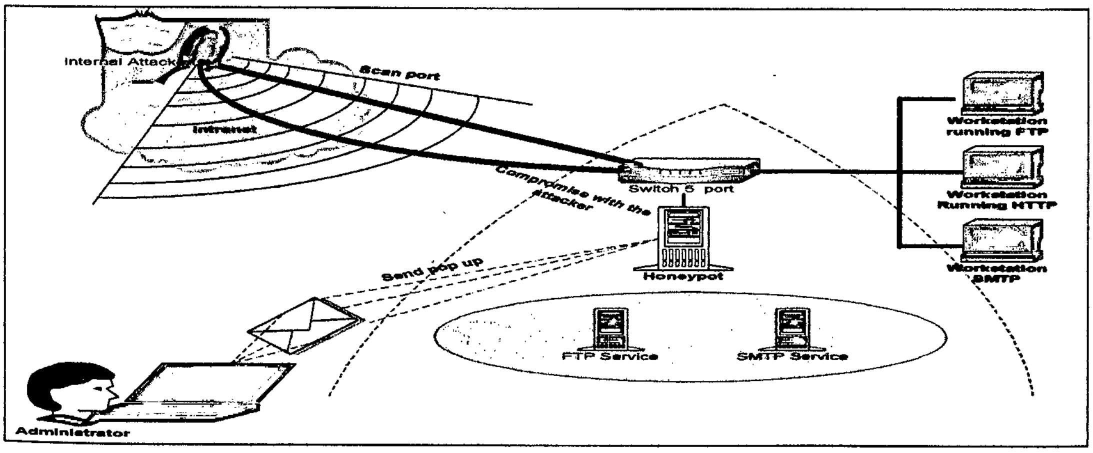


Figure 1.2: Using the honeypot to detect the attackers

1.2 Objectives of the System

The objective of this project covers for three (3) out on *Research Honeypot.* The objectives of the system are listed below:

(i) To simulate honeypot application.

(ii) To provide record of attacker activity when they break into honeypot computer.

(iii) To simulate FTP and SMTP application.

1.3 Scopes of the System

The scope of this project, it just focuses on *Research Honeypot* and the all capabilities of honeypots. This honeypot is base on High involvemet. Beside that, this project, it covers three (3) functions are describes below:

(i) Implement a specific service

Implement real specific service which are FTP and SMTP and make the attacker break into the target host on the network.

(ii) Detection

Detect the attacker when they break into the target host by implement specific service.

(iii) Notifiation

Notification is use to send pop up message to administrator.

Many honeypots simulate or implement service on well-known port that would be an interest to attacker. This project will touch on two (2) ports such as SMTP (25) and FTP (21). This honeypot is implemented in FSKKP Computer Laboratory by using Switch 5 port or wireless network.

CHAPTER 2

LITERATURE REVIEW

This chapter provides a general overview of hacking methodology. It also describes how honeypot detect an atacker and how many level honeypot that already exist on network security area. Honeypot are very helpful for administrator who want to know their network vulnerabilities.

2.1 Attacks

The explosive growth of the internet has brought many good things such as electronic commerce, collaborative computing, and e-mail and so on. With the growth of the internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the internet for electronic commerce, advertising, information distribution, and access, and other pursuits, but they are worried about the possibility of being attack. Therefore, the definition of the attacker and computer network attacks as below:

(i) Attacker

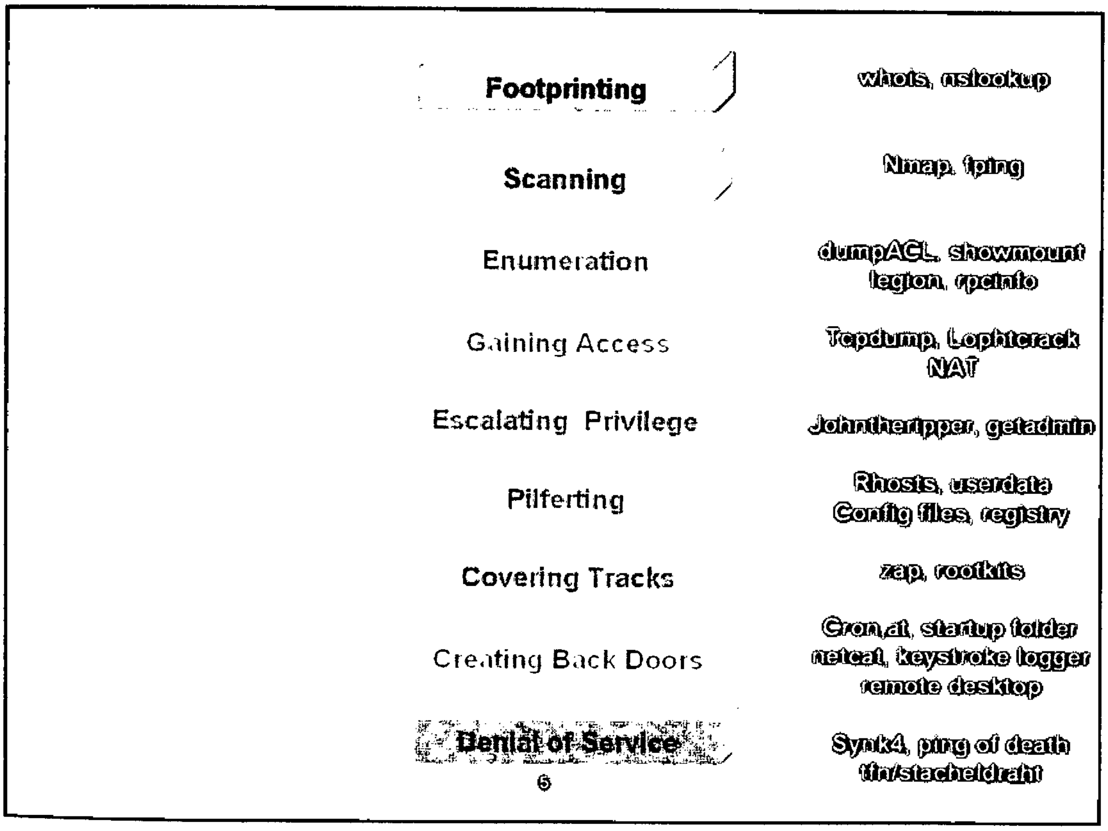
A person who enjoys learning the details of computer systems and how to stretch their capabilities as opposed to most users of computers, who prefer to learn only the minimum amount necessary. Refer Appendix C for more information.

(ii) Computer Network Attack

A computer network attack is any operation intended to disrupt, deny, degrade, or destroy information held in computers or computer networks. Refer Appendix C for more information.

2.2 Hacking Methodology

Figure 2.1 show about methodology that attacker always use in order to hack host on the network. Refer Appendix J for more information.



Footprinting	whois, nslookup
Scanning	Nmap, fping
Enumeration	dumpACL, showmount legion, rpcinfo
Gaining Access	Tcpdump, Lophtcrack NAT
Escalating Privilege	Johntheripper, getadmin
Pilferting	Rhosts, userdata Config files, registry
Covering Tracks	zap, rootkits
Creating Back Doors	Cron,at, startup folder netcat, keystroke logger remote desktop
Denial of Service	Synk4, ping of death tfn/stacheldraht

Figure 2.1: Hacking Methodology Steps

2.2.1 Footprinting

Footprinting is information gathering. It will find out target Internet Protocol (IP) address or phone number range. Network Topology visual Route. It is essential to a surgical attack. The key here is not to miss any details. Table 2.1show the technique and tool will be use in footprinting methodology. Refer Appendix J for more information.

Table 2.1: Footprinting Step

Techniques	Tools
Open Source Search	Google, search engine, Edgar
Find domain name, admin, IP addresses name servers	Whois (Network solution; arin)
DNS zone transfer	Whois (Network solution; arin)

2.2.2 Scanning

Scanning is a bulk target assessment. Which machine is up and what ports services are open. It focuses on most promising avenues of entry. To avoid being detect, these tools can reduce frequency of packet sending and randomize the ports or IP addresses to be scan in the sequence. Table 2.2 shows the technique and tool will be use in scanning methodology. Refer Appendix J for more information.

Table 2.2: Scanning Step

Techniques	Tools
Ping sweep	Fping, icmpenum,WS_Ping ProPack,Nmap
TCP/UDP port scan	Nmap,Superscan,Fscan
OS detection	Nmap,queso,Siphon

2.2.3 Enumeration

Identify valid user accounts or poorly protected resource shares. Most of the intruders like probing than scanning step. Table 2.3 shows the technique and tool will be use in enumeration methodology. Refer Appendix J for more information.

Table 2.3: Enumeration Step

Techniques	Tools
list user accounts	Null sessions,DumpACL,Sid2usre,onSiteAdmin
list file shares	Showmount,NAT,Legion
identify applications	Banner grabing with telnet or netcat, rpcinfo

2.2.4 Gaining Access

Based on the information gathered so far, make an informed attempted to access the target. Table 2.4 shows the technique and tool will be use in gaining access methodology. Refer Appendix J for more information.

Table 2.4: Gaining Access Step

Techniques	Tools
Password eavesdropping	Tcpdump/ssldump,L0phtcrack,readsmb
File share ,brute forcing	NAT,legion
Password ,File grab	Tftp,Pwddump2(NT)
Buffer,overflow	Ttdb, bind,IIS .HTR/ISM.DLL

2.2.5 Escalating Privilege

If only user level access has obtained in the last step, seek to gain complete control of the system. Table 2.5 shows the technique and tool will be use in escalating privilege methodology. Refer Appendix J for more information.

Table 2.5: Escalating Privilege Step

Techniques	Tools
Password cracking	John the ripper,L0phtcrack
Known Exploits	Lc_messages,Getadmin,sechole

2.2.6 Pilfering

Based on the information gathered so far, this step will gather info on identify mechanisms to allow access of trusted systems. Table 2.6 shows the technique and tool will be use in pilfering methodology. Refer Appendix J for more information.

Table 2.6: Pilfering Step

Techniques	Tools
Evaluate Trusts	RhostsLSA secrets
Search for clear text passwords	User data, Configuration filesRegistry

2.2.7 Covering Tracks

Once total ownership of the target has secured, hiding this fact from system administrators become paramount, less they quickly end the romp. Table 2.7 shows the technique and tool will be use in covering track methodology. Refer Appendix J for more information.

Table 2.7: Covering Tracks Step

Techniques	Tools
Clear Logs	Zap, Event Log GUI
Hide tools	Rootkits file streaming

2.2.8 Creating Back Door

Trap doors will lie in various parts of the system to ensure that privilege access is easily regained whenever the attacker decides. Table 2.8 shows the technique and tool will be use in creating back door methodology. Refer Appendix J for more information.

Table 2.8: Creating Back Doors Step

Techniques	Tools
Create rogue user accounts	Members of wheel, admin
Schedule batch jobs	Cron, AT
Infect startup files	rc, startup folder, registry keys
Plant remote control services	Netcat, remote.exeVNC, B02K remote desktop
Install monitoring mechanisms	Keystroke loggers, add acct. to secadmin mail aliases
Replace appls with Trojans	Login, fpnwcint.dll

2.2.9 Denials of service

If an attacker is unsuccessful in gaining access, they may use readily available exploit code to disable a target as a last result. Table 2.9 shows the technique and tool will be use in denials of service methodology. Refer Appendix J for more information.

Table 2.9: Denial of Services Step

Techniques	Tools
Syn flood	synk4
ICMP techniques	Ping to death smurf
Identical src/dst SYN requests	Land Latierra
Overlapping fragment/offset bugs	Netcat, remote.exe,VNC, B02K remote desktop
Out of bounds TCP options (OOB)	Keystroke loggers, add acct. to secadmin mail aliases
DDoS	Trinoo,TFN,stacheldraht

2.3 Types of Attack

(i) Unauthorized access

This simply means that people who should not use someone computer services are able to connect and use them. For example, people outside UTEC might try to connect to student host or to UTEC server. There are various ways to avoid this attack by carefully specifying who can gain access through these services.

(i) Exploitation of known weaknesses in programs

Some programs and network services are not originally designed with strong security in mind and are inherently vulnerable to attack. The best way to protect from this attack is to disable any vulnerable services or find alternatives. [2]

(ii) Denial of service

Denial of service attacks cause the service or program to stop functioning or prevent others from making use of the service or program. These may be performing at the network layer by sending malicious datagram that cause network connections to fail. They may also be performed at the application layer by using commands are given to a program that cause it to become extremely busy or stop functioning [2]. Preventing suspicious network traffic from reaching hosts in UTEC network area and preventing suspicious program commands and requests are the best ways of minimizing the risk of a denial of service attack.

(iii) Spoofing

This type of attack causes a host or application to mimic the actions of another. Typically, the attacker pretends to be an innocent host by following IP addresses in network packets. To protect against this type of attack, verify the authenticity of datagram and commands. Prevent datagram routing with invalid source addresses. [2]

(iv) Eavesdropping

This is the simplest type of attack. A host configured to listen to and capture data not belonging to it. Carefully written eavesdropping programs can take usernames and passwords from user login network connections. Broadcast networks like Ethernet are especially vulnerable to this type of attack. To protect against this type of threat, avoid use of broadcast network technologies and enforce the use of data encryption. [2]

(v) Port scans

Port scans are very noisy as they provoke a lot of network traffic. A properly configured Intrusion Detection System (IDS) or even firewall will trigger an alarm immediately when a port scan is started. This can be avoided if the port scan is done during a long period, therefore is spread over multiple days. Most IDS will not recognize this as a port scan and will not trigger an alarm. [2]

(vi) Finger

Finger is a daemon running on the target system, which does provide additional information about local users. This information can reveal some real identities or user settings like the used shell, last login as well as if there are some unread mails. Finger does not run on most systems, as it is a security threat, which reveals login names and other useful information for attacking a host. [2]

(vii) Active Fingerprinting

It can be useful to know what kind of operating system the attacker is using. For this purpose of a machine can be finger printed. By sending different packets with different flags and checking if a flag gets checked, deleted or skipped the running operating system can be guessed. Unfortunately, some packets are sent to the attacking host to get the according responses. The attacker could watch for these incoming packets and be warned. As with finger, port scans and active fingerprinting, the danger of being detected can be quite high and the results of these active information-gathering attempts are not that important or informative to justify the risk of being detected. [2]

2.4 Effects of Attack

There are four ways an attacker can cause harm an organization by attaining unauthorized access to their computer system. [3]

(i) Breach of confidentiality. When an attacker breaks into a system, he can freely go through all the files. This in turn makes the organization lose control over its own information. Confidential records can be read or stolen or illegal copies of software can be made.

(ii) Damage to information integrity. When there is damage to the integrity of information, the organization may lose credibility in the marketplace.

(iii) Breach of authenticity. Authenticity can be breached if attackers pick up the identity of users on the system they penetrate. Once a hacker has a new identity he can use it to do just about anything and not be held accountable.

(iv) Cut off availability. After gaining access to a computer network, an attacker can shut down any service that the organization may provide. For example, a hacker could shut down a Web site or a power grid.

2.5 Honeypot

Attacks on information systems and networks are becoming increasingly frequent and sophisticated. Moreover, traditional security measures are often unable to deal with the modern malicious acts. For this reason, a more advanced tool is needed to fight the evil. The solution, research honeypot is used as a primarily tool for detecting attacks.

A honeypot is a program, machine, or system that located on a network as bait for attackers [6]. The idea is to deceive the attacker by making the honeypot seem like a legitimate system. Honeypots was running services and open ports, services, which one might find on a typical machine on a network. These running services are meant to attract the attention of attackers so that they spend valuable time and resources try to exploit the machine while the attacker is being monitored and recorded by the honeypot. There are two (2) main types of honeypots where is:

(i) Research Honeypots
(ii) Production Honeypots

2.5.1 Research Honeypot

One (1) of the biggest issues facing today is that network organizations do not know who these attackers are. The techniques, tools, and methods employed by these attackers. The main purpose of the research honeypot is to collect information about attacker as much as possible. After collect information network administrator, will analysis that to determine what their network vulnerabilities. Honeynet is one (1) of the research honeypot. From this it give organizations the capabilities to learn more on their own.

2.5.2 Production Honeypot

The concept of production honeypots is to emulate specific service to make attackers spend time on the system. Production honeypot used for protect the real host in network from attacker. By using the production honeypot it will be generate a few alerts and send e-mail to administrator when attacker tries to compromise with it.

2.6 Concepts of Level of Involvement

One (1) characteristic of a honeypot is its level of involvement. The level of involvement does measure the degree an attacker can interact with the operating system. Figure 2.2 shows all level involvement of honeypot. Three (3) groups of involvement are listed below:

(i) Low-involvement
(ii) Mid-involvement
(iii) High-involvement

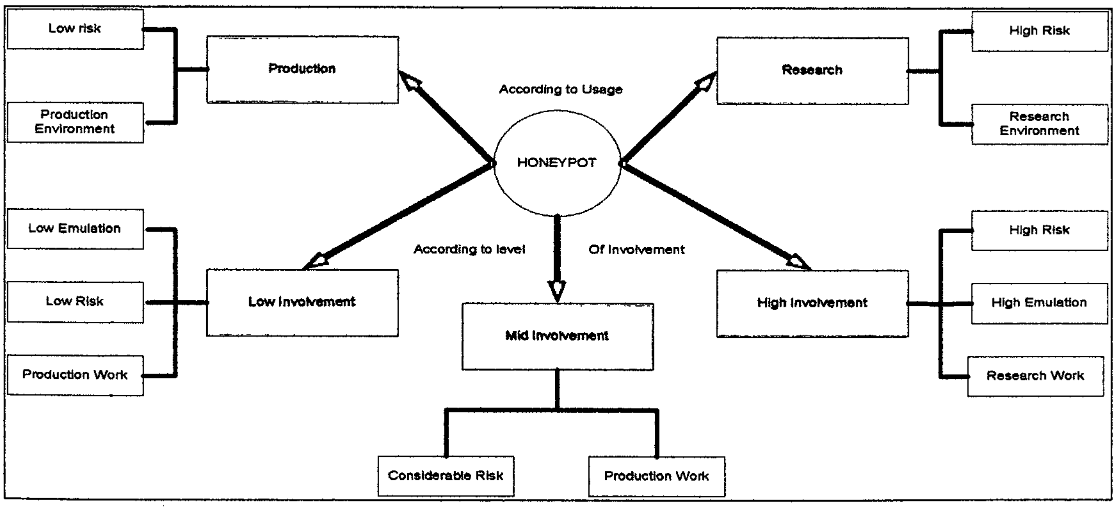


Figure 2.2: Classification of honeypots

2.6.1 Low-involvement

They are listening on a certain port for incoming connections. All packets logged by low involvement honeypot. No answer sent to the request. Low