**“A Research On Securing Data From Intruder Using Honey Pot”**

**ANAND KUMAR GUPTA**

***DIRECTORE K-TECH SOFTWARE TRAINIG AND CUNSULTANCY INDORE***

***ASSISTANT PROFESSOR COMPFEEDERS AISECT COLLEGE OF PROFESSION STUDIES RR CAT RAU ROAD INDORE***

**ABSTRACT**

A modern technology in the area of Intruder detection is Honey Pot technology that unlike common IDSs tends to provide the attacker with all the necessary resources needed for a successful attack. Honey Pots provide a platform for studying the methods and tools used by the intruders (black hat community), thus deriving their value from the unauthorized use of their resources. This paper discusses the design of a dynamic honey pot, which is an autonomous Honey Pot capable of adapting in a dynamic and constantly changing network environment. The dynamic Honey Pot approach integrates passive or active probing and virtual Honey Pot. This approach addresses the challenge of deploying and configuring virtual Honey Pots. Security in the enterprise has lately become the primary concern of both IT managers and other executives. The challenges of securing enterprise networks in the face of intruders armed with the tools of compromise have become overwhelming and are still growing. To improve their network security, organizations have sought solutions such as firewalls, Virtual Private Networks (VPNs), and intruder detection variants. All of these solutions, however, continue to leave proprietary data accessible to determined intruders. The Computer Security Institute/FBI *2003 Computer Crime and Security* *Survey* indicate that the total annual losses reported in the 2003 were $201,797,340 [1].

Moreover, many of the more advanced current network security solutions require a good deal of administration, with consistent needs for reconfiguration, management, and report analysis.

With security administrators supporting an every growing number of users, such consistent interaction with security mechanisms has become impractical. Therefore, today’s enterprise requires a security solution that will not only prevent the most advanced intruder, but will as well accomplish this with minimal configuration and supervision.

**INTRODUCTION**

As Small Data Sets: Honey pots only collect data when someone or something is interacting with them. Organizations that may log thousands of alerts a day with traditional technologies will only log a hundred alerts with honey pots. This makes the data honey pots collect much higher value, easier to manage and simpler to analyze.

As Reduced False Positives: One of the greatest challenges with most detection technologies is the generation of false positives or false alerts. The larger the probability that a security technology produces a false positive the less likely the technology will be deployed. Honey pots dramatically reduce false positives. Any activity with honey pots is by definition unauthorized, making it extremely efficient at detecting attacks.

As Catching False Negatives: Another challenge of traditional technologies is failing to detect unknown attacks. This is a critical difference between honey pots and traditional computer security technologies which rely upon known signatures or upon statistical detection. Signature-based security technologies by definition imply that "someone is going to get hurt" before the new attack is discovered and a signature is distributed.

Statistical detection also suffers from probabilistic failures - there is some non-zero probability that a new kind of attack is going to go undetected. Honey pots on the other hand can easily identify and capture new attacks against them. Any activity with the Honey Pot is an anomaly, making new or unseen attacks easily stand out.

As Encryption: It does not matter if an attack or malicious activity is encrypted, the Honey Pot will capture the activity. As more and more organizations adopt encryption within their environments this becomes a major issue. Honey pots can do this because the encrypted probes and attacks interact with the Honey Pot as an end point, where the activity is decrypted by the Honey Pot.

As IPv6: Honey pots work in any IP environment, regardless of the IP protocol, including IPv6. IPv6 is the new IP standard that many organizations, such as the Department of Defense, and many countries, such as Japan, are actively adopting. Many current technologies, such as firewalls or IDS sensors, cannot handle IPv6.

As Highly Flexible: Honey pots are extremely adaptable, with the ability to be used in a variety of environments, everything from a Social Security Number embedded into a database, to an entire network of computers designed to be broken into.

As Minimal Resources: Honey pots require minimal resources, even on the largest of networks. A simple, aging Pentium computer can monitor literally millions of IP addresses.

**OBJECTIVES**

The goal of the project is to implement a **Intrusion Detection Systems…**

* **Short Term Goal**

A short term goal is something to be accompolished in a short period of time.There is no specific length of time related to the definition of a short term goal. It is concerned with intermediate task.

Short term goal of our project can be considered as the successful implementation of various phases and sub-phases concerning with project and the milestones predefined.

* **Long Term Goal**

A long term goal is an achievement set to be reached over a long period of time. It would be appropriate to define a long term goal for this week, month, year, lifetime, etc. They are used in a variety of areas:

* + Financial
  + Educational

Long term goal of our project can be considered as a successful implementation of Dynamic Honey Pot Design for Intrusion Detection within the constraints of feasibility, reliability and maintainability.

**PURPOSE, SCOPE & APPLICAPABILITY**

**Purpose**

Intrusion detection is the process of monitoring computers or networks for unauthorized entrance or activity. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack. There are two basic types of intrusion detection: host-based (HIDS) and network based (NIDS). Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages.

**Scope**

Security in the enterprise has lately become the primary concern of both IT managers and other executives. The challenges of securing enterprise networks in the face of intruders armed with the tools of compromise have become overwhelming and are still growing. To improve their network security, organizations have sought solutions such as firewalls, Virtual Private Networks (VPNs), and intruder detection variants.

**Applicability**

the users within the organization are almost gifted with omnipotence when compared to an external entity for gaining knowledge of network construction. Much of the knowledge that an internal user can gather through social interaction and engineering will be *a priori* giving them significant advantage when attacking systems. As an example, they would know that the main routers and switches of a network are a particular model and type because they will have sighted this in their physical locale (typically most devices display their brand and

model visibly on the front panel). This type of internal intelligence gathering presents significant challenges for the composition of internally focused Honey Pot systems to effectively deceive and ensnare internal miscreants.

**NETWORK**

In the world of computers, **Networking** is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. A computer network is a group of interconnected computers. Networks may be classified according to a wide variety of characteristics. A computer network allows computers to communicate with each other and to share resources and information. The Advanced Research Projects Agency (ARPA) funded the design of the "Advanced Research Projects Agency Network" (ARPANET) for the United States Department of Defense. It was the first operational computer network in the world. Development of the network began in 1969, based on designs begun in the 1960s. Networking, routers, routing protocols, and networking over the public Internet have their specifications defined in documents called RFCs. Computer networking is sometimes considered a sub-discipline of telecommunications, computer science, information technology and/or computer engineering. Computer networks rely heavily upon the theoretical and practical application of these scientific and engineering disciplines. There are three types of networks. A computer network is any set of computers or devices connected to each other with the ability to exchange data. Networks are : LAN, MAN, WAN, KAN. All networks are interconnected to allow communication with a variety of different kinds of media, including twisted-pair copper wire cable, coaxial cable, optical fiber, power lines and various wireless technologies. The devices can be separated by a few meters (e.g. via Bluetooth) or nearly unlimited distances (e.g. via the interconnections of the Internet).

###### Types of Network

### **LAN - Local Area Network**

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.

### **WAN - Wide Area Network**

As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

### **Other Types of Area Networks**

While LAN and WAN are by far the most popular network types mentioned, you may also commonly see references to these others:

**Wireless Local Area Network** - a LAN based on Wi Fi wireless network technology

**Metropolitan Area Network** - a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.

**Campus Area Network** - a network spanning multiple LANs but smaller than a MAN, such as on a university or local business campus.

**Storage Area Network** - connects servers to data storage devices through a technology like Fiber Channel.

**System Area Network** - links high-performance computers with high-speed connections in a cluster configuration. Also known as Cluster Area Network.

**Networking devices**

## Repeaters

Repeaters are Internetworking devices which operate at the physical layer. It deals with signal reproduction and retransmission of data. A simple amplifier will amplify not only the signal but also any noise accompanying the signal. But a repeater strips the digital data & saves it. It then reconstructs and retransmits the signal. The new signal is an exact duplicate of the original transmitted signal, able to travel over the new network segment. A repeater does not incorporate any changes to, or even analysis of, the addressing or structure of the data associated with other layers (higher). It simply reconditions received data & passes it on.

#### Hubs

Hubs are nothing but multi port repeaters. Any signal received on one port gets retransmitted on the other ports of the Hub. In general hubs are stable devices that perform signal regeneration, packet forwarding, routing and other functions adequately. Some hubs even have a management module which has an added function of a network manager. Ethernet Hubs can also be used as repeaters which extend the segment length of the particular type of cable that is used The Hub should regenerate and retime the signals on its ports.

#### Switches

An Ethernet Switch provides dedicated bandwidth to every port connection. It improves performance through micro-segmentation – reducing the number of users per segment and so increasing the available bandwidth of the LAN for each user. Delay from input to output of a switch is very less when compared to Bridges. It achieves this by routing the data to the port that connects the Node whose address is in the destination address portion of the Ethernet packet. Using this address, the switch can send the packet to the desired destination port only. This results in reduced traffic on the other ports and higher total throughput.

#### Routers

Routers have access to information from all three lower OSI layers (Physical, Data Link & Network).Routers offer more functionality as compared to Bridges, in being to do, routing and management of traffic & filtering the data across the network. Routers send information using logical address information. Logical addresses are assigned normally as a logical segment is called as “segmentation. A specialized network device that determines the next network point to which a data packet is to be forwarded toward its destination. Works on OSI layer 3.Unlike a gateway, it cannot interface different protocols

#### Gateway

It is a device sitting at a network node for interfacing with another network that uses different protocols. Works on OSI layers 4 to 7.Gateway interconnects two or more sub networks that use different protocols above the network layer. Gateways can connect any network to any other network. They provide full range of functionality from bit handling at the physical level up through framing, error detection routing, flow control, etc.

**Networking Topologies**

**Ring**

In this LAN, each computer is connected to the network in a closed loop or ring. Each machine computer has a unique address that is used for identification purposes. The signal passes through each machine or computer connected to the ring in one direction. Ring topologies typically utilize a token passing scheme, used to control access to the network. By utilizing this scheme, only one machine can transmit on the network at a time.

**Mesh**

The type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-point link this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

**Star**

In this topology, each machine is connected to a central hub. The star topology allows each machine on the network to have a point to point connection to the central hub. All of the traffic which transverses the network passes through the central hub. The hub acts as a signal booster or repeater which in turn allows the signal to travel greater distances. As a result of which each machine is connected directly to the hub. An advantage of this is the simplicity of adding other machines. The primary disadvantage of this is the hub is a single point of failure.

## Bus

In this topology, each computer or server is connected to the single bus cable through some kind of connector. A terminator is required at each end of the bus cable to prevent the signal from bouncing back and forth on the bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the MAC address or IP address on the network that is the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data.

## Tree/Hierarchical network

In this topology a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy.

Security in the enterprise has lately become the primary concern of both IT managers and other executives. The challenges of securing enterprise networks in the face of intruders armed with the tools of compromise have become overwhelming and are still growing. To improve their network security, organizations have sought solutions such as firewalls, Virtual Private Networks (VPNs), and intruder detection variants. All of these solutions, however, continue to leave proprietary data accessible to determined intruders. The Computer Security Institute/FBI *2003 Computer Crime and Security Survey* indicate that the total annual losses reported in the 2003 were $201,797,340.

Moreover, many of the more advanced current network security solutions require a good deal of administration, with consistent needs for reconfiguration, management, and report analysis. With security administrators supporting an ever growing number of users, such consistent interaction with security mechanisms has become impractical. Therefore, today’s enterprise requires a security solution that will not only prevent the most advanced intruder, but will as well accomplish this with minimal configuration and supervision.

Honey Pot is an exciting new technology with enormous potential for the security community. It is resource which is intended to be attacked and compromised to gain more information about the attacker and his attack techniques. The most of the attacks by a hacker would like to attack on the database concerning the username, the password and their respective account numbers. After acquisition of the same the hackers would very conveniently trespass the security walls of authentication and authorization and thereby making the transaction official.

The primary goal of computer security is to defend computers against attacks launched by malicious users. They are a number of ways in which researchers and developers can work to protect the software that they write. Some are proactive, like code reviews and regression testing, while others are reactive, like the pwn2own contest where new vulnerabilities are used to exploit browsers. Some tools can take on aspects of both; one class of these tools is Honey Pots.

A Honey Pot is a computer which has been configured to some extent to seem normal to an attacker, but actually logs and observes what the attacker does. Thanks to these modifications, accurate information about various types of attacks can be recorded. The term Honey Pot was first presented by Lance Spitzner in 1999 in a paper titled To Build a Honey Pot.

Honey Pots are unique because they allow a security researcher to see and record what actions a malicious user takes on a compromised computer without necessarily interfering or revealing to the attacker that they are being monitored. Because of this invisibility, valuable intelligence can be gathered about the actual strategies of an attacker. A Honey Pot can be configured to be either proactive or reactive to attacks, depending on the needs of the person who set it up.

**PROBLEM STATEMENT**

The most of the attacks by a hacker would like to attack on the database concerning the username, the password and their respective account numbers. After acquisition of the same the hackers would very conveniently trespass the security walls of authentication and authorization and thereby making the transaction official.

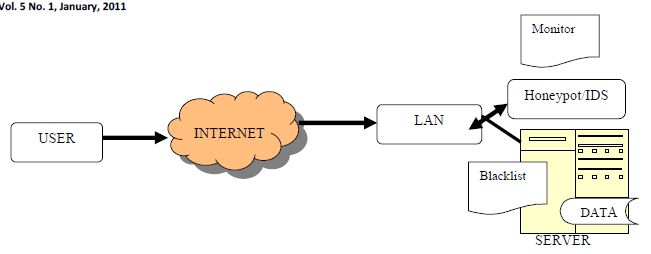
As it is necessary to maintain the security of a system or network where confidential data is processing, the data which should be remain confidential, there was a need for an intrusion detection system which not only protects the network from intruders but also gathers information about the attacker like the place from where he is trying to intrude the network, type of activities in which the intruder is interested, a system which provides the information of methods and tools used by the intruders (blackhat community), thus deriving their value from the unauthorized use of their resources. A number of intrusion detection systems are available which can prevent the intrusions but they do not provide the purpose behind the attack, the methods used by the attacker etc.

**PROPOSED SOLUTION**

To divert the attention of the attacker from the real network in a way that the actual information resources are not compromised. To build attackers profiles in order to identify their preferred attack methods. Criminal profiles, therefore, can be used by law enforcement, in order to be punished or to sue.

Intrusion detection is the process of monitoring computers or networks for unauthorized entrance or activity. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack. There are two basic types of intrusion detection: host-based (HIDS) and network based (NIDS). Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages. The users within the organization are almost gifted with omnipotence when compared to an external entity for gaining knowledge of network construction. Much of the knowledge that an internal user can gather through social interaction and engineering will be *a priori* giving them significant advantage when attacking systems. As an example, they would know that the main routers and switches of a network are a particular model and type because they will have sighted this in their physical locale (typically most devices display their brand and model visibly on the front panel). This type of internal intelligence gathering presents significant challenges for the composition of internally focused Honey Pot systems to effectively deceive and ensnare internal miscreants.

**ARCHITECTURE USED**



The proposed system architecture using Honey Pot as IDS to protect a network. The users or attacker will access the network either Internet or direct. Within a LAN, IDS with Honey Pot and a centralized server with database layers as described above are being connected. Once the user will access the network, all its interactions low or high will be monitored by the IDS and make a log file for that user. IDS will decide to make a user as blacklisted or not, also server’s data will be checked for integrity and identify the source of the user. Database layers also are checked for integrity by the system. Our proposed system for banking system, which will divide internal database into three layers, first, the public database, which will have all the information for the public to view like new policies or schemes by the bank or some new promotion stunt for e.g. some added bonuses or credits for making a current or saving account with them in some specific time. The point being the data which helps bring business more than nuisance will be placed in the public database. Second layer will be the main database, which will be real data of various users for the system, like the database for the list of account holders or for that sake the policies that are on their way to the market but still not disclosed due to assent of some senior authorities or due to some current market conditions. The third layer is the dummy database, which holds the information having no relevance to the real life world. This data will be automatically generated by the system by shuffling of the existing system. This is the data that the system will offer to the attacker and it is to this that we propose to set our eyes on to monitor the attack. With respect to above three layers of database, we have four modules in our system are described below.

3.1.1 Port Scanner: In this module, scanning of the open ports of the system is made. Open ports are the easiest and most convenient method of attacking. This module can work easily well if we were to increase the number of servers for effective handling the ever growing needs for performance and the originally assumed server will be able to check the open ports on the new server without actually deploying the entire software on the new machine. The proposed algorithm is:

Step 1: Start with the UI for port Scanner.

Step 2: Enter IP Address of the Server.

Step 3: Enter the range of port numbers required to be scanned on the server machine.

Step 4: Click on “Start”.

Step 5: If port is available for use then display the port number on the interface,

Else exit.

3.1.2 Attack Finder: In this module, in which actually blacklisting of the IP address of the attacker is made. The input being the server address and the port to be monitored there will be constantly monitoring the open ports and if in case there are any probability for any malicious activities and there is a constant request from the same particular IP then it will be blacklisted. We have assumed a threshold of 60 requests but it can be very easily altered according to the requirements of the hour.

The proposed Algorithm is:

Step 1: Enter IP address and port number of the client

Step 2: Add to watcher list.

Step 3: Monitor the number of requests or packets sent.

Step 4: If number of requests less than limit specified by server then

Step 5: Disconnect client from server.

3.1.3. System File Watcher: In this module, a constant watch on the files having the dummy data stored in it is made. To the outside world, the data will be seeming and correct but actually it is not. The system file watcher will continuously monitor the files and as soon as there are changes in the content of the file it will be alerting the administrator with a pop up message as to which file and when the file has been modified.

The Proposed Algorithm is:

Step 1: Specify the path of the file which needs to be watched by clicking on.

Step 2: Add the file to the watch list by clicking on “Add to Watcher”.

Step 3: Click on “Start” to start monitoring any modifications being made

Step 4: If any modification is made to the file, it is reported on the UI specifying the date and time along with the file being modified.

Step 5: Click on “Stop” to stop monitoring the file.

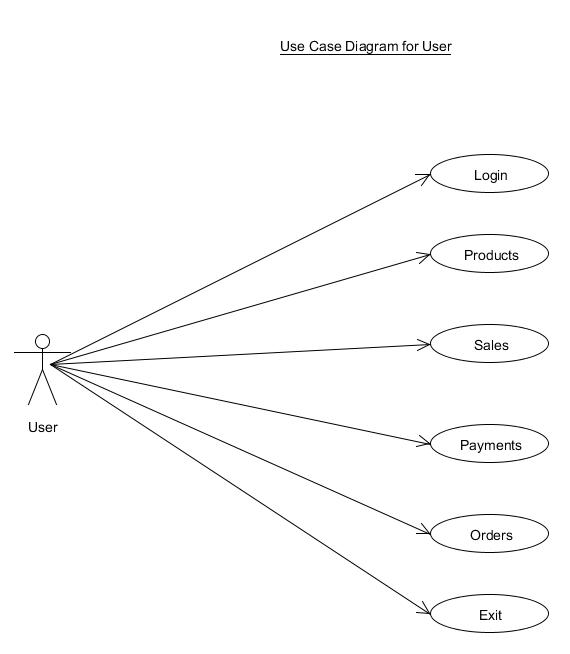
**EXISTING SYSTEM**

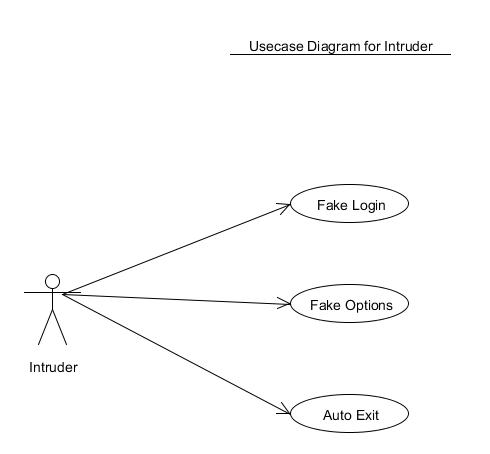
There are no such existing systems and the work on Honey Pots may take a little bit longer to surface but there have been some serious attempts to deploy the most from the concept and the finest example to it may be the new honey monkeys that Microsoft are coming up with the most of the attacks by a hacker would like to attack on the database concerning the username, the password and their respective account numbers. After acquisition of the same the hackers would very conveniently trespass the security walls of authentication and authorization and thereby making the transaction official.2.1 pitfalls in the current architecture

2.1.1 There is the risk of detection: once the true identity of a honey pot has been identified, its value is dramatically reduced. Attackers can ignore or bypass the honey pot, 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 honey pot, misleading the data analysis.

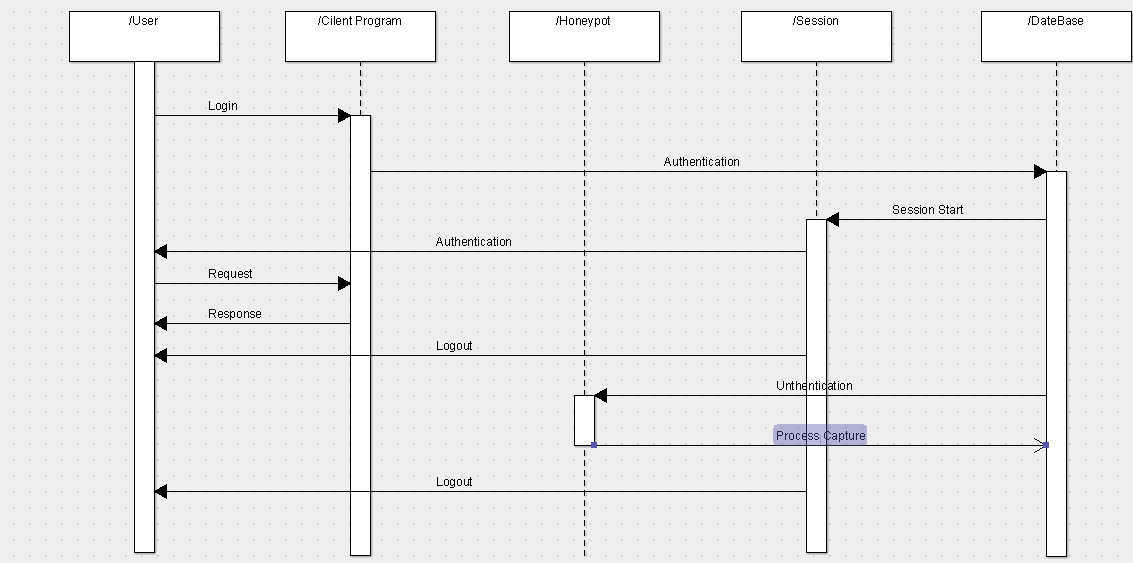
2.1.2 There is the risk of disabling honey pot functionality: this could be an attack against either data control or data capture routines. Attackers may want to not only detect a honey pot's identity, but disable its data control or data capture capabilities, potentially without the honey pot administrator knowing that functionality has been disabled. For example, an attacker may gain access to a honey pot within the honey net, and then disable data capture functionality on the honey pot. The attacker could then feed the honey pot with bogus activity, making administrators think data capture is still functioning and recording activity, when it’s not. Having multiple layers of data control and data capture helps mitigate this risk, as there is no single point of failure.

**Use Case diagram**

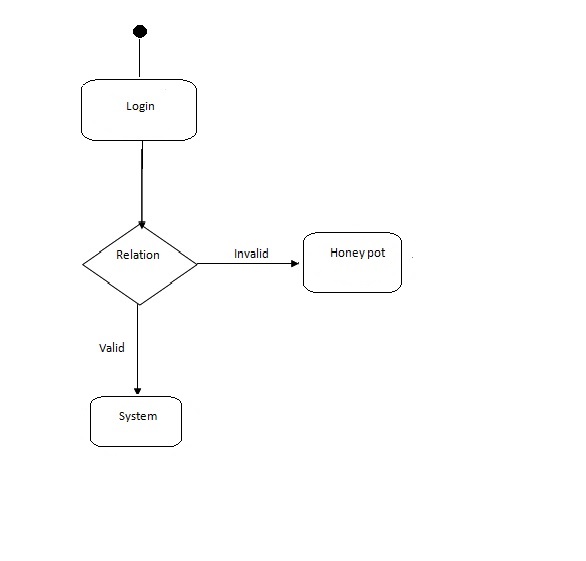
****

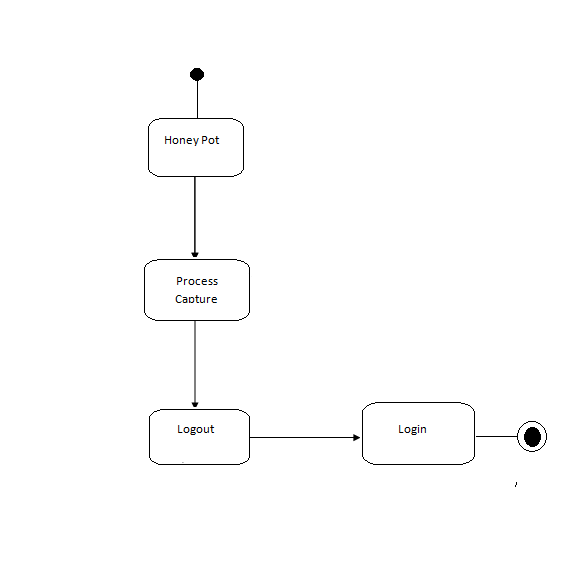
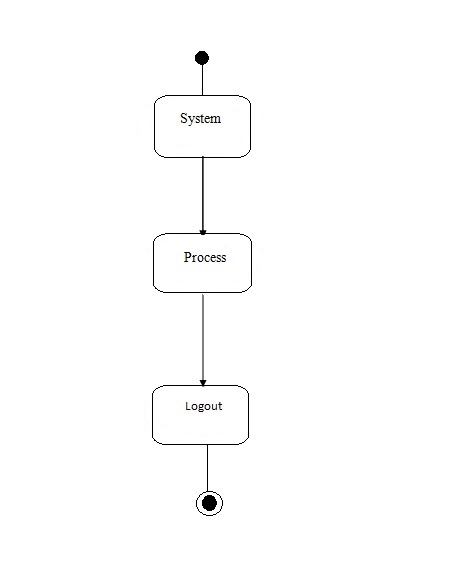
****

**Sequence diagram**



**3.2.5 Activity Diagram**

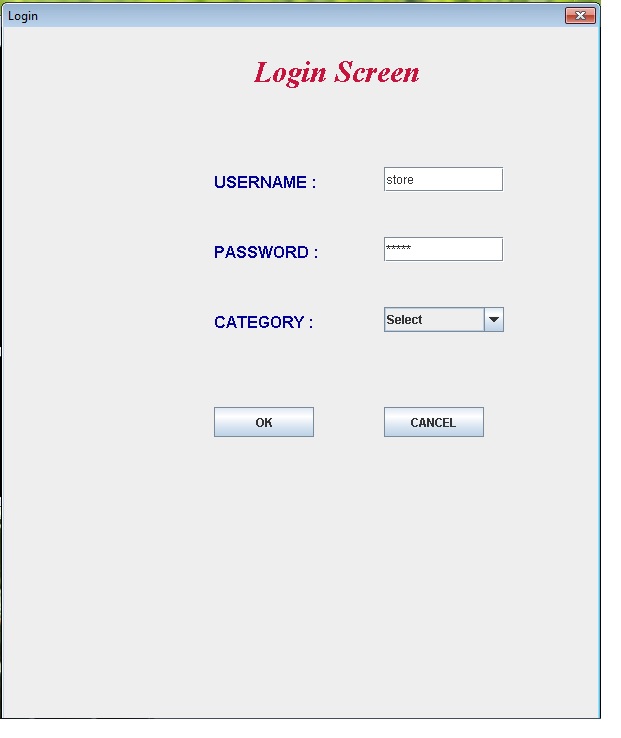


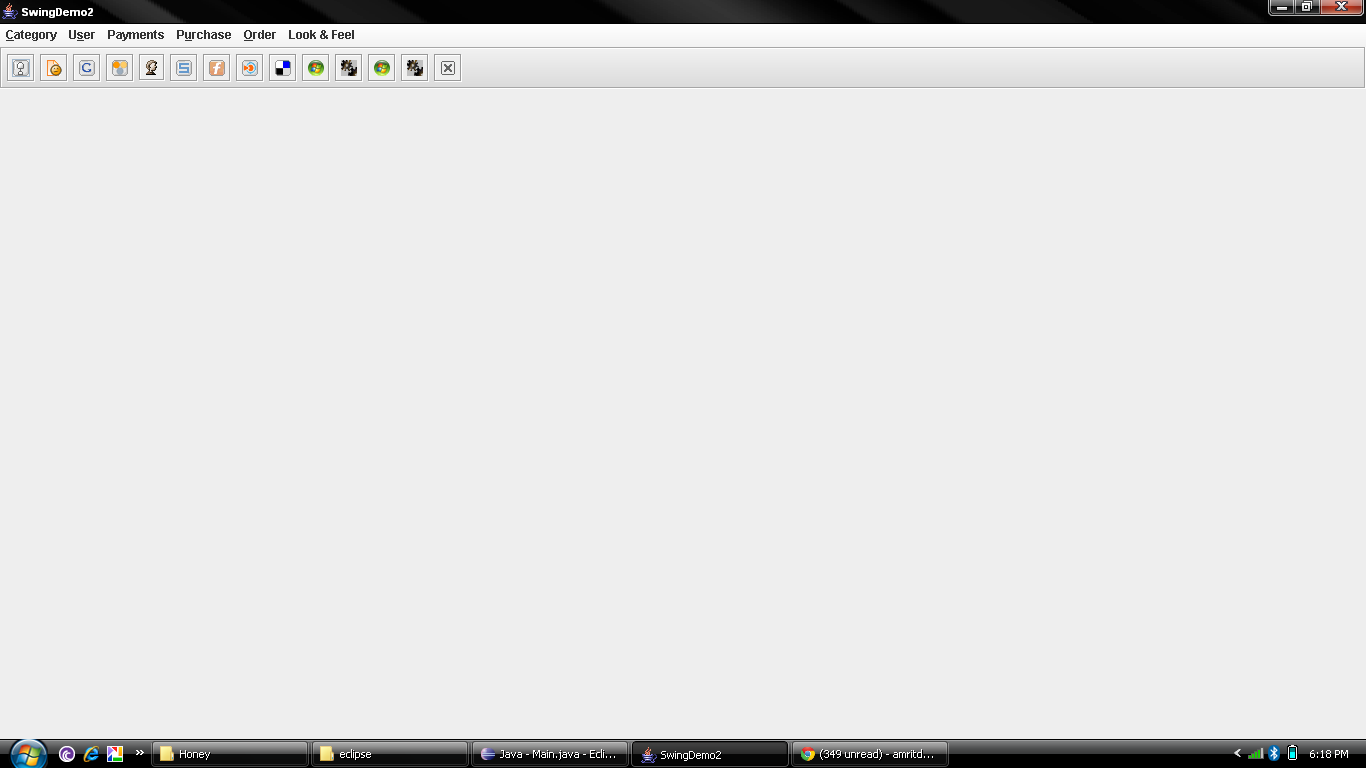
**RESULT**

This paper has given an in depth knowledge about Honey Pots and their contributions to the security community. A Honey Pot is just a tool. How one uses this tool is upto them.  
Honey Pots are in their infancy and new ideas and technologies will surface in the next time. At the same time as Honey Pots are getting more advanced, hackers will also develop methods to detect such systems. A regular arms race could start between the good guys and the blackhat community.

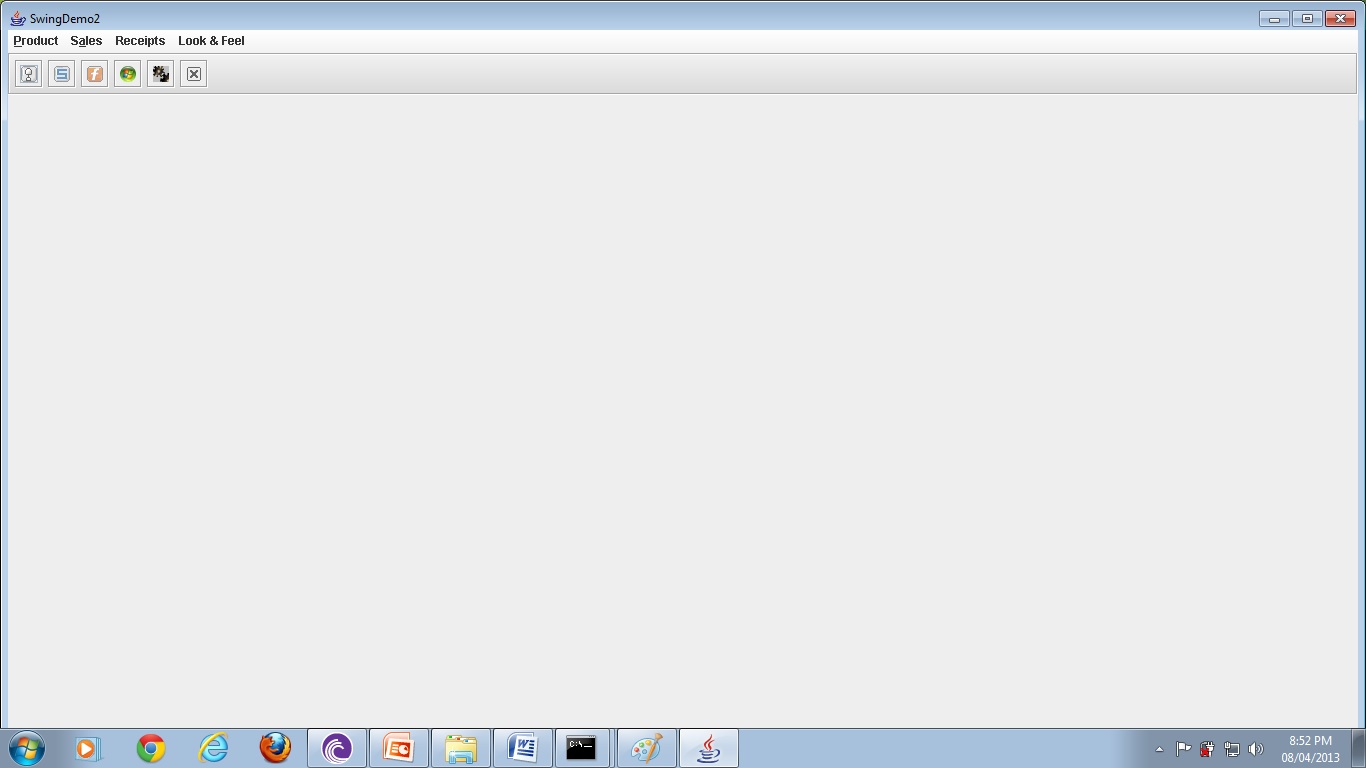
Honey Pots are an emerging technology, with extensive potential. They have tremendous advantages that can be applied to a variety of different environments. They dramatically reduce false positives, while providing an extremely flexible tool that is easy to customize for different. Traditionally, Honey Pots have been applied against external threats or common internal threats. By combining the capabilities of honey tokens and Honey nets, Honey Pots contribute to the early indication and confirmation of advanced insider threats. The research in this area is still in the early stages, with the intent of greater testing and development in the future.



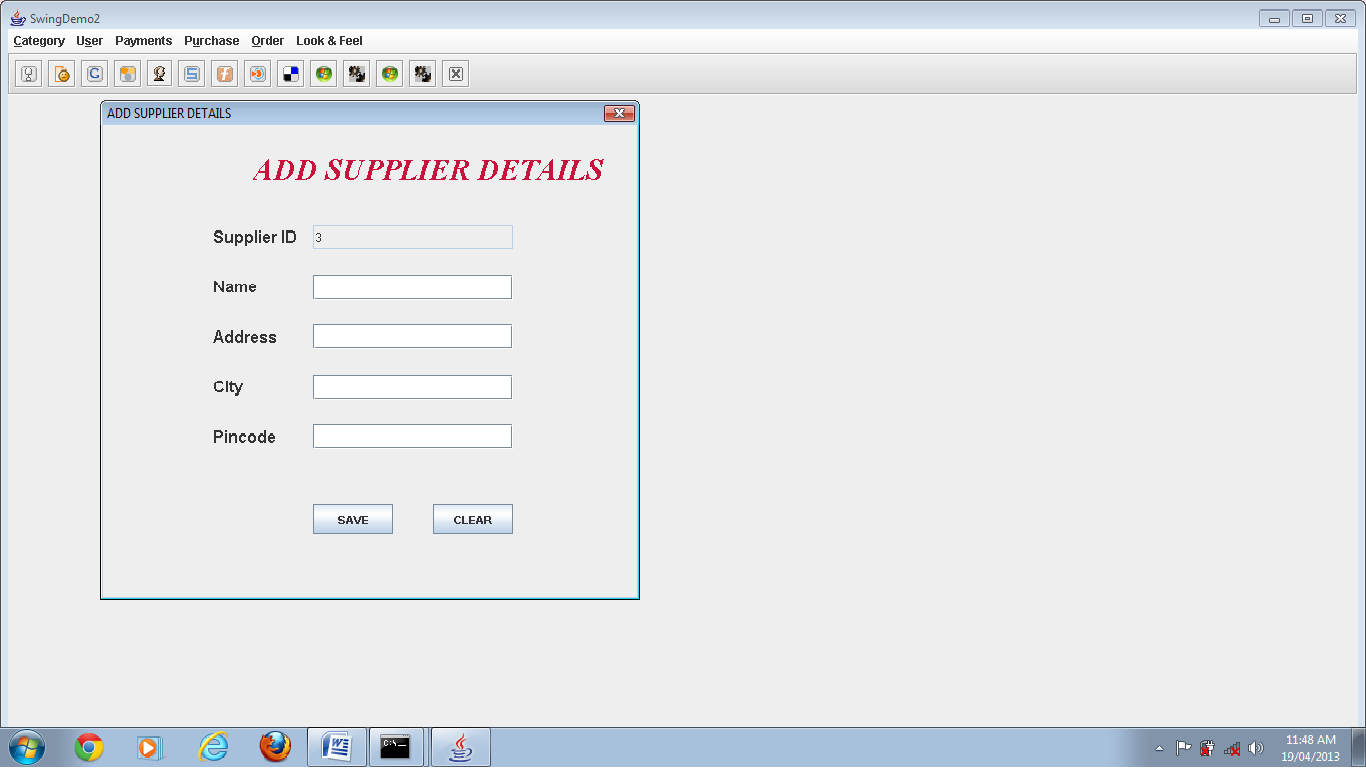
**LOGIN SCREEN**

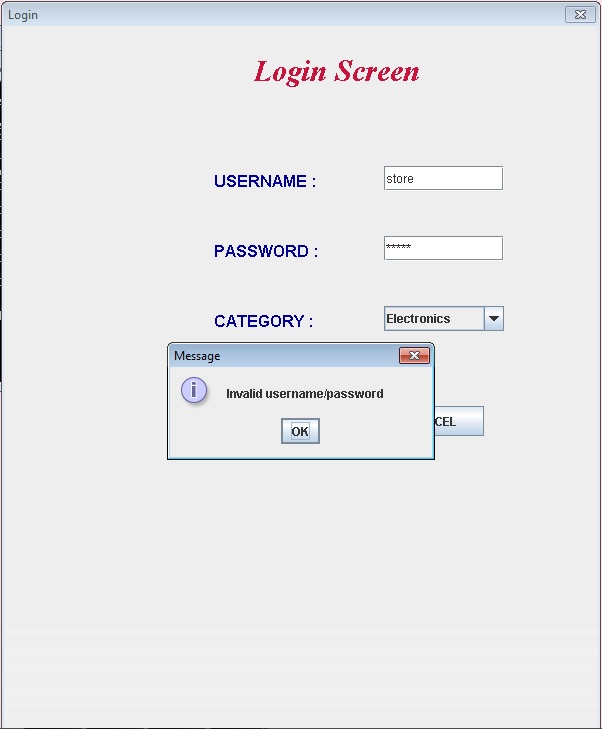


**ADMIN SCREEN**

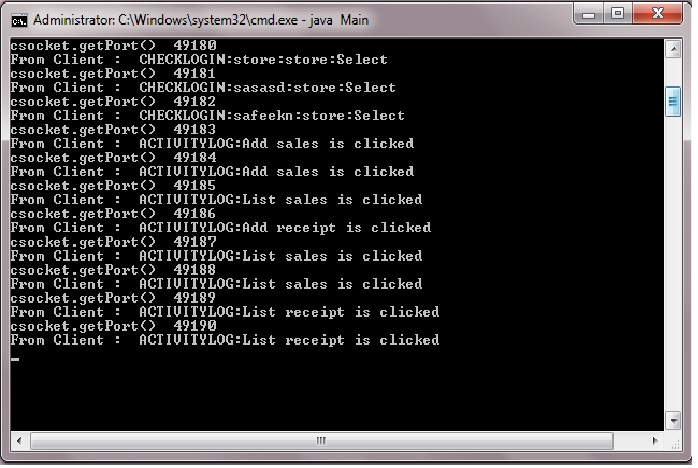


**USER SCREEN**

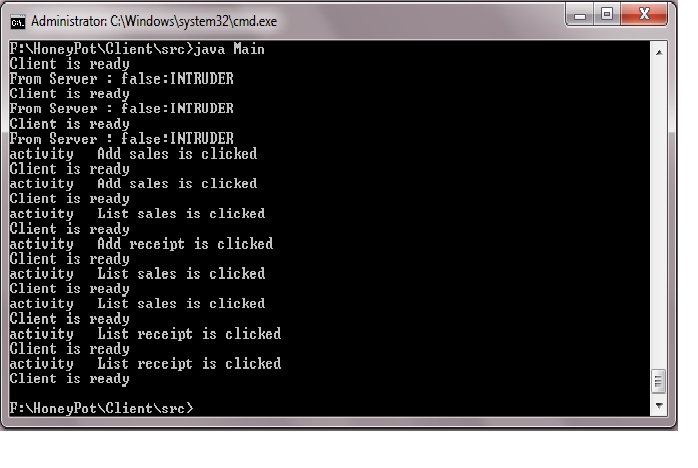
****

**ADMINSCREEN**  
  
**LOGIN SCREEN OF INTRUDER**

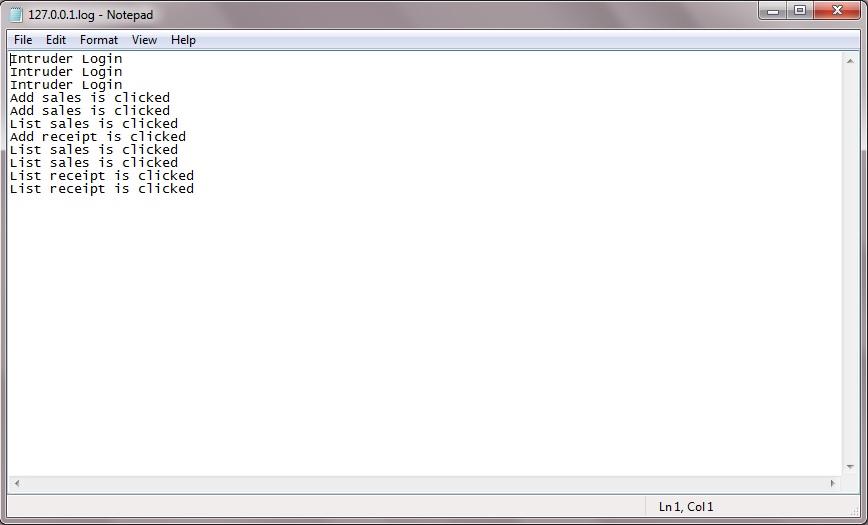
**INTRUDER SCREEN**

****

**SERVER SITE**

****

**CLIENT SITE**

****

**CAPTURED FILE**

**CONCLUSION**

The purpose of this topic was to define what Honey Pots are and their value to the security community.

Limitations of the Research:

Like any technology, Honey Pots also have their weaknesses. It is because of this they do not replace any current technology, but work with existing technologies.

* Limited View: Honey Pots can only track and capture activity that directly interacts with them. Honey Pots will not capture attacks against other systems, unless the attacker or threat interacts with the Honey Pots also.
* Honey Pots are no different, they have risk also. Specifically, Honey Pots have the risk of being taken over by the bad guy and being used to harm other systems. Depending on the type of Honey Pot, it can have no more risk then an IDS sensor, while some Honey Pots have a great deal of risk.

**Future Enhancements**

Honey Pots can be used for production purposes by preventing, detecting, or responding to attacks. Honey Pots can also be used for research, gathering information on threats so we can better understand and defend against them.

**References and Bibliography**

1. Lanz Spitzner, “Know Your Enemy: Learningwith User-Mode Linux Building Virutal

Honeynets using UML”[4] Lanz Spitzner, “Know Your Enemy: GenII Honeynets,” <http://www.honeynet.org,May,2005>..

With the help of this research paper i got concept of Honey Pot and Introduction of Honey Pot, as well as i knew working of Honey Pot and its architecture.

1. http://www.seminarprojects.com/ThreadHoney Pots-seminar-report#ixzz1YOSPf8Ka

Cormac Herley and Dinei Florencio, “Protecting Financial Institutions from Brute-Force Attack.

With the help of this link we are improve our designing phase.

1. <http://www.networkcomputing.com/1217/1217f2.html>.

With the help of this web site we got the information of networking and how to use this project for IP tracing and working of Ip. what is IP?

1. <http://project.honeynet.org>.

In this web reference we got the detail of Tools for tracing a IP.and how to trace IP using tools

1. <http://www.keyfocus.net/kfsensor/overview.php>

Using this url we got a information of attacks. How to attack on websites and how to busy any server at hacking time and how to trace a hacked account. How to store the information of intruder. Using this web reference we knew about hacking system. How to hack account and its techniques.

**Books:**

* Know Your Enemy: Honeynets
* “Honey pots - Definitions and Value of Honey pots”
* Reto Baumann, Christian Plattner “White Paper Honey Pots” 2002.