Honeypot security system : An efficient approach of securing E-Banking network

Mrs. Sonali Nemade
Dr. D.Y. Patil A.C.S. College, Pimpri

Mrs. Madhuri.A. Darekar
Dr. D.Y. Patil A.C.S. College, Pimpri

Mrs. Jyoti Bachhav
Dr. D.Y. Patil A.C.S. College, Pimpri

ABSTRACT
In today’s world many people are interacting with internet for online shopping, paying utility bill, online money transaction etc. While doing this activity they are not familiar with the security services which has been implemente . They are not aware about risk factor of being affected by the malicious software. From personal and business point of view it is one of the difficult tasks to protect their data from the threats. Firewall, Intrusion Detection System (IDS), and Honeypot are some of the security services available in the market. In this paper, we discuss a secure system for banking application using honey pots.

KEYWORDS: Honeypot, Information Security and Attacks.

INTRODUCTION
Honeypot is a computer system which can be defined as a fixed system but looks like a real system. Its goal is to attract hackers to fall into it to watch and follow their behaviour. In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

Classification of Honeypots:

![Architecture of HoneyPot Security System](image_url)
Low-interaction Honeypots

They are designed to emulate certain services and its operating systems has limited interaction through users. Such as, an emulated FTP service listening on a particular port may only emulate an FTP login, or support a various FTP commands.

Low-interaction honeypots are simple and easy to deploy and maintain. It reduces the potential risks. Low-interaction honeypots obtain limited information and it is possible that experienced attackers will easily recognise a honeypot. They are easy to deploy and maintain

Medium-interaction honeypot

A medium-interaction honeypot only implement the HTTP protocol, such as Apache.

High-interaction Honeypots

High-interaction honeypots are more complex. In this honey it involve real operating systems and applications. For example, a FTP server will be built. FTP server or services collect the information about attacks. Attackers real systems to interact with, no restrictions are imposed on attack behaviour. It is possible that attackers might take over a high-interaction honeypot system and use it as a stepping-stone to attack other systems within the organisation. Therefore, sufficient protection measures need to be implemented accordingly. The network connection to the honeypot may need to be disconnected to prevent attackers from further penetrating the network and machines beyond the honeypot system itself.

Production Honeypots

Production honeypots are easy to use. It capture only limited information, and are used primarily by companies. Production honeypots are present in the production network with other production servers by an organization because to improve their overall state of security. Production honeypots are low-interaction honeypots. It is easier to deploy. It is requires less information about the attacks or attackers than research honeypots is used. It emulate specific services and operating systems to invite attackers. It is to copy real production systems and resource attacking them as opposed to the production or critical systems and it provide the way they exploit vulnerabilities in production environment. They can also emulate different backdoors, viruses and trojans to attrack the attackers. The other very interesting part of production honeypots is that, they can be very well deployed internally to find out the internal loopholes and attackers within. For an example to examine attacks on web servers a production honeypot emulating the Web server and fake services can be deployed.

Research honeypots

Research honeypots is very complex to deploy and maintain. It is to gather information about the motives and tactics of the Black hat community targeting different networks. Research honeypots do not add direct value to a specific organization and instead of, they are used to research the threats that organizations face. It is to learn how to better protect against those threats. It is used to capture extensive information, and is used primarily by research, military, or government organizations. This intelligence gathering is one of the most unique and exciting characteristics of honeypots. Also, research honeypots are excellent tools for capturing automated attacks, such as auto-rooters or Worms. Since these attacks target entire network blocks, research honeypots can quickly capture these attacks for analysis. Honeypots can add value in research by giving us a platform to study the threat. What better way to learn about the bad guys then to watch them in action, to record step-by-step as the attack and compromise a system. Of even more value is watching what they do after they provide a system, such as communicating with other black hats or uploading a new tool kit.
WORKING OF HONEYPOT

Honeypot system works on the traffic coming to the Honeypot system when it is suspicious. It looks like real server but the only difference between Honeypot system and real server is the location of the machine related to the real server. This means real server is hidden or invisible to the attackers. Honeypot system are generally devised to monitor the activity of an attackers or intruders, save log files, and records events such as processes started, compiles, file adds, deletes and changes. This data is used to measure the skill level of the attackers, their intention and even their identity. By gathering such information Honeypot system improves the overall security system of the corporation. If sufficient information is gathered it may be used to prosecute in serious condition.

Fig: Flowchart of Honeypot security system

There are three layers to gather the information of intruder which includes:

1) Login Test:
   This step includes the login test and IP address tracing. Once person login into the system first of all IP address is noted down. If you fails to login for couple of times you will be entered into the fake system. In Honeypot security systems which are present currently there will be denial of service if a person fails to login for defined iterations.

![](login.png)

2) Psychometric test:
   In this test to detect that is the person a regular and customer or a hacker hacking other person’s account. It is provided set of questions which will be asked to the person. The answers to the questions will be known to the original user only. If the person fails to answer the questions more than two times then he will be transferred into the fake system.
3) **Captcha image:**

Captcha image is used to check whether the logged person is a person or machine. Many times it is possible that a person can use software to perform iterations and will get the password. If the password is 6 letters long then there will be 6 loops and by the combination he can get the password.

---

**The main roles of honeypot**

This part describes the main 3 roles of honeypot in the production systems.

1 **Prevention:**

The honeypot actually works as the trap for intruders. It has 2 different levels of working. The first is the prevention based on the knowledge of intruder. If the intruder detects, that this system is only the honeypot, the intruder might leave this system, because the honeypot might report the unwanted behaviour and the security system starts defence routines. The second is the trap for potential intruders. The honeypot must be the attractive target for the attacker. The both of these levels help improve the infrastructure security.

2 **Detection:**

The basic role of each honeypot is a detection. If the prevention role is failed, the most important operation is the detection of intruder. These detection routines contain method for: detection of malware and other intruders, collection of information about the attack and its source.

3 **Reaction:**

At the end of honeypot security system is the reaction phase. In this reaction phase when the attacker breaks the production system security and might provide the real server. In this case honeypot is the 1:1 copy of the production server. The difference is only in contained data. The honeypot does not contain the real data. It has only the collection of blank information. The system might be stopped and send to the forensic analyse every time. The honeypot contain the attack vendor and there were be information about attacker source address and its way back.
COMPARISON BETWEEN FIREWALL, IDS AND HONEYPOT:

<table>
<thead>
<tr>
<th>HoneyPot</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>- It attracts the hacker to attack the system</td>
<td>- It keep the attackers out of the network</td>
</tr>
<tr>
<td>- The logs are only due to non-productive Systems</td>
<td>- Log activities and logs also contain events related to production systems</td>
</tr>
<tr>
<td>- Log contains 5-10 entries.</td>
<td>- Log contains 1000 entries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HoneyPot</th>
<th>IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- It requires less amount of data</td>
<td>- It requires large amount of data</td>
</tr>
<tr>
<td>- Honeypots are designed to capture all known and unknown attacks directed against them</td>
<td>- signature matching or statistical models to identify attacks. This means that unknown or novel threats may not be detected.</td>
</tr>
</tbody>
</table>

CASE STUDIES

The detection of production honeypot cases in corporate sector is difficult task. Many commercial or financial organizations internally handle honeypot information system. Even though honeypots are not production systems, they still present potential vulnerabilities that could happen on ‘live’ systems. This type of information may demoralize customers who do not understand the purpose of the honeypot system.

**Case Study 1**

Honeypots were deployed in corporate sector which contains around 6000 total computers including servers and workstations and 300 custom. In this sector each honeypot was considered as a normal server and it was not specially named nor publicized. This honeypot was monitored regularly by the staff for the hits. It was discovered honeypot had approximate 300 hits per week. Monitored staffs have given the observation that 80 % hits were accidental and 20 % hits were deliberate. It was also observed that most of the deliberate hits were commenced with the intention to look for critical applications, files or individuals who wanted to exceed the authority assigned to them. To reduce the problem of hits the corporation had to take a decision to set up central honeypot monitoring machine.

**Case Study 2**

Some of the Security Staff of one of the corporations investigated Yahoo stock bulletin board. Investigation includes confidential posting or inaccurate information which appeared to be malicious. To identify the attackers, they created the web site which gave some offers. This offers includes greeting card which was sent with the yahoo identity messages. This web site implements question-and-answer mechanisms and technical mechanism which helped the staff to know about the individual identity. The individual did not "bite" and the staff shut down the site after a three-week wait.

**Case Study 3**

Vulnerabilities in Web browsers might allow malicious Web pages to install malware into the system. Now a day’s exploited pages, and thus their manual detection and analysis is not practical. Honeypots Client can automate detection at least partially and help out in analysis. HoneyMonkey is a high-interaction client honeypot for detecting exploits. The system consists of a set of Windows XP instances with various levels of patches running in virtual machines. In honeypots system is provide a list of URLs that a modified Web browser within a virtual machine visits one by one. During the URL visits, the state of the system, files and registry, is checked. If there were any modifications present the outside the browser’s working area, the URL would be reported as an exploit and marked for further analysis. In that case, the exploited virtual machine instance is discarded and a
clean one is started. So this is the main objective of the honeypot security system for the intrusion detection system.

We have selected these case studies because each case study present us with different honeypot scenario and outcomes. The case studies showed the different ways honeypots were deployed, the different kinds of intruders that are caught, the reasons why a honeypot can fail its objective(s) and how they were successful.

EFFICIENT USE OF HONEYPOT SECURITY SYSTEM:

1. Data Capture and Data Store Method:
   Now a day’s permanent problem is how to capture the data and store it. By using kernel module of honeypot OS, attacker’s activity can be detected, which encapsulates and the captured data with a spoofed IP and common use protocol such as NetBIOS. Capture data in kernel module make it independent of the communication means, such as SSH, SSL, or IPSEC. Spoofed ip and encapsulation are used to trick attackers. Honeypot gateway actively captures, decrypts, and reconstructs these data.

2. Virtual Honeypot:
   Virtual honeypot even can simulate different kinds and different number of honeypot in a device. Related technologies includes virtual environment in home OS, IP stack simulator and application simulator.

3. Encryption:
   Honeypot system does not matter if an attack or malicious activity is encrypted. The honeypot will capture the activity easily. Honeypots can do this because the encrypted probes and attacks interact with the honeypot as an end point, where the activity is decrypted by the honeypot.

4. Small Data Sets:
   Thousands of alerts a day may log a hundred alerts with honeypots system are logging in many organization. Honeypots only collect data while interacting with them. This makes the honeypots data collect much higher value, easier to manage and simpler to analyze.

5. Catching False Negatives:
   Some traditional technologies are fail to detect unknown attacks. The traditional computer security technologies use the statistical detection which also suffers from probabilistic failures. Honeypots system easily identify and capture new attacks against them. Any activity with the honeypot is an anomaly, making new or unseen attacks easily standout.

6. Highly Flexible:
   Honeypots are easily adaptable, with the ability to be used in a variety of environments and a Social Security Number embedded into a database, to an entire network of computers designed to be broken into.

7. Lossless:
   The environment create by using Honeypots system to attract the intruder and all the transactions and processing done on the system is fake. Hence it does not make any loss to accounts or data which is being hacked [4].

8. Minimal Resources:
   Even on the largest of networks, Honeypots needs minimal resources.

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

10. Positive Identification:
   Positive identification is a model where the user is required to input some secret information only known to him in order to identify himself. It is applied as a second authentication method.

11. Transaction Monitoring:
   In the present work even though this method is not thoroughly analyzed. Transaction history analysis and Honeypots system that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

12. Highly Flexible:
   Honeypots are easily adaptable and use in a variety of environments, very thing from a Social Security Number embedded into a database, to an entire network of computers designed to be broken into.

13. Resources:
   Network Intrusion Detection Devices may not be able to keep up with network activity, dropping packets, and potentially attacks while centralized log servers may not be able to collect all the system events. Honeypots do not have this problem; they only capture that which comes to them [3].

CONCLUSION
Honeypots are clearly a useful tool to attract and trap attackers, to capture information and generate alerts when someone is interacting with them. Honeypot security system can be used in various banks for online procedures e.g. E-banking. It can be used for scientific or government purposes for confidential data. It may affect customer’s confidence toward online business transaction in a variety of privacy risk assessments by consumers. Most research studies have indicated that the common problem affecting information security and privacy of customers is e-services provider’s lack of security control which allows damaging privacy losses. Apart from that, another problem is the subsequent misuse of consumers’ confidential information, as in identity theft. Honeypots system implements security. It is up to the development team to be both proactive and reactive in handling security threats, and up to the consumer to be vigilant when doing business online.
REFERENCES:

5. Lanz Spitzner, “Know Your Enemy: Learning with User-Mode Linux Building Virtual Honeynets using UML”