ISSN:0975-9646

An Autoconfigurated Hybrid Honeypot for Improving Security in Computer Systems

Shyamasundar L B[1]

[1]Department of Computer Science and Engineering
CMR Institute of Technology, Bangalore, Karnataka, India

***Abstract*— Providing computer system security is one of the important areas of consideration in Information Technology. There is a rapid advancement in this area because no one exactly wants his system to be attacked by an intruder and the data to be compromised. An experienced attacker may get to know the weaknesses of the system and may obtain the sensible data. So its necessary to give protection against intrusion. So, we make use of honeypots that have some *autoconfiguration feature* based on the collected parameters.**

***Keywords*— Honeypots, IDPS, Network Security, Pattern Detection, firewalls**

I. Introduction

Providing computer system security is one of the important areas of consideration in Information Technology. There is a rapid advancement in this area because no one exactly wants his system to be attacked by an intruder and the data to be compromised. An experienced attacker may get to know the weaknesses of the system and may obtain the sensible data. So its necessary to give protection against intrusion. Providing security against intrusion is not an easy task. It is very complex. Today firewall, in combination with Intrusion Detection System(IDS) is used for this purpose.

If once the attacker gains access to the firewall system, then he will be able to get the access to the host system. After that there is nothing to prevent the attacker from obtaining valuable data.

Traditional approaches to security largely focuses on defense. With the presence of booby traps it is possible to simulate system weaknesses and attract the attackers. It begins interaction with the attacker and starts to gather detailed information. The gathered information is then analyzed to eliminate security weaknesses. This advanced decoy is called *Honeypot.* [1]

The proposed hybrid architecture consists of an *autoconfiguration* characteristic that provides autoconfiguration process based on the collected parameters with the help of *passive fingerprinting method.*

Passive fingerprinting method passively collects all the activities of the attacker. It also determines the identity of the OS. It captures the changes occurring continuously and keeps the Honeypot updated.

Some security equipments like Honeyd [2] are being used for enhancing system security and for protecting valuable data [3]. The proposed architecture is based on Honeypots using already existing tools and methods. e.g. Snort [4], Sebek [5] and Dionaea [6].

II. Intrusion Detection and Prevention System

Today, Intrusion Detection System(IDS) is being used in combination with firewall to give protection against intruders. IDS is a security application that controls the activities within the computer system. On detection of any suspicious activity, IDS starts by generating reports for a control station. IDS monitors and records data of any event in the network that will not meet the standard behavior.

A. *Classification of IDPS*

Based on usage in various environments,[1]

- Host-based IDS (HIDPS): It performs monitoring and analyzing of the system using activity logs and audit data.
- Network-based IDS (NIDPS): It recovers from unauthorized access by using traffic analysis tool on an event of malicious activity.

Based on method used for intrusion detection,[1]

- Anamoly detection: It detects the patterns that are deviating from standard behavior, then starts identifying penetrations.
- Misuse detection: There will be some recorded attack patterns. The users' activities are compared with that of the recorded patterns of attacks. A major disadvantage with this is that, new attack patterns will not be detected as they are not recorded with the known attack patterns.
- Hybrid mode detection: It is the combination of the above two methods. It significantly reduces the generation of false negatives and false positives.

B. *Components of an IDPS*

There are several parts in IDS. The IDS sensor, which is the most important part of IDS is responsible for the detection of intrusion based on the collected information from the three sources:

- Audit notes
- System records(log files)
- IDS knowledge database

In the process of intrusion detection these data have direct impact on the future functionality of the IDS system.

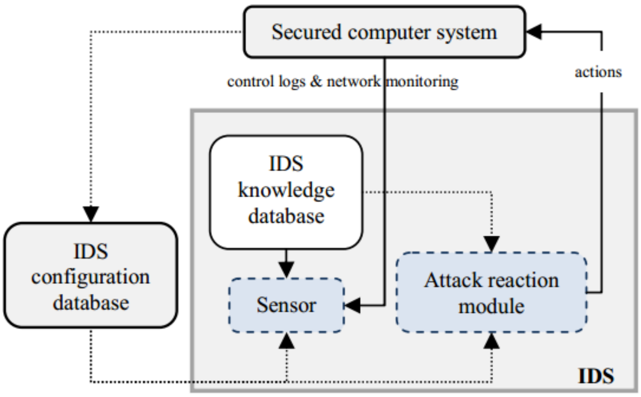


Fig. 1 Components of an IDPS

C. *Structure of IDPS*

In IDS the sensor is connected to the event generator which contains its own evaluation policy which defines filtering notifications. Event generator is combined with a list of security policies which in combination produces a set of events.

These events can be subsequently stored as a file which is secured outside the current system.

The sensor has its own database of the history of intrusions. The database will contain configuration parameters wrt IDS and the communication method with the reaction module.

There are several tools for intrusion detection. Based on the deployment, the implementation method is being considered. One such tool is Snort which increases the security of the system in combination with the Honeypot, which is an open-source product. It can detect and alert the suspicious behaviors in the system that too against the Honeypot.[4]

Snort can identify the packets that are causing network load due to attacks on the system. This information will be very critical for further analysis of the security of the system. It uses rules and several methods of protocol detection.

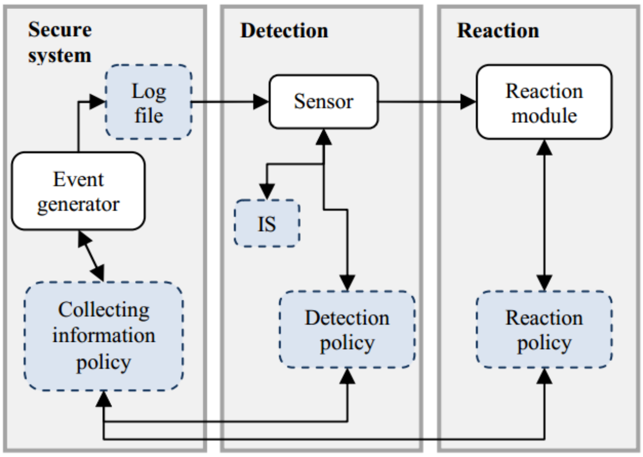


Fig. 2 Structure of an IDPS

III. EXISTING SYSTEM

There is no explicit definition for Honeypot because it is still a new and evolving technology. It can be adopted into various areas of security[7] such as,

- Detection
- Prevention
- Information collection

The main advantage is the property of its universality and is not specific to any environment. It is a high flexible tool which can be adopted in several areas, which depends on our goal of security.

Honeypots are available in different shapes and sizes used for different purposes. Another advantage is that it can be placed both in front of the firewall as well as behind the firewall also.

Most of the attackers once they gain access to the system, they try to get the information to a maximum extent. This can be monitored with the help of a Honeypot. Honeypot has null influence on the deployment environment. It uses an IP address that can initiate interaction with anyone. Any interaction havin that IP address is obviously doubtful and suspicious.

A. *Honeypot Algorithm Steps*

- Attract the potential attacker by exposing poor security and vulnerability.
- Here the layer that has been exposed to the attacker is a dummy layer.
- Then all the activities that are performed by the attacker are recorded.
- The recorded activities are then analyzed thoroughly in a detailed manner.
- Then improve the security by removing security holes and weaknesses.

B. *Types of Honeypot*

Based on the purpose:[8]

- **Research Honeypot:** Primarily focuses on gathering and extraction of information based on tools, procedures, attacks and intruders. It also explores vulnerability and explores cyber threats. It identifies the organization of the attackers and understand their behaviors. In the process of deployment, research honeypots are very complex. It is difficult in the stream of installation and maintenance also.
- **Production Honeypot:** Primarily focuses on enhancing system security. With this, the deployment of the Honeypot becomes easier. This type of Honeypot obtains only a very small amount of data. It can slowdown an attack and can reduce information security risk by isolating intruders.It becomes a part of the network after it has been deployed, which attracts the attacker for initiation of interaction. In this manner Honeypot obtains the data and analyses it and thus improves the security by removing security loops and weeknesses. It has minimum security prevenvtion. [8]

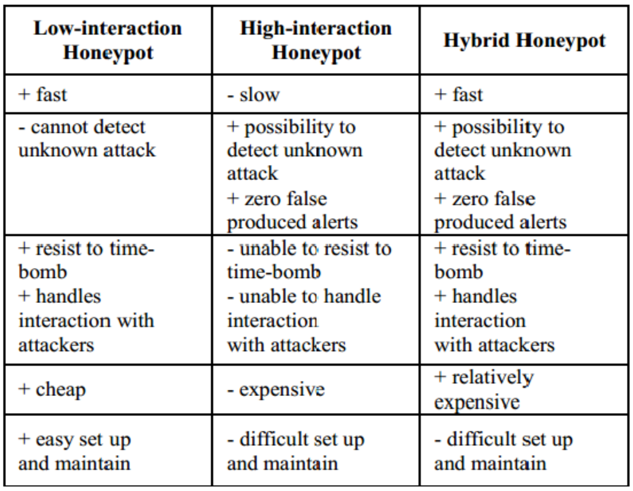
Based on the interaction level:[9]

The strength of the system depends on the ability to transact with the attackers. The operation principle of all the honeypots are same. To select a particular Honeypot its important to consider to what extent the attacker is allowed to interact. There are three interaction levels.

- **Low-interaction Honeypot:** It doesnot contain its own operating system. It actually slowsdown the attack and doesnot give full access to the system and its services. The period of interaction that an attacker can interact is very short in time which makes the attacker very difficult to access the system. Attackers can connect only to a small number of ports. These can be maintained and deployed easily. An example for low-interaction Honeypot is Honeyd.[7]
- **Medium-interaction Honeypot:** It is same in principal as that of low-interaction Honeypot. It provides the attacker with the illusion of having an OS. Attacker communicates with a large number of simulated services. With this it is possible for recording automated attacks. Information about malicious code can be obtained. Examples are tools that include Diaonea and honeytrap.
- **High-interaction Honeypot:** This is the most advanced decoy. This is more complex. This has the highest threat because it exposes itself to the attacker for a long period of time. That is the period of interaction is very high. It contains its own OS. It has to be kept under continuous monitoring because of the security risks. An example for high-interaction Honeypot is Honeynet.[10]

Hybrid Honeypot:

Hybrid honeypot is a combination of several decoys with different interaction levels. This helps in minimizing the disadvantages of both to a minimum extent and maximizing the advantages of both in combination. Hybrid Honeypot has increased success rate in detection mechanism. So an effective solution is a combination of honeypots with low and high interaction levels(TABLE 1). An example is Sebek.



Low-interaction Honeypot	High-interaction Honeypot	Hybrid Honeypot
+ fast	- slow	+ fast
- cannot detect unknown attack	+ possibility to detect unknown attack + zero false produced alerts	+ possibility to detect unknown attack + zero false produced alerts
+ resist to time-bomb + handles interaction with attackers	- unable to resist to time-bomb - unable to handle interaction with attackers	+ resist to time-bomb + handles interaction with attackers
+ cheap	- expensive	+ relatively expensive
+ easy set up and maintain	- difficult set up and maintain	- difficult set up and maintain

TABLE I ESSENCE OF HYBRID HONEYPOT

C. Advantages and Disadvantages of Honeypot

Advantages:

- Minimizes the generation of number of false positives and false negatives.
- Captures only the malicious activities within the system. This can be done with the help of low end parameters. So minimal resources are sufficient.
- Simplicity.
- Flexibility.
- For their functioning they donot need any complex algorithm or operation.
- Captures and records each and every activity.
- Can discover new tactics of attacks.
- Produces small amounts of data that are of very high in quality.

Disadvantages:

- If the Honeypot only is incorrectly configured, then the attacker can gain access to the Honeypot itself and can retrieve all the collected data.
- There is no autoconfiguration process. It needs 100% human interaction to remove loose poles and security weaknesses.

IV. METHODOLOGY

The hybrid Honeypot uses IDS detection mechanism with an autonomous feature that allows to be deployed in any environment. It consists of combining several tools like Snort IDS, Sebek and Dionaea. The tools are to be selected depending on the properties, level of interaction and requirement.

It uses a client-server architecture consisting of centralized main server and multiple clients. Clients record suspicious activities occurring in the system and records the malicious code. This recorded data is then sent to the server workstation for further processing. The server then analyses the received data and then decides whether to issue a security warning or not and then the information is displayed through an interface.

By this way we can obtain an early warning against an attack on the system.

Server architecture:

The server is actually connected to multiple clients and the server is centralized. All the received messages are stored in a knowledge database. The server actually consists of three main parts[7]:

- Sebek server
- Dionaea server
- Verification process

Sebek server filters incoming data.

Dionaea server receives malicious code and sends it to Dionaea client.

Verification process is the process of intrusion detection.

Client architecture:

Clients are placed in the same domain as they all are performing the same activity of observing the attacker activities. The parts are independent of each other and are activated independently. The data that has been obtained is delivered back to the server to perform further analysis and updation of security of the system.

Client architecture consists of three components[7]:

- Sebek client
- Dionaea client
- Snort

Sebek client records the behaviors of the attacker while the attacker is in interaction with the Honeypot.

Dionaea Client attracts the attacker and captures the activities of the attacker and the corresponding vulnerabilities.

Snort monitors and filters all the packets in the network during identification of intrusion by the attacker.

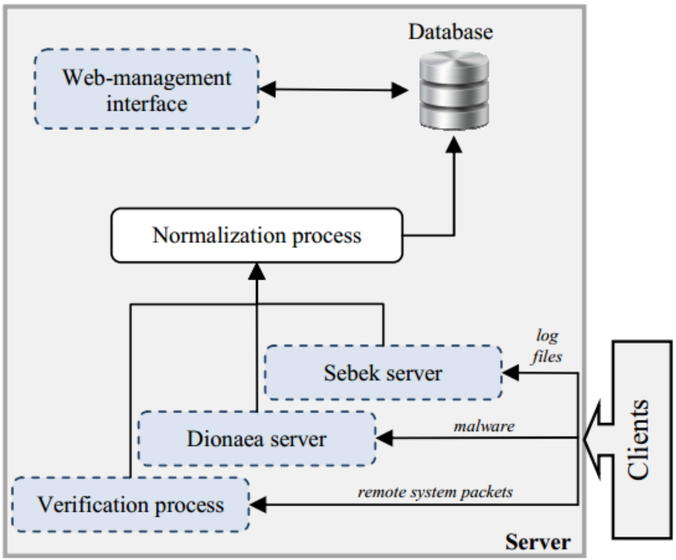


Fig. 3 Server Architecture

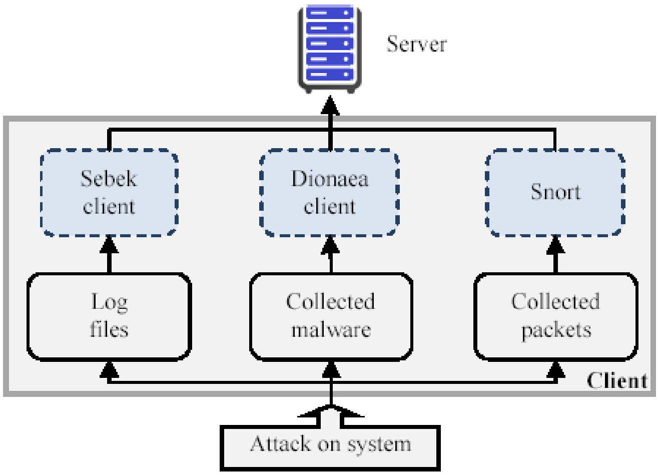


Fig. 4 Client Architecture

Hybrid Honeypot:

When all the configurations are performed automatically, optimal condition for the deployment of the Honeypot is obtained. After deployment Honeypot must be able to adopt to the changes in the environment. So the optimal solution is to use passive fingerprinting method. [3]

Passive fingerprinting method passively collects all the data about the attacker activities. It also determines the identity of the OS. This method is continuous which captures the changes in real time and thus the Honeypot is kept updated for a very long time.

The honeypot is physically connected to the computer system. With the help of passive fingerprinting method the number and type of OS, running services, host communications are identified.

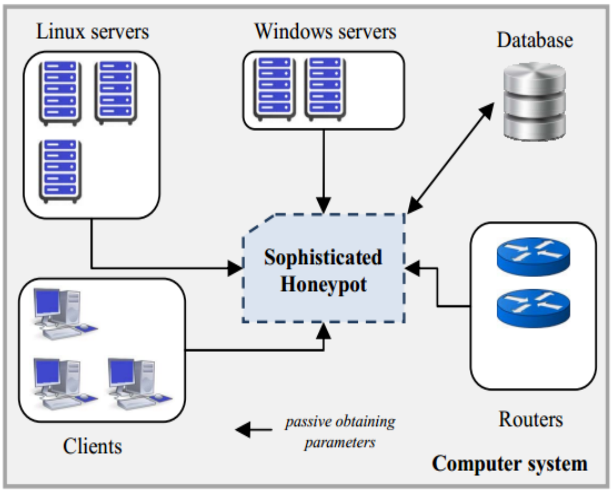


Fig. 4 Getting system parameters using passive fingerprinting method

With the combination of Honeyd and passive fingerprinting method, we can implement autonomous sophisticated Honeypot that merges with the surrounding environment and minimizes risk by the intruders.

Thus the usage of honeypots results in a cost effective solution for enhancing security thereby reduces the risk of identification by the attackers since it has been merged with the surrounding environment.

V. FUTURE ENHANCEMENT

The existing system requires human interaction to a maximum extent. The proposed system allows us to reduce the amount of human interaction needed and allows *autoconfiguration process* based on the collected parameters, by observing and analyzing the activities of the attacker.

VI. CONCLUSION

Now we know the importance of the Honeypot and its use. The existing system uses the Honeypot without *autoconfiguration process*. So now we need to improve this disadvantage and *add some automation.* So that we can have a Honeypot that does *autoconfiguration process* based on the collected parameters thereby eliminating loose poles and security vulnerabilities and thus reduces human interaction and also manual errors.

ACKNOWLEDGMENT

I would like to thank V.N. Narayana, Sanjay Chitnis and Arokia Swamy for their valuable guidance and feedback which was a major requirement for the creation of this work.Thanks also to the reviewers for their helpful comments.

REFERENCES

[1] J. McHugh, A. Christie, J. Allen, “Defending Yourself: The Role of Intrusion Detection System,” IEEE Software, IEEE Computer Society, pp. 42-51, October 2000.

[2] R. Chandran, S. Pakala, “Simulating Network with Honeyd,” [online] Technical Paper, Paladion Networks, December 2003. Available on: <http://www.paladion.net/papers/simulating_networks_with_honeyd.pdf>.

[3] F. G. Lyon, “Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning,” [online], Nmap Project, USA, ISBN 978-0979958717, January 2009. Available on: <http://nmap.org/book>.

[4] Snort [online]. Available on: <http://www.snort.org>.

[5] Sebek [online] Available on:<http://www.honeynet.org/tools/sebek/>.

[6] Dionaea catches bug [online] Available on: <http://dionaea.carnivore.it/>.

[7] P. Fanfara et al., “Autonomous Hybrid Honeypot as the Future of Distributed Computer Systems Security”

[8] S. Karthik, B Samudrala, A. T. Yang, “Design of Network Clients virtual Honeypots

[9] L. Spitzner, “Honeypots: Tracking Hackers,” Boston, USA: Addison-Wesley, Parson Education, ISBN 0-321-10895-7, 2003.

[10] L. Spitzner, “The Value of Honeypots, Part One: Definitions and Values of Honeypots,” Security Focus, 2001.