Honeypot Advanced Multilevel Security System

[1]Jincy G Varghese, [2]Prof. Anand Deepak George Donald
[1] Department of Computer Science and Engineering
Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India.
[2] Department of Computer Science and Engineering
Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India.

***Abstract*:** To provide security to the server data is the big challenge. Security activities are for keeping intruders out of the system or network, preventing the violation of information sent through the Internet and internal damage caused by viruses. Counter measures are made to prevent malicious attacks. Most of the counter measures are made on known facts, known attack patterns. Security software such as network intrusion detection systems and firewalls are based on detection and prevention mechanism. An Intrusion Detection System (IDS) is a software application or devices for malicious activities. The problem with current IDS is high rate of false alarms. Whereas honeypots are efficient way to increase the security of the network. They are easy to use, gather the required data and they are mainly used by the corporate companies to protect their networks from the unauthorized users.

***Index Terms*: Honeypot, Honeynet, Network Security.**

I. INTRODUCTION

Most of public and private organizations transfer their data through the Internet. Today, the attack or intrusion to the system is the big problem for secure network. The first step to protect system against online attacks is to recognize the tools and nature of the attacks. One of the way to provide security to server data, is to implement fake services using honeypot. Honeypot is a fake server that provide emulated services same as to the real services that is running on the actual server. Whenever attacker tries to attack the actual server, then the attacker is redirected into the fake server that is honeypot and eventually attacker gets trapped in honeypot. Honeypot then collect the information regarding the attacker. This information can be used as counter measures and can be used to take legal actions against the attacker [6].To detect malicious or inappropriate activities, there are already some techniques such as IDS, Firewalls etc. But they have some limitations of anomaly detections and high rate of false alarm, alerts generated does not have sufficient information for the analysis purpose. Honeypot is a platform by which online attacks can be detected [7]. It is a versatile more efficient security tool that is designed on the principle of deception. Its functions information gathering on attacks on server side services and client applications and browsers, attack diversion etc.

II. CLASSIFICATION OF HONEYPOTS

2.1 Low Involvement Honeypots

A low involvement honeypot only provide fake services. Attackers can only connect to several ports and scan the data. On a low involvement honeypot there is no real system on which attacker can operate. The risk on the system is less as intruder has only limited access or activities that can be done [4].

2.2 Medium Involvement Honeypots

A medium involvement honeypot provides more services and data for attacker to interact with, but still does not provide a real operating system. The fake system are more sophisticated and have a deeper knowledge about the services they provide. So the risk also increases with it. The probability of the attacker to find a vulnerability or security hole is getting intense due to which the complexity of the honeypot increases. The higher level of interaction allow more complex attacks and can be analyzed and logged. When the attacker gets an illusion of a real system, Probability of interaction with the system is more. Developing a medium involvement honeypot is time consuming and complex. More attention has to be given for security checks as all developed fake services need to be as secure as possible. Definitely developed system should be more secure than the real counterparts. The knowledge required for developing such system is very high as each service and protocol needs to be understood [8].

2.3 High Involvement Honeypots

More complex than the other two is the high involvement honeypots as they involve the deployment of a real applications and operating system. The risk included with this type is huge but it also provide more attractive system and gathering of information is also more by allowing the intruders to interact with real systems, every action done by intruder can be recorded and monitored. A high involvement honeypots provide wide services and offer same environment as real system. As attacker gets into the system after few steps attacker has to compromise to get to another level.

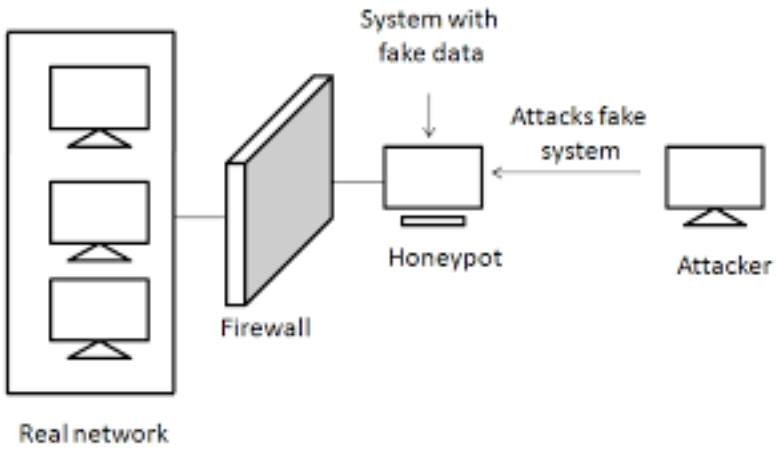
III. EXISTING METHODOLOGY

Server computing takes place in distributed environment. Therefore they can be easily targeted and exploited by the attackers. Attackers can pretend that they are the legitimate users and can use the services maliciously. Providing secure network in a distributed system require more than user authentication with passwords and confidentiality in data transmission [2]. Intrusion detection system can be used to provide efficient security measures for the distributed network by checking logs, configurations, and user actions and system traffic to identify attack behavior. IDS is able to keep check on each and every node in cloud environment and it's able to alert other nodes in the environment. The IDS use two methods of Intrusion Detection that are behavior based and knowledge based. It has two components that are Alert System and analyzer. Behavior Analysis in this method it compare recent user actions to the usual behavior. Knowledge Analysis: The knowledge based method detects certain sequences of actions from a user who might represent an attacker and known trails left by attacks.

IV. PROPOSED METHOD

An analysis is evaluation of a proposal designed to show the difficulty in carrying out a designated task. A feasibility study precedes project and implementation technical development. A feasibility study is an analysis or evaluation of the potential impact of proposed project. A honeypot is used in the area of cryptography and internet security and Honeypots are a modern approach to network security. It is a resource, which is intended to be compromised and attacked to gain more data about the intruder and the strategy used. It can be deployed to divert and attract an intruder from their real targets. Honeypots have the larger advantage that they do not generate false alerts on each observed traffic that seems doubtful, because no productive actions are taking place on the system. This fact enables the system to log every byte that flows through the honeypot and from the network and to relate this information with other resources to draw a picture of the attacker and attack. By knowing strategies of attack taken place, countermeasures can be upgraded and anomalies can be fixed. One of the main target of honeypot is to gather as much information as possible. Web Based Honeypot Network is a type of server for accessing the Services like Uploading, Downloading and Mailing. It provides a way of use the services. A honeypot is an instrument for learning and gathering information. It is an information system resource whose value lies in the illicit and unauthorized use of that resource. Generally a honeypot is a trap set to discover attempts and strategy at unauthorized use of information systems and divert attacker.

Main function of Honeypots is to detect malicious action by attackers and divert them from the real servers. It will make attacker to compromise while using fake system in order to move to next level. Many security levels are developed to authorize the user if authorized user then he will move to the actual system otherwise will move to the fake server that is similar to the actual server. Many services are developed that is similar in both fake and actual server where it pretends as if the services are real but it is used to divert the attacker and monitor all the action taken by attacker. After failing in any security level admin of organization will get email on his mail id. By this measures honeypots deployed in distributed network of an organization can help gather information and prevent actual system from the attack.



Honeypot Architecture [9]

V. EXPECTED OUTCOME

Study of this system gave me an opportunity to learn honeypot system in detail. It is efficient for organizations to have a secure transaction of data and their digital assets by detecting and preventing malicious attacks. Honeypots are used as a valuable tool to gather information about the action of attackers in order to design and implement better counter measures. The proposed method gives the details about the implementation of Honeypot System. Levels of security authorization is being used and moving attacker to fake server and providing them similar services to monitor on their action is being implemented. Hence it can be concluded that honeypot are used as most efficient tool to provide security for servers.

VII. REFERENCES

[1]Anjali Sardana and R. C. Joshi an Integrated Honeypot Framework Proactive Detection, Characterization and Redirection of DDoS Attacks at ISP level". Journal of Information Assurance and Security (2008)

.[2]Babak Khosravifar, Jamal Bentahar, "An Experience Improving Intrusion Detection System False Alarm By Using Honeypot", IEEE of the 22nd International Conference On Advanced Networking and Application, 2008.

[3]C. Hecker, K. L. Nance "Dynamic honeypot construction", In Proceedings of the Colloquium for Information Systems Security Education, June 2006.

[4]Hamid Mohammadzadeh. e. n, Roza Honarbakhsh, and Omar Zakaria, "A Survey on Dynamic Honeypots", International Journal of Information and Electronics Engineering, March 2012.

[5]Nithin Chandra,S.R, Madhuri , "Cloud Security using Honeypot systems", International Journal of Scientific and Engineering Research Volume 3, Issue 3, March -2012.

[6]Reto Baumann, Christian Plattner, "White Paper: Honeypots",International Conference on Web Services Computing 2011, Proceedings published by International Journal of Computer Applications.

[7]Sebastian Biedermann, Martin Mink. "Fast Dynamic Extracted Honeypot in Cloud Computing".

[8]Implementation of Honeypots for Server Security Akshay Somwanshi, Prof. S.A. Joshi International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 03 | Mar-2016

[9]International Research Journal of Engineering and Technology (IRJET) on Honeypot Security Satish Mahendra.