Honeypot Advanced Multilevel Security System Using AES Encryption

[1]Jincy G Varghese, [2]Prof. Anand Deepak George Donald

Department of Computer Science and Engineering
Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India.

***Abstract*: A honeypot is a system attached to network set up as a decoy to attract cyber intruders and to detect, confuse or learn hacking attempts in order to gain unauthorized access to data systems. The function of a honeypot is to make itself as a potential target for attackers in internet usually a server and to gather data and notify defenders of any attempts to access the honeypot by intruder. Honeypots are most often used by large tool and by companies involved in cybersecurity research to identify and prevent attacks from advanced persistent attacker**

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

I. INTRODUCTION

A honeypot operation consists of a computer [3], data and application that replicate the behavior of a real system and appear to be a part of network, however, the honeypot is closely monitored. Because there is no reason for valid users to access a honeypot, any attempts to communicate with a honeypot is considered hostile.

Logging and viewing this activity can help improve security by providing knowledge into the level and types of threat a network faces while distracting intruder away from services of real value. Researchers find that some cybercriminals use honeypots themselves to gather information, intelligence about researchers that act as decoys and to spread misinformation.

Virtual machines are mainly used to host honeypots, so if it is compromised by malicious act, for example, the honeypot can be quickly restored. Honeynet is when two or more honeypots are on a network and a centralized collection of honeypots and analysis tool is called honeyfarm.

II. CLASSIFICATION OF HONEYPOTS

There are two main types of honeypots based on design and deployment that are production and research. Research honeypots perform close analysis of activity by attacker and aim to find how these intruder develop and progress in order to get knowledge of how to better prevent systems against attacks. Information placed in a honeypot with unique identifying properties can help analysts track stolen information and identify connections between attackers in an attack.

Production honeypots are deployed inside the production networks with production servers. The honeypot acts as a decoy as a part of the production network intrusion detection system (IDS). A production honeypot is designed to appear real even though its simulation server and contains data to distract hackers from real server to waste their time and resources, ultimately giving administrators more time to access and mitigate any vulnerabilities in the actual production systems.

Honeypots can also be classified as pure, high-interaction and low-interaction. A pure honeypot is the full-fledged production system that cover the honeypot link to the network. A high-interaction honeypot simulate the activities of the production systems that host a variety of services and captures extensive data. A low-interaction honeypot simulates only the services that intruder frequently request; therefore, they are less risky also easier to maintain. The goal of a high-interaction honeypot is to entice an intruder to gain root access on the server and then monitor their activity.

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

The proposed modules of Web Based Honeypot System are specified below. Each module will provide the basic features of inserting, viewing and managing records. Encryption/Decryption done by advanced AES algorithm. Pseudo Random number generator algorithm is used for generating OTP Four layers of security level is there which provides authorization of user if intruder

tries to invade into system then intruder is directly send to the fake server exactly replicating the actual server. First Layer: Authenticating with Mail is and password that is already registered. Second Layer: OTP send to mobile if correct and then enter that OTP. Third Layer: OTP send to mail id of registered user. Fourth layer: security question is asked which is already registered. Fifth Layer: Google Captcha to verify authentication.

Registration – This module will allow the user to register himself on Network with various information like name, address, DOB and also Enter Login Info. Which is useful for Login Process.

Login Using Kerberos – This module will allow the user to login with 5 levels. If any one level is wrong then he goes to the honeypot server for accessing the services. Otherwise he go to the application server.

Server Services – This module will allow the user to access the services like download file, upload and mailing from server.

Packet and Log Monitoring – This module will used to monitor the user Information like Login/Logout time, which type of file download/Upload, etc.

V. RESEARCH COMPONENT

The AES [2] is often called as a one-way function because from the cipher text the plain text cannot be retrieved from the guess made by any other malicious act. Thus, the AES algorithm is an efficient one which could be used for the encryption techniques. But the problem here is that the AES algorithm is affected by the brute force attack and also by many side channel attacks. So, honey encryption has to be used. The honey encryption is the technique which is used to distract the hacker with the generated fake message which looks like a real, so the attacker get confused in choosing the correct key. The AES hardware mode is also changed in to reduce the cost and time of implementation of AES by increasing the rounds in the algorithm.

VI. RESULT

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.

Module 1: Login page and registration

Here only the registered user and login those who registered already through Admin Panel. If Login is done by valid user it will send to another security layer. If Login is incorrect it will send to the fake Honeypot server that offers same services as actual server. Login done using Kerberos.

Module 2: Admin Page

Admin Page consists of Admin Login Where only admin of organization can login. It has a registration page where all the details of user has to be entered. Registration page has the security question along with username and password. User List where all registered *user is displayed.*

Module 3: Pseudo Random Number Generator (PRNG)

PRNG is used to generate OTP via Mail id and SMS where SMTP protocol is used. These algorithm secure the server by only allowing authorized user to access to another page to go to the real application server.

Module 4: Security Question and Google Captcha

Security question is asked and the answer is verified. If valid then the user is send to another security level google captcha to verify its user or any machine trying to invade. If verified then send to the Actual Application server which also offers various services like any other website.

VII. FUTURE SCOPE:

In future, the complexity of the Honeypot System can be increased to protect the system from attackers. Honeypot could be extended to Honeynet, where attackers deals with bunch of honeypots. Future challenge will be combining two Honeypots and design a hybrid kind of Honeypot.

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] Screening the covert key using honey encryption to rule out the brute force attack of AES—a survey P Dharshini, P Mohan Kumar , J Arokia Renjith published 03 February 2017.
[3] searchsecurity.techtarget.com/definition/honey-pot contributor(s): Casey Clark, Michael Cobb
[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.