ISSN 2395-1621

Implementation on Honeyd: A system for analysis of network attacks

[#1]Nikita A. Mane, [#2]Vinod B. Thorat, [#3]Kunal N. Shirke,
[#4]Prof. Mrs. Premlatha G.

[1]nikitamane2828@gmail.com
[2]vinod.b.thorat@gmail.com
[3]kunalnshirke@gmail.com
[4]premlathag22@gmail.com

[#1234]Department of Computer Engineering,
JSPM's
Imperial College of Engineering and Research, Wagholi.
Savitribai Phule University, Pune

ABSTRACT

A honeypot is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Generally as the number of users for a web service increases , the issues related to security arise too. So does the need arise to secure these systems for reliable and efficient working-One such tool is-Honeypot. As the flow of data increases, the probability of gaining access to confidential data is also high. So detecting vulnerability becomes a preliminary task in order to overcome such malicious activities. In this study, the simulated computers on network are been secured using Honeypot's design and Framework which helps in many fields such as detection of worms, adversaries, illegitimate traffic, spread of spam email. The honeypots deployed on the network monitors the traffic for any anonymous users and track him to prevent further attacks.[1]

ARTICLE INFO

Article History

Received: 1st June 2017

Received in revised form :

1st June 2017

Accepted: 5th June 2017

Published online :

6th June 2017

Keywords: IDS, IPS & Honeypot, SQL injection, Tempering detection.

I. INTRODUCTION

Numerous exploits are being used to compromise the network. These exploits are capable of breaking into any secured networks. Thus, to secure the network we are combining features, functions and methodology of IDS, IPS and Honeyed and making Intrusion Detection System more effective, accurate and responsive.

Honeyed are mirrored servers which appear as actual servers for attackers and maintain logs of intruding activities. IDS detect the attack, and IPS takes actions as configured. Intrusion detection system monitors the data packets and looks for intrusion, when such event occurs an alarm will get triggered resulting analysis of captured packets and corrective action taken by IPS if necessary.

This alert will activate IPS which will take preventive actions depending on the type of attack. Featuring log analysis and capturing into our proposed system will enable security expert to investigate such events sophisticatedly. We also study the different attacks in network system this system is more secure for finding the attacker when any one tries to attempt attack on the network.

The rest of the paper is organized as follows. Section 2 Design of proposed system. Section 3 explain system architecture. Section 4 gives analysis result. Finally, Section 5 concludes the paper.

APPLICATION

1. Network Decoys: The traditional role of a honeypot is that of a network decoy. Our framework can be used to instrument the unallocated addresses of a production network with virtual honeypots. Adversaries that scan the production network can potentially be confused and deterred by the virtual honeypots. In conjunction with a NIDS, the resulting network traffic may help in getting early warning of attacks.

2. Security for Control Network in Company System:
Our system can be used in a company's network for security purposes and improvement of network security.

3. Military: In Government projects, especially military networks which are always on enemy radar for attacks and spying purposes. Our system can be of use since intrusions are well detected and prevented.

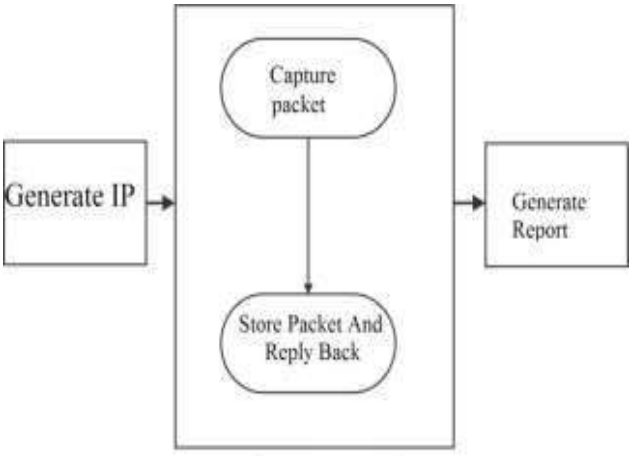
4. In the research field: Knowing trends in the attacks domain & knowing one's enemies is involved here and so our system can do it efficiently.

II. DESIGN

The design of the honeypot framework consistes of following Data flow diagrams explained in two levels as given.

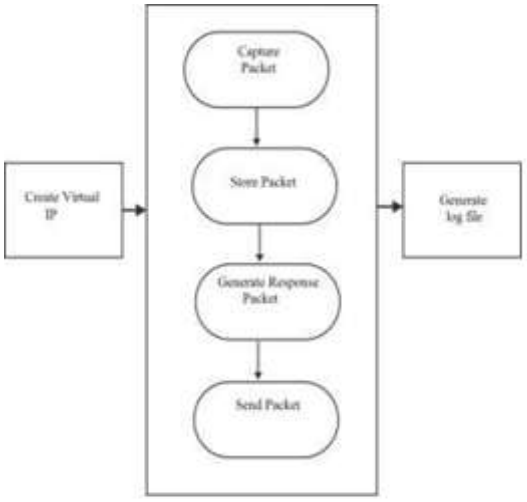
A. Level 0

In 0 level to begin with IP deal with is generated then that IP is ahead via packets and this packet sends information to database for storage motive. Every time that information is crucial it takes or get proper of entry to from database through using respond decrease returned approach. After this method one document is generated.[2]



B. Level 1

In level 1 virtual IP can be generated, after that packet is created for this IP and that packet is saved in database. After that one response packet is created to offer reaction to purchaser from server and ship that through the honeypot layer. At some point of this transmission one log record is generated for all of the approach. The log document contain all the information it truly is ship and get keep of with the id of the customer and server.[2]



III. PROPOSED SYSTEM

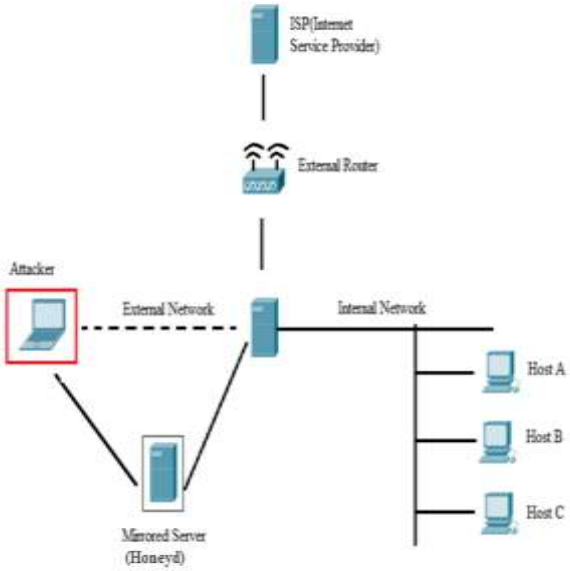


Fig 1. System architecture

In proposed system one virtual server is used to protect the multiple servers. Here complexity between the hardware is minimum. In above fig.1 one virtual server is protecting the internal severs. Also here host A, host B and host C are communicating with this server. Virtual server is working like a deceptive system. Which is protecting the multiple servers. Also it helps in detecting the attackers & hackers. It also creates the log of users. In log user IP address, time, date & MAC address are identified.

User Interface: In this product Administrator must give the range of the network and also provide the plug-in which will different for different honeypot.

Log Report: Honey-pot create log which will tells the following,

1) IP Addresses
2) Packet Received By that particular IP
3) Packet send to the that particular IP
4) Route of that IP

Note:
Network Administrator will take that Log and tells Which IP is an Attackers IP . By using that logs he also knows the attackers way to attack, so he will provide patches for that particular attack. In this product no human interface is required for generating the logs.

Module:
Attack Module (user):
Login
Registration
Attacking server
Send packet
System (admin) : log maintain

Network admin:
Send request
Generate IP
Maintain log

IV. RESULT

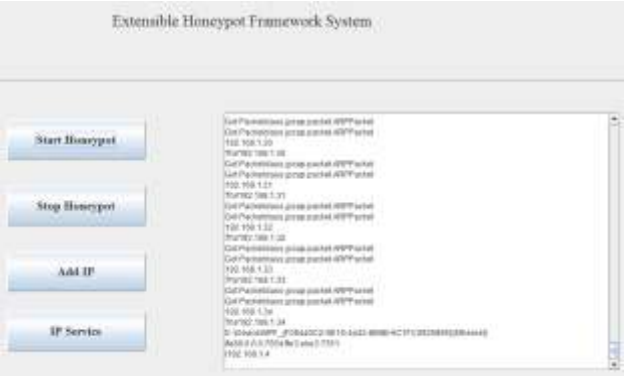


Fig 2. Maintain the analysis log

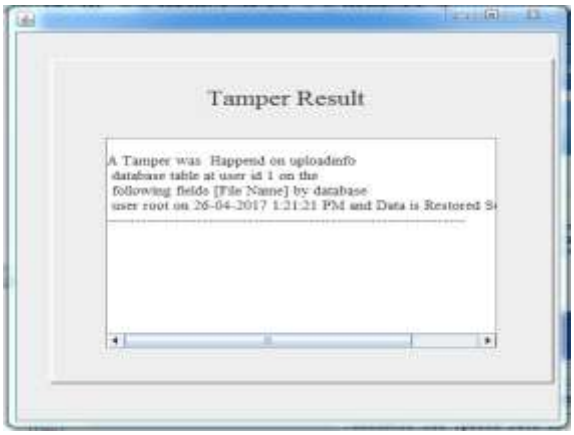


Fig 3. Tempering attack result detection

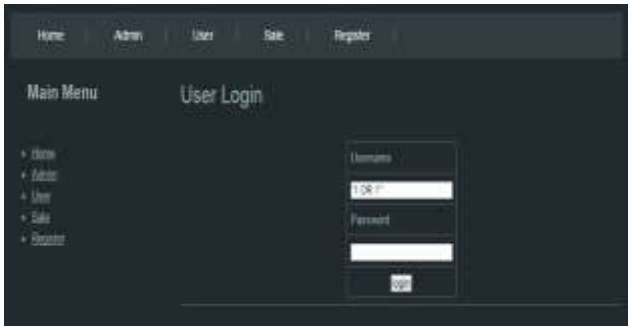


Fig 4. SQL Injection Query

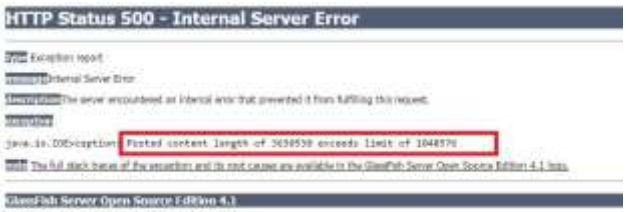


Fig 4. Limit size for uploading the any file

V. CONCLUSION

The idea behind this proposed security solution is to develop a conceptual dynamic security approach against hacking strategies and various kinds of attacks. We believe that the security of the entire Server relies on the security of the network and endpoints.

VI. ACKNOWLEDGEMENT

We would like to acknowledge our heartfelt gratitude to our guide Prof. Premlatha G. of Imperial College of Engineering And Research, Wagholi for her guidance and motivation.

REFRENCES

[1] D. Canali And D. Balzarotti, “Behind The Scenes Of Online Attacks: An Analysis Of Exploitation Behaviors On The Web,” In Proceedings Of 20th Annual Network & Distributed System Security Symposium (Ndss 2013), Feb. 2013.

[2] C.H. Yeh And C.H. Yang, "Design And Implementation Of Honeypot Of System Based On Open Source Software", In Intelligence And Security Informatics, 2008.Isi 2008. International Conference On,2008, Pp.256-266.

[3] E. Albin "A Comparative Analysis Of The Snort And Intrusion Detection Systems", Monterey California. Naval Postgraduate School 2011.

[4] Harek Haugerud "Intrusion Detection And Firewall Security".

[5] John E Canavan, "Fundamentals Of Network Security".

[6] A Survey:Recent Advances And Future Trends In Honeypot Research,Published Online Sept 2012 In Mecs.

[7] T. Yagi, N. Tanimoto, And T. Hariu, “Intelligent High- Interaction Web Honeypots Based On Url Conversion Scheme,” Ieice Transactions On Communications, Vol. 94, No. 5, Pp. 1339–1347, May 2011.

