Implementation on Honeyd: A system for analysis of network attacks

[#1]Aastha Patil, [#2]Dnyaneshwar Bhadane, [#3]Asharaf Shaikh, [#4]Ashlesha More,
[#5]Prof.Amol Rindhe.

[#12345]Department of Computer Engineering
JSPM's Bhivrabai Sawant Institute of Technology & Research College of Engineering,
Wagholi, Pune, India.

Abstract: Various attacks today are used by attackers to compromise the network security these days. These exploits of attacks are capable of exploiting into any secure networks. So to secure the server in network we are here combining features, functions and methodologies of IDS (Intrusion Detection System), IPS (Intrusion Prevention System) and Honeypot to make Intrusion Detection System more accurate, effective and responsive against these attacks. Honeypots are mirrored servers or host which appear as actual servers for attackers and maintain the logs of intrusions and intrusive activities. IDS detects the attack, and IPS takes actions against these attacks as configured. Intrusion detection system monitors all the data packets coming inward the network and looks for possible attempts of intrusion, when an intrusion event occurs an alarm will automatically be raised. The resulting analysis of captured packets is done and corrective measures are taken by Intrusion Prevention System if there is a necessity. This alarm will activate the Intrusion Prevention System which will take preventive measures depending on the type of attack and exploit used. Featured capturing, logging and analysis into our proposed system will enable security expert to investigate such events even more sophisticatedly.

Keywords: IDS, IPS & Honeypot, SQL injection, Network security.

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.

A. Contribution:

We propose a new system based on network security for analysis unauthorized access to the server and maintain the all details of the user.

- For minimizing the loss of the data from unauthorized user
- For minimizing the disclosure risk
- To maintain the security using honeyed server and avoid the attack from attacker.
- Minimized security risks.

B. Observation:

A honeypot is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

Honeypots are not always designed to identify hackers. Honeypot developers are often more interested in getting into the minds of hackers, which then permits them to design more secure systems, as well as to educate other professionals about the lessons learned through their efforts.

Overall, honeypots are considered an effective method to track hacker behavior and heighten the effectiveness of computer security tools.

II. RELATED OF LITERATURE

.

[2] Ram Kumar Singh, "Intrusion detection system is using advanced Honeypots", in this paper the number and size of the Network and Internet traffic increase and the need for the intrusion detection grows in step to reduce the overhead required for the

intrusion detection and diagnosis, it has made public servers increasingly vulnerable to unauthorized accesses and incursion of intrusions [1]. In addition to maintaining low latency and poor performance for the client, filtering unauthorized accesses has become one of the major concerns of a server administrator.

[9] Renuka Prasad, Dr Annamma Abraham and Abhas Abhinav, "Design and efficient deployment of Honeypot and Dynamic rule based live Network Intrusion collaborative system.", A Honeypot based Network Intrusion Collaboration System which is capable of generating dynamic rules during any anomalous behavior in the network or a possible intrusion is presented [8]. The NICS designed is a collection of several existing Free and OpenSource Software's customized for the specific need that helps in implementing both preventive and detective mechanisms of network security.

[8] Hemraj Saini, "Extended honeypot framework to detect old/new cyber Attacks. " To propose an approach to detect the new malicious objects with an optimal cost. Honeypots are generally used to detect the new malicious objects. The available honeypot frameworks are too costly to be afforded by an average organization. Therefore, we are proposing a low cost honeypot framework to detect malicious objects named extended honeypot. The approach is not only cost effective but also better than other approaches in some situations such as in the Intranet which is having more than one LANs and every LAN is having double honeypot.

[7] Atinder Pal Singh, Birinder Singh, "Design and implementation of Linux based hybrid client honeypot incorporating multilayer detection.", In current global internet cyber space, the number of targeted client side attacks are increasing that lead users to adversaries' web sites and exploit web browser vulnerabilities is increasing, therefore there is requirement of strong mechanisms to fight against these kinds of attacks [6]. In this paper, we present the design and implementation of a client honeypot which incorporate the functionality of both low and high interaction honey client solution and incorporate the multilayer detection mechanisms to fight against client side targeted attacks.

III. SYSTEM ARCHITECTURE

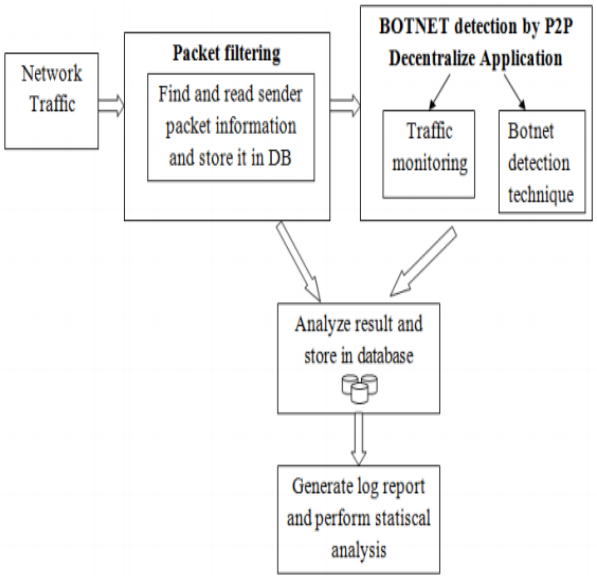

Fig 1. System architecture

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.

Algorithm:

Step 1. Start secure application on designated Honeypot in each analysis cluster to trap the unwanted network access and malware activities.

Step 2. We detecting some unauthorised user entered the local network by entering his info and password.

Step 3. If secure application detects any malwares, then following action going on,

(i) Firstly redirect the network same to designated high secure Honeypot application and all information gather for further process.

(ii) At the high secure Honeypot application, avoid the modification made to the file system and check its changes original file or not.

(iii) After analysis the file, the compares changes made to the file system with the originals stored. All the changes records added and modified files and restore the system back to original state.

(iv) Afterwards this step generates an web log, comprising of the IP, mac address, other information.

(v) A server log of all the information given in Step (iv), is stored text file for further analysis and also sent to the central repository.

(vi) The central database normalizes the these log files and store them to the database.

(vii) All process done analysis data is sent to a web application from where it could be presented to the users to give them knowledge about various security attacks going on currently in various cluster's.

Else

(i)Keep running application and keep checking continuously that it is working properly or not.

Step 4. End

Using this proposed application and algorithm approach, we achieve a secure network and number of goals.

In first step, we need to check a small number of high interaction Honeypot since the area of the traffic that will be routed to them is limited network.

Secondly, the above steps over we analysis honeypots are under strict monitors, so if the honeypot gets infected it will be very soon detected and also recovered.

Thirdly, the information about the unauthorised access and attacking techniques is also catch from the secure server immediately. Also, the low interaction honeypots where honeyd is working emulates different machines running in the network. So we can map several machines which run on the same operating system.

IV. SYSTEM ANALYSIS

We use NetBeans IDE 8.0.1 and MySQL for the implementation and run on 2.30 GHz Intel Core I3 Processor machine with 2 GB RAM.

The Microsoft Windows XP and above Professional is used as an operating system.

For this project we use special package for reading the packet or modifying the packet which will be listed as following

1) JPCAP
2) Win cap

V. RESULT AND DISCUSION

In this proposed system gives the better result when any unauthorized network and user can access the server. Here we implement the secure server for detecting the unauthorized (hacker) user for performing unwanted activity. Proposed system generates the log when any user can access the network for analysis to the server.

Log Report:

Sat Jan 09 17:58:08 PST 2020

Sat Jan 09 17:57:28 PST 2020
REQUEST FROM :192.168.43.138
Sat Jan 09 17:57:28 PST 2020
GET /LoginStrutsApp HTTP/1.1
Host: 192.168.43.138:8085
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=6533087197bc727cdb29075d4782

VI. 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.

VII. FUTURE SCOPE

A great deal of the proposed system based on the already exists system, it's developed for use against external threats from unauthorized user. As part of future work, we would like to identify malicious web servers with our low interaction client honeypot and compare the results. Intrusion Detection System and drastically reduce false positives hence enhances the overall efficiency of the Intrusion Detection System

VIII. ACKNOWLEDGEMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. Amol Rindhe for him time to time, very much needed valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

IX. REFRENCES

[1] Aastha Patil, Dnyaneshwar Bhadane, Asharaf Shaikh, Ashlesha More, Prof.Amol Rindhe, "Botnet Detection Techniques in Cloud Computing", International Engineering Research Journal (IERJ), Volume 3 Issue 3 Page 5921-5924, 2019 ISSN 2395-1621.

[2] Ram Kumar Singh, Prof. T. Ramajujam "Intrusion Detection System Using Advanced Honeypots", Submitted on 27 Jun 2009.

[3] Rajalakshmi Selvaraj ,Venu Madhav Kuthadi, Tshilidzi Marwala :Ant-based distributed denial of service detection technique using roaming virtual honeypots.

[4] Sanmorino, A., Yazid, S.: DDoS attack detection method and mitigation using pattern of the flow. Int. Conf. of Information and Communication Technology (ICoICT), 2013,pp 61-67.

[5] Tsai, C.-L., Tseng, C.-C., Han, C.-C.: Intrusive behavior analysis based on honey pot tracking and ant algorithm analysis. 43rd Annual Int. Carnahan Conf. on Security Technology, Zurich, 2009, pp 248 – 252

[6] Jain Y.K., Singh S.: Honeypot based secure network system, Int. J. Comput. Sci. Eng.,2011, pp 612-620.

[7] Atinder Pal Singh, Birinder Singh Design and Implementation of Linux Based Hybrid Client Honeypot Incorporating Multi-Layer Detection, September- October 2012,.

[8] Hemraj Saini, Extended honeypot framework to detect old/new cyber-attacks, March, 2011.

[9] Renuka Prasad.B, Dr Annamma Abraham, & Abhas Abhinav, Design and efficient deployment of honeypot and dynamic rule based live network intrusion collaborative system, 2, March 2011 .

[10] D. A. Shea, Critical infrastructure: Control systems and the terrorist threat, Libr. Congr., Rep. Congr. RL31534, Jan. 2004.

[11] Y. Huang et al., Understanding the physical and economic consequences of attacks on control systems, Int. J.Crit. Infrastruct. Prot., vol. 2, no. 3,pp. 7383, Oct. 2009.

[12] Jin Zhigang, Wang Ying "P2P botnet detection based on user Behavior sociality & Traffic entropy function". CECNet IEEE 2012, 1953 – 1955.

[13] HosseinRouhani, AzizahBt Abdul Manaf," Botnet detection by monitoring similar communication pattern". IJCSIS, Vol. 7, No. 3, 2010.

[14] Alirezashahrestani, Maryam feily, rodina Ahmad, Sureswaranramadass,in " Discovery of invariant bot behavior through visual network monitoring system". IEEE 2010, Page(s): 182 – 188.

[15] HosseinRouhani, AzizahBt Abdul Manaf, in IEEE 2010 "Botnet Detection based on Traffic Monitoring ".Page(s): 97 – 101.

[16] Osman salem, Ali Makke,Jeantajer," Flooding Attack detection in Traffic of backbone network". LCN' IEEE 2011, Page(s): 441 - 449