Honeypot System: An Intrusion Detection System

Mr. Ajinkya S. Gudadhe
2nd Sem M.E. Computer Science & Engineering
PRMIT&R, Badnera

Prof. D. H. Deshmukh
Asst. Professor, Computer Science & Engineering
PRMIT&R, Badnera

Prof. Kalbande
Asst. Professor, Computer Science & Engineering
PRMIT&R, Badnera

Prof. F. M. Shelke
Asst. Professor, Computer Science & Engineering
PRPCE&M, Amravati

Abstract:-The following paper points in the direction of extending and effectively utilizing the honeypot technology for developing an IDS module that will use the PID track technique and will have the capability of detecting the attacker and working out a response. The whole module developed can be further extended for future use and at the same time it will ensure that the intrusion detection is carried out in the fastest possible time.

Keywords *:Honeypot Technology, IDS,PID*

*****

1. INTRODUCTION

The fast paced growth of Internet has led to the development of various different systems for preventing attacks on the valuable data and other resources of an organization. All the systems developed are of varying complexities and not universally efficient throughout different platforms. The process of combining honeypot to other modules is a relatively new approach which may come across as a much needed relief to offer safe and secure solutions to keep intruders at bay. The honeypot technology adds a strong balance to ID Sand can greatly reduce the load of IDS while giving the least degree of access to the intruder. In this paper, we discuss the traditional intrusion detection system based on honeypot technology.ID Scan be traced back through the Honeypot system to achieve inter oper bility between the various components of the honeypot system. Further implication of this IDS system can be to record the mining methodologies of the intruders and keep them saved to prevent further attacks.

Method of attack is more complex, a single based pattern matching or statistical methods of analysis have been difficult of in number of attacks.

The existing intrusion detection systems can not exchange information, makes it difficult to find the attack the source of the attack, and even to the intruder has created vulnerabilities. Existing intrusion detection systems and other net- work security products can not interoperate.

The proposed model has more advantages that can response accurately and swiftly to unknown attacks and life times after for the network security. In future the network can be preserved by getting the information regarding the attacker from the Honeypot system.

2. TRADITIONAL INTRUSION DETECTION SYSTEMS AND THEIRLIMITATIONS

Intrusion detection systems may be divided into anomaly detection systems and misuse detection systems, i.e. these into two categories according to different methods of intrusion detection. Misuse detection systems can only detect those pattern characteristics which are known, characteristic patterns of unknown attacks can not be detected. The anomaly detections system uses the system's current activities and previous behavioral models for the purpose of comparing the methods that can effectively understand new, unknown attacks and can detect them. As the network continues to expand, increasingly complex it becomes.

Traditional intrusion detection systems when in use revealed the following deficiencies:

- Misuse detection and intrusion detection technology features related with the diversification of network attacks and new attacks continue to emerge, there are inevitably omissions. In addition, the intrusion detection system using the right pattern matching algorithm to match the data to detect the presence of invasion .Once a packet matches the content and signature, immediately issued a warning not to judge it is not really attack, so there could be false positives.

- Signature data base updates are very difficult .Most traditional intrusion detection systems use pattern matching analysis, which requires the Eigen values of attack signature data base should be up to date. However, the existing intrusion detection system does not always provide a good way to update the signatures. Information encryption, attacker increasing number of widely used mobile code (Java, ActiveX, etc.), false alarms are traditional intrusion detection systems are facing great challenges.

3. SYSTEMSTRUCTURE AND MAIN FUNCTIONS

Fig.1depictsthehoneypot system model, honey wall, proxy server, the honeypot client module, database, and a left generator that features five major rules Among them the data capturing module, data alert generator module and response module static Agent and Mobile Agent using a combination of ways.

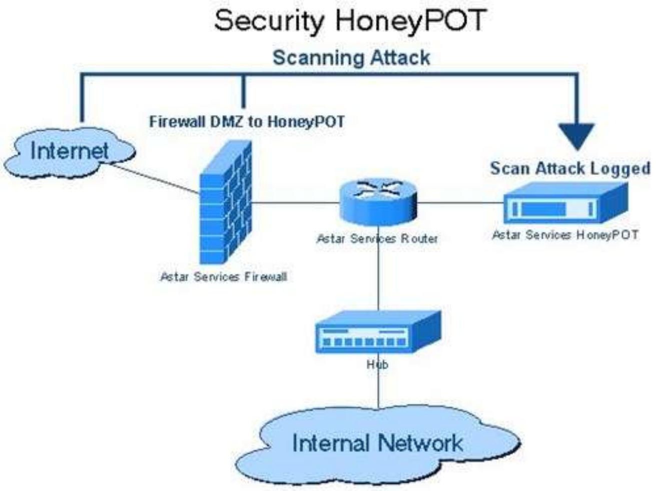

Fig. 1:HoneypotSystemModel

3.1 Data Capturing Module

The main function of the Data capturing module is to collect system logs, audit data and network data pack et sand then it also undertakes the task of preprocessing the data and then further passing it onto the data alert generator module for analysis. Thus the main task performed by the data preprocessing is that it can classify and separate the useless information by using rules in the data alert generator module to improve real time.

3.2 Data Alert Generator Module

Data Alert generator module (like SNORT) is composed mainly by the client agent. The destination host, the data collected from the local client received at the data, analysis and processing, to determine whether they are system or network intrusion.

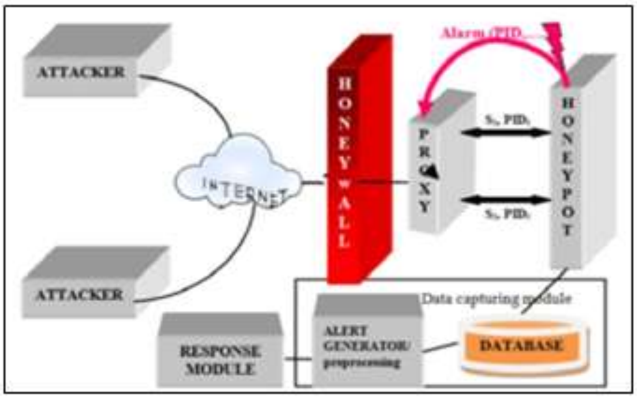

Fig. 2:HoneypotProcesses and Elements

This reduces the transmission of information in the network to ensure data security, while enhancing the response in real time. The module contains a variety of data detection client component rule, along with the different data sources to achieved if ferent alert tasks. They work together to complete complex intrusion detection. Client specific discovery can be divided into host and network testing client, respectively, the client audit data and network data packets to be monitored [6].

3.3 The Honey pot Client

Fig.3,givesthedescription of the internals of architecture of the honeypot host which consists of the honey pot service ,the HIDS-manager(hidsmgr), the honeypot monitor(monitor)and the host intrusion detection system (HIDS). Honey pot service, monitor and HIDS manager run in user space, However the HIDS is located in the kernel space.

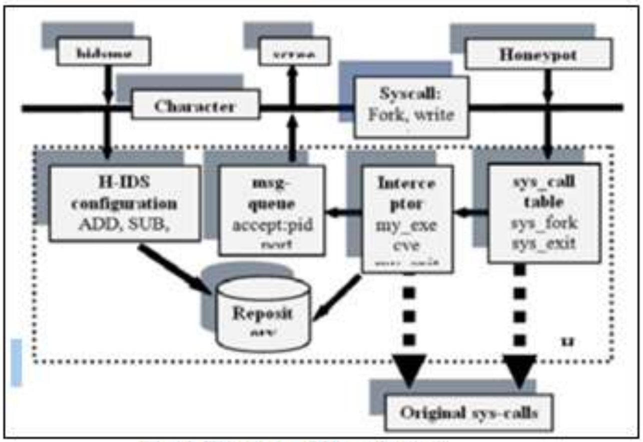

Fig.3:HoneypotClient System

Generally, most commonly used operating systems make a individual differentiation between application and operating system. Every time a user space process will require an operating system Service(e.g. the process of opening of a network socket) the service must be able to respond by sending a system call to the kernel. Kernel tests the request of the process and then it makes a decision whether to fulfill it by inserting a HIDS into kernel space and by redirecting the system-calls to the HIDS, it is possible to extend the functionality of the kernel. In this case it's also possible to observe simply on the basis of system-call level what a process in user- space actually does. And it is possible to introduce more detailed decision criteria in the Kernel to determine whether the desired action is allowed or not(a same type mechanism has also been addressed for performing access control on active networking node

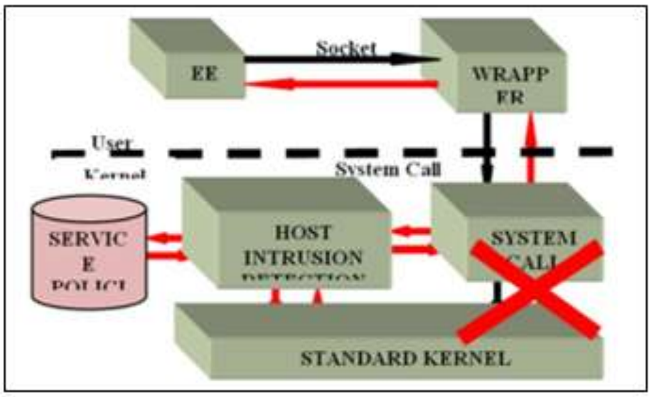

Fig.4:Interception ofa SystemCall

The Logging Proxy

Logging proxy looks for connection requests to the honeypot service which originate from a potential hacker. Other side proxy server acts itself as a client on behalf of the user or attacker and forwards the request (using its own IP address) to the honeypot services. This forwarding, the proxy server also creates an individual log file for each forwarded session(session ID)in addition and also contains the IP address of the attacker, ports and a time stamp. For attacker, the proxy server is invisible and all the honeypot service requests or back responses appear to be directly from the proxy host. The proxy logs the connection data of the honey-pot service. Main task is to match attack session and PID of the corresponding process on the honey pot host which is a difficult task. Reason behind this difficulty is that one host keeps the logs while the other one detects heat tacks. In case a new client connection is initiated by an attacker then proxy sends the new session ID via the control channel for monitoring the honey pot. Thus one gets acknowledgement of successful connection of the proxy to the honeypot service. A message to the proxy server is send which contains the PID of the corresponding child process and the ports of the incoming connection. These ports are used to track which connection and session ID belong together. Proxy server have one advantage that it maintains a list of currently established connections to the honeypot service. On a fork of the honeypot service anew PID message is automatically sent by the honeypot service monitor to the proxy server. On condition when process tries to execute a series of an unauthorized system-calls (attack signature)then honeypot monitor triggers an alert and sends a corresponding message to the proxy server. This alert message contains the PID of the honeypot service process which violated the security policy. This alert message of proxy server tags the corresponding session and adds the alert information to the proper log file.

3.4 Response Module

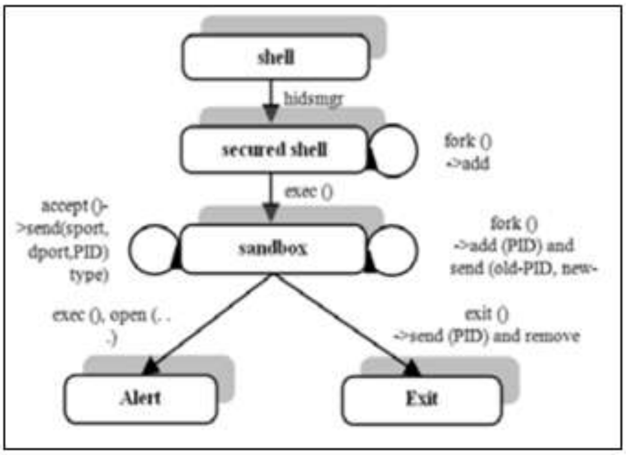

Fig. 5:ProcessID (PID) Tracking

Response module is designed as part of the invasion and track record of the source part of the invasion. This Tracking technology helps to track and allows the use of reverse invasion intruder to determine the source IP. If any host detects suspicious invasion, it will be redirected to the honeypot system, by the honey pot system monitor and record all information and suspicious behavior, the Mobile Agent login to the router from the victim host recently to monitor the router packet to determine the direction of migration to continue. Reverse tracking refers to the detected attack, attack path from the end of the actual attack path along the opposite direction back to the source of the attack. Until you reach the best track was the source, reconstruct attack path, to determine the source of the attack.

Rule base complements the process of providing the description of the role of the user whilst using the system of normal and abnormal behavior or describing the used system defects and other known methods of intrusion attack mode. Intrusion detection system improves the Performance, while preserving the rule base(abnormal and normal rules),so that one can match with the exception rules to determine a more accurate intrusion. At same instant, by comparison with the normal rules, we can determine the unknown intrusions. Honeypot system when used for determining the behavior of an unknown event for the invasion of the rules will be updated after a data base intrusion detection system in order to achieve self-learning.

4. CONCLUSION

The vast expansion of computer networks makes it very difficult to detect intruders and keep them at bay. The honey pot technology combined with intrusion detection systems can help provide a complimentary level to the defense system. Also to further reduce the complexities of dealing with an intrusion detection system, dynamic honey pot technology can be further improved and developed and has immense future scope.

5. REFERENCES

[1] Verword T,HuntR.,"Intrusion detection techniques and approaches", Transaction on Computer Communication, pp. 1356-1365, 2012.

[2] A.Hess,G.Schafer, "Realizing a flexible access control mechanism for active nodes based on active networking technology", In IEEE International Conference on Communications (ICC 2004), Paris, France, June 2014.

[3] Tao Wenlin,"VMware-based virtual honey net System", transaction on Computer Application and Software ,pp. 131-136, 2014.

[4] MukkamalaS,Sung Ah,Abraham,"Intrusion detection using all ensemble of intelligent paradigms", Journal of Network and Computer Application,2015, pp. 167-182.

[5] Zhang Chao, "Honey net and intrusion detection and firewall linkage techniques", Technology market economy, pp. 42-44,2007.

[6] Zheng Jun jie, Xiao Jun mold, LiuZhihua, "Based on Honey pot technology and network intrusion detection system", University of Electronic Science and Technology, pp. 257-25, 2013.

[7] Ji giang Zhai,Yining Xie,"research on network intrusion prevention system based on Snort", IEEE, in international forum on strategic technology (IFOST),Vol.2, pp.1133-1136, Aug2011.