International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

JAVA Based Honeypot: Intrusion Detection System

Nilesh Kakade[1], Mayur Shinde[2], Akshay Gawali[3], Ajinkya Bhoite[4]

[1,2,3,4] *Dept. of Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India*

Abstract – *Network Security is one of important concept related to network. A Honeypot is a system which helps in providing a network security. It traps attack, and record intrusion information. We implement a Java based Honeypot, which detects the malicious activity of non authenticated user. This is done by log capture and log analysis. It also prevents the attacks. The proposed system has the feature to blacklist the attackers IP address in order to avoid future attacks from same IP address. System includes detection and prevention of various types of attacks. This makes the Network Security stronger. We implement a mechanism to prevent Ransomware attack.*

Key Words: Honeypot, Intrusion, Log analysis, Log capture, Network Security, Ransomware.

1. INTRODUCTION

The threads of Internet attack is the big disadvantage of internet. That is why, there is a need of such technology which will make the network secured. The need of Honeypot arises due to Security Threads. The traditional System are not able to provide security against newly develop attacks. Day by day new attacks are being develop. So any system is not 100% efficient . The System need to be updated to defend newly develop attacks. Recently a new attack called as "Ransomware" got much popular. It affected more than 2,00,000 Organization in 150 Countries. It takes the control of computer System and block the access to System. Ransomware demands payment after launching cyber attack . It is difficult to identify the Hacker but attack can be prevented. There are various tools for intrusion prevention but none of the tool was able to detect and prevent Ransomware .

Honeypot is new security Technology for intrusion detection and prevention. It is unique for a reasons , it does not fix a specific problem. Instead, they are a highly flexible tool which contain many application for security, from preventing attacks, to detect malicious or unauthorized activity and to gather hackers Information[2]. There are various terms related to honeypot which will discuss in this part.

The amount of activity perform by attacker with honeypot is called Interaction level [1]. The different types of Honeypots are, Low Interaction Honeypot and High Interaction Honeypot [1]. Low interaction honeypot captures only small information related to Hackers. Minimum interaction is provided between the System and the hacker. In low interaction honeypot, the attacker is not allow to access whole Real Operating System. High level interaction honeypot interacts maximum with the attacker. The attacker is given the access to real operating system. So, as to capture more information about hacker .

Previous Honeypot were written in C language and they were built for only UNIX platforms [3]. The Java based Honeypot overcome this above limitation . they are platform independent can run on multiple platform . Honeypot uses two type of detection methods, signature based detection and Rule based detection and Statistical anomaly detection. In signature based it looks for specific patterns , such as byte sequences in network traffic. These patters are pre-defined patterns which differentiate between a legitimate users activity and hackers activity. In Statistical anomaly detection statistics are formed from logs to detect anomalies from normal user behavior. Most systems rely on learning about past behavior of users. Analysis of logs over time determine what is behavior normal of users. Any deviations in behavior generate alerts. Another approach is rule-based anomaly detection. In this , the system analyzes data from logs and automatically develops a set of rules to describe normal behavior. Rule-based anomaly detection relies on the rules generated from previous statistics. So data about each new event is tested against the rules to see whether it is normal. A large database of rules is needed for rule-based anomaly systems to work well.

2. RELATED WORK

The introduction section gives the brief information about Honeypots . This section will explain about the related work done. Also address the various technique used in the field. Previous a low interaction honeypot develop by Niels Provos which was written in C language [3]. This system was only for UNIX platform . It was not capable for monitoring and intrusion detection. So , a J-Honeypot[3] was develop which was platform independent , supports multiple platforms. A rule based intrusion detection engine is used by J-honeypot. It works by the analysis of real world attack data. J-Honeypot includes a web based monitoring tool which help network administrators to understand network traffic and possible attacks. To improve the significance of recorded events and to analyze network traffic by a network security operator can be obtain by combining three main components: 1. a packet filter, 2. a proxy host and 3. A honeypot host. Session individual logging of network traffic is perform by proxy host . Honeypot host executes network services. For any detection of suspicious behavior it reports back to proxy host [4]. In [6] ,the author explains the

concept of electronic deploy. Honeypots are the electronic baits. Sebek [7] is the data capturing tool. This tool is used to capture the unauthorized activity on honeypot . The paper [1] propose a use of virtualization technique. The existing security problems are overcome. Existing problem was that only single network detection was possible . But due to use of virtualization technique, network across organization detection was possible . Due to many virtual systems ,lot of time of attacker was wasted. This result in obtaining more information about the attacker. Honeynet , Honeyd and Honeypots are the three concepts used in this approach. The Honeyd has the capability to interact with the attacker, that is the reason Address Resolution Protocol Daemon (ARPD) is required. ARPD detects the one who is requesting to interact with non existent host . The author et al. [8] propose two algorithms for the improvement of system. First one is Honeypot Redirect Inbound (HRI). Second one is Honeypot Redirect Outbound (HRO) algorithm. This gives the advantage as higher flexibility and usability. Depending upon the need each module can be customization of each module can be done. [2] Adding to this , a system which is used to identify the black hats. It also record their activities like when they break in and what is their motive . For achieving this it uses the mechanism like Data control , Data capture , Data Duplication mechanism.

3. IMPLEMENTATION

Implementation

The figure illustrate the Java based Honeypot Architecture. Graphical User Interface is provided. This makes easier to perform action and to view the events that occurred to honeypot. There are various module in the proposed system.

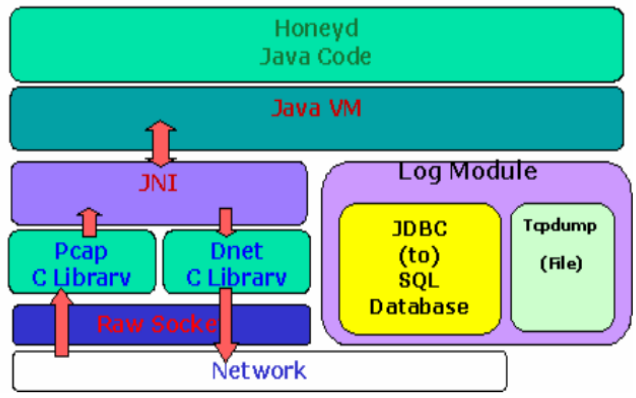

Fig 3.1 Honeypot Architecture

Log Capture: Log Capture module collects and records the activity. The tools like snort and sebek are used to capture data. While performing this activity the attacker does not know that they are being watched. The captured data is stored in database for analysis purpose. Only the necessary information is stored , not everything. The attackers activity may be in encrypted form , but this is also being captured.

Log Analysis : In Log Analysis , the captured data is analyzed ,so as to determine whether the activity is malicious or not. Various types of attacks can happen. For ever attack different detection methodology is used. There are various signature use for detecting a attack.

In case of DOS attack, the TCP port number 80 is use for the attack. Port 80 gets lots of request. The messages like GetRequest, GetNextRequest, SetRequest are some of the signatures. Through this the denial of service takes the control of system.

Blacklist : This will contain the information related to malicious users. The users who try get access of the system or carried out some unauthorized activity are blacklisted. This means , the IP address of these users will get blocked and stored in blacklist database.

HoneySMB : SMB services are emulated by this honeypot, in which data can be share with other devices and log every activity of hacker. SMB provides a logging less entry to the users . SMB protocol provides 3 workgroup : TMP, TPC, DEMO. There are some dummy files shared in this group. All the information will be stored in the .pcap file.

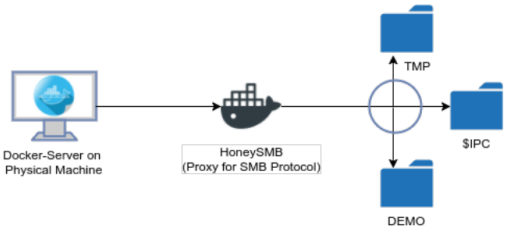

Fig 3.2 Design of HoneySMB

HoneyWeb-Sqli : This is a system for http protocol. HoneyWEB-Sqli is system in which SQL injection vulnerability are exposed, So as to analyse the attacker and its methods used to attack on SQL Database. Firstly it create clone of the website to mount volume of Docker-compose for static serving. Now it adds dummy logging page. This dummy page is connected to the fake SQL database. But this fake database also has capabilities of logging all quires fired by dummy page. The post Docker compose 80 is mapped with actual system's port 80. The fig. 3.3 illustrate design of HoneyWeb-Sqli

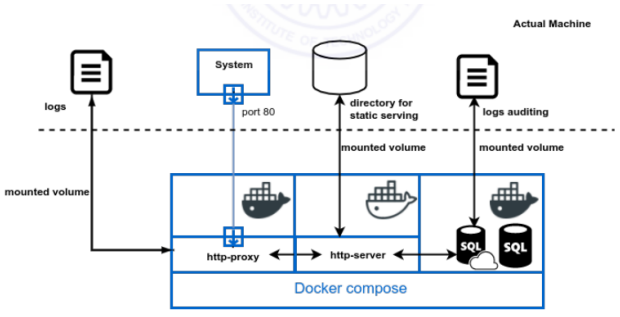

Fig 3.3 Design of HoneyWEB-SQLi

Ransomware detection and prevention:

This is system designed to analyse and detect the attackers activity for Ransomware attack. . Ransomware takes the control of computer System and block the access to System and demand for ransome. The Ransomware uses a cryptography techniques to encrypt the files. There are two types of encryption scheme mostly used , CryptoLocker and CryptoWall. Once the file is encrypted using these technique then it is impossible to decrypt without the key. For decryption victim has to pay for ransome. Some of the methods can be used for detection.

Firstly approach can be, the user behaviour analysis[9], to keep track of normal activity. When abnormal activity happens like ,in short time thousands of file gets modified, an alert to the administrator should be send that some unusual activity has occurred. This can immediately detect the attack and attack can be prevented.

Second approach is, cross the network some key files can be placed, and can be monitor for a change [9]. The service is stopped if the file is tampered i.e. undergo some change.

Experiment performed by [9], is illustrate in fig 3.4

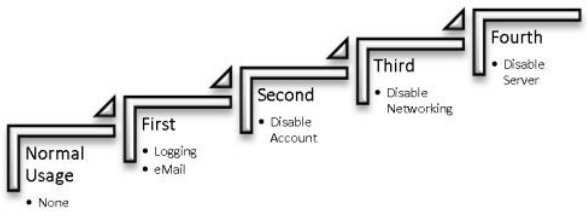

Fig 3.4 Tried response to detection

1.First

When change is found it triggered. It email the system administrator about the modification in folder.

2. Second

It is triggered when even more of the activity has been encountered. In this level the username and related information of the malware is determined. When this information the user can disable their account.

3. Third

The Network services are stopped in this level.

4. Fourth

This level is triggered when the activity is not been stop even after disabling account. So the last option left is to stop server. To stop the damage, server is shutdown.

4. CONCLUSION

In this paper we have approach a java based honeypot. This tool is capable of detection and preventing the attacks. Ransomware is the area which was focused more while implementation. We provided a convenient GUI, which makes operating honeypot easier.

ACKNOWLEDGEMENT

Thanks to prof. Rohini Agawane, Savitribai Phule Pune University for encouragement on developing this paper.

REFERENCES

[1] Janardhan Reddy Kondra Santosh Kumar Bharti, Sambit Kumar Mishra, Korra Sattya Babu, "Honey Based Intrusion Detection System: A Performance analysis ," 2016 IEEE.

[2] V.Maheswari and P.E. Sankaranarayanan, Defeating Hackers Through a Java Baased Honeypot Deployment. Information Technology Journal 6(7):1080-1084,2007.

[3] Yuqing Mai , Radhika Upadrashta and Xia Su "J-Honeypot: A Java-Based Network Deception Tool with Monitoring and Intrusion Detection ," 2004 IEEE.

[4] P. Diebold, A. Hess, G. Schafer, "A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks ,"In Proc. Of 14th kommunikation in Verteilten Systemen 2005, Kaiserslautern, Germany, February 2005.

[5] T. Holz , F. Raynal, "Detecting honeypots and other suspicious environment, in:" Procceding from the sistth Annual IEEE SMC Information Assurance Workshop, 2005.IAW '05.,2005,pp.29-36.

[6] "Sebek." Internet: http://honeynet . org/papers/honeynet/ tools/sabek/, 2004.

[7] A. Herrero, U. Zurutuza, E. Corchado, A Neural-Visualization IDS for Honeypot Data, International Journal of Neural System, 22(2012).

[8] Chris Moore ,"Detecting Ransomware with Honeypot techniques, " 2016 Cybersecurity and Cyberforensics Conference .