International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

INTRUSION DETECTION USING RASPBERRY PI HONEYPOT (SNORT) FOR NETWORK SECURITY

E. Bharathi[1], M. Keerthana[2], G. Ramsundar[3]

[1]E. Bharathi, Dept of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore.
[2]M. Keerthana, Dept of Computer Science and Engineering and technology, KPR Institute of Engineering and Technology, Coimbatore.
[3]G. Ramsundar asst. Prof, Dept of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore.

Abstract - In the present world, communication through network has raised and it is easier to transfer information over network but security has become the major issue. To strengthen network security and to improve network activity, the security applications like intrusion detection are used. Intrusion detection is a technology used to detect unauthorized intrusion into computer network or system. In this technology honeypot is implemented using snort tool, which creates confusion for attackers by providing bogus data. The properly designed and configured Honey Pot provides data such as the IP address, attracts the attackers for entering the system and behavior of those attacker can be monitored. Honeypot along with raspberry pi makes network security strong and easy to implement, cost efficient. How the data is attacked, attacker's activity and further improvement in network security are explained.

***Key Words*: Raspberry pi, honeypot, network security, Intrusion detection.**

1. INTRODUCTION:

Computer security have several security related objectives among them the three fundamental objective are: Secrecy i.e. to protect information; Incorruptibility, to protect information accuracy; lastly Access, to ensure information delivery. It is necessary to put high priority to system security, minimize loop holes and secure the computer system against intrusion. The standard form of implementing security is firewalls along with intrusion detection system. A intruder is a hacker whose intensions are to cause harm or mischief. The intruder can be classified into two types, one who has something to gain by the intrusion and the other a curious person trying to probe the security of the system. The first type is popularly termed as a "cracker". Crackers attack websites or database servers in an attempt to gain critical information such as credit card or social security information. Second type is "hacker". A Hacker is a person with intelligent computer knowledgeable person. The aim of this intruder is to compromise as many systems as possible. The intruder is aided by the easy-to-use tools that scan a range of IP addresses looking for a vulnerable computer. One of the defense mechanism that has come to the fore are Honeypots. Honey pot acts as a Booby trap equipment which are configured as a system weakness to attract intruders and gather all the information to eliminate future attacks. The proposed architecture is based on Raspberry Pi-Honeypot using already existing tools and methods like Snort. This security system will be using IDS combination with Raspberry pi-honeypot, which is simple to implement and cost efficient.

2. INTRUSION DETECTION:

Intrusion detection system is a security based application for networks and computer system. There are two types of IDS available. They are host based intrusion detection system(HIDS) and Network based intrusion detection system(NIDS). HIDS is a intrusion detection system which scans for host related system activities. NIDS is a intrusion detection system which scans all the packets in the network and detect the unauthorized activity into network.

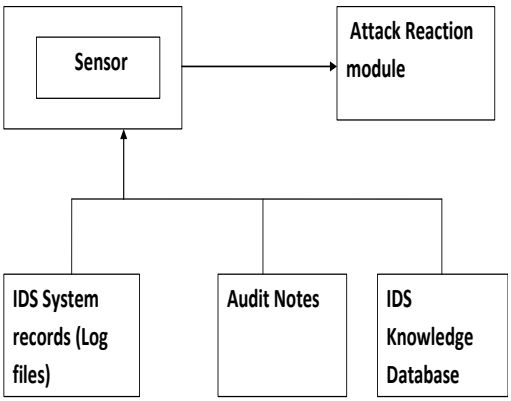

Fig -1: Intrusion detection

2.1 TOOLS USED FOR INTRUSION DETECTION:

Snort is based on libpcap (for library packet capture) a tool used in TCP/IP traffic sniffers and analysers. Snort also combines abnormal behaviour detection signatures and different methods of protocol detection. Snort is a network intrusion detection system (NIDS), a packet sniffer that

captures and scans network traffic in real time, examining each packet closely to detect an intrusion.

3. HONEYPOT:

Honeypots are an addition to your traditional internet security systems; they are an addition to your network security systems.Honeypots can be setup inside or outside of a firewall design or any strategic location within a network. In a sense, they are variants of standard Intrusion Detection Systems (IDS) but with more of a focus on information gathering and deception. The main goal of this system is to gather as much data as possible in a manner that will protect the system and network from future attacks.

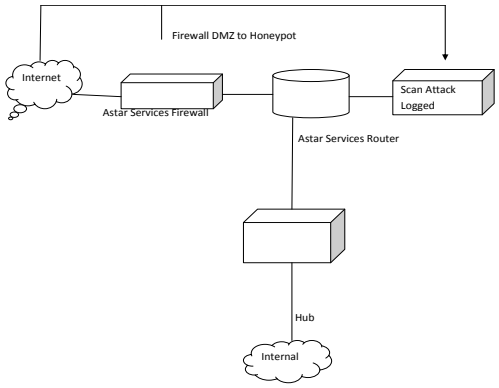

Fig -2:Honeypot

3.1 TYPES:

- Research honeypot
- Production honeypot

3.2 LEVEL OF INTERACTION:

- **Low interaction level honeypot:**

  Low interaction level honeypot does not contain a real time system. They are utilised for gathering information thus low interaction honeypots cannot be used to utalize the full potential of a honeypot. These type of honeypots are easy to deploy and maintain.Honeyd is a type of low interaction level honeypot.

- **Medium interaction level honeypot:**

  Medium interaction level honey pots give an illusion of false operating system with which the attacker can communicate. Thus capturing all the attackers activities.Honeytrap is a type of medium action Honeypot.

- **High interaction level honeypot:**

  High interaction level honey pots are the most advanced honeypots, but are complex and difficult to setup. These type of honeypots have their own OS. Thus the risk of deploying is high. Honeynet is an example of this type of honeypot. It is a combination of decoys all working as one with different interaction level.

3.3 PROS AND CONS OF RASPBERRY PI-HONEYPOT:

- Easy to implement
- Cost efficiency
- Data integrity

4. RASPBERRY PI:

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse.The Raspberry Pi has the ability to interact with the outside world; it plugs into a computer monitor or TV anduses a standard keyboard and mouse. Programming languages like Scratch and Python are used. Low power consumption with headless setup. Pi can simply turn into a powerful Honeypot or attack detector.

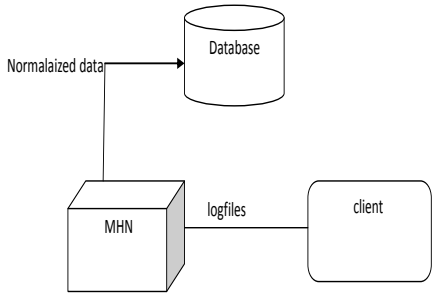

Fig-4.1: Client side architecture:

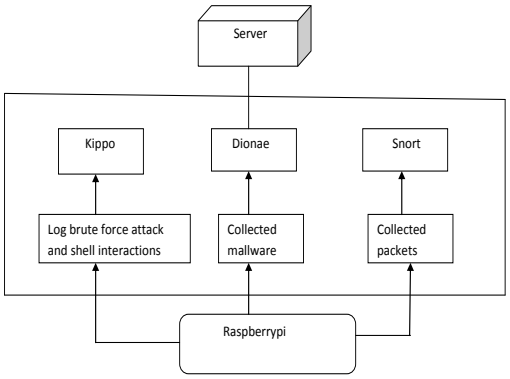

Fig-4.2: Server side architecture:

5. INTRUSION DETECTION USING RASPBERRY PI-HONEYPOT:

The Architecture deals with implementing a Raspberry Pi-Honeypot with Snort IDS. Thus a solution to minimize failures in detection process and collection of important data based on honeypot consists of combining security tools: Snort IDS.

Raspberry pi honeypot is implemention as client-server architecture.It has a central main server interacting with multiple clients in the network.

This proposed Honeypot is developed as a separate device (Raspberry Pi) physically present in the network. It will be deployed with Dionaea or Glastopf or Kippo which will collect all the data and send it to the server. Raspberry Pi-Honeypots can merge in any environment making them more difficult to identify and reveal. Deployment of multiple Raspberry Pi-Honeypots are easy and affordable.

6. CONCLUSIONS:

The usage of Raspberry Pi-Honeypot as a decoy in the network represents a simple and an efficient solution for enhancing network security using raspberry pi and open source tools.

Deployment and management of raspberry pi as a honeypot is cost effective and also provides easy integration.

This mechanism combines the security tools in order to minimize the disadvantages and maximize the security capabilities in the process of securing the network.

7. REFERENCE:

[1]L. Spitzner, The value of Honeypots, Part One: Definitions and value of Honeypots, Security Focus.

[2] Liberios Vokorokos, Peter Fanfara, Ján Radusovský and Peter Poór,Sophisticated Honeypot Mechanism - the Autonomous Hybrid Solution for Enhancing Computer System Security, SAMI 2013 IEEE 11th International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia.

[3] Article Title: http://www.snort.org

[4] Esmaeil Kheirkhah, Sayyed Mehdi Poustchi Amin, Hediyeh Amir Jahanshahi Sistani, Haridas Acharya,An Experimental Study of SSH Attacks by using Honeypot Decoys,Indian Journal of Science and Technology.

[5]ArticleTitle: http:/www.raspberrypi.org/help/what-is-a-raspberry-pi/.

[6] Jian Bao and Chang-peng Ji, and Mo Gao, "Research on network security of defense based on Honeypot", IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302.

[7] Chao-Hsi Yeh and Chung-Huang Yang, "Design and Implementation of Honeypot Systems Based on Open-Source Software", IEEE International Conference on Intelligence and Security Informatics (ISI), 265-266.

[8] Anjali Sardana, R. C. Joshi, "Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level", IEEE International Symposiums on Information Processing (ISIP), pp. 505-509.

[9] Yaser Alosefer and Omer Rana, "Honeyware: a web-based low interaction client honeypot", Third IEEE International Conference on Software Testing, Verification, and Validation Workshops (ICSTW), pp. 410 – 417.