Survey: Raspberry PI Techniques and Applications

Harshal R. Khairnar[1],Yogita P. Shewale[2]
Departement of Information Technology[1], Departement of Information Technology[2,] MET ,Nashik[1]
,SNJB's KBJ COE[2],Chandwad,Savitribai Phule Pune University, India[1,2]

Abstract
In Recent Trend and fast data communication , Peoples uses and need larg volume data and fast internet speed,inexpensive Internet connection and fast paced software development, security has become more and more of an issue. Security is one of the basic requirements in today's world as any type of interaction and storage of data on the internet is becoming unassertive. Protecting the information access and data integrity are the basic security characteristics of computer security. A decoy based technology, Honeypot along with a Raspberry Pi makes network security cost effective and easy to implement. This paper is devoted to implement a Raspberry Pi based C in a network that will attract attackers by simulating vulnerabilities and poor security. Honeypot will record all the attackers' activities an d after data analysis not only displays the type of attack but allow improvements in security of the network.
***IndexTerms* -** Communication, Security, Information, Honeypot, Raspberry Pi, Data Analysis, Security, Network

I.Introduction

Information is strategic resource, organizations spend a significant amount of their budget on managing information resources. 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. Today's standard of security implement a configured firewall along with an intrusion detection system. If an intruder is able to acquire a weakness in the network by scanning the host network, he can easy penetrate into the system and obtain valuable data. If an intruder is masking his identity for a firewall enabled service, intrusion detection systems cannot minimize the damages.

Most of the security approaches now a day's focus on defense rather than aggressive form of a security. One of the aggressive for of defense mechanism that has come to the fore are Honeypots. It 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 thus eliminating security loop holes, these are known as Honeypots. For example honeypots like Honeyd[1] are already being used to detect attackers and protect information

The proposed architecture is based on Raspberry Pi-Honeypot using already existing tools and methods like Snort [3], Modern Honeypot Network (MHN) [4], Kippo[5], Dionaea[6],Glastopf[7].This architecture puts forth a simple, cost effective and an autonomous deployment in any

Most of the security approaches now a day's focus on defense rather than aggressive form of a security. One of the aggressive for of defense mechanism that has come to the fore are Honeypots. It 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 thus eliminating security loop holes, these are known as Honeypots. For example honeypots like Honeyd[1] are already being used to detect attackers and protect information.

The proposed architecture is based on Raspberry Pi-Honeypot using already existing tools and methods like Snort [3], Modern Honeypot Network (MHN) [4], Kippo[5], Dionaea[6], Glastopf[7].This architecture puts forth a simple, cost effective and an autonomous deployment in any environment.Subsequent chapters contain a description of the security system using IDS in combination with Raspberry Pi Honeypot.

II Intrusion Detection System

IDS is a security application for computers and networks that gather and analyze information by scanning all the inbound and outbound network activities and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

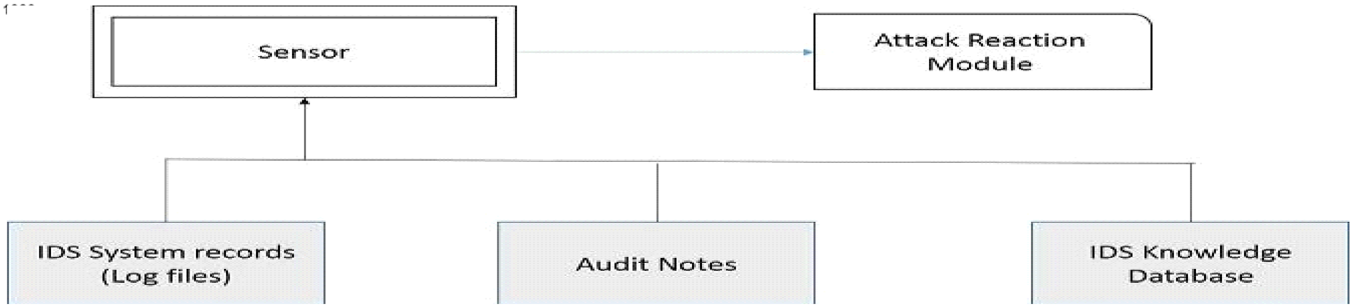

Figure 1 Intrusion Detection System

IDS Classification

- Host-based IDS(HIDS) :

  The HIDS is an IDS that is on the host machine and scans the host system for activities. It is deployed usually on a single machine.

- Network-based IDS(NIDS) :

It scans all the packets in a network and detects unauthorised access or intruders in a particular network

- Hybrid IDS :

The hybrid intrusion detection system combine's both host based and network based IDS to examine all data packets in a network Some of the methods of intrusion detection are:

- Anomaly detection: detects patterns, which are contrary to standard behavior.
- Misuse detection: identifies and compares user's activities with recorded attack patterns.
- Hybrid mode detection: a combination of anomaly and misuse detection, this method significantly reduces producing false positive or false negatives.

2.2 Tools for Detecting Intrusions

Snort is a versatile and an open source tool used for intrusion detection. It 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. 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.

Observing vindictive exercises in PC frameworks is perplexing and costly. Using a Raspberry Pi in a network makes the network administrators work less complex and easy to implement. Described form of protection provides use of advanced security method called Honeypot along with a Raspberry Pi.

3. Honeypot

Honeypot are a decoy system setup to gather information regarding an attacker or intruder into your system. 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.

Honeypots are deployed on an unused IP address which is monitored by the administrator. This decoy system is waiting for attackers to start an interaction with the system. Any type of interaction with the honeypot is considered suspicious.

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 and thus remove any computer as well as network security loop holes.

3.1. Honeypot types:

3.1.1 Purpose Honeypot

These are specific to the area of deployment[8].

- *Research Honeypot*

  Research honepots are difficult to deploy and maintain. Their sole purpose is to extract information about intruders, attackers their methods and tools.

- Production Honeypot:

  Production honeypot these are designed for directly enhancing system protection. They provide real time security by slowing down an attack on real system targets.

3.1.2 Level Of Interaction

Honeypots are categorized into three types depending upon the level of interaction[9].

- **Low-interaction Honeypot**:

This type of 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[10] is a type of low interaction Honeypot..

- **Medium-interaction Honeypot:**

These type of Honeypots give an illusion of a false operating system with which the attacker can communicate. Thus capturing all the attackers activities. Honeytrap is a type of medium action Honeypot.

- **High-level of interaction Honeypot**:

These 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[11].

3.1.3 Hybrid Honeypot

Monitoring malicious activities in computer systems is complex and expensive. Using a Raspberry Pi in a network makes the network administrators work less complex and easy to implement. Described form of protection provides use of advanced security method called Honeypot along with a Raspberry Pi.

Table 1
Difference between Honeypot and Raspberry Pi Honeypot

Honeypot	Raspberry PI- Honeypot
Expensive	Relatively Cheap
Difficult to implement and	Easy to implement and setup
setup	
Not easily available	Easily available
Not autonomous	Autonomous

3.2 Raspberry Pi-Honeypot Advantages and Disadvantages

Using the Raspberry Pi-Honeypot has some significant advantages:

- Cost Effective: As Raspberry Pi are very cheap and easily available, also setting up a Raspberry Pi is very easy. Hence setting up a Raspberry Pi-Honeypot in a network becomes easy.

- Simple – Honeypots do not require any complex operation or algorithm for deployment. They are flexible.

- Record new tactics – they capture all interaction with the intruder and discover new tactics.

- Data – They produce high quality data. Honeypot technology also has its drawbacks [12] :

- Gain control: attacker can gain control of a honeypot and retrieve all the information.

- Divulge identity – An experienced attacker can detect presence of incorrectly configured system acting as a decoy.

- **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 and uses a standard keyboard and mouse. It uses programming language like Scratch and Python. Low power consumption with headless setup. It can simply turn into a powerful Honeypot or attack detector.

- **Usage of Raspberry Pi-Honeypot with an Intrusion Detection System**

Proposed 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 , Modern Honeypot Network, Kippo, Dionaea, Glastopf . This detection mechanism based on Raspberry Pi-Honeypot is implemented as a client server architecture. It has a central main sever interacting with multiple clients in the network.

Client work station serve to capture suspicious activities or directly record the malicious code which is then sent to server for processing. Server analyses received data decides to issue or not to issue a security warning and display cumulative information through a web interface.

5.1 Server Architecture

Due to centralization of collected data the server is connected to multiple clients and is set to receive all incoming messages which are stored in knowledge database. The proposed server architecture consists of:

- Modern Honeypot Network (MHN): you can observe and control the honeypot from a central location.

- Verification Process: receive the amount of data from client and integrates diversified data formats.

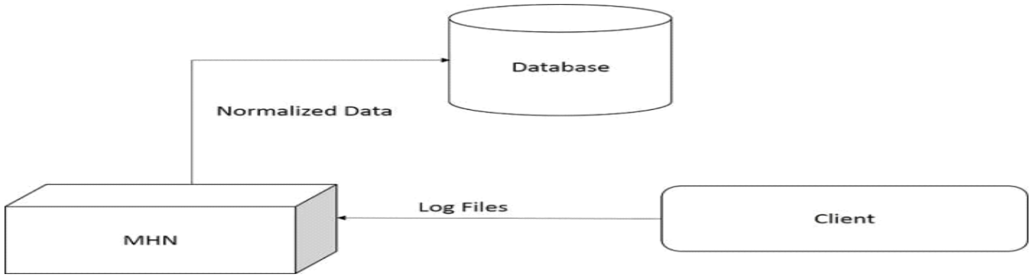

Figure 2 Server Side Architecture

5.2 Client Architecture

This architecture consists of Raspberry Pi-Honeypot which captures all the attackers' activities .The data is delivered to the server for further analysis and updating network security.

Client architecture consists of:

- Kippo: it is a SSH Honeypot tool written in python that will log brute force attacks and shell interaction performed by the attacker.
- Dionaea: will capture the patter malware by simulating basic system services and vulnerabilities.
- Glastopf: it is a web application Honeypot, it gathers data by emulating thousands of vulnerabilities. Unlike many other honeypots, Glastopf focuses on replying the correct response to the attacker exploiting the targeted Web application, and not the specific vulnerability.
- Snort: Intrusion detection system that monitor's and filter packets during detecting intrusion.

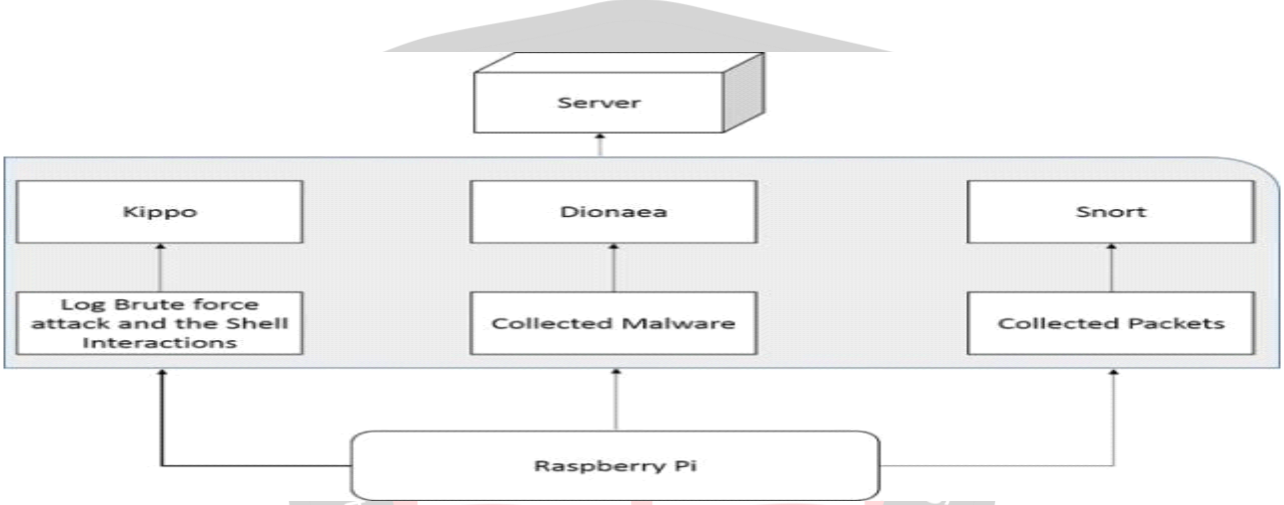

Figure 3
Client Side Architecture

- **Raspberry Pi-Honeypot**

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.

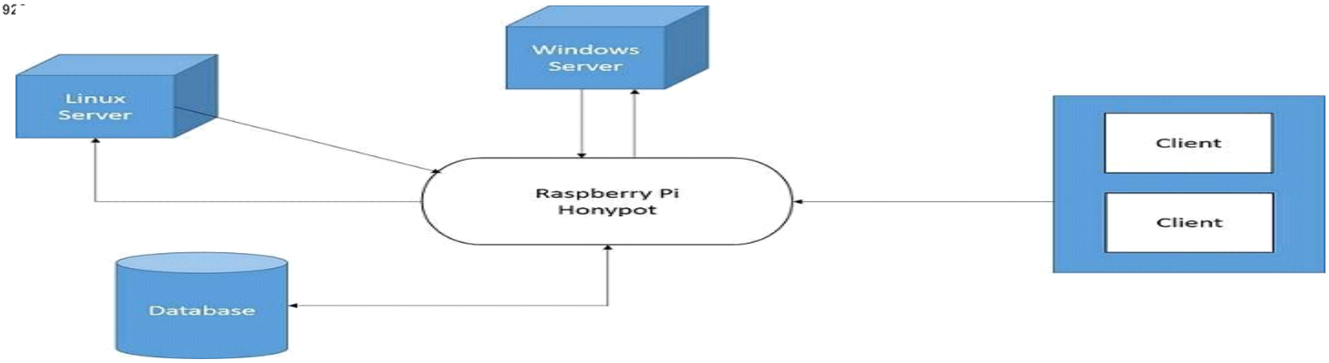

Figure 4
Raspberry Pi-Honeypot Deployment Diagram

- **Conclusion**

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.

The apport of this work is to introduce a new and cost effective mechanism for network security. This mechanism combines the security tools in order to minimize the disadvantages and maximize the security capabilities in the process of securing the network.

REFERENCES

[1]LiberiosVokorokos, Peter Fanfara, JánRadusovský 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, January 31 - February 2, 2013, Herl'any, Slovakia.

[2]R. Chandran, S. Pakala, Simulating Network with Honeyd, Technical Paper, Paladion Networks, December 2003.

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

[4]Article Title: https://www.zeltser.com/mpdernhoneynetworkexperime nts/

[5]Article Title: http://bob.k6rtm.net/kippo.html

[6]Dankova et al.,An Anomaly-Based Intrusion Detection System, Electrical Engineering and Informatics 2,Kosice,ISBN 978-80-553-0611-7,2011.

[7]Article Title: http:/www.glastopf.org/

[8]Kareem Sumner ,Honeypots Security on Offense, Security Architecture 774.716,July 10, 2002.

[9]EsmaeilKheirkhah, Sayyed Mehdi Poustchi Amin, Hediyeh Amir Jahanshahi Sistani, HaridasAcharya,An Experimental Study of SSH Attacks by using Honeypot Decoys,Indian Journal of Science and Technology, December 2003, 6(12),Doi no:10.17485/ijst/2013/v6i12/43618

[10]L. Spitzner, Honeypots: Tracking Hackers, Boston, USA: Addison- Weasley, Parson Education, ISBN 0-321-10895-7, 2003.

[11]L. Spitzner, The value of Honeypots, Part One: Definitions and value of Honeypots, Security Focus, 2001.