International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Implementation Of Securing Iot Networks Using Honeypot Mechanism For Embedded Applications

K. Sita, M.Tech- Student,
Vignan's Lara Institute of Technology and Science,
India

Mr.K.Vijaya Vardhan, M.tech
Assistant Professor, Vignan's Lara Institute of Technology and Science,
India

ABSTRACT: In the modern day, most of the enterprises have decided to move their services to a web based system which is more convenient and easily accessible to all the customers. With the advent of Internet of Things, several thousand more devices transmit data through the internet to perform various tasks that optimize our issues. These devices can provide a possible security loophole for unauthorized or illegal access. 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 Honeypot in a network that will attract attackers by simulating vulnerabilities and poor security. Honeypot will record all the attackers' activities and it blocks certain privileges after data analysis not only displays the type of attack but it allow improvements in security , it blocks the IP address of the attacker and it sends a alert notification to admin of the network.

Keywords: Communication, Security, Information, Honeypot, Raspberry Pi, Data Analysis, Security, Network

I.INTRODUCTION

In the rapidly advancing world of technology, we are dynamically evolving to efficiently improve our day to day lives by innovating around our handheld devices and utilize the internet to facilitate the same. One of the most important emerging trends and the way forward in the future of technology is the Internet of Things where we have several devices that can communicate with each other by transmitting data over a network. This communication by these peripheral devices over the network offer an access point for the attacker to target and exploit the loophole in the network, resulting in them gaining access to these devices and open up an intrusion pathway into the network and obtain access to the data and information present on the network.

In order to secure our networks from this possible security loophole when all households adapt to the concept and trend of internet of things, the suggested method or mechanism to tackle the threat would be to create a facility to secure the peripheral devices (Raspberry Pi or Arduino) like our conventional Personal computers have inbuilt defense systems. This will ensure end to end security for our networks. An attack

on the web sites of the US government [6] also indicate that none of the systems can be totally secure and thus a considerable amount of work needs to be done in development of a model that is efficient in capturing the trends followed by the attackers and ways to predict attacks based on these trends.

Increasing security of honeypot has been substantially subject of research during the past years [1][4].A honeypot is a network decoy system under strict surveillance [2], which attracts attacks by genuine or virtual network and services. honeypot is a source of information that is usually designed with the aim of detecting and trapping any attempt to penetrate into an experimental system [8].

The system is made to appear exactly the same as the main system to be protected, so that when there is a penetration then it would seem to the attacker that he/she has managed to get into the system, when in fact the attacker has entered a trap [3].However, all actions, tools, and techniques used in the attack have been recorded for study by the System Administrator concerned through the data and information presented by the honeypot [9]. The purpose of the high-involvement honeypot is to provide access to a real operating system to attack where there is no limit set [10].

A. Intrusion Detection System: Intrusion Detection System[5] IDS is a security application for computers and networks that gather and analyze information by scanning all the inbound and outbound activities of network and the patterns are recognized which may define a network or system attack. In addition, IDS capability is limited to knowing the incoming attacks in the form of alerts, in the absence of follow-up [7].

B. IDS Classification Host-based IDS (HIDS): The HIDS is aIDS that is on the host machine and scans the host system for activities. It is established usually on a single machine.

Network-based IDS(NIDS): It scans all the packets in a network and detects unauthorized 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.

II. PROPOSED SYSTEM

The proposed approach is in line with the internet of Things (IoT) trend where we have several smaller devices that communicate over the internet to share information and enhance efficient processing of our systems. We consider the Raspberry Pi (or any other smaller computer) that acts as the peripheral device to be the access point for a possible intrusion attack into the network.

Our conventional computers are loaded with different mechanisms to counter such threats. The idea is to do the same for these peripheral devices, hence leaving them equipped enough to deal with the intrusion attempt. Ideally, the Honeypot proposed will be a low interaction honeypot that will be able to safely collect attack information that

can be used for our analysis of attack patterns and enable us to consistently evolve in the field of network security as we see new threats rising each and every day. Adapting to these new threats is the challenge and accurate attack information if obtained can go a long way in curbing the menace of intrusion attacks by making the network immune to such attacks by adapting as required based on the pattern.

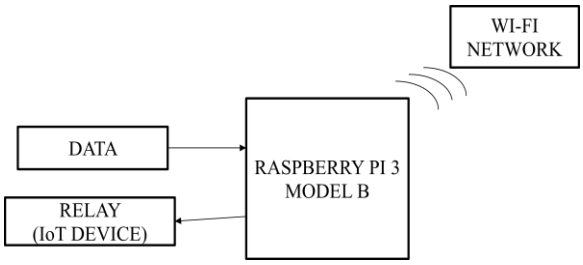

FIG 1. IOT SERVER

This IOT server consists of Raspberry Pi-Honeypot which captures all the attackers activities. the network admin puts a dummy data to attract the client The client data is delivered to the server for further analysis and updating network security.

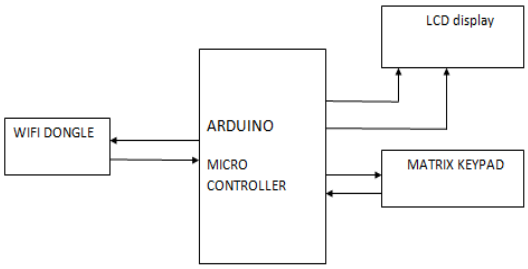

FIG 2. CLIENT

To demonstrate the attack, Arduino Uno is taken as a client and acts as a medium for attacking. The network admin allows the client into a system with the user name and password will be very generic which can be cracked. The client connects to the server with a Wi-Fi dongle When the attacker enters into the system and he breaks the password of system admin. Intruder will throw different types of attacks using matrix keypad on to the network admin system.LCD display displays what type of attack is used by intruder. Then alert notification will sent to the network admin. Honeypot detects the attacker access, it blocks the certain privileges and send message to the admin through IOT. Here whenever the attack is made by client automatically the relay which is connected to IoT device will be on. Honeypot detects the type of the attack. It displays the IP address blocking; it identifies the system information and secures the network from future attacks.

III. TYPES OF ATTACKS

We consider the three types of attacks namely Quality of service, Denial of service and worm attacks.

QUALITY OF SERVICE ATTACK: QoS methods are used as a network bandwidth sharing policy. Its role is to ensure a given amount of network bandwidth for special kind of traffics, for example enough bandwidth for Voice over IP calls, videoconferencing, transferring mails or a special kind of user who has to be treated in special way which will not lead to unordinary network latency. QoS methods are widely utilized by the network administrators. For the preparation of the administrator has to configure the whole

network equipment: switches, routers and firewalls.

DENIAL OF SERVICE ATTACK: A DoS attack is when attacker floods a system with more packets than its resources can handle. This causes the system to overload and shut down. The source address is spoofed by creating it strenuous to trace where the attacks are taking place.

WORM ATTACK: A worm attack is independent malware computer program that reproduce itself which spread to variant computers. This attack utilizes a network on computer to spread itself and relying on failures of security on the target computer for accessing it. This attack produces little harm to the network by consumption of bandwidth and corrupts viruses or modifying the files on a targeted computer.

HONEYPOT TECHNOLOGY: Honeypot technology is a decoy system setup to collect information concerned to an attacker or intruder into the system. Honeypots are an addition to the traditional internet security systems; they are also an addition to the network security systems. Honeypots can be framed inside or outside of a firewall design or any strategic location within a network. Variants of standard Intrusion Detection Systems (IDS) are there but more of a focus on gathering of information 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.

A system which contains several honeypots is known as a honeynet. If the attacker breaks into the system or server, then the honeypot that resembles the original server will be assaulted by the attack, while the actual system remains safe and untouched as a server behind the honeypot. For those who are not experienced attackers, they tend to think that they have easily managed to hack the system / server.

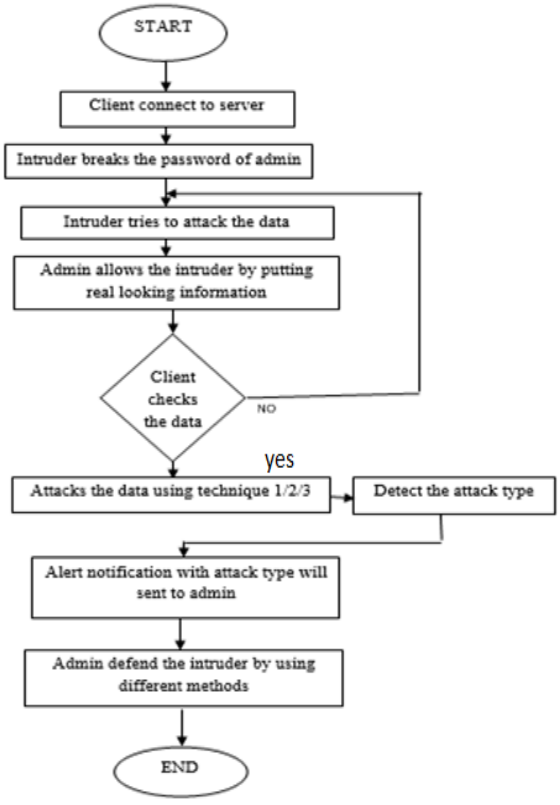

FIG 3. FLOW CHART

Initially, the client connected to the server then intruder breaks the password of admin server. Intruder tries to attack on the data

then the admin allows the intruder by putting real looking information to the server. The client checks the data if no data is present in the admin's server again intruder tries to attack on data in the system. If data is present then intruder attack on the data by using three techniques (DOS, QOS, Warm attacks). Honeypot detect the type of attack. Then alerts the admin by sending IP address and system information through message. Finally, admin defend the attacker by utilizing various methods such as IP address blocking, attack type detection and alert notification.

IV.RESULTS

FIG 4. HARDWARE IMPLEMENTATION OF SERVER AND CLIENT

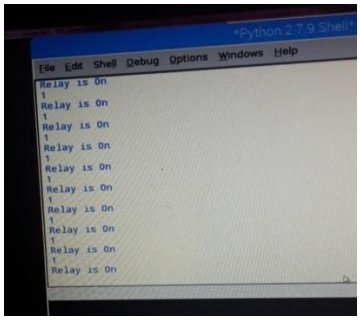

FIG 5.WHEN ATTACK IS OCCURRED AUTOMATICALLY RELAY (IOT DEVICE) WILL BE ON

The attack.php is a webpage which is used to create the attack the admin's system. It is shown in below figure.

FIG 6. CREATION OF ATTACK

Index.php is a webpage which is utilized to identify the type of attack. The below figure shows that attacker attacked through DoS. It also gives information about date and time, Attackers IP address and system Info.

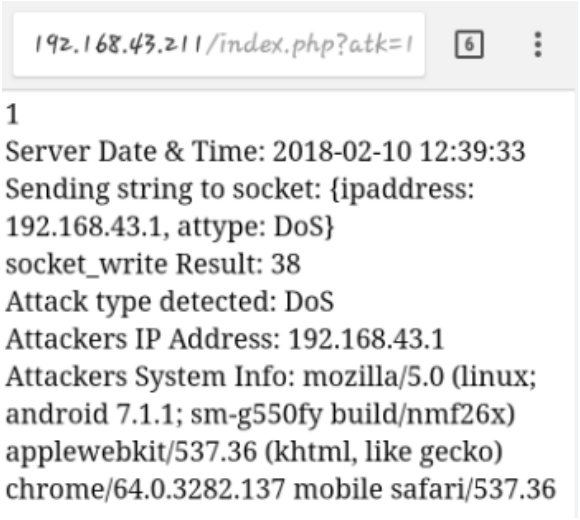

FIG 7. DOS ATTACK

The below figure shows that attacker attacked through QoS. It also gives information about date and time, Attackers IP address and system Info.

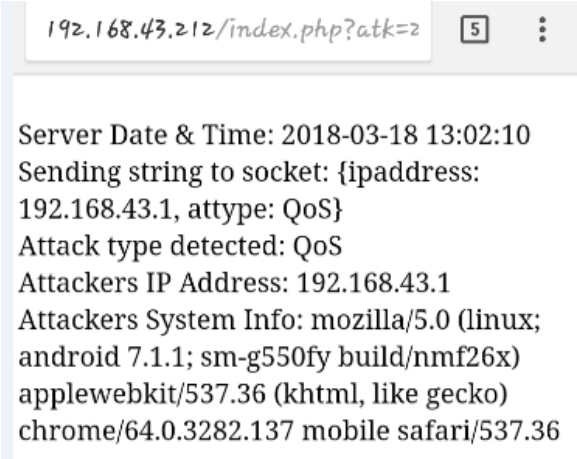

FIG 8. QOS ATTACK

The below figure shows that attacker attacked through Worm Attack. It also gives information about date and time, Attackers IP address and system Info.

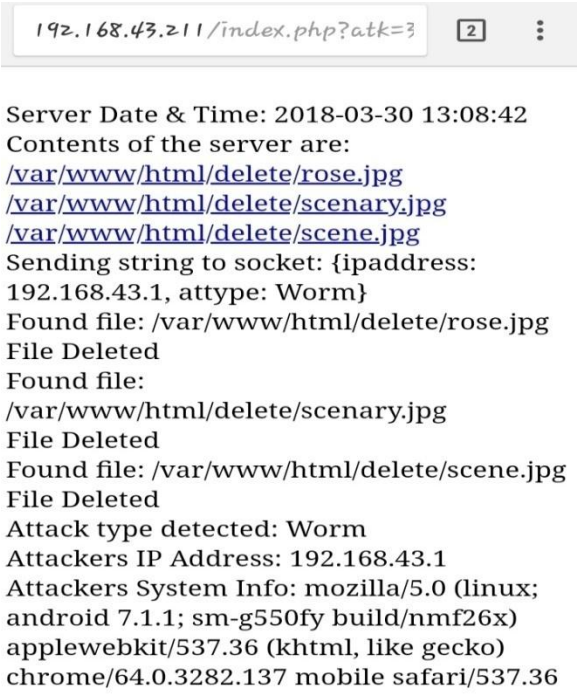

FIG 9. WORM ATTACK

If the attacker wants to attack second time our Honeypot send a notification to attacker shown in below figure.

FIG 10. BANNED IP ADDRESS

FIG 11. IP ADDRESS ATTACK IDENTIFICATION THROUGH MESSAGE

The above figure shows the message which is send to the admin about the information of trying to attack and attackers IP address and system Info.

The webpage blocked.php is used for to show the blocking list ofthe IP address along with the time stamps of the attacker. The below figure shows the blocked IP address and on which date, time it is blocked.

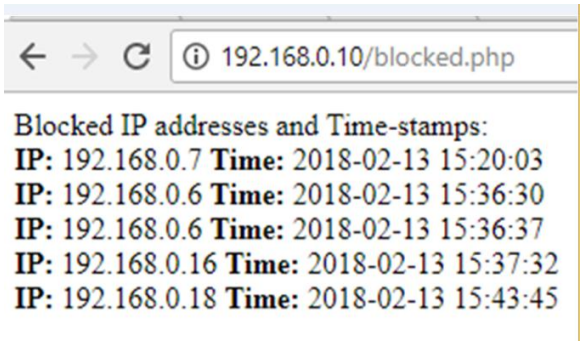

FIG 12. BLOCKED IP ADDRESS WITH DATE AND TIME

V.CONCLUSION

The usage of Raspberry Pi-Honeypot as a decoy in the network represents a simple and an efficient solution for enhancing network security by 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 paper is to introduce a new and cost effective mechanism for network on security. This proposed mechanism combines the security tools to minimize the disadvantages and increase the security capabilities in the process of securing the network.

VI.REFERENCES

[1] M. H López and C. F.Reséndez. "Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and ourses". Proceedings of the Informing Science & IT Education Conference (InSITE), 2008.

[2] Lance Spitzner. Definitions and Value of Honeypots [EB/OL]. http://www.tracking-hackers.com /papers/honeypots.html, 2003-05-08.

[3] B. Tambunan, W. S. Raharjo, and J. Purwadi, "Design and Implementation of Honeypot with Fwsnort and PSAD as Intrusion Prevention System," *1 / Vol.5 / Sept.2013*, vol. 0, no. 0, pp. 1–7, 2013.

[4] G. M Bednarski and J. Branson. "Information Warfare: Understanding Network Threats through Honeypot Deployment". Carnegie Mellon University. March, 2004.

[5] *S. Mardovich*. "Network packet payload analysis for intrusion detection". ".accepted 9 February 2007 Available online February 2007.

[6] McMillan, Robert., "Online attack hits us government web sites." Jully7 2009, http://www.computerworld.com/s/article/9135274/Online attack hits US government Web sites.

[7] S. A. Budiman, C. Iion system swahyudi, and M. Sholeh, "Implementation of intrusion detection system(IDS)using social networking as a media notification," in *Prosiding Seminar Nasional Aplikasi Sains & Teknologi(SNAST)*, 2014.

[8] R. C. Joshi and A. Sardana, "*Honeypots: A New Paradigm to Information Security*. "Science Publishers, 2011.

[9] I. P. A. E. Pratama, "Handbook computer network :theory and practice based open source".Informatika, 2014.

[10] C. S. Bayu, "Analysis and implementation of security networks using IDS and Honeypot," Universitas Dian Nracuswantoro, 2014.