International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 12th Mar 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: **IMPLEMENTATION OF SECURING IOT NETWORKS USING HONEYPOT MECHANISM ON A RASPBERRY PI**

Volume 08, Issue 03, Pages: 161–166.

Paper Authors

GUNTUPALLI TEJASWI, BPV.SUBBARAO

St. Ann's college of engineering & technology, Chirala, Prakasam District, Andhra Pradesh

International Journal for Innovative Engineering and Management Research ★

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IMPLEMENTATION OF SECURING IOT NETWORKS USING HONEYPOT MECHANISM ON A RASPBERRY PI

[1]GUNTUPALLI TEJASWI, [2] BPV.SUBBARAO
[1]M.Tech scholar, Dept of ECE, St. Ann's college of engineering & technology, Chirala, Prakasam District, Andhra Pradesh
[2]Assistant Professor, Dept of ECE, St. Ann's college of engineering & technology, Chirala, Prakasam District, Andhra Pradesh

ABSTRACT: In today's everlasting technological world, information and data communication create more devices stay connected to the internet. This lead to achieving development for building different software and internet connection very inexpensive this affected privacy and security. Security today became of the most important issue because day-by-day new technologies are put forward for different purposes of study while these come with a lot of vulnerabilities which makes the exploitation of the data. IoT is also such kind technology which is available for exploiting. For preserving information from such type of attacks we use honeypot which serves as a decoy based technology in a network and these are cost effective and works as a deception model which entice attackers with low vulnerabilities and security. 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 detects the attacker access, it blocks the certain privileges. It detects the type of the attack. It displays the IP address blocking, it identifies the system address and secures the network from future attacks. To demonstrate the attack, Arduino Uno is taken as a client and acts as a medium for attacking.

KEY WORDS: Raspberry pi, Raspbian jessy, Python language, Embedded C, Matrix keypad,LCD display, Wi-Fi dongle, Arduino Uno

.

I.INTRODUCTION

With the fast increase of various kinds of applications based on network, the process arrangement of many issues and business becomes dependant on network. Since the concept of the traditional network security belongs to the passive defense, it is hard to protect the information security due to the unknown network attacks of various kinds. Honeypot technology sets up a system with security risks deliberately to lure attackers into the controlled network environment it sets up. The technology uses various monitoring techniques to capture the attackers' behaviors for the record of their tools and technologies which are then analyzed with the vulnerabilities in the application system so that the security performance of the network can be improved and network security threats can be reduced.

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. 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 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.A honeypot is a network decoy system under strict surveillance, 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.

Honeypot is a new network security technology based on the inveiglement theory developed in recent years. A honeypot is a network inveiglement system under strict surveillance, which attracts attacks by genuine or virtual network and services so as to analyze the blackhat's activities during honeypot being attacked by hackers, delay and distract attacks in the meantime. Using honeypot technology, the network administrators of a network could expand the network topology space, delude the attackers, delay attacking and distract targets, deplete the attackers' resource, protect productive network. Meanwhile network and information security community can track, record and analyze the hacker's actions focused on the honeypots comprehensively to discover and get acquainted with the internal and external threats to the network, the common attacking tools, methods and rules, so as to amend the network security architecture, to revised security management principles of all levels, to adjust the firewall configuration to enhance the holistic security of a network. 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 willattract attackers by simulating vulnerabilities and poor security.

II. TYPES OF ATTACKS

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

A. 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.

B. 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.

C. 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.

III. RELATED WORK

Here,a modified algorithm is proposed, and a high degree of interactivity level of the virtual honeypot network is developed on this basis, It can give good reference to the network maintenance personnel. This paper proposes the application of honeypots in the

LAN system, where the virtual and physical honeypots are placed in a specific location. In this way, you can learn about the latest attack methods and tools, updating Firewall and intrusion detection knowledge base and to some extent deterring the intruder. This thesis focuses on the combination of a variety of defense technology to explore completely the advantages of Firewall, intrusion detection and honeypot technology to enhance the local area network security. we propose a new data collection architecture that addresses the need for both rapid comprehension and detailed analysis by providing two data access methods: a relational model based fast path, and a canonical slow path. They also presented a set of tools based on this architecture.Honey pot is placed just after the Firewall and intrusion system have strongly coupled synchronize with snooping agents Monitoring is considered at packet level and pattern level of the traffic. Simulation filtered and monitor traffic for highlight the intrusion in the network. Further attack sequence has been created and have shown the effects of attack sequence on scenario which have both honey pot and snoop agent with different network performance parameters like throughput, network load, queuing delay, retransmission attempt and packet.With the development of digital campus construction, the campus network size has been rapid growth, but there are also many network security problems. The honeypot technology is introduced and based on the development of net technology, combined with the campus network security problem. A hybrid and adaptable honeypot-based approach that improves the currently deployed IDSs for protecting networks from intruders. The main idea is to deploy low-interaction honeypots that act as emulators of services and operating systems and have them direct malicious traffic to high-interaction honeypots, where hackers engage with real services.Honey pot security is provided through data analysis with Artificial Neural Network (ANN). An approach to detect presence of computer malcode in the honeypot based on ANN while using the computer's behavioral measures. their use in modern computer networks and their implementation in educational environments. The purpose is to overview the honeypot and honeynet technologies, based on thorough analysis of the deficiency of obtain employment information network’s security their concealment and security, a design of high concealed and high safe honeypot system has to be implemented successful. A unique method to secure hosts inside the home network is proposed. After securing these hosts the attacker traffic is redirected to honeypots for further analysis.

IV. 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 thatcan 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.

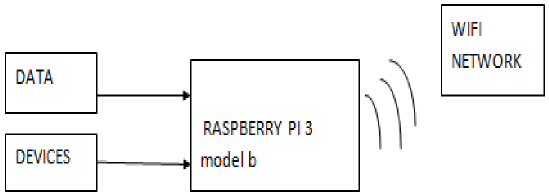


Fig. 1 IOT SERVER

This IOT server consists of Raspberry PiHoneypot 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.

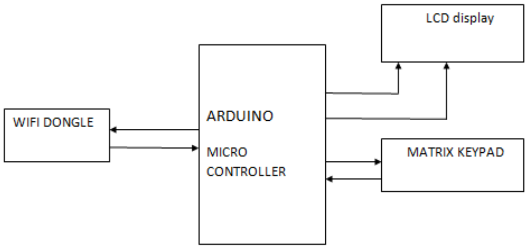
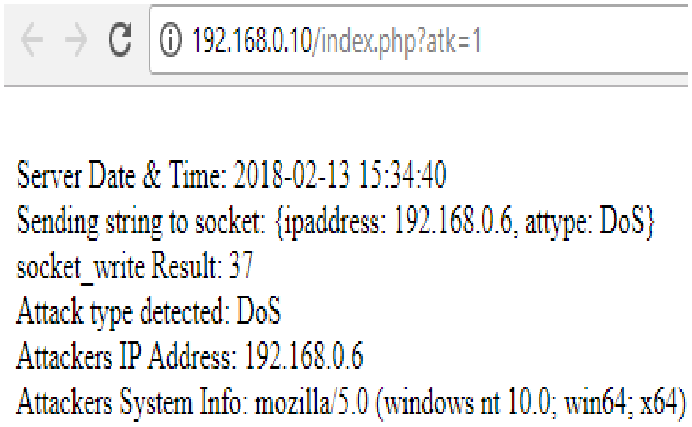


Fig. 2 ATTACKER MODULE

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.

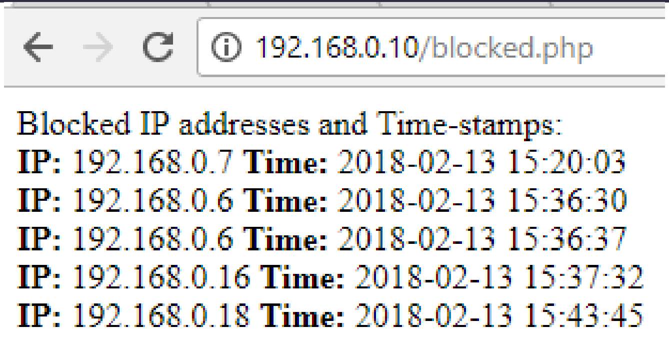
V. RESULTS

The below figure(3) shows that attacker attacked through DoS. It also gives information about date and time, Attackers IP address and system Info The below figure (4) shows the blocked IP address and on which date, time it is blocked.



```
Server Date & Time: 2018-02-13 15:34:40
Sending string to socket: {ipaddress: 192.168.0.6, attype: DoS}
socket_write Result: 37
Attack type detected: DoS
Attackers IP Address: 192.168.0.6
Attackers System Info: mozilla/5.0 (windows nt 10.0; win64; x64)
```

FIG.3: DOS ATTACK.



Blocked IP addresses and Time-stamps:
IP: 192.168.0.7 **Time:** 2018-02-13 15:20:03
IP: 192.168.0.6 **Time:** 2018-02-13 15:36:30
IP: 192.168.0.6 **Time:** 2018-02-13 15:36:37
IP: 192.168.0.16 **Time:** 2018-02-13 15:37:32
IP: 192.168.0.18 **Time:** 2018-02-13 15:43:45

FIG. 4: BLOCKED IP ADDRESSES

VI.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.

VII.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.trackinghackers.com

[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/91 3527 4/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.