

USE OF HONEYPOT TO SECURE IOT NETWORK

Harshita Shetty ¹, Shrinidhi Shetty ², Jasmine Shukla ³, Prof. Aparna Bannore ⁴

Department of Computer Engineering

SIES Graduate School of Technology, Navi Mumbai, India

ABSTRACT: A major concern with every new emerging technology is security. Internet of Things (IoT) being one of the latest trends, has many vulnerabilities waiting to be exploited. Home Security is an unavoidable commodity in our day to day lives. Thus, in order to secure our houses Home Surveillance System came into existence which is an IoT network formed using IP cameras. In IoT Networks, the DoS attacks play a major threat in pulling the entire network down. It is basically a cyberattack in which the attacker seeks to make a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Honey pots are systems which act as the main system to attract potential hackers who wish to gain unauthorized access of the system. It makes the attacker to fall in trap by allowing them to some exploits. This device will not create a blockade for the attack but will provide us with information about the attacker. This project provides a solution for IoT network devices (IP Cameras) against Denial of Service (DoS) Attacks by using Honey pots and help us find out about attacker, as Honey pot acts as a vulnerable device and lures the attacker towards it thereby protecting the network from them. This honeypot device will then check the request, store the attacker information in the log and notify users of the network about the same.

KEYWORDS: Dos Attack, Honey pot, IoT

I. INTRODUCTION

International Network, or as we refer to it INTERNET is a global network connecting the computers, laptops, cellular mobile phones, and other electronic device around the world. Where as the World Wide Web (WWW) is just an online content network which is then formatted into HTML web pages and are accessed using HTTP; all the interlinked pages can be accessed through the Internet. So, the Internet and the World Wide Web are not one and the same thing. Internet is a huge infrastructure of network. It is a network of networks used as a communication medium between various electronic devices that can have internet.

Internet is a group or gathering of different resources and services, and thus plays a very important role in our daily lives with communication being the foremost service that it provides. It removes the time and space concept figuratively and creates its own CyberSpace. With a rapid increase in the usage of Internet, its various applications have been discovered. Internet of Things (IoT) being one of the major advent of the internet.

These days, we see the implementation of IoT everywhere from the smart cities to home automation systems. An Internet system comprises of devices or sensors which can talk to the cloud using a kind of connectivity, Internet being the backbone of that connectivity. In general terms, we can say that these are the things that can sense and gather data as well as send the data gathered to or over the Internet, converting the device from a normal one to the smart one. Internet of Things (IoT) is an ever-growing physical objects network where in each device has an IP Address for Internet connectivity, as well as the communication taking place between each of these physical objects or devices.

Internet of Things (IoT) is a system in which the computing devices, digital and mechanical machines are interrelated and interconnected to each other where a unique identifiers (UIDs) are given to each object, animal or person along with the capability of transferring data over the network without any requirement of human to human or human to computer interaction.

The number of things connected to the Internet has already exceeded the human population and tends to increase ever since as it is delivering substantial benefits to the end users. Initially the term IoT, known to the tech savvy people and was just a fancy term for the the ordinary individuals has now being popular to the entire world due its major applications unveiled. However, the unprecedented challenges in security always comes along with any technological boon.

The devices that are connected using any IoT network shares an implicit amount of trust among each other, therefore automatically transfer their data to each other on recognition at that particular instance without even running any of the malware detection tests.

Thus, as the demand for IoT keeps increasing, the security threats imposed will also increase directly. The reasons for IoT devices being less secure is shown in the figure [1]. There is huge amount of confidential data transferred and stored on the IoT cloud, it is vulnerable to attacks and thus needs extra protection.

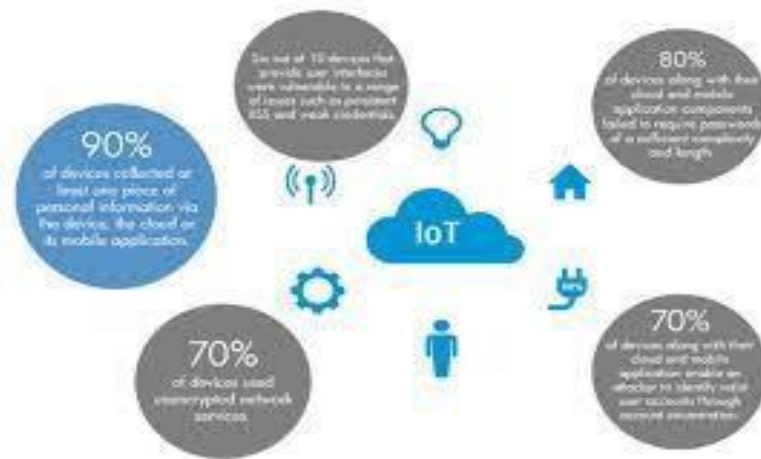


Fig 1. IoT Devices are Insecure

There are various security challenges or threats hampering the use of IoT technology which are as follows:

- 1) Device Cloning - Over here an attacker device which a foreign hardware will act or behave exactly as the original device and then overload the servers with bad data as well as getting access to the confidential data because it is also difficult to differentiate between the two.
- 2) Sensitive Data Exposure - It usually takes place when the sensitive data is not well protected by the application with a good encryption technology and is exposed to the unauthorised users.
- 3) Denial of Service - The DOS attacks are known for flooding the servers of the network with large amounts of useless data thus bringing the entire network down. These attacks sometimes also target the vulnerabilities and target the weak devices. The Denial Of Service (DOS) attacks has catastrophic effect which can eventually pull down the entire organisation.
- 4) Unauthorized Access or Control - With the breaching of private, sensitive information stored at the IoT cloud, IoT is an unauthorized access and control. Nobody wants any malicious or spiteful user to take access of the information, and try to strengthen the network by identifying the vulnerabilities.

The demand for IoT is ever-increasing as it is been used by many organizations for developing various kinds of projects. The main aim is to securing the IoT networks and the technologies applied uptil now are having some or the other loopholes. The reason is that a new device can easily get connected to the IoT network and start transferring data by merely logging into it using some username and password. To avoid all this we propose security through honeypots.

Honeypots are basically a decoy system which is mainly setup to accumulate information regarding an attacker/perpetrator into the system that we have. They are mainly used to underscore our traditional internet system of security. Deployment of these honeypots is usually done on an unused IP Address which the administrator mentions by themselves. The system here functions by waiting for a perpetrator or an attacker in order to begin the process of

interaction with the system.

The main aim of our system over here is to collect as much data as possible in a way that provides the required amount of protection to the system and the network from any further attacks and thus eradicate any computer along with the loopholes in the network security.

Honeypots are classified into various categories based on

I) The purposes that they serve:

- a) Research Honeypots - Mainly required for studying about the intruder as well as the security measure to be used.
- b) Production Honeypots - Mainly they are placed in a network to serve as a decoy as a part of some Intruder Detection System (IDS).

II) The design and complexity or level of interaction:

a) Low interaction honeypot - These are the easiest honeypots to install, configure, deploy and maintain, however its customised to more specific attacks because there is no interaction with the Operating System (OS) that is underlying. They are limited in number as they are easy to detect. It is having low interaction with the fixed replying logic and the also the interaction level is limited, thus not strong enough to pass a check and has a possibility of failing to capture real attacks. Due to the heterogeneity within the various devices connected to the IoT network (communicating with the devices having multiple protocols) which is challenging to copy the interaction of the IoT devices from a different vendor.

Considering the IP camera over here for simulating or visualising this behavior in a way that is realistic, one will need not only broadcast some video to the perpetrator but also needs to faithfully react to the commands such as fitting the cameras.

b) High Interaction honeypot - They give the perpetrator with a real Operating System where there is nothing emulated or restricted. It usually functions by controlling the attacker at the network level itself and thus also stores and provides information about the attacker, the motivation behind their actions, tools they are using and much more. These are more complex, furthermore deployment and maintenance take more risk are involved while deploying it since the perpetrator has a complete control of it and can abuse it. The cost of dealing with a real device as well as lack of emulator make it impossible to build such a honeypot.

We decided on attempting this because security is the foremost priority while building and using IoT networks. In the past 2-3 years various threats were discovered and the figures [2] and [3] given below shows that major attacks were telnet attacks and most of the attacks took place on IP cameras and therefore we have planned on implementing our project using it. Also it shows the major countries that were affected by IoT attacks.

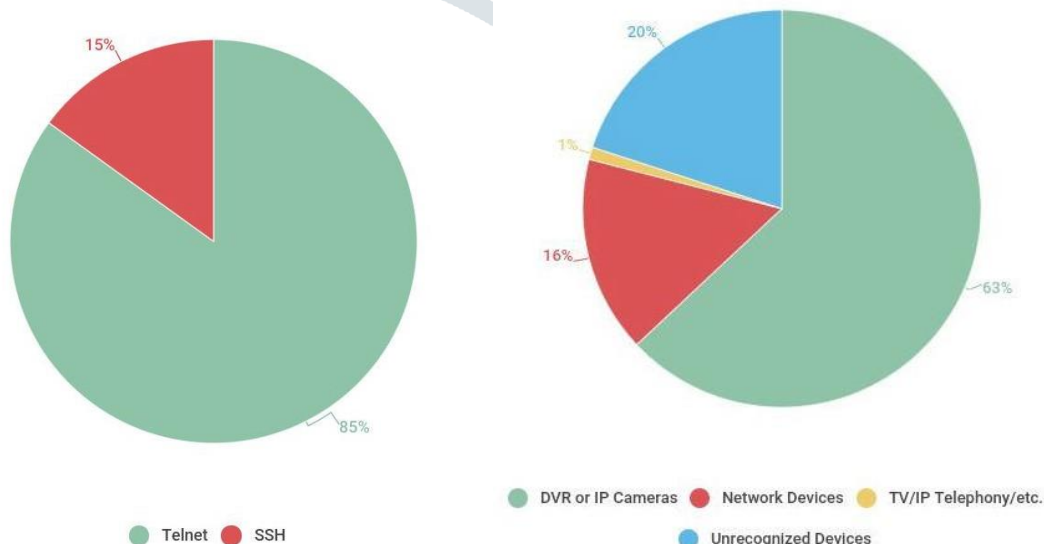


Fig 2 The components on which the Attacks

Fig 3 Attacks on IoT

Telnet attacks are nothing but just a distributed syn attack which is widely adapted by botnet operators in order to have a malicious act performed by sending a syn-flood attack to all the target machines.

The leading countries like USA and Canada and also all the others have been affected by these threats, hence finding an alternative security is a need of an hour because the technology is growing widely with each passing hour and it is necessary all of it is secured.

LITERATURE REVIEW

However, IoT comes with its set of limitations considering the layered architecture of the technology. Naik et al [3] mentions about various vulnerabilities which are faced by the IoT devices due to heterogeneous technologies and limited resources. Basically, a generic Iot model has three main key layers i.e, Perception, Network and Application. Each of these layers has its own technologies which brings some security threats along with it. From this paper, we learnt that the most common threats to the IoT architecture is DoS attack as it is related with all the three layers of IoT architecture. So, in this project we are going to mainly focus on mitigating DoS attacks on the IoT Network.

We know that, there are many applications of IoT and one of the most common and well known amongst them is IoT based Home Surveillance. Shrikant Ambatkar et al [8] mentions on how the Home Surveillance system can be set up using Webcam, Raspberry Pi and a motion sensor. The work presented basically says that if the motion is detected on the image captured by the webcam connected to the Raspberry Pi, then it must notify the authorized person by sending a text and an email message to that concerned person.

DoS attacks are one of the major attacks launched by cyber criminals. They are simple to launch but can cause havoc due to its operation. Anirudh et al [1] Provided us with a detailed study about how DoS attacks can be prevented using Honeypots in IoT networks in a simulated environment. The results of this stimulated system, according to a study, showed that there is about 55-60 percent increase in the efficiency of the system by the use of honeypots. In our project, we are going to implement honeypots in real-time IoT network.

Honeypots are therefore attractive traps set up in the network which helps in better security of the devices. Luo et al [6] deals with the theoretical implementation of honeypot. The authors implemented honeypot which is based on machine-learning for acquiring the behavioral knowledge of the IoT devices and introduced a new type of honeypot known as, "Intelligent-Interaction". From this paper we studied about various drawbacks about the existing honeypots and why they could not be used in the IoT networks.

With regard to DoS attacks on IoT we would like to highlight the research undertaken and the ideas proposed to deal with this disastrous attack. Sudip Misra et al [7] proposes learning automata based approach to deal with DoS attacks in IoT systems. A Learning Automata(LA) based approach is used to build a DDoS prevention strategy in IoT systems built on Service Oriented Architecture (SOA). There has also been research previously undertaken into the usage of honeypots to mitigate DoS attacks in IoT systems. However, at the present juncture this research remains theoretic with only theoretic models being proposed. The practical implementation of honeypots in IoT systems for the purpose of DoS attack prevention is an avenue that remains unexplored.

PROPOSED SYSTEM

In the proposed system, the overall representation is as shown in the figure below:

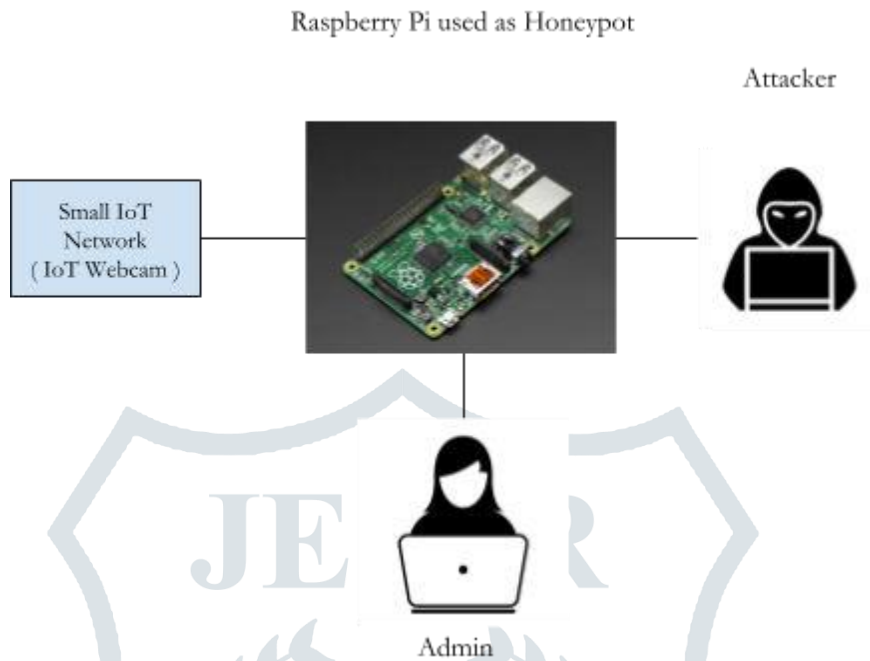


Fig 4 Raspberry Pi used as Honeypot

As given in Figure [4], the system consists of the IoT Webcam, Honeypot, Attacker and Administrator.

The Honeypot acts as an interface between the Attacker and the real IoT Network.

Honeypot, by default, is designed to see only the “bad” traffic. Configured with its own set of vulnerabilities, the wave of requests from the Attacker will be detected and reported to the administrator, indicating the presence and potential of malicious content.

The Honeypot will keep all logs and traffic of the network which can be used by the Administrator to get information of the Attacker that helps in safeguarding the data and IoT Network against such future potential attacks. The Honeypot, in all, will emulate the IoT device in the network and will catch all the malicious intention.

The Attacker will mainly interact with the front end of the Honeypot that acts as a decoy system, while in the back end, the Honeypot will log the details of the Intruder as well as provide storage of information to provide better insight into the attack methodologies to provide better protection to the real network.

The Proposed Model will run in two phases. In Phase 1, the IoT Webcam will be made to function without the use of Honeypot and the resulting effect will be observed. In Phase 2, the IoT Webcam will have the presence of Honeypot in its vicinity, which will attract most potential malicious traffic and which in turn will trace all the information of the said traffic.

To provide a brief description, referring Figure [5], all the requests from the Client / Attacker will scan the network and perform the attack. The malicious traffic will be detected and will be further entertained by the Honeypot.

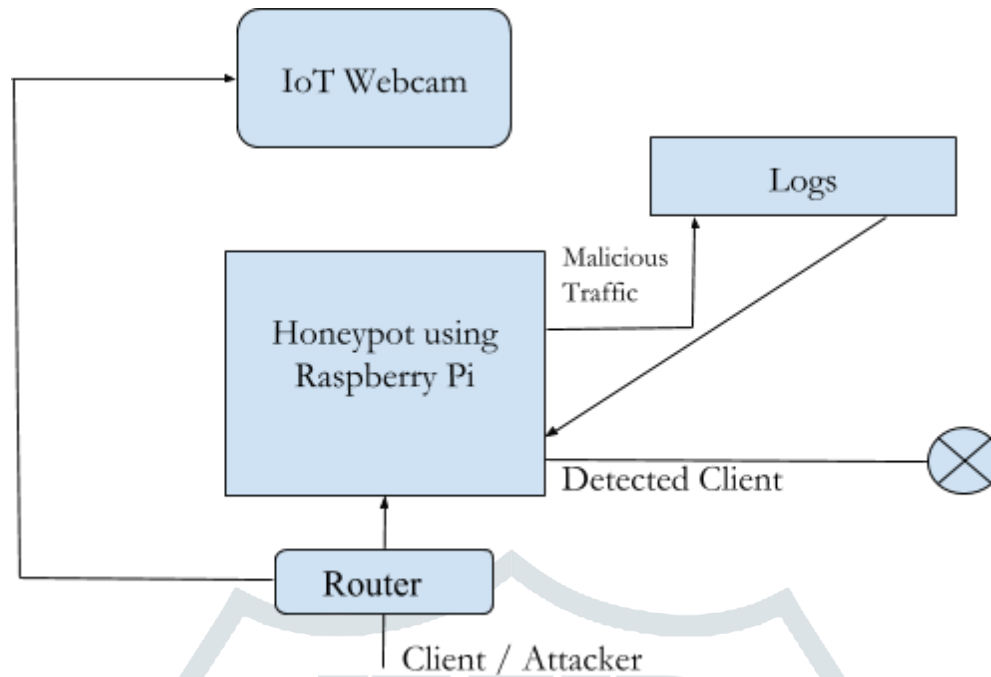


Fig. 5 Overall Functioning of Honeypot

The malicious traffic is then logged by the Honeypot to give details about the Attacker including the tools, methodologies and intentions.

These logs can then be used to check other client requests. If there is a match, the client is said to be a detected client and further requests from them are blocked. The usual primary clients are allowed to carry on their requests to the IoT Webcam. The spam requests and traffic are generally targeted towards the Honeypot as the Honeypots come with their own set of emulated loopholes, thus diverting the Attackers attention and time away from the actual system.

II. IMPLEMENTATION DETAILS

The methodology which we have adopted includes the setup of two Raspberry Pi devices initially. Both the RPIs are powered on using USB cables connected to a display device such as a Laptop. Both Raspberry Pis are configured with the Raspbian OS. After the initial configuration, we use the Logitech C310 HD Webcam, which we connect to this RPI for video streaming of the surroundings. The intent of doing this is to build a Home Surveillance system using IoT, which we wish to secure. This device is connected to the Router using the Ethernet cable which helps it acquire IP address, enabling the communication through internet. The other RPI is then initialised with the Honeypot setup and is also connected to the same router using another Ethernet cable for acquiring IP address in the network. This RPI is then connected to a Breadboard through jumper wires which enables the connection of an LED light we intend to use for notifying the users of the attack.

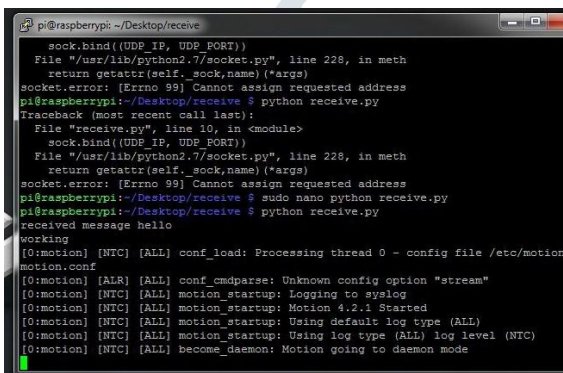
III. RESULTS AND DISCUSSION

The primary purpose of the generated report is to serve as an indicator of the potential impact of the suspect file, and quantify it in meaningful but easily understandable parameters. These are represented as an overall threat score as well as a listing of identified Indicators of Compromise. Results from additional analysis modules may be queued, both conditionally and as routine. To emphasize the integrity of our results, we integrated our analysis process with an existing database of known threats. Standing on the shoulder of giants, this intelligence comes from over 50 antivirus research bases, aggregated by VirusTotal. The final score is provided in the interval [0-10], directly proportional to malevolent impact, with 0 indicative of completely benign sample

This section contains the output from attacker's as well as victim's point of view, which will provide us with more clarity about what the project does. In this chapter, the project is explained in depth.

1. Setting up the Network

Initially we set up WebCam on Raspberry Pi and accessing the Raspberry by putting its IP address on PUTTY. Then, we install and configure the WebCam on raspberry and start the live video streaming.



```

pi@raspberrypi: ~/Desktop/receive
sock.bind((UDP_IP, UDP_PORT))
File "/usr/lib/python2.7/socket.py", line 228, in meth
return getaddrinfo(self._sock_name)(*args)
socket.error: [Errno 99] Cannot assign requested address
pi@raspberrypi:~/Desktop/receive $ python receive.py
Traceback (most recent call last):
File "receive.py", line 10, in <module>
sock.bind((UDP_IP, UDP_PORT))
File "/usr/lib/python2.7/socket.py", line 228, in meth
return getaddrinfo(self._sock_name)(*args)
socket.error: [Errno 99] Cannot assign requested address
pi@raspberrypi:~/Desktop/receive $ sudo nano python receive.py
pi@raspberrypi:~/Desktop/receive $ python receive.py
received message hello
working
[0:motion] [NTC] [ALL] conf_load: Processing thread 0 - config file /etc/motion/
motion.conf
[0:motion] [ALR] [ALL] conf_cmdparse: Unknown config option "stream"
[0:motion] [NTC] [ALL] motion_startup: Logging to syslog
[0:motion] [NTC] [ALL] motion_startup: Motion 4.2.1 Started
[0:motion] [NTC] [ALL] motion_startup: Using default log type (ALL)
[0:motion] [NTC] [ALL] motion_startup: Using log type (ALL) log level (NTC)
[0:motion] [NTC] [ALL] become_daemon: Motion going to daemon mode

```

Fig. 6 Setting up RPi Webcam

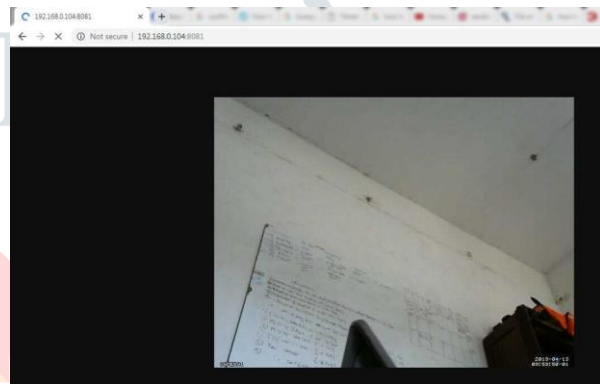
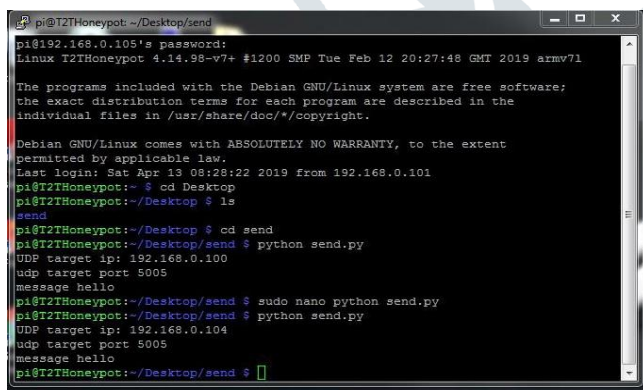


Fig. 7 Webcam Video Streaming

Similarly we set up the Honeypot Raspberry Pi and access it through PUTTY. Afterwards, we arrange the LED light, which will blink if any attacker tries to attack it.



```

pi@T2THoneyPot: ~/Desktop/send
pi@192.168.0.105's password:
Linux T2THoneyPot 4.14.90-v7+ #1200 SMP Tue Feb 12 20:27:48 GMT 2019 armv7l
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 13 08:28:22 2019 from 192.168.0.101
pi@T2THoneyPot: $ cd Desktop
pi@T2THoneyPot:~/Desktop $ ls
send
pi@T2THoneyPot:~/Desktop $ cd send
pi@T2THoneyPot:~/Desktop/send $ python send.py
UDP target ip: 192.168.0.100
udp target port 5005
message hello
pi@T2THoneyPot:~/Desktop/send $ sudo nano python send.py
pi@T2THoneyPot:~/Desktop/send $ python send.py
UDP target ip: 192.168.0.104
udp target port 5005
message hello
pi@T2THoneyPot:~/Desktop/send $

```

Fig. 8 Setting up RPi Honeypot

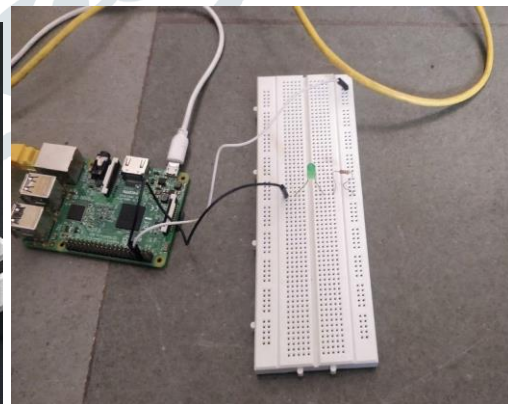


Fig. 9 LED connection for attack notification

2. Performing attack

Firstly, the Attacker performs Port Scanning using nmap tool to identify the weaker device in the network which shows port 23/tcp providing telnet service as open. The attacker will then try to access these ports.

After scanning, the attacker will then attack the most vulnerable device by using attacking tools like LOIC. In LOIC tool, the attacker will enter the IP Address of the weak device, change the default settings according to the need. In the end, click on Attack to start the DoS Attack. The progress of the same will be displayed in graph format in the tool as shown in Figure [10]



Fig. 10 Launching DoS attack using LOIC tool

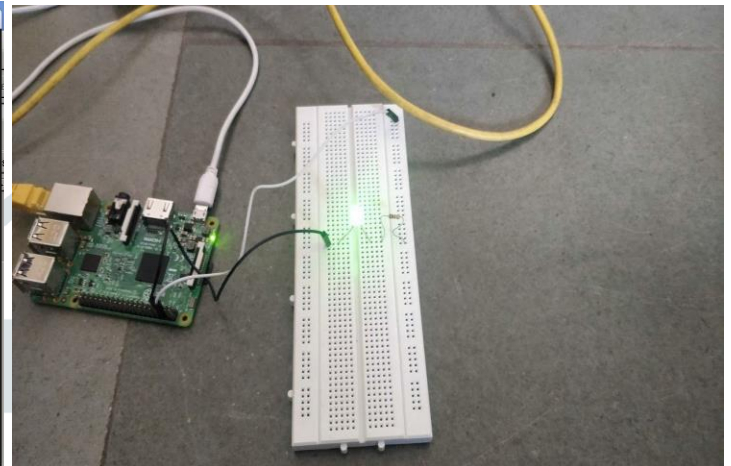


Fig. 11 After DoS attack

As the attacker attacks the most vulnerable device i.e. Honeypot. Now, this attempt causes the LED light attached to the Honeypot device to blink, notifying the users of the attack.

After launching this attack, on further attempts by the Attacker, he/she will not be able to access the device and 'Connection refused' message is displayed to the attacker. This error occurs when the attacker's request is not able to reach the device. Refer Figure [12].

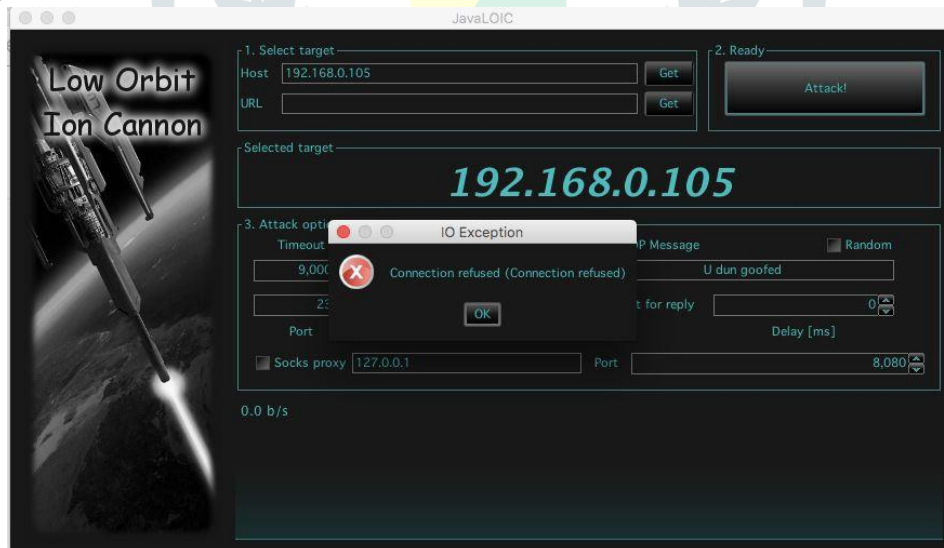


Fig. 12 LOIC tool after DoS attack

IV. CONCLUSION

Therefore, we tend to develop an IoT network having heterogeneous devices connected and having HoneyPot as one of the device which will in turn act as a gate or door which filters the request that has been sent to various devices connected in the network. Detecting the request to be malicious and storing, tracking requests includes as its main role. The HoneyPot is built in such a way that it appears vulnerable or weak to the attackers and act as the target machine to them so that any harm to the machine can be prevented and thus protecting the system from getting crash. Prevention of IoT is very necessary and therefore we decide to choose this topic and ensure to try implementing most of the objectives proposed.

Future works would be to collect and analyze results for the proposed model implemented in a real-time environment where various microcontrollers are interfaced with a central server. The idea of deploying honeypots to handle DoS attacks could also be extended, by deploying a honeypot system which is capable of handling DDoS attacks using botnets, since the verification system for this project might prove incapable there. Moreover, the use of honeypot could be extended for other types of attacks as a research based honeypot to collect details.

REFERENCES

- [1] Anirudh, M., Thileeban, S.A. and Nallathambi, D.J., 2017, January. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)* (pp. 1-4). IEEE.
- [2] Hota, J. and Sinha, P.K., 2015. Scope and challenges of internet of things: an emerging technological innovation. In *International Conference on Futuristic Trends in Computational analysis and Knowledge management*.
- [3] Naik, S. and Maral, V., 2017, May. Cyber security—IoT. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 764-767). IEEE.
- [4] Šemić, H. and Mrdovic, S., 2017, November. IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks. In *2017 25th Telecommunication Forum (TELFOR)* (pp. 1-4). IEEE.
- [5] Frustaci, M., Pace, P., Aloï, G. and Fortino, G., 2017. Evaluating critical security issues of the IoT world: present and future challenges. *IEEE Internet of Things Journal*, 5(4), pp.2483-2495.
- [6] Luo, T., Xu, Z., Jin, X., Jia, Y. and Ouyang, X., 2017. Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices. *Black Hat*.
- [7] Misra, S., Krishna, P.V., Agarwal, H., Saxena, A. and Obaidat, M.S., 2011, October. A learning automata based solution for preventing distributed denial of service in Internet of things. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 114-122). IEEE.
- [8] Patil, N., Ambatkar, S. and Kakde, S., 2017, April. IoT based smart surveillance security system using raspberry Pi. In *2017 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0344-0348). IEEE.
- [9] "No surprise, IoT devices are insecure", TechRepublic, 2019. [Online]. Available: <https://www.techrepublic.com/article/no-surprise-iot-devices-are-insecure/>. [Accessed: 24-Apr-2019]
- [10] ResearchGate, 2018. [Online]. Available: <https://www.researchgate.net/figure/Client-Honeypot-Architecturefig1202141516>. [Accessed: 22-Apr-2019]
- [11] V. Kuskov and M. Kuzin, "Honeypots and the Internet of Things", Securelist.com, 2017. [Online]. Available: <https://securelist.com/honeypots-and-the-internet-of-things/78751/>. [Accessed: 24-Apr-2019]