Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 8, August-2017, pp. 319-324 www.ijcert.org

A Honeypot for a Small Network using Raspberry pi

Rodney Anthony Raj[1], Chayapathi A R [2]

[1] *Student, Information science and engineering, Acharya Institute of Technology,_ Doctor Sarvepalli Radhakrishnan Rd, Bengaluru, Karnataka 560107, India.*

[2] *Assistant Professor, Acharya Institute of Technology,_ Doctor Sarvepalli Radhakrishnan Rd, Bengaluru, Karnataka 560107, India.*

Rodney.mtcf.15@acharya.ac.in[1], chayapathiar@acharya.ac.in[2].

Abstract: - The security is the biggest worry around the world let it be in any field or life. It is nothing different in cyber or network where the security is the biggest concern thinking about attacks which could happen anytime. So, this project is upon security, cyber security. Where a forensic device is built to monitor the network, and find the details of attackers[1].

This device does not act as an antivirus rather pulls the attacker to run some exploits and make them fall into the trap, a honeypot device which will perform all this when connected to a network. This device can also be used in forensics during crime scene to identify if any attacker is trying to steal any data.

This device will not completely screen off the attacker or the attack but rather will notify and keep us on the tab by telling us there's attack which may happen or happening. Attacks will never be stopped if we are connected to the internet. Hence, the solution provided here is to find out the attackers[3].

Keywords: - Malware, Raspberry pi, Honeypot, Cybercrime, Rootkits, Attacker, network, PUTTY, Nmap and Hacker.

---

1. Introduction

Security has become a mainframe in every aspect of technology, and without security, your work is not safe. Let's start with a basic example of money at home, where we need a locker to safeguard. The same way we need security in networks and cyber. This project is about the safety of the small network, and the device collects information rather than just protect.

Computer crime denotes to a criminal action involving a computer. The PC might be utilized as a part of the charge of misconduct, or it might be the objective. Cybercrime alludes to criminal exploitation of the Internet. Cybercrimes are basically a assortment of these two components and can be best very much considered as "Offenses that are committed against people or congregations of people with a thought process to purposefully hurt the status of the casualty or make physical or mental damage the objective specifically or by allegation utilizing current media transmission systems, for example, the Internet (Chat rooms, messages, see sheets and gatherings) and cell phones (SMS/MMS)"[2].

In its most simple form, digital wrongdoing can be characterized as any ill-conceived movement that uses a PC as its prime usefulness. The U.S. Division of Justice augments this definition to incorporate any illegal action that uses a PC for the capacity of confirmation. The term 'digital wrongdoing' can allude to wrongdoings including criminal action against information, encroachment of substance and copyright, extortion, unapproved get to, kid explicit entertainment and digital stalking.

Computer forensics is the act of gathering, examining and giving an account of advanced

information in a way that is legitimately permissible. It can be utilized as a part of the recognition and aversion of wrongdoing and in any question where confirmation is put away carefully. PC crime scene investigation takes after a comparable procedure to other measurable teaches, and faces related issues.

Digital evidence or electronic evidence is any probative data put away or transmitted in computerized shape that a gathering to a court case may use at trial. Before tolerating advanced confirmation, a court will decide whether the proof is significant, regardless of whether it is bona fide, on the off chance that it is gossip and whether a duplicate is adequate or the first is required.

An attacker is a person who intends to steal or hack some data or information from another person or a system which holds some essential or sensitive data. The victim can be an individual or an organization where the data lies. Nowadays the attack starts from a basic small network and which is the main cause for DDOS. The malware's planted by attackers are the main reason for DDOS as millions of machines are taken under control[4 5]. Victims fall prey for all the scenarios created by attackers such as sending a message which reads you've won 1000$ and with a link where most of them knowing it is hoax they try to click on the link to check this is a basic level of being a victim. So, victims are more in number because of our foolishness.

So, any person who tries to steal, fraud, and more are termed attackers or cyber criminals. We have to be quite conscious about it and shouldn't fall prey to it. To overcome these scenarios, we need to be aware of things. Even a computer engineer or a software engineer fall prey to attacks by clicking links or entering a malicious site to just finish their work[4 5 6 7].

An attacker can be stopped if and only if we do not fall prey and none of the security mechanism work until and unless we are not vulnerable. Imagine a high-security system can be hacked if the passwords are given out which a term is known as social engineering. Where we fall into the trap.

We can even stop the attacks by regularly updating our machines and running scans and even by not installing the products which we are unaware of. However, all this does not provide real time solution, and by stopping the attacker, we would never know his/her intentions. Regardless what if we collect all the info and check what attacker needs. This project is based on that by collecting the information about the attacks[14 15].

2. Problem Definition

This area introduces the point by point data about this postulation. On the early on the note, we begin talking about the issue inspiration, issue articulation contrasted and the venture objective, existing framework that conflicted with and indisputably proposed framework is examined[11].

There are multiple instances where forensic is required in the everyday life of every individual. Be it for personal use or enterprise needs. So, each time when things are required, it is not ideal to approach professionals seeking for help. Because it takes up time and money, and also trust factor plays a major role in the process. Many individuals will have knowledge but the lack of tools for the job to be done[8 9 10].

So, there is a need for a tool or a device which meets the requirements of individuals with a variety of Knowledge.
The Major objective of the paper is:

- To enable forensic properties hidden in the single chip ARM processor of the raspberry pi device.
- To make sure the device is feasible and can also be easily configured according to the needs of the individual.
- To make the forensic process as cost-effective as possible.
- Help in the forensic investigations for the collection of various evidence.

A. Existing system

In the existing system, many forensic devices such as cyber black box or sleuth kits are used to make the attacker roam away from the network or is used to check the details after an attack to find out what evidence are stored. However, these are complex and expensive that only certain professionals have access to. They also use tools such as Nessus (network vulnerability scanner), Galleta, Pasco etc. which require licenses for them to operate effectively[11 12 13].

B. Proposed System

A device which can keep all logs and traffic of the network and can be accessed to get the information of the attacker or use it as a forensic device in the crime scene to check whether any outside traffic is coming into the network to safeguard data.

C. Selection of board

The board selected is the Raspberry pi B+ since it has built in Wireless hardware which makes it more portable and does not need to be connected to any

adapter which might make the device bulkier and the stealth property is compromised.

The board can be setup with multiple operating systems and can be assigned static IP address so that it can be connected and utilized from anywhere for any purpose.

D. Operating system and tools used

The operating system Ubuntu is selected since it is readily available for ARM processors and also it has all the basic forensic tools inbuilt or easily installable from various sources according to the needs of the individual.
A built Honeypot server for vulnerability analysis is used. It can be executed from command line, and the working and database are present in the server or localhost.

3. System Requirement Specification

A. Hardware Requirements

The Basic Hardware requirements for the project to be up and running are as follows:

- Raspberry Pi 3 model B+
- Micro USB Cable
- Bluetooth Keyboard and mouse (only for one-time configuration)
- Router.

B. SOFTWARE REQUIREMENTS

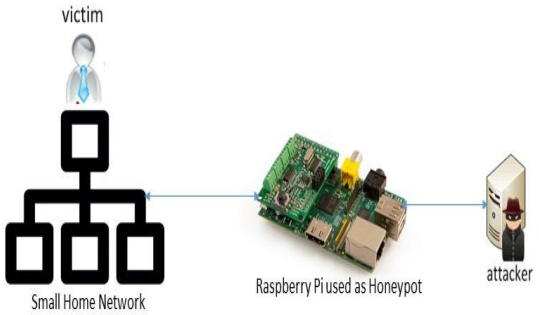
The software components required for the project are:

- Ubuntu Operating system
- Honeypot software
- Python

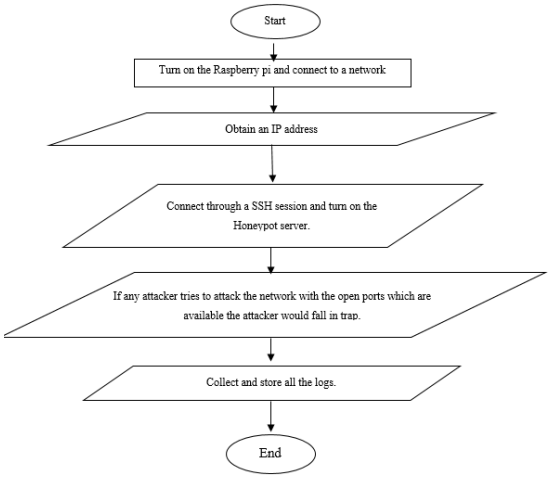
4. System Design

The connection architecture of the project is explained as below:

- **Network:** The network is the interconnection between the device, virtual machine and the investigator who is performing a live acquisition.
- **Raspberry pi:** The device which is configured and connected to the network to perform desired forensic procedure.
- **Investigator:** The Professional or any individual performing test on the machine.



Control Flow



5. Implementation

Implementation is the phase where all the steps that are required to carry out the procedures are explained using diagrammatic representation.

A. Configure Raspberry pi

For the first time, we need a separate display and all the needed cables such as power cable, HDMI, and patch cord to complete the configuration. Later we can just use a power cable with Wi-Fi, or we can connect the power cable and connect a Patch cord to a modem and lease IP addresses. To configure the pi, we use a tool called win32diskmgr which is used to write the OS onto the flash memory installed on the pi. After that, we connect the HDMI to a Monitor and configure the SSH which will be seen in the later part of this chapter.

B. Configuration of Honeypot

The configuration of a honeypot is our main module to proceed in any further understanding of the project. The honeypot software is a program code of Python. However, the configuration plays the real game here. The honeypot is configured in such a way where it opens all the ports which are configured, and these ports are seen open to the attacker. Such a way that if the attack is made through a certain port, we get all the details such as IP address, protocol and port number with date and time. Where these are stored in the database.

C. Install the honeypot on raspberry pi

Once the configuration of a honeypot is complete, we place the same on Pi and install the required and supported packages to run pi such as python**.**

D. Connect the raspberry pi to the network.

After setting up the honeypot on the pi. Now, we connect the pi to a network to make it a part of the network and make it visible to outsiders by showing a device on the network as all its ports open, and it is vulnerable to attack which will in return pull the attacker into the trap.

E. Get the IP address of raspberry pi.

So, now the pi is connected to the network which will indeed have an IP address or we configure the network adapter to get an IP address. After getting an IP address, we have to make sure we open the port 22 for SSH session to interact with pi without connecting HDMI to the monitor. This is required for our interaction with pi to check the logs.

F. Connect to an SSH session using PUTTY.

To obtain an SSH session, we are using a tool called PUTTY, which is an open source terminal widely used to communicate with Linux machines and others. As we are using Linux in our pi and the port 22 is opened we can use putty to configure the pi or honeypot and use the same to check the logs too.

G. Enter login credentials to access pi.

To perform all the above, we need a basic security entity which is our login credentials for the pi. As we are using Ubuntu, we will not have root permissions. We can either obtain it by entering sudo as a prefix to all commands, or we can enter into the root of the OS by using "sudo –i" and enter the credentials to obtain root access.

H. Now, start the honeypot server, by running the honeypot.

After setting up all the things, we can now start the honeypot server which is on the pi and connected to the network with an IP assigned to it. After the server is on, we have to keep checking the logs and expect some attacker to sneak through and if by chance someone does the honeypot starts obtaining their info. Attacks can happen anytime because we are connected to the internet, and 80% of the world machines are connected to the internet, and 90% are connected to the network.

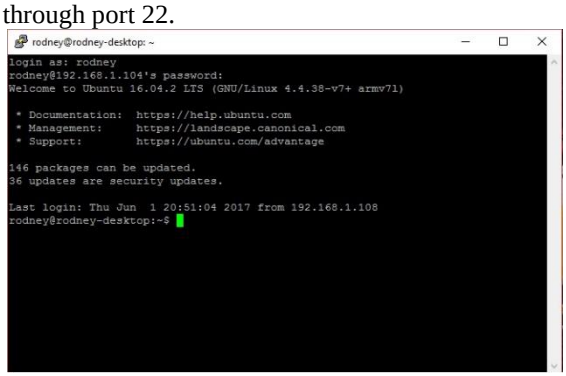
By setting these our implementation is completed, and we can start collecting the information and what the attacker in return gets is nothing but falling in the trap.

6. Results

This section contains the output of project from victim view and attacker view which will give us a clear picture of what the project does. Here we will see the project detailed, with an explanation.

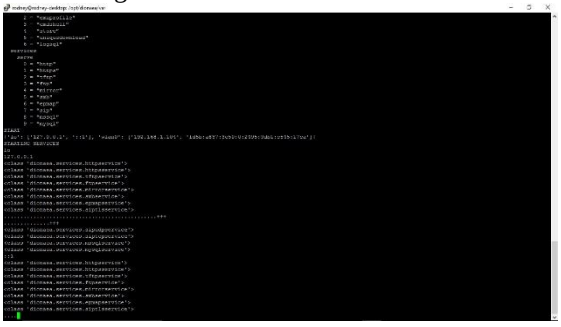
After setting up the honeypot to the network, we need to figure out the IP to access honeypot through SSH to start the honeypot server. We use NMAP to scan for the IP inside the network, and we access the raspberry through PUTTY.

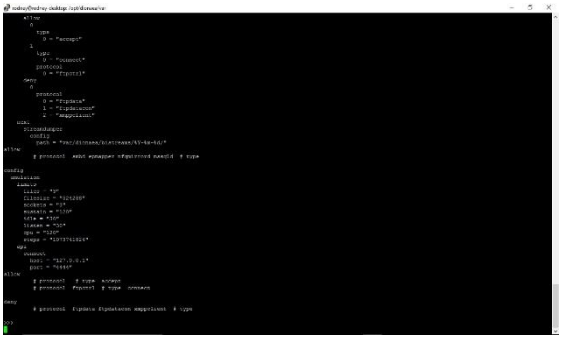
Once we get to know the IP of the raspberry we log in using a PUTTY terminal and access the server through port 22.



A. Starting the Honeypot server.

Now, it's time to start the server and wait for any attacker to try to attack or break into the network. Now we must turn on the honeypot server as shown in below figure.





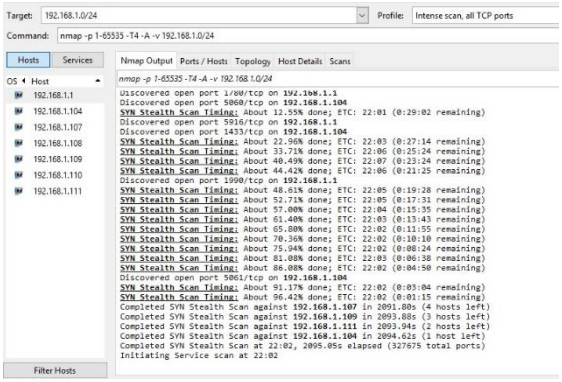
Now that the server is turned on we have to wait for an attacker to communicate with the ports which are open and if when someone does, we should start getting the details and logs.

B. **Collecting the info of attacker.**

First, even the attacker would try to check the network with scan to test the IP addresses.

So, a /24 scan of a class C network is scanned to know the available IP's. Once we get the IP's which are alive attacker will run a port scanning to check which ports are open for an attack then he would run the port scanning for individual IP and as well-run OS scanning a basic fingerprinting will be completed to find out the information about the machine.

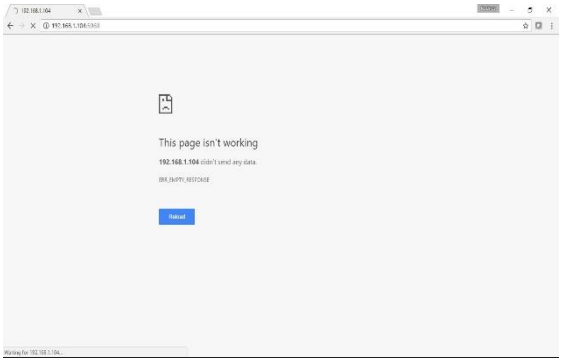
This will give the attacker an ample amount of information to attack or hack the machine in the network and so we are opening all these ports for the attacker to attack.



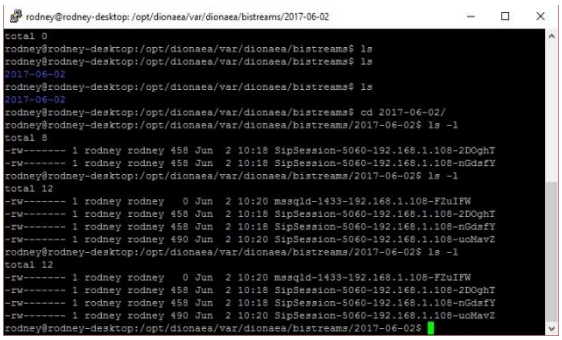
This will be the NMAP command run by the attacker to know open ports, and he/she will start their exploit by basically checking what's available? The attacker will try to access these ports.

The attacker, as sees the port 80 is open may think there's a site which is hosted and can try to check that. So, they can try the httpd service and can test the sip protocol used for VOIP by using 5060 ports and try to get database access through 1433 port and can run these through browser or any other tool.

So, these logs should be stored in the honeypot and later can be accessed for investigating or considering a scenario where the crime scene is under attack and the traces can be identified.



Where the above figure shows that the attacker has tried an available port and tried to access the information. The below figure shows a different attack with different port.



These are the information about the attacker and attacks attempted by the attacker. Which can be seen in the above figures. This shows how we can track the attackers or make them fall in a trap and save our network.

7. Conclusion

As we see even providing this sort of security can and will go in vain if we are not security proof enough. The project does not claim that this gives complete security, but this will help in finding out the attacker as well as intentions. However, still very much possible to break into the network by using social engineering or by getting access to the network and the user giving him/her full access will overcome the security the device provides.

This device provides security from an outsider who tries to break into the network with loopholes, but if any other machine is not updated or the ports are open, it is an invitation for attack. The security, prevention, or protection is not enough to protect us from an attack. We must be careful too.

Future Enhancement

a. Planned to send all the logs to a centralized server.
b. Shutting all 135-139 ports within the network towards the honeypot.
c. Monitoring network through sensors.

References

1. 2016: Current State of Cybercrime, RSA whitepaper.
2. Basic survey on Malware Analysis, Tools, and Techniques. Dolly Uppall, Vishaka Mehra, and Vinod Verma, 2013.
3. A survey of cybercrime. Zhicheng Yang., 2012.
4. Detecting and Classifying Morphed Malware: A Survey Sanjam Singla, 2012.
5. Evolution, Detection, and Analysis of Malware for Smart Devices Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, and Arturo Ribagorda, 2012.
6. A Survey on Techniques in Detection and Analyzing Malware Executables Kirti Mathur, 2012.
7. Malware Analysis and Classification: A Survey Ekta Gandotra, Divya Bansal, Sanjeev Sofat, 2012.
8. Malware and cyber crime. House of Commons, Science and Technology Committee. 2012.
9. Malware and Malware Detection Techniques: A Survey. Jyoti Landage, 2011.
10. A Survey on Malware Attacks on Smartphones Kireet, Dr.Meda, and Sreenivasa Rao, 2011.
11. Cybercrime and it's types, analysis, and prevention techniques, Alpna, Sona Malhotra 2016.
12. Web based Forensic Systems, srivathsa rao, vinaya hegde, jyothi Prasad, ijsrt, 2011.
13. Y. Li and A. Nosratinia, "Security in cyber forensics," Wireless Communications, IEEE Transactions on, vol. 11, no. 1, pp. 328–337, 2011.
14. Cyber Black Box: Network intrusion forensics system for collecting and preserving evidence of attack, Jong Hyun Kim, Australian Fornsics, 2015
15. Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks Conteh, Schmick, 2016

