**Protecting Network Structures by Deploying Honeypots**

by

Pavan Raj Seeramdas

Submitted in partial fulfilment of the requirements for the degree of

MASTER OF ENGINEERING

Major Subject: Internetworking

at

DALHOUSIE UNIVERSITY

Halifax, Nova Scotia   
April,2023

© Copyright by Pavan Raj Seeramdas, 2023

**Dalhousie University**

**Faculty of Engineering**

**Internetworking**

The undersigned hereby certify that they have read and award a pass in INWK 6800 for the seminar project entitled " Protecting Network Structures by Deploying Honeypots " by Pavan Raj Seeramdas in partial fulfilment of the requirements for the degree of Master of Engineering.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ying Hu

**DALHOUSIE UNIVERSITY**

**INTERNETWORKING PROGRAM**

**AUTHORITY TO DISTRIBUTE REPORT**

Title:

**Protecting Network Structures by Deploying Honeypots**

The Internetworking Program may make available or authorise others to make available individual photo/microfilm or soft copies of this report without restrictions after 26-04-2023

The author attests that permission has been obtained for the use of any copyrighted material appearing in this report (other than brief excerpts requiring only proper acknowledgement in scholarly writing) and that all such use is clearly acknowledged.

Full Name of Author: Pavan Raj Seeramdas

Signature of Author: Pavan Raj Seeramdas

Date: 26-04-2023

Table of Contents

LIST OF FIGURES vi

LIST OF SYMBOLS AND ABBREVIATIONS vii

ACKNOWLEDGEMENTS viii

EXECUTIVE SUMMARY ix

1 INTRODUCTION 1

1.1 Honeypot As Network Defense Mechanism 2

1.2 Securing Network Perimeters 2

1.3 Outcomes 3

1.4 Outline 4

2 DESCRIBING HONEYPOT TYPES AND ATTACK VECTORS 5

2.1 Honeypot Types Depending on Organizational Demands 5

2.1.1 High Interaction Honeypot 6

2.1.2 Low Interactions Honeypot 6

2.1.3 Pure Honeypots 6

2.2 Honeypot Types Depending on Data Collection 7

2.2.1 Based Upon Events 7

2.2.2 Based Upon Attacks 7

2.2.3 Based Upon Intrusion 7

2.3 Responsibilities of Attack Vectors 8

2.3.1 Compromised Credentials 8

2.3.2 Issues In Misconfigurations 8

2.3.3 SQL Injection Attacks 8

2.3.4 Man in the Middle Attacks 9

2.4 Summary 9

3 METHODOLOGY 10

3.1 Steps in Network Prevention 10

3.1.1 Virtual Private Networks (VPN) 11

3.1.2 Sandbox Environment 11

3.1.3 Firewalls 11

3.1.4 Intrusion Detection & Prevention Mechanisms 12

3.2 Working With Raspberry Pi 13

3.3 Working With GitHub 14

3.4 Summary 15

4 IMPLEMENTATION 16

4.1 Download Kali Linux on Local System 16

4.2 FLASING IMAGE ON RASPBERRY PI 18

4.3 CONNECTING TO RASPBERRY PI AND INSTALLING THE PENTBOX 19

4.4 EXTRACTING THE FILES 21

4.5 SUMMARY 22

5 OUTCOMES 23

5.1 RUNNING THE HONEYPOT 23

5.2 GENERATING A HTTP ATTACK 25

5.3 GENERATING A TELNET ATTACK 26

5.4 GENERATING A RDP ATTACK 27

5.5 Summary 30

6 CONCLUSIONS AND RECOMMENDATIONS 31

6.1 Conclusions 31

6.2 Recommendations 31

REFERENCES 32

BIBLIOGRAPHY 33

LIST OF FIGURES

Figure 1.1 Securing Network Infrastructure [1] 1

Figure 2.1 Different Honeypots Categories [2] 7

Figure 2.2 Common Attack Vectors [3] 9

Figure 3.1 Securing Networks Through Various Layers of Security [4] 10

Figure 3.2 Firewall Process to Hinder Traffic [5] 12

Figure 3.3 Working IDS/ IPS models [6] 12

Figure 3.4 Raspberry Pi 4 Motherboard and SD Card 13

Figure 3.5 GitHub Account 14

Figure 4.1 Kali Organization webpage for downloading the image 16

Figure 4.2 Downloading the compatible image 17

Figure 4.3 Extracted Kali Linux image 17

Figure 4.4 balenaEtcher 18

Figure 4.5 Flasing Kali Linux Image Over SD Card 19

Figure 4.6 Putty session to Raspberry Pi 20

Figure 4.7 Downloading Pentbox Over Kali Linux on Raspberry Pi 20

Figure 4.8 Extracting Files From Pentbox 21

Figure 4.9 Successful Installation of Pentbox Over Kali Linux on Raspberry Pi 21

Figure 5.1 Running the Pentbox Script 23

Figure 5.2 Network Tools Selected 24

Figure 5.3 Running Honeypot Over Pentbox 24

Figure 5.4 Running Honeypot With Fast Auto Configuration 25

Figure 5.5 Accessing HTTP port on Honeypot 25

Figure 5.6 Pentbox Detecting the User Connections 26

Figure 5.7 Running Honeypot With Manual Configuration with Telnet 26

Figure 5.8 Telnet session using Putty Terminal 27

Figure 5.9 Tcpdump of telnet session 27

Figure 5.10 Running Honeypot With Manual Configuration with RDP 28

Figure 5.11 RDP Session using Remote Desktop Connection 29

Figure 5.12 Tcpdump capture of RDP port 29

Figure 5.13 Tcpick of rdp.pcap 30

LIST OF SYMBOLS AND ABBREVIATIONS

DMZ Demilitarized Zone

OS Operating System

VM Virtual Machine

SQL Structured Query Language

VPN Virtual Private Network

IOT Internet of Things

RDP Remote Desktop Protocol

ACKNOWLEDGEMENTS

I am truly grateful for the support and guidance that Ying Hu has provided me throughout this project. Her mentorship has been invaluable in helping me navigate through the challenges and complexities of the research. She has generously shared her expertise, offered constructive feedback, and helped me to stay motivated and focused on the project goals. I am thankful for her patience, dedication, and commitment to my success. In addition, I would like to express my gratitude towards Dr. Bill Robertson and Dr. Shelley Caines for their encouragement and support. Their belief in my abilities has been a great source of motivation, and I feel fortunate to have had the opportunity to work with them. Overall, this project has been a tremendous learning experience for me, and I could not have done it without the support of these amazing individuals. I am truly grateful for their time, expertise, and guidance, and I hope to carry forward the lessons and skills I have gained from this project in my future endeavors.

EXECUTIVE SUMMARY

Network structures are arranged over an organization in such a way that it provides the better connectivity in transferring the information across the same network as well as the outside world. The attackers are possibly out there targeting these networks to form a session on the devices and extract the sensitive information stored over the same. Different network security mechanism out there for the security of the data where this report will focus on the honeypots as the device implanted on the network so as to divert the attacks onto this system and avoiding the loss of data from the original devices present on the network. These devices are deployed in such a way that it attracts the attackers as if some valuable information is presiding over them having some vulnerable versions running and further analyze the different attacks performed by the attackers and processing the security of the original devices according to that.

The honeypots systems can be deployed in either of the way that is hardware-based honeypots or the software-based honeypots. The deployment of these honeypots depends on the security risk to the network structure, which will be discussed in my report . In this report I will be describing various other protection mechanisms with the various honeypots that can be deployed on the network such as the tools and the hardware involved.

For the implementation or the outcome part of my report I will be using a dedicated hardware system which can be a Raspberry Pi 3 or 4 model based on the availability as this will help me in understanding how honeypots in real world are deployed as an external entity on the network protecting from attacks. In my scenario my local network will have few devices such as laptop and mobile devices where this raspberry Pi microcomputer will be deployed, and all the attacks will be performed on this honeypot as this will be visible as an easy to attack device on the network. In the implementation section I will be describing in detail about the scripts, or the tools used over this Raspberry Pi system such as Pentbox including the installation steps involved and further upon successful installation of the honeypot system on this micro board I will be analyzing the packets received from the attacker as in my case will be my local laptop which will be try to connect to the majority of the ports such as HTTP, Telnet, and RDP which are majority ports used by the attackers to access the target systems and all the data received of a possible connection will be recorded using tools such as Tcpdump, etc. All the steps that are involved in the setting up of the access on the Raspberry Pi honeypot to capturing the packets and displaying the results will be described in detail in this part of my report. The network capture will help as an owner to restrict access to these services by applying strong security measures. In this report I will be also discussing about various other possible options and tools that can be deployed in the achievement of deploying a honeypot on the network. This will cover the working of how the software-based honeypots work and how they can help in protecting the original system from being compromised.

# INTRODUCTION

Properly configuring the measures while deploying the network security mechanisms over the organization in order to protect the sensitive data or the transmission happening from both outside to the organization and vice versa is an important process and shall be given an utmost priority and time while designing and implementing the same. The main purpose of having a defensive line over the organizations perimeter is to avoid the possible attacks data are continuously being hammered on the organization network so as to gain the unauthorized access over the system or the gathering of private data that is being stored in the network. There are many different type of network attacks as well as the protective techniques which can be applied over any scale of organization which will be discussed in more detail in the upcoming chapters of this report. The main notion which is depicted from a secured network is the presence of CIA policy where the data stored on the network should be confidential, always available and deprived of any alteration thus maintaining the integrity.

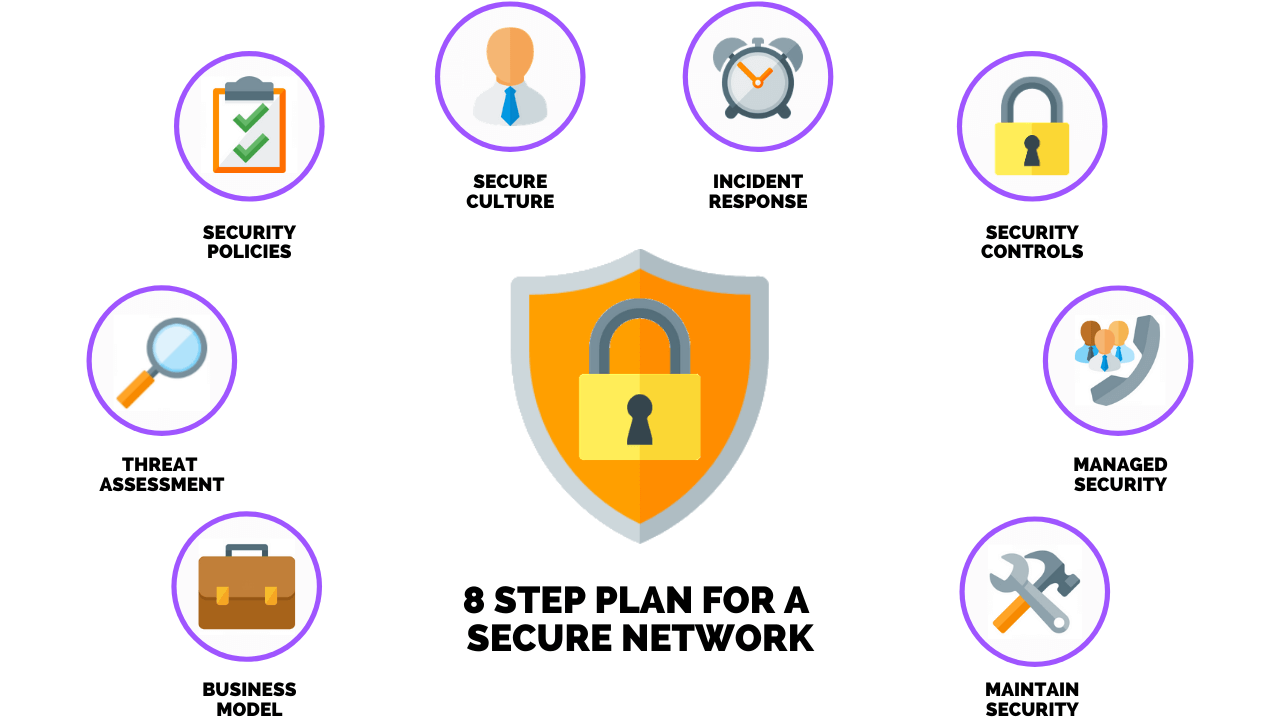


Figure 1.1 Securing Network Infrastructure [1]

## Honeypot As Network Defense Mechanism

Honeypot is one of the network defense mechanisms that are out there so as to protect the organization from the threats that are continuously trying to penetrate into the network and finally into the end devices such as systems as database servers. The honeypots functions by setting up an external vulnerable server that will attract the attackers to perform the different attacks and getting into this setup an environment which is closely monitored by the security team of an organization to learn about the techniques used by the attacker and apply the necessary hardening over the rail system. The honeypot systems work greatly over the network as these can closely monitor the attacks that can happen on the real system and as known the techniques involved in these attacks are greatly changing the security team in an organization should keep a thorough note of these attacks and apply necessary changes on the actual systems so as to protect these from the similar attacks. The honeypots are cleverly developed to attract the attackers in search of sensitive data or to the open ports that are found on these honeypot systems. The honeypot can contain different tools as per the research over attacks which consists as follows:

* Keylogger Applications
* Packet Capturing Tools
* Devices on Network, etc.

## Securing Network Perimeters

There are multiple other network security tools that will be discussed in detail in the upcoming chapters. Also, there is a high need of use of these different protective measures on the network perimeter as there no reliability over the single mechanism to be sure that this will work 100% all of the time and avoids the attacks from the outside. I will discuss various network security agents over in detail which shall include:

* Firewalls
* DMZ Network
* Virtual Private Network
* Intrusion Detection/Prevention Systems
* Segmentation of Network, etc.

## Outcomes

In this report over analyzing the network security and implementation of the honeypot system over the network so as to protect the real systems, I will be building an actual honeypot based system using the Raspberry PI micro board which will be setup over my environment so as to lure the attacks into it from the attackers machine for which I will be using the Kali Linux OS and shall be installed over the Raspberry Pi. I will also be explaining in brief about the other security mechanisms in the chapters of this report to have an insight over other measures as well as compared to the honeypots.

## Outline

The material in this report is organised into 4 chapters. The chapters deal with the following topics:

Chapter 2 shows the need of honeypot system based on security needs and the different attack vectors which are there to spread the malicious codes online.

Chapter 3 will display the specification of the raspberry pi board with its characteristics and the role of prevention in network security by different mechanisms.

Chapter 4 develops the honeypot system on Raspberry Pi 4 model board and finding the attached attacker on it.

Chapter 5 shows the results obtained from the deployment and making connections to the honeypot system.

Chapter 6 shows the conclusion of my report and the procedure involved in completing the same. Also, it holds the future recommendations section of my report.

# DESCRIBING HONEYPOT TYPES AND ATTACK VECTORS

In this part of the report, I will be describing various types of honeypots that can be used by the organization depending upon the requirements as well as the threats which are happening over the network. I will also be describing the various attack vectors that are responsible for a successful attack against a network over this part.

## Honeypot Types Depending on Organizational Demands

The honeypots that are deployed on the organizations solely depends on the requirements and the complexity with which the honeypot can be deployed and used to test out on the different attacks made by the attackers. There are different types of the honeypots system which will be discussed in detail further to understand the need of deploying the each one of them. Software used as bait for luring hackers into honeypots is called honeypot software. Hackers are particularly interested in applications and data that act like legitimate computer systems, contain sensitive data, and are not secure. By creating an open or otherwise deliberately vulnerable decoy, honeypots will misdirect cyberattacks away from critical IT systems. Data and files are fabricated and mimicked from those systems. Security analysts can better understand cybercriminals’ intentions, their methods and their goals by monitoring traffic to honeypot systems. When honeypots are monitored, it can be determined whether certain security measures are working, or if they should be improved. Furthermore, honeypots serve as real-time observation systems that assist IT security professionals in understanding cybercriminals attacks. It provides organizations with the ability to detect unauthorized access and usage. As a result, they can gather crucial information about the attackers.

### High Interaction Honeypot

The main usage of the high interaction honeypots lies in the fact that these are somewhat similar to the main systems in the organization in the fact that these also host the services being used and available on the main system or device on the network to lure the attackers inside. The different services allow the attacker to think of the system as the real one and exploit it in any possible way. The high interaction honeypots require a limited level of expertise to setup and deploy the mechanism on the network.

### Low Interactions Honeypot

The one of the majorities developed honeypots in the organizations which are responsible for handling the attacks raised from the outside where these have a little interactivity with the actual services being hosted by the system or server. From the study it can be seen that these honeypots are the easiest to deploy and don’t require much expertise by the technical staff in the organization.

### Pure Honeypots

As the name suggests these honeypots are the exact replica of the production environment where the services and the open ports that are present and running over the original servers are configured over the honeypot or replica server and this server is exposed to the internet for the attackers to try and test the security of the organization and managing the possible entry points on continuous monitoring of this system.

So, these are few of the honeypot categories which are deployed on the network based on the complexity and manageability of these replicas to lure the attackers and test out the different entry points possible in the system and these will then be analyzed to secure the production environment from any unauthorized access and extraction of information.

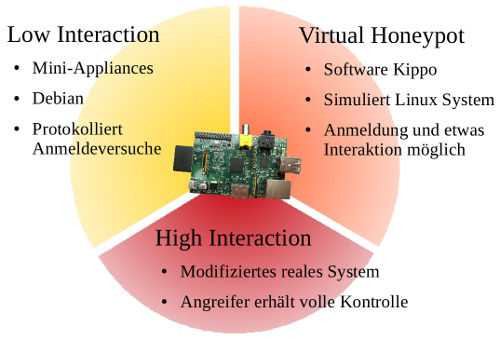


Figure 2.1 Different Honeypots Categories [2]

## Honeypot Types Depending on Data Collection

Honeypots can also be classified under the different data types it collects after its deployment is done. They can detect and record various types of data, considering the important once those are listed below:

### Based Upon Events

These can be considered as the things that takes place and alter the honepots contents

### Based Upon Attacks

These can be considered as the malicious user attempts to take advantage of a vulnerability

### Based Upon Intrusion

These can be considered as the successful attacks that breach the honeypot

Most honeypots can give some information from each of the three types of data which can eventually reveal useful details about the malicious user.

## Responsibilities of Attack Vectors

The attack vectors are the instances that are responsible for the transmission of the malicious code to the target systems where these are responsible for the generation of the remote access on the system. There are different attack vectors that are used by the attackers which will be discussed further in this chapter.

### Compromised Credentials

There are frequent data breaches in the present times where the credentials are being leaked to the internet and these credentials are freely available to anyone on the internet with proper access. These credentials that are already compromised in the past are the ones which can be used by the attackers to again target the users and perform various malicious operations using these further as well.

### Issues In Misconfigurations

All the services and the applications that are running on the target system or the entire ecosystem the users dedicated to the deployment of these may make mistakes in the configuration settings that are made because of the unwanted scenarios while handling the same. These misconfigurations can lead an attacker to exploit the weakness and get into the system easily.

### SQL Injection Attacks

Multiple web applications are vulnerable to attacks that allows an attacker to view and access the internal hidden files which can also include the database content from the internal server. The one of the major attacks in this is the SQL injection attack where the attacker tries to query the internal information stored in the database using the commands at the various user input forms present in the web applications that are present there for the user to interact with the users.

### Man in the Middle Attacks

One of the attacks that lets the attackers to sniff and view the packets sent from the local system to the internet and back makes the attacker to listen for all the sensitive information that can be used in multiple ways to exploit and target the user where further attacks can be made such as identity theft, bank thefts, accounts takeover, etc. These types of attacks carry the attacker to engage with a lot of information which can be used as an attack vector to perform various attacks on the target.

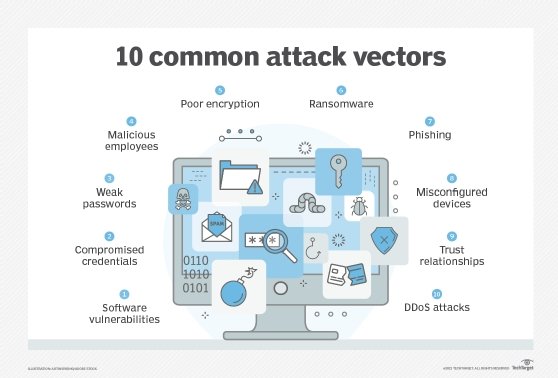


Figure 2.2 Common Attack Vectors [3]

## 2.4 Summary

In this chapter I have learnt about the different attack vectors that are responsible for the different attacks made on the user or the different systems on the network and gain privileged access on the same using different information gathered. I have also seen the various types of honeypot systems depending on organization demands and data collection that are classified.

# METHODOLOGY

In this chapter of the report, I will be discussing the different other network security prevention mechanisms which can also be implemented with the honeypots so as to provide an extra layer of defense against attacks from outside. I will also be describing about the micro board that will be used to deploy the actual honeypot in the final chapter of this report.

## Steps in Network Prevention

In addition to the honeypot system that can be deployed onto the network to prevent the attacks that are engaged by the attacker to exploit the target system and gain the access on the system there are multiple other preventions steps or the techniques which are present to build a better network security measure as the only one layer of honeypot system on the network cannot protect the systems from every attack possible on the network as with the better security features more and more sophisticated attacks are being engaged by the attacker for which the other layers of protections are also required to discuss and understand while securing networks.

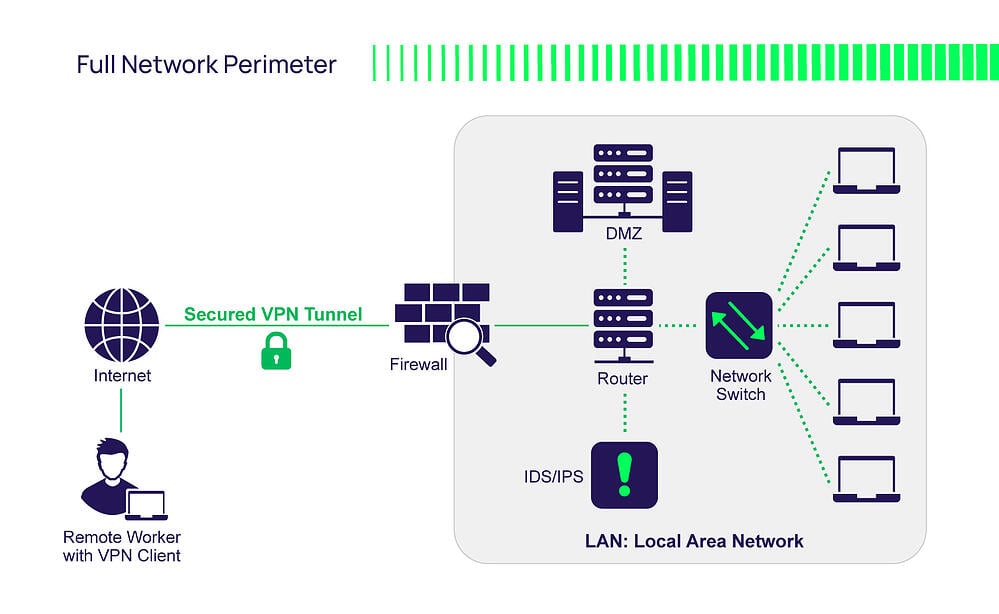


Figure 3.1 Securing Networks Through Various Layers of Security [4]

### Virtual Private Networks (VPN)

The VPN services are used to setup a distant session which is encrypted using the technique used in the technology itself to protect the network from being sniffed from the attackers as the channel is encrypted all the information being sent is transferred across the channel in the form of ciphered form where if the attacker is able to get into the network he/she won’t be able to deduce the messages real meaning without decrypting the same which is very difficult because of the use of stronger algorithms.

### Sandbox Environment

While performing any operations such as testing new applications from the web or any type of content that has the background emerging from the untrusted sources the sandboxed environment should be setup in the organization where these types of files or applications can be launched so as to provide security on the main system in the organization from being compromised and protecting form the loss of confidential data stored in the systems.

### Firewalls

Firewall is another protection mechanism that can be added to the present security posture of the organizations where these can be very helpful in describing the network inbound and outbound rules that will manage the traffic being sent from user machine to outside and vice-versa. The firewalls are the boundary security mechanism which can protect the malicious packets or data sent by the attackers to enter the system. There are different types of firewalls which are out there to be used in the process of avoiding the packet entry into the network which are as follows:

* Proxy Firewall
* Packet Filtering Firewall
* Stateful Inspection Firewall, etc.

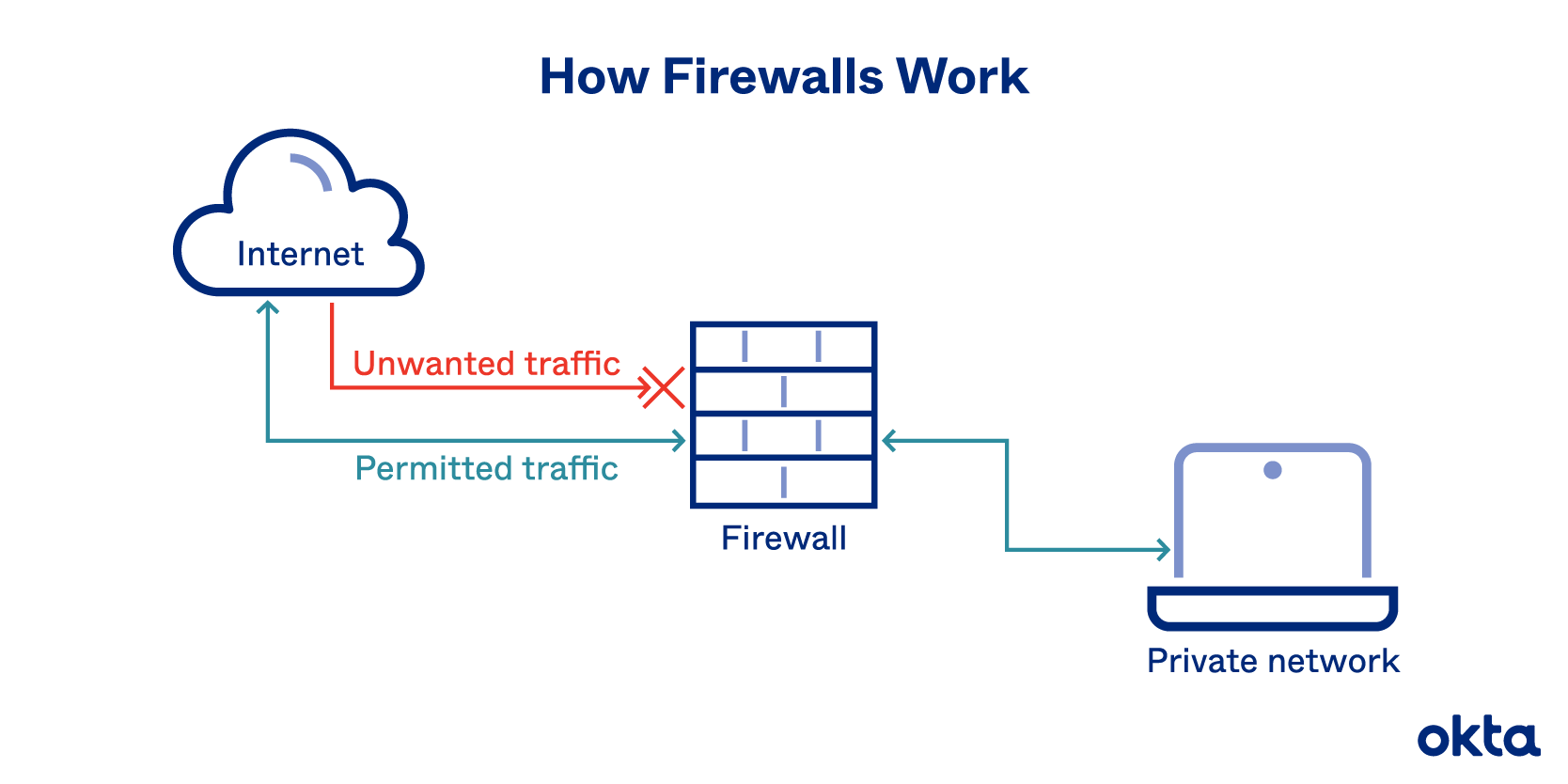


Figure 3.2 Firewall Process to Hinder Traffic [5]

### Intrusion Detection & Prevention Mechanisms

When intrusion detection system is the one which is used to protect the networks from any malicious activities by analyzing, detecting and updating the user about these activities. The intrusion prevention system is different in a way that it automatically analysis and raise the further protective mechanisms on its own and without the requirement of owner to take an action at the time of any malicious entry into the system.

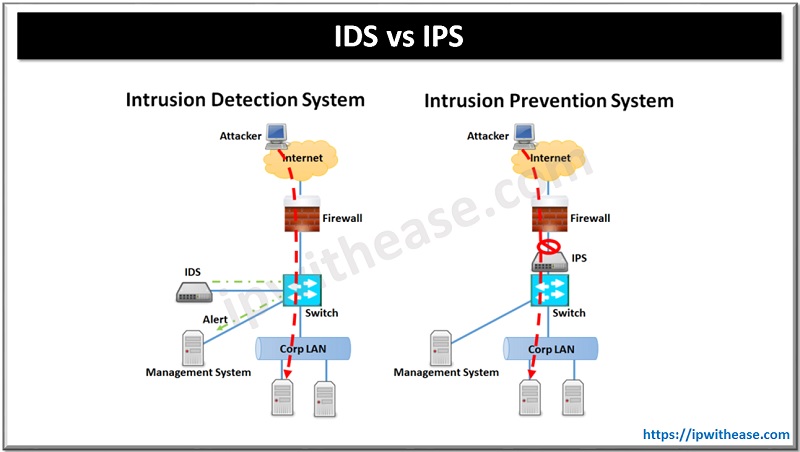


Figure 3.3 Working IDS/ IPS models [6]

## Working With Raspberry Pi

In the implementation chapter further of my report I will be working weather Raspberry based microcontroller where I will be using a Raspberry Pi 4 model which is one of the latest boards developed by the Raspberry Pi foundation. Some of the features which were the key advantages over which I have chosen this board to develop and deploy the honeypot system are as follows:

* High performance which has quad core 64bit processor.
* High resolution display support that allows up to 4K support to an external display
* RAM speed has been increased with the highest of 8GB capacity.
* Dual band wireless capabilities for Wi-Fi on board
* Power connector with USB Type-C socket
* Bluetooth Low energy module inbuilt for custom IOT projects.

A close-up of a circuit board

Description automatically generated with medium confidence

Figure 3.4 Raspberry Pi 4 Motherboard and SD Card

## Working With GitHub

I have the penbox software in my GitHub repository. This is in form of a tar file, where I will be cloning the repository into the Raspberry Pi and untaring all the files which will be shown in Implementation chapter of my report. Below is the link of my GitHub repository.

<https://github.com/Pavan-1997/pentbox.git>

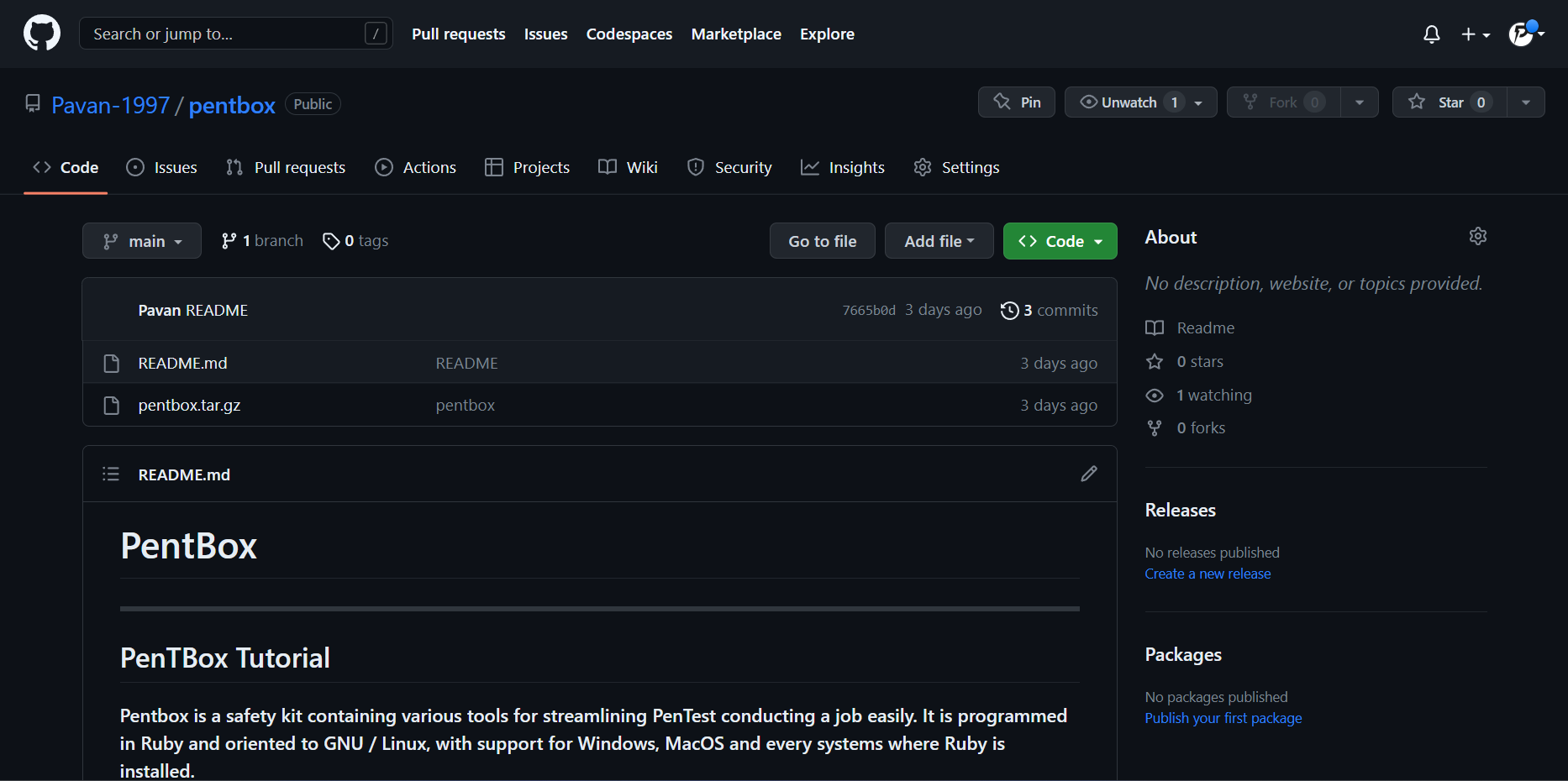


Figure 3.5 GitHub Account

## Summary

Here in this chapter, I have learned about the various network security mechanisms and that can be incorporated with the honeypot systems that was the major topic of my report to provide more security and robust features as compared to using a single security device in the environment having multiple areas of interest where the attackers can target and extract the information. I have also shown the Raspberry Pi and my GitHub account that will be used later in the implementation chapter to deploy a honeypot interface on my microcontroller through which I will be learning how these devices can help in managing security risks.

# IMPLEMENTATION

Here I will implement a honeypot similar to any real-world system so as to learn how the attacks on the real systems can be controlled by having this test system running parallelly and making the attacker attack this system where some services will be intentionally left running so as to allow attackers to penetrate into the system.

For this report I will be learning the process of deploying the honeypot system on my micro board as discussed in the previous chapter. Here I will be using the Kali Linux platform which will be installed over this Raspberry Pi 4 board and the further steps in the process of managing the honeypot will be displayed further moving in this chapter.

## Download Kali Linux on Local System

This is the first step to setup the Honeypot system, here I’m downloading the Kali Linux Image for the Raspberry Pi 4 on my local system which is my laptop

Going to the official page of the Kali Organization for kali platforms and selecting the ARM as the microcontroller is based on that processor

Graphical user interface, website

Description automatically generated

Figure 4.1 Kali Organization webpage for downloading the image

Now selecting the AMD 64 bit and downloading it into my local system

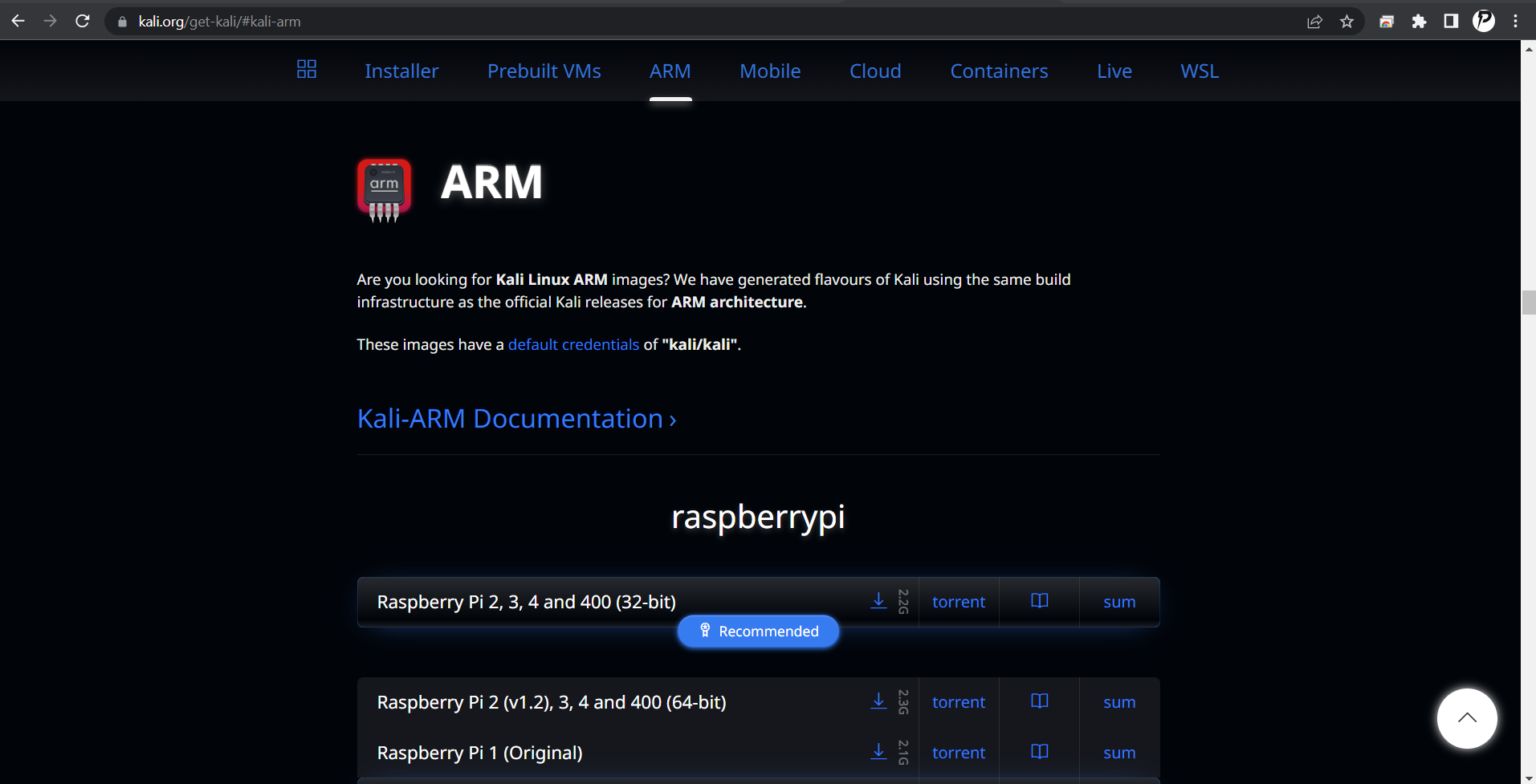


Figure 4.2 Downloading the compatible image

Later I have unzipped the file and have the office image for the Kali Linux

Graphical user interface, text, application

Description automatically generated

Figure 4.3 Extracted Kali Linux image

## FLASING IMAGE ON RASPBERRY PI

Now I have installed a mounting tool called Etcher on my local system , which is used to flash my Kali Linux image on Raspberry Pi over the Micro SD card

I formatted the micro SD card, although it is new it is recommended before flasing the image onto it for this I have used SD Card Formatter software

Now opening the Etcher and selecting the flash from file and select target which is my Kali Linux image and SD Card respectively

A screenshot of a computer

Description automatically generated with medium confidence

Figure 4.4 balenaEtcher

Flashing the image on my Raspberry Pi

Graphical user interface, application

Description automatically generated

Figure 4.5 Flasing Kali Linux Image Over SD Card

Once this is done, I loaded the SD card into my Raspberry Pi 4 and powered on the same to start the Kali. For display output I have user micro HDMI to HDMI and connected the other end to my monitor and observed the setup. Here the default credentials remain same for all Kali installations which are **kali:kali** . I have connected to my WIFI network. Immediately I have installed the OpenSSH server for my remote connection and used putty to connect to it which will be shown.

## CONNECTING TO RASPBERRY PI AND INSTALLING THE PENTBOX

Now from my local system I’m using putty to connect to the Raspberry Pi where the 192.168.2.101 is the IP address that is assigned by my router.

Graphical user interface, application

Description automatically generated

Figure 4.6 Putty session to Raspberry Pi

Giving credentials **kali:kali**

Now I’m installing the Pentbox which is an open source security tool that will be installed over the Kali Linux to deploy the Honeypot based solution over the Raspberry Pi and test the working of this tool.

The tool is present in my GitHub repository, cloning it to my microcontroller

Text

Description automatically generated

Figure 4.7 Downloading Pentbox Over Kali Linux on Raspberry Pi

## EXTRACTING THE FILES

Once the Pentbox is downloaded over the Kali Linux in Raspberry Pi and now extracting the tar file in the same directory

Text

Description automatically generated

Figure 4.8 Extracting Files From Pentbox

Once extracted going into the file we can see the pentbox-1.8

Text

Description automatically generated

Figure 4.9 Successful Installation of Pentbox Over Kali Linux on Raspberry Pi

## SUMMARY

In this chapter I was able to download Kali Linux image on my local system and flashed the image on the microcontroller using Etcher which led me to connect to the device and installed the Penbox software and extracting the tar file. In which this tool will be further helping me in achieving the honeypot being deployed on my network and test it to check for the possible incoming connections as an attacker to gain the access on the system

# OUTCOMES

In this final chapter I will be working with the previously configured Pentbox on the microcontroller to be used as a honeypot and using this tool to detect for the possible incoming connections to the system. I will showcase the steps in which I as an attacker and analyzer will check for the logs created over this tool.

## RUNNING THE HONEYPOT

In order to run the honeypot system on the Raspberry Pi we have to use the penbox ruby file and run this script which can attract the attackers towards this system.

Text

Description automatically generated

Figure 5.1 Running the Pentbox Script

Once the script is loaded, I used the Network tools option to proceed further where I moved towards the Honeypot option as seen in the below image.

Text

Description automatically generated

Figure 5.2 Network Tools Selected

Text

Description automatically generated

Figure 5.3 Running Honeypot Over Pentbox

I selected the third option over the previous set of instructions which enabled me to setup the instructions for the honeypot and the necessary actions to be taken before applying or deploying the honeypot. There are two options for the same where the one is a Fast Auto Configuration which is basic deployment and the other one is Manual Configuration which is more advanced deployment. For the report I have shown the results for both Fast Auto Configuration and Manual Configuration

## GENERATING A HTTP ATTACK

For doing the HTTP attack I have gone with Fast Auto Configuration

Text

Description automatically generated

Figure 5.4 Running Honeypot With Fast Auto Configuration

Once my honeypot was started on the Kali Linux I tried to access my Raspberry Pi assigned IP addreess over the browser followed by the port number (192.168.2.101:80) as in order to detect the connections made on the server. I found that the pentbox was able to identify the same.

Graphical user interface, text

Description automatically generated

Figure 5.5 Accessing HTTP port on Honeypot

As you can see in the below image honeypot has detected the user connection from the browser using the port number 80 (HTTP)

Text

Description automatically generated

Figure 5.6 Pentbox Detecting the User Connections

## GENERATING A TELNET ATTACK

For doing the Telnet attack I have gone with Manual Configuration. Now Im running the honeypot in manual configuration to test the telnet connection when a user tries to establish it. The below image shows the options that are selectedwhile running the honeypot on port 23

Text

Description automatically generated

Figure 5.7 Running Honeypot With Manual Configuration with Telnet

Here Im trying to take a telnet session to my Raspberry Pi IP address using the telnet port 23 (192.168.2.101:23) in the putty terminal.

Graphical user interface

Description automatically generated

Figure 5.8 Telnet session using Putty Terminal

To view the log of the telnet session the user has attempted, I’m using tcpdump to listen to the port 23 as shown in the below image

Text

Description automatically generated

Figure 5.9 Tcpdump of telnet session

## GENERATING A RDP ATTACK

For doing the RDP attack I have gone with Fast Auto Configuration

In this last attempt I’m trying run my honeypot with the manual configuration with RDP port number 3389 and selecting the options as shown below

Text

Description automatically generated

Figure 5.10 Running Honeypot With Manual Configuration with RDP

In the below image Im trying to take a RDP session of my Raspberry Pi IP address with the port number 3389 (192.168.2.101:3389) using the Remote Desktop Connection from my local windows machine which is connected to my home wifi network.

Graphical user interface, application, Teams

Description automatically generated

Figure 5.11 RDP Session using Remote Desktop Connection

In the below image I’m running the tcpdump and writing the output of it in rdp.pcap file. The tcpdump is actively listening on the port 3389 and captures the packets when the RDP session is formed.

Text

Description automatically generated

Figure 5.12 Tcpdump capture of RDP port

Now Im reading the rdp.pcap file below using the tcpick which is used for analysing the network traffic and below is the output of the pcap file that has been captured earlier. In this we can see the packets captured of RDP session that has established between my local windows machine to the Raspberry Pi

Graphical user interface, text

Description automatically generated

Figure 5.13 Tcpick of rdp.pcap

## Summary

In this chapter marking the completion of my report I have shown the use of Raspberry Pi in the process of managing the basic honeypot using the network communication protocol such as HTTP, Telnet and RDP which are few of the targeted protocols while gaining access on the remote system and also the web servers are continuously running over these servers. I have shown all the steps undertaken in the process to complete the report on learning the honeypot system.

# CONCLUSIONS AND RECOMMENDATIONS

## Conclusions

In the implementation part of this report I have used the Raspberry Pi 4 motherboard to build and show the working of a honeypot system over the home lab where I was able to perform and fetch the network traffic from the attacker system making connections to the honeypot system. I have learnt how the different tools in addition to the one used in the implementation section to deploy and to be start working with the honeypot system. I have seen multiple varieties of the honeypot which are deployed on the system depending on the need of the owner and to the extent the attack needs to be managed on the network.

## Recommendations

For the future studies related to this topic I shall be using the advanced methods and protocols in developing a honeypot system which will look alike my Raspberry Pi system and also storing some files and launching the same on the internet to find if the attackers get lured in or not.

REFERENCES

[1] M. Swanagan, “How to develop & Implement A Network Security plan,” *PurpleSec*, 25-Mar-2022. [Online]. Available: https://purplesec.us/network-security-plan/. [Accessed: 11-Feb-2023].

[2] Shail, “Types of honeypots - low interaction honeypot, high interaction honeypot,” *Snabay Networking*, 04-Feb-2023. [Online]. Available: https://snabaynetworking.com/types-of-honeypots/. [Accessed: 11-Feb-2023].

[3] M. E. Shacklett, “What is attack vector?,” *Security*, 13-Apr-2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/attack-vector. [Accessed: 11-Feb-2023].

[4] J. Carson, “Guide to network security and hardening,” *PAM Solutions*, 01-Nov-2022. [Online]. Available: https://delinea.com/blog/network-security-and-hardening. [Accessed: 11-Feb-2023].

[5] “Firewall: Definition, how they work & why you need one,” *Okta*, n.d.. [Online]. Available: https://www.okta.com/identity-101/firewall/. [Accessed: 11-Feb-2023].

[6] R. Bhardwaj, “Difference between IPS and ids - download detailed comparison table,” *IP With Ease*, 23-Jun-2022. [Online]. Available: https://ipwithease.com/difference-between-ips-and-ids-in-network-security/. [Accessed: 11-Feb-2023].

BIBLIOGRAPHY

[1] “What is a honeypot? how it can trap cyberattackers: CrowdStrike,” *crowdstrike.com*, 19-May-2022. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/#:~:text=A%20honeypot%20is%20a%20cybersecurity,methods%20and%20motivations%20of%20adversaries. [Accessed: 11-Feb-2023].

[2] NortonOnline, “What is a honeypot? how it is used in cyber security?,” *Norton*. [Online]. Available: https://us.norton.com/blog/iot/what-is-a-honeypot. [Accessed: 11-Feb-2023].