**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   
January, 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

Table of Contents

LIST OF FIGURES iv

EXECUTIVE SUMMARY v

1 INTRODUCTION 1

1.1 Honeypot As Network Defense Mechanism 2

1.2 Securing Network Perimeters 2

1.3 Outcomes 3

1.4 Outline 3

2 LITERATURE REVIEW 4

3 METHODOLOGY 5

4 OUTCOMES 6

5 CONCLUSIONS AND RECOMMENDATIONS 7

5.1 Conclusions 7

REFERENCES 8

LIST OF FIGURES

Figure 1.1 Securing Network Infrastructure [1] 2

EXECUTIVE SUMMARY

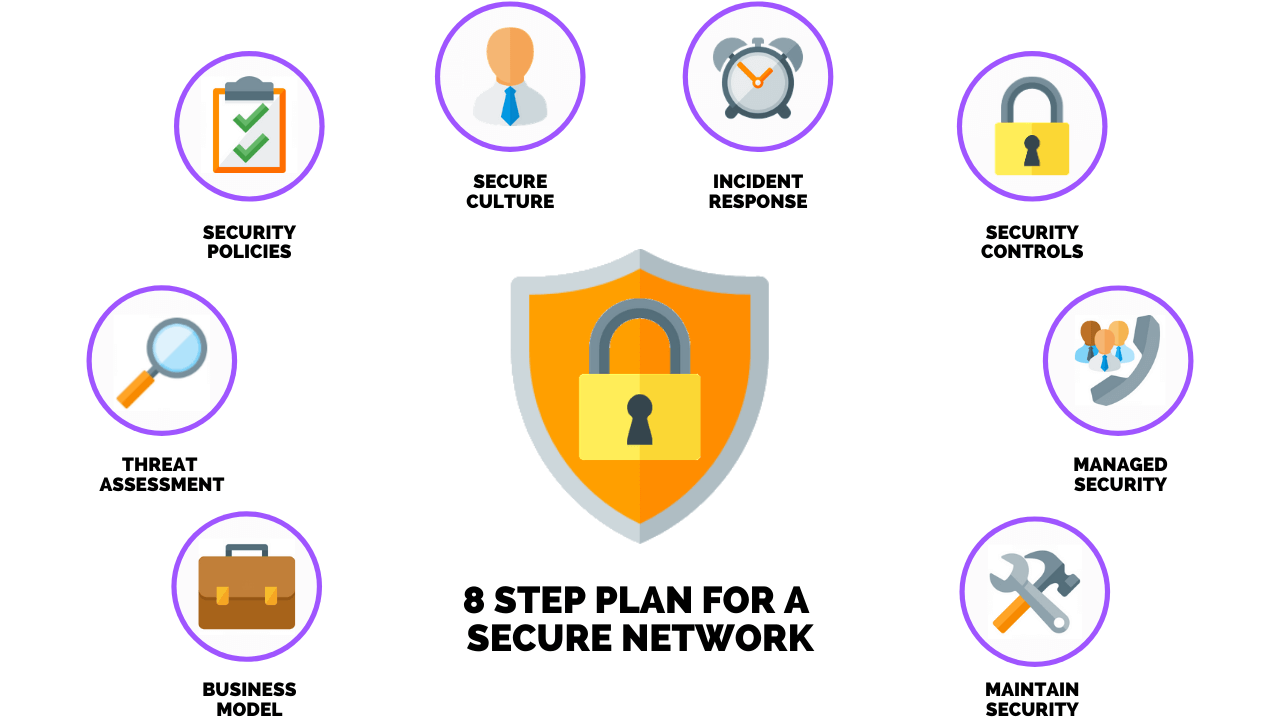
Network structures are arranged over an organization in such a way that it provides the better connectivity in transferring the information across the same network as well as the outside world. The attackers are possibly out there targeting these networks to form a session on the devices and extract 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 residing 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. In this report I will be discussing in detail about the two as well as the working of the same to understand the processes. I will also be learning about different levels of interaction-based honeypots working in detail. The deployment of these honeypots depends on the security risk to the network structure which will be discussed in my report as well. 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 DShield or HoneyPi 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 SSH, RDP, or SMB 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 Virtual Machine (VM). 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.

# literature review

In the literature review part of this 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.

# 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 the 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.

# outcomes

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.

# CONCLUSIONS AND RECOMMENDATIONS

There are at least two sections here that are absolutely required. The preamble sentence is not required.

## Conclusions

The results of experiments performed, and the conclusions made for the work done in this project.

REFERENCES

[1] V.R. Algazi, K.L. Brown, M.J. Ready, D.H. Irvine, C.L. Cadwell, S. Chung, “Transform Representation of the Spectra of Acoustic Speech Segments with Applications-I: General Approach and Application to Speech Recognition”, IEEE Transactions on Speech and Audio Processing 1(2):180-195, April 1993.

[2] S. Chen, C.F.N. Cowan, P.M. Grant, “Orthogonal Least Squares Learning Algorithm for Radial Basis Function Networks”, IEEE Transactions on Neural Networks, 2(2):302-309, March 1991.

[3] Cisco Online, “Understanding Frame Relay Subinterfaces”, http//www.cisco.com/warp/public/779/smbiz/service/knowledge/wan/subifs.htm, Feb. 27, 2000.

[4] V.N. Gupta, M. Lennig, P. Mermelstein, P. Kenny, F. Seitz, D. O’Shaughnessy, “Using Phoneme Duration and Energy Contour Information to Improve Large Vocabulary Isolated-Word Recognition”, Proceedings ICASSP’91, 341-344, 1991.

[5] D.R. Hush, B.G. Horne, “Progress in Supervised Neural Networks: What’s New Since Lippmann?”, IEEE Signal Processing Magazine, 10(1):8-39, January 1993.

[6] R.P. Lippmann, “An Introduction to Computing with Neural Nets”, IEEE ASSP Magazine, 4(2):4-22, April 1987.

[7] S.M. Marcus, A.K. Syrdal, “Speech: Articulatory, Linguistic, Acoustic, and Perceptual Descriptions”, in *Applied Speech Technology*, ed. A. Syrdal, R. Bennett, S. Greenspan, CRC Press, Boca Raton, Florida, 1995.

[8] J.W. Picone, “Signal Modeling Techniques in Speech Recognition”, Proceedings of the IEEE, 81(9):1215-1247, September 1993.

[9] L.R. Rabiner, B.H. Juang, *Fundamentals of Speech Recognition*, Prentice-Hall, Englewood Cliffs, NJ, 1993.

[10] L.R. Rabiner, R.W. Schafer, *Digital Processing of Speech Signals*, Prentice-Hall, Englewood Cliffs, NJ, 1978.

[11] T. Svendsen, K.K. Paliwal, E. Harborg, P.O. Husoy, “An Improved Sub-Word Based Speech Recognizer”, Proceedings ICASSP’89, 108-111, May 1989.

[12] C. Tosuner, *Single Spoken Digit Recognition Using RBF Networks*, Unpublished Master’s Thesis, Technical University of Nova Scotia, Halifax, Nova Scotia, 1996.

[13] J.T. Tou, R.C. Gonzales, *Pattern Recognition Principles*, Addison-Wesley, MA, 1974.