

**Defensive Honeypots for IP IoT  
Devices:  
Quantitative Comparison between  
Vanilla and Sandboxed  
Honeypots**

Franek Kruczynski

September 2025

# Contents

# Chapter 1

## Introduction

### 1.1 Background

Abstract of the project goes here

The Internet of Things (IoT) is vastly expanding, driving a brand new and complex wave of device inter-connectivity worldwide, with an approximate 27-billion devices by the end of 2025 (Jinesh, 2025)

### 1.2 Aims & Objectives

#### 1.2.1 Aim

To evaluate how effective isolation and containment mechanisms (*sandboxing and segmentation*) are at preventing malware propagation within IP IoT honeypot environments, compared to a non-contained (*vanilla*) honeypot – whilst utilising the same data set.

#### 1.2.2 Objectives

The objectives are as follows:

- To design and deploy a controlled Honeypot framework for IoT IP devices, seated within Virtual Machines
- To deploy a minimum of two separate honeypots:
  1. Low-interaction Vanilla Honeypot,
  2. High-interaction Honeypot within a secure container.

- To create a virtual network, where each IoT device and VM have logical addressing and are protected through subnets,
- To collect and store the following malware properties for quantitative comparison and analysis:
  1. Network traffic,
  2. Payloads,
  3. Malware type
  4. Activity data
  5. Propagation attempts outside the container.

## 1.3 Product Review

### 1.3.1 Scope

The project will design and build a **contained IoT Honeypot environment** for IP devices, comparing two separate deployments (*segmented vs vanilla*). It is designed to help understand the theoretical importance of deploying honeypots within a secure container, and evaluate its success against low-interaction vanilla honeypots (Kocaogullar, 2023); considered low security.

What is its purpose ?

How will it work?

### 1.3.2 Audience

Who is this project for?

# Chapter 2

## Background Review

### 2.1 Existing Approaches

Add on to 1.1, provide overview of similar products and why they aren't sufficient

### 2.2 Related Literature

Self explanatory

- Look through thesis provided by supervisor

# Chapter 3

## Methodology & Techniques

### 3.1 Approach

- Link back to objectives?
  - Two separate VMs
  - Lab VM = honeypots
  - Analysis VM = protected

### 3.2 Technologies

### 3.3 Version Control & Management

Introduce GitHub & Supervisor Google Drive

# Chapter 4

## Project Management

### 4.1 Activities

### 4.2 Schedule and Time Management

- Calendar - Allocating times during week

### 4.3 Data Management

- How is this data going to be stored? (Analysis VM using pcaps) - CSV files for extracting

### 4.4 Deliverables

## Chapter 5

## References



# Bibliography

- Jinesh (2025). *How Many IoT Devices Are There in 2025?* URL: <https://autobitslabs.com/how-many-iot-devices-are-there/>.
- Kocaogullar, Y et al. (2023). *Hunting High or Low: Evaluating the Effectiveness of High-Interaction and Low-Interaction Honeypot*. URL: <https://kar.kent.ac.uk/102122/1/STAST2022.pdf>.