Defensive Honeypots for IP IoT Devices: Quantitive 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 the effectiveness of isolation and containment mechanisms *(sandboxing and segmentation)* at preventing malware progatation within IP IoT honeypot encironments, compared to a non-contained *(vanilla)* honeypot – whilst utilizing 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 secure machines *(VMs)*,
- To deploy a minimum of two separate honeypots:
  1. Low-interaction Vanilla Honeypot, mimicking usual IoT devices,
  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 using 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 involves the development and deployment of 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 creating honeypots within a secure container, and evaluating its success against low-interaction vanilla honeypots (Kocaogullar, 2023); further supporting research of malware propagation.

The honeypots will be implemented using Cowrie, a medium-interaction SSH/Telnet based honeypot framework (Oosterhof, n.d.), that has capabilities for both medium and high-interaction modes *(shell and proxy)*. The sandboxed honeypot will be deployed using a combination of Cowrie, FireJail, Doker and, Linux-based kernel security *(AppArmour/seccomp)*. The framework will exist within a Linux-based Virtual Machine, where a separate VM is used for malware data analysis.

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.

Oosterhof, Michel (n.d.). *What is Cowrie?* URL: https://docs.cowrie.org/en/latest/README.html#what-is-cowrie.