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 the effectiveness of containment and sandboxing mechanisms, in preventing malware propagation (specifically its spread into external systems) within a IoT IP device Honeypot framework. Such will be achieved through quantitatively comparing the same malware programs on two separate Honeypots, contained high-interaction against vanilla low-interaction.

1.2.2 Objectives

The objectives are as follows:

- Design, develop and deploy a secure Honeynet framework within Virtual Machines,
- To deploy two separate Honeypots:
  1. **Vanilla Honeypot:** Low-interaction with no advanced security,
  2. **Sandboxed Honeypot:** High-interaction within a secured container.

- To create and design a virtual network, providing both logical addressing to all IoT IP devices, Virtual Machines and, providing security through sub-netting. In essence mimicking a small office network.
- 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.
- Quantitatively compare the data of all malware, and conclude whether attack behaviors differ based on environment.

1.3 Product Review

1.3.1 Scope

The project involves the design, development and deployment of a contained IoT Honeynet environment for a range of various IoT IP devices and varying Honeypots, within a small office network. Each executed piece of malware will have its data collected from both Honeypots, which will then be stored and processed within a separate Virtual Machine outside the environments subnet.

It is designed to evaluate the succesfulness of a high-interaction contained Honeypot against a low-interaction implementation, with the aim to further support pre-existing research regarding malware propagation and identify attacker behaviour patterns *(Kocaogullar, 2023)*.

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.