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

Franek Kruczynski

September 2025

Contents

Chapter 1

Introduction

1.1 Background

The Internet of Things (IoT) is exponentially expanding, with an expected 27 billion devices by the end of 2025 *(Jinesh, 2025)*. Consequently, this surge resulted in much higher malware sophistication and deployment against IoT devices *(Alasmary, 2019)*. Such poses a significant risk to IoT devices, consumers and infrastructures.

Security researchers and organisations now face rapidly growing challenges in Cyber-attack mitigations. IoT devices often lack robust security measures, use outdated firmware *(Gurunath, 2019)* and vary in network defence levels, leaving them susceptible to malware propagation attacks (its spread).

As a result, malware analysis has become a fundamental practice in Cyber research. Traditional defences like IPS/IDS systems and VPNs often fail against Zero-Day and malicious attacks; while Honeypots (decoy systems mimicking IoT devices) provide effective environment control to attract and analyse attackers *(Narendran, 2025)*.

However, the level of interaction with a Honeypot greatly affects containment and data quality. Low-interaction (vanilla) Honeypots provide easier setup with a constraint on security, whereas high-interaction (sandboxed) Honeypots offer greater analytical processing *(Kocaogullar, 2023)*. The balance of containment and interactivity remains a vague area of research.

This project aims to quantitatively compare sandboxed and vanilla Honeypots, to assess benefits of containment and sandboxing effectiveness in preventing malware mitigation within IoT Honeypot frameworks.

1.2 Aims & Objectives

1.2.1 Aim

To evaluate the effectiveness of containment and sandboxing mechanisms in preventing malware propagation in IoT Honeypots, through quantitatively comparing identical samples across vanilla and sandboxed Honeypots.

1.2.2 Objectives

- Design and deploy a secure Honeynet framework within Virtual Machines (VMs),
- Deploy two separate Honeypots:.
  1. **Vanilla Honeypot:** Low-interaction with no advanced security,
  2. **Sandboxed Honeypot:** High-interaction within a secured container.
- Create a virtual network with logical addressing and sub-netting for all IoT IP devices and VMs to mimic a small office network.
- Collect malware properties regarding network traffic, payloads, malware type, activity data and external propagation attempts.
- Quantitatively compare the malware data to conclude whether attack behaviours differ based on environment.

1.3 Product Review

1.3.1 Scope

The project involves development of a secure IoT Honeynet environment, simulating a small office network composed of two Honeypots, executed sequentially within a singular Lab VM. A separate Analysis VM will store and process sample data using **ElasticSearch** to guarantee full isolation from external networks.

Each malware sample will be executed in sequentially running Honeypots under identical conditions, where the collected data will be stored securely, aiming to reveal the impact of containment.

In essence, findings will lead to a greater understanding regarding the importance of Honeypot segmentation. It'll aid in IoT security through identifying

attacker patterns *(Kocaogullar, 2023)* and help expand existing research into secure Honeypot environments and design.

1.3.2 Audience

The primary audience relates to Cyber Security researchers, network analysts and academic institutions studying digital forensics and malware analysis. Such groups will benefit from access to data, from a quantitative dynamic analysis, to strengthen threat detection for security improvement of developing Honeypots.

Furthermore, the framework will also support students and lecturers by providing a secure and safe virtual environment for malware experimentation and research, to demonstrate analytical and ethical practices.

Lastly, a comprehensive analysis of malware may support IoT administrators seeking to develop secure intrusion prevention systems (IDS) *(Fortinet, 2025)*, through ensuring critical flaws are unable to be exploited based on historical data.

Chapter 2

Background Review

2.1 Existing Approaches

Research in malware mitigation includes static analysis and sandboxing systems. Static analysis, such as a Windows-based framework *(Moser A, 2008)* designed to execute malware within a container focused on registering system changes based on run-time behaviour. However, this framework lacks advanced IoT device emulation and has scalability issues regarding resource management, allowing for exploitation.

Systematic and dynamic behavioural analysis of common malware samples *(Genç, 2019)* within a Cuckoo Sandbox provided deep insight into malware attacker patterns. Unfortunately, the ransomware *TeslaCrypt* evaded detection until post-execution, masking the true payload. This demonstrates the concern of poor sandboxing measures in Honeypots.

2.2 Related Literature

IoT-targeting malware research focuses on understanding behavioural patterns and defensive techniques. A graph-based analysis *(Alasmary, 2019)* focused on polymorphic malware utilising unreachable code, improving general malware classification. However, the use of only historical data lacked real-time dynamic collection, crucial for IoT systems.

(Genç, 2019) explored analysis within a popular Sandbox, revealing modern malware's ability to supress execution and remain undetected. It further proved containment alone is not sufficient for IoT system security, therefore Honeypot environments require a combination of containment and deception to secure systems

effectively.

Lastly, *(Narendran, 2025)* highlights the importance of Honeypots within IoT modern architectures, vital for threat intelligence. However, varying integrations across devices remains a vague area of research.

Chapter 3

Methodology & Techniques

3.1 Approach

The project follows an experimental quantitative comparison to evaluate effectiveness of malware containment within IoT architectures to create a controlled testing environment. Two separate VMs will be deployed using **Ubuntu** (Lubuntu) within **Oracle VirtualBox**:

- **Vanilla Honeypot**: **Cowrie** instance operating without additional containment.
- **Sandboxed Honeypot**: Identical **Cowrie** instance inside a **FireJail** & **Docker** container, reinforced with **seccomp** and **AppArmor** to restrict system calls and filter network packets.

A separate Analysis VM will collect data, process logs and analyse packets using **ElasticSearch**, ensuring the VM remains disconnected from external networks. Each sample executed within either Honeypot will run within identical conditions to avoid skew. Metrics like network traffic (pcaps), payload data and program events will be stored securely in CSV files.

Integrity will be enforced via kernel-level kill switches, VM snapshot rollbacks and sub-netting to enforce traffic isolation. Lastly, all collected sample data will be compared statistically to determine whether sandboxing truly improves containment security.

3.2 Technologies

The project will employ various open-source technologies to support controlled analysis. The core framework will operate within **Oracle VirtualBox**, chosen

for its flexibility in sandbox implementation, snapshot management and inter-VM connectivity. Each VM will operate inside **Ubuntu**, a lightweight and stable Linux distribution.

The Honeypots will be implemented in **Cowrie**, an SSH/Telnet Honeypot used for capturing IP-based malware, widely used for its logging capabilities for analysis. The sandboxed Honeypot will be containerised within **Docker**, providing lightweight low level system isolation; while **Firejail** & **AppArmor** will enforce kernel-level security by limiting system calls.

For analysis, **ElasticSearch** will provide real-time log indexing and storage using the RESTful engine complemented by **WireShark** for packet capturing. **Python** scripts will extract sample data and format them into appropriate CSV files for final quantitative comparison.

3.3 Version Control & Management

All configurations, documentations and scripts will be maintained in **GitHub** for transparent project development history, with branching used for different development stages and frequent commits.

Backups will be uploaded to **Google Drive** for redundancy to ensure data synchronisation. Lastly, sensitive data (malware samples and system configs) will remain within the Analysis VM, to ensure ethical and security compliance.

Chapter 4

Project Management

4.1 Activities

Project activities align directly with Section 1.2.2:

- **Management Space:**
  - **(1)** Implement a Linux **nftables** kill switch (kernel-level) to block all IP traffic if containment fails.
  - **(2)** Establish a management level framework for network addressing, VM management and, snapshot rollsbacks.
- **Virtual Framework:**
  - **(1)** Deploy the Lab VM running **Cowrie** for both Honeypots.
  - **(2)** Configure an Analysis VM isolated from external networks.
  - **(3)** Configure sub-netting and a demilitarised zone to separate Honeypots from the host OS.
- **Simulation:**
  - **(1)** Execute both Honeypots on **Cowrie** within **Lubuntu**, with the sand-boxed Honeypot contained.
  - **(2)** Simulate a small office network to replicate realistic attack patterns.
  - **(3)** Execute malware samples under strict controlled conditions.
- **Data Analysis:**
  - **(1)** Capture sample payloads, types and logs.

(2) Use **ElasticSearch** and **Python** to process data and format into CSV.

(3) Conduct quantitative comparison on sample data, analysing relationships across environments.

4.2 Schedule and Time Management

The project will follow a weekly schedule for continuous development:

- **Supervisor Meetings:** Weekly meetings for formative feedback.
- **Calendar Planning:** Personal calendar to dedicate slots for all aspects of development.
- **Time Management:** Personal study will be allocated in daily chunks to balance coursework with dissertation.

Finally, a Gantt chart will aid visualise clear milestones with VM snapshot rollbacks integrated into the timeline to avoid test errors.

4.3 Data Management

All sensitive data (pcaps, logs and samples) will remain within the isolated Analysis VM. Relevant documentation will remain accessible through **GitHub**.

Key policies:

- **Ethical Compliance:** No raw sample will leave the contained Honeypots.
- **Backups:** Frequent backups to **GitHub** and **Google Drive** to ensure synchronisation.
- **Isolation:** Strict VM isolation from external networks.
- **Storage:** Process data stored in CSV files for formatted analysis.

4.4 Deliverables

The project will deliver a secure IoT Honeypot framework with secure sandboxing and a virtual network. The isolated environment will be capable of analysing executed samples.

Additionally, a quantitative dataset containing malware payloads, traffic activity and various logs will be delivered, indexed by **ElasticSearch**. A comprehensive version-controlled repository will house all scripts, documentation and code.

Lastly, a final analytical report evaluating the effectiveness between malware propagation in Honeypot environments.

In essence, the project aims to deliver a practical research tool and verifiable evidence regarding the effectiveness of containment in IoT Honeypots.

Bibliography

Alasmary, H et al. (2019). *Analyzing, Comparing, and Detecting Emerging Malware: A Graph-based Approach*. URL: https://arxiv.org/abs/1902.03955.

Fortinet (2025). *What Is An Intrusion Detection System (IDS)?* URL: https://www.fortinet.com/uk/resources/cyberglossary/intrusion-detection-system.

Genç, Z. A et al. (2019). *Case Study: Analysis and Mitigation of a Novel Sandbox-Evasion Technique*. URL: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/34760373/cecc2019GLS.pdf.

Gurunath, R et al. (2019). *An Overview: Security Issue in IoT Network*. URL: https://ieeexplore.ieee.org/abstract/document/8653728.

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.

Moser A, Y et al. (2008). *Limits of Static Analysis for Malware Detection*. URL: https://ieeexplore.ieee.org/document/4413008.

Narendran, Vaideeswaran (2025). *What Is a Honeypot?* URL: https://www.crowdstrike.com/en-gb/cybersecurity-101/exposure-management/honeypots/.

Appendix A

Ethics Form

OXFORD BROOKES UNIVERSITY

Faculty of Technology, Design and Environment - Ethics Review Form E1

- This form should be completed jointly by the **Supervisor and Student** who is undertaking a research/major project which involves human participants.
- It is the **Supervisor** who is responsible for exercising appropriate professional judgement in this review.
- Before completing this form, please refer to the University **Code of Practice for the Ethical Standards for Research involving Human Participants**, available at https://www.brookes.ac.uk/sites/research-support/research-ethics-and-integrity/policies-procedures-and-useful-documents/obu-urec-code-of-practise-policies and to any guidelines provided by relevant academic or professional associations.
- Note that the ethics review process needs to fully completed and signed **before fieldwork commences**.

(i) Project Title: Defensive Honeypots for IP IoT Devices: Quantitative Comparison between Vanilla and Sandboxed Honeypots

(ii) **Name of Supervisor and School in which located: Mudassar Aslam, Sch Engineering Comp & Mathematics**

(iii) Name of Student and Student Number: Franek Kruczynski 19260104

(iv) Brief description of project outlining where human participants will be involved (30-50 words): Quantitively comparing vanilla and sandboxed Honeypots to identify the benefits of containment. No human participants are physically involved, only the student within testing malicious samples within a secure, virtual and contained environment.

		Yes	No
1.	Does the study involve participants who are unable to give informed consent (e.g. children, people with learning disabilities)?		X
2.	If the study will involve participants who are unable to give informed consent (e.g. children under the age of 18, people with learning disabilities), will you be unable to obtain permission from their parents or guardians (as appropriate)?		X
3.	Will the study require the cooperation of a gatekeeper for initial access to groups or individuals to be recruited (e.g. students, members of a self-help group, employees of a company)?		X

4.	Are there any problems with the participants' right to remain anonymous, or to have the information they give not identifiable as theirs?		X
5.	Will it be necessary for the participants to take part in the study without their knowledge/consent at the time? (e.g. covert observation of people in non-public places?)		X
6.	Will the study involve discussion of or responses to questions the participants might find sensitive? (e.g. own traumatic experiences)		X
7.	Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants?		X
8.	Will blood or tissue samples be obtained from participants?		X
9.	Is pain or more than mild discomfort likely to result from the study?		X
10.	Could the study induce psychological stress or anxiety?		X
11.	Will the study involve prolonged or repetitive testing of participants?		X
12.	Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?		X
13.	Will deception of participants be necessary during the study?		X
14.	Will the study involve NHS patients, staff, carers or premises?		X

Signed:		**Supervisor**
Signed:	Franciszek Kruczynski	**Student**
Date:	16/10/2025	

What to do now:

1. If you have answered **'no'** to all the above questions:

   (a) The student must **send** the completed and fully signed E1 form to their **Dissertation Module Leader.**
   (b) The student must keep a copy of the E1 form which must be bound into their dissertation as an appendix.
   (c) The supervisor must keep a copy of the E1 form as they are responsible for monitoring compliance during the fieldwork.

2. If you have answered **'yes'** to **any** of the above questions:

   (a) The supervisor and student must complete the TDE E2 form available at https://www.brookes.ac.uk/sites/research-support/research-ethics-and-integrity/research-ethics/ethics-application-process-forms/forms-and-templates-for-masters-and-undergraduate
   (b) Note that the information in the E2 must be in **sufficient detail** for the ethical implications to be clearly identified.
   (c) The signed E2 and signed E1 Form must be emailed to Tim Jones (tjones@brookes.ac.uk) who is the Faculty Research Ethics Officer (FREO) for review. Please allow **at least two weeks** for this review process.

(d) If/when approved the FREO will issue an E3 Ethics Approval Notice.
(e) The student must send the E1, E2 and E3 Notice **to the Dissertation Module Leader**.
(f) The student must also keep copies which must be bound into their dissertation as an appendix.
(g) The supervisor must keep a copy of documentation to monitor compliance during field work.

3. If you answered 'yes' to any of questions 1-13 and 'yes' to question 14, an application must be submitted to the appropriate NHS research ethics committee. This is an onerous and time consuming process so the supervisor should liaise early with the FREO if the student is considering this.