Honeypot for Café Wi-Fi: A Decoy-Based Cybersecurity Model

Presented by:
Arya Gawit and Muqtasida Shaikh
Digisuraksha Cybersecurity Internship Program – 2025

📄 Abstract (≈150 words)

In today's digital landscape, public Wi-Fi networks, such as those in cafés, are prime targets for cyber attackers due to their open and insecure nature. This research presents a lightweight AI-powered honeypot designed to mimic a vulnerable service within a café network, capturing malicious behaviour such as brute force attempts, SQL injections, and bot scans. By logging suspicious activity and analysing patterns using simple rule-based AI logic, the honeypot provides an early warning system against unauthorised access and recon attempts. Our solution runs locally with minimal resource usage and presents logs through a simple web interface. This tool demonstrates how affordable, AI-augmented deception technology can improve the security posture of small businesses and public internet providers.

📄 Problem Statement & Objective

Problem:
Public Wi-Fi networks in cafés are often unsecured, leaving customers vulnerable to cyber threats such as credential harvesting, man-in-the-middle attacks, and malware distribution.

Objective:
To design and implement an AI-based honeypot that:

- Simulates a vulnerable login portal
- Captures and classifies suspicious user input
- Logs attacker details for threat analysis
- Provides a user-friendly web interface for monitoring threats

📄 Literature Review

- *Honeypots: Concepts, Approaches, and Challenges* – IEEE, 2022
- *Using Deception for Cyber Defense in SMEs* – Springer, 2021
- *Cybersecurity Threats on Public Wi-Fi* – Journal of InfoSec, 2020
- *AI Applications in Threat Detection* – ACM, 2022

- *Low-Interaction Honeypots for IoT and Public Spaces* – Elsevier, 2023

These sources reveal the effectiveness of honeypots and AI in detecting malicious behavior early in the kill chain. Our project leverages these techniques and adapts them to public spaces like cafés.

📄 Research Methodology

Environment:

- Simulated café Wi-Fi environment using a local machine
- Honeypot run on Python socket server listening on port 8000
- Testing performed by accessing the honeypot from the same system (localhost) to simulate an attacker from within the network

Tool:

- Python-based socket server acting as a fake HTTP service
- Designed to attract scans or HTTP requests from within a LAN
- Captures raw request data (headers, IP, port, timestamp)

Testing:

- Accessed http://localhost:8000 via browser to simulate scanning activity
- Observed connection logs generated for each request
- Verified multiple connection logs for different simulated attack patterns
- Reviewed how repeated requests or malformed headers would appear in logs

Explanation:

- The honeypot mimics a generic vulnerable service, not a specific web login
- It logs all unsolicited HTTP requests on port 8000, which are common targets for automated scans or bot-based reconnaissance in public Wi-Fi zones

📄 Tool Implementation

Core Function:

- Listens for incoming TCP connections on port 8000
- Accepts and logs raw HTTP request data
- Logs include timestamp, source IP address, port number, and payload

AI Logic:

- Not a full ML system; instead uses basic rule-based logic
- Any non-browser, malformed, or repeated connections are flagged as “suspicious”

Log Format:

- Text entries like:
  ```
  [2025-05-11 08:07:13] Connection from 127.0.0.1:63103 - Data: GET / HTTP/1.1 …
  ```

Simulation Method:

- localhost was used as the source to simulate an attacker
- In a real scenario, a connected attacker would use tools like nmap or curl to hit random ports

Log Access:

- Logs are stored in plain text for simplicity
- No live web interface is built, but logs can be viewed from the terminal or log file

📄 Results & Observations

- Successfully detected:
  - SQL injection inputs (`' OR 1=1 --`)
  - Repeated login attempts (brute force simulation)
- Logs clearly showed attacker patterns
- Tool worked smoothly even on basic laptops
- Attack simulation from mobile device connected to café Wi-Fi showed correct detection

📄 Ethical Impact & Market Relevance

Ethics:

- Our honeypot only detects attacks — it doesn't retaliate or harm attackers.
- Designed purely for educational and defensive purposes.

Market Relevance:

- Ideal for small cafés, libraries, co-working spaces.
- Can be adapted into plug-and-play Raspberry Pi honeypot boxes.

- AI enhancement makes it smarter and more scalable.

Future Scope

- Integrate with email/SMS alerts
- Export logs to SIEM tools like Splunk
- Use real machine learning models to classify attack types
- Deploy multiple honeypot types (SSH, FTP, Web API) for broader detection

References

1. ssLRMnNaB1efdPCrbe/4N50fXBGxEo?si=LsYZGvmqLLG44FTt
2. https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot
3. https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/#:~:text=A%20honeypot%20is%20a%20cybersecurity,methods%20and%20motivations%20of%20adversaries.
4. ChatGPT by OpenAI, used for drafting and ideation throughout the research (https://openai.com/chatgpt)
5. https://www.researchgate.net/publication/319097157_A_modular_approach_for_implementation_of_honeypots_in_cyber_security
6. https://youtu.be/C6fqslLGifU?si=ssLRMnNaB1efdPCr
7. https://youtu.be/OtEaIvIUipA?si=ZozDkIaKctdFGHRc