## **Hackathon Problem Document**

**Revolutionise Network Penetration Testing**

#### ***Problem Statement***

Wireless communication networks, including Bluetooth, NFC, RFID, and proprietary radio frequencies, are increasingly vulnerable to sophisticated attacks due to their growing complexity. Many existing tools fail to provide comprehensive coverage across these diverse protocols, limiting the ability of security professionals to detect and mitigate potential threats effectively. The absence of a cost-effective, modular solution that can be easily customised to meet evolving security challenges highlights the need for a new approach to penetration testing.

#### ***Objective***

The goal of this project is to develop a versatile network penetration tool using a Raspberry Pi 3, integrated with various wireless modules like CC1101, NFC, RFID, and Bluetooth. This tool will offer comprehensive testing capabilities across multiple wireless protocols, providing a flexible and cost-effective solution for security professionals

#### **References to Existing Tools**

1. **Flipper Zero :** [**website**](https://flipperzero.one/)
2. **Hak5 Wi-Fi Pineapple :** [**website**](https://shop.hak5.org/)
3. **Proxmark3 :** [**website**](https://proxmark.org/)
4. **Chameleon Minic :** [**website**](https://github.com/emsec/ChameleonMini)
5. **Galkan-Tools :** [**website**](https://github.com/galkan/tools)

**Conclusion :**

In conclusion, this project seeks to address the deficiencies of current market tools by creating a modular and versatile network penetration tool utilising Raspberry Pi 3 along with various wireless communication modules. The developed tool will offer extensive testing functionalities across a range of wireless protocols, while also being cost-effective and user-friendly. This makes it an essential resource for both individual security researchers and organisations striving to protect their wireless networks from emerging threats.