# **Performance Testing and Risk Analysis Document**

## **Project: Wi-Fi WPA2 Key Extractor GUI**

### **1. Introduction**

**Purpose:** This document outlines the performance testing plan and risk analysis for the Wi-Fi WPA2 Key Extractor GUI project. It aims to validate the system's responsiveness, resource efficiency, and resilience under expected and adverse conditions, while also identifying and mitigating potential risks.

**Scope:** Covers all performance-critical functionalities including network scanning, packet capturing, deauthentication, and GUI responsiveness. Also assesses operational, technical, and security-related risks.

### **2. Performance Testing Strategy**

**Objectives:**

* Measure system responsiveness under normal and high-load conditions
* Evaluate resource utilization (CPU, RAM)
* Ensure GUI remains responsive during long-running subprocesses
* Validate performance of subprocess interactions (aircrack-ng tools)

**Test Environment:**

* OS: Kali Linux
* CPU: Minimum dual-core
* RAM: Minimum 4GB
* External USB Wi-Fi Adapter (monitor mode capable)

**Tools Used:**

* Python 3 profiler (cProfile)
* htop or top for runtime monitoring
* Manual stopwatch for GUI interaction delays

**Test Scenarios:**

1. **Network Scan Latency**
   * Measure time taken from clicking "Scan Networks" to list population
2. **Attack Sequence Timing**
   * Time from "Start Attack" to handshake capture
3. **UI Responsiveness Under Load**
   * Test GUI reaction during background subprocess execution
4. **Resource Usage Profile**
   * Measure CPU/memory during scanning and attack phases

**Acceptance Criteria:**

* Network scan completes in < 10 seconds under typical network conditions
* GUI does not freeze during subprocess execution
* Memory usage stays under 300MB during normal usage
* CPU utilization does not spike above 85% for more than 3 seconds

### **3. Risk Analysis**

**Risk Management Objectives:**

* Identify threats to the stability, security, and legality of the tool
* Classify risks by severity and likelihood
* Propose mitigations

**Risk Table:**

| **Risk ID** | **Description** | **Severity** | **Likelihood** | **Mitigation** |
| --- | --- | --- | --- | --- |
| R1 | Wi-Fi adapter not supporting monitor mode | High | Medium | Include adapter check with error handling |
| R2 | GUI freezing during subprocesses | Medium | High | Use threading for all subprocesses |
| R3 | Incorrect parsing of network scan | Medium | Medium | Improve string parsing and add fallback for nmcli |
| R4 | Running without root permissions | High | High | Alert user and exit with proper message |
| R5 | Legal misuse of tool | High | Medium | Include disclaimer and restrict usage documentation |
| R6 | Aircrack-ng not installed | Medium | Medium | Validate environment and alert user |
| R7 | Unresponsive networks or handshake failures | Medium | High | Add retry mechanism and user feedback |

### **4. Monitoring and Reporting**

* Logs will be printed in GUI and optionally saved to a file (future enhancement)
* Performance results and anomalies will be manually recorded during testing

**Report Template Example:**

Test: Network Scan

Start Time: 12:05 PM

End Time: 12:06 PM

Duration: 1 min

Result: Success

Resource Usage: CPU avg 30%, RAM peak 120MB

### **5. Review and Updates**

* This document will be reviewed after each major feature addition
* Risks will be reassessed biweekly or after critical changes

**Document Owner:** Laxmish Saini  
 **Last Updated:** March 31, 2025