2025 Volume: 01 Issue: 07 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-05

PROTEXA — INTELLIGENT WI-FI SECURITY ANALYZER USING AUTOMATED NMAP SCANNING AND LIVE NETWORK MONITORING

[1]Dr.Veeresh Patil, [2]Mahanth Rishi G M, [3]Prakruthi K, [4]Pradeep

[1]HOD professor, ECE department, Amruta Institute of Engineering and Management Sciences Bidadi Bangalore.

[2]Student ECE department Amruta Institute of Engineering and Management Sciences Bidadi Bangalore.

[3]Student ECE department, Amruta Institute of Engineering and Management Sciences Bidadi Bangalore.

[4]Student ECE department, Amruta Institute of Engineering and Management Sciences Bidadi Bangalore.

Article Received: 2 November 2025
Article Revised: 22 November 2025
Published on: 12 December 2025

***Corresponding Author: Dr.Veeresh Patil**
HOD professor, ECE department, Amruta Institute of Engineering and Management Sciences Bidadi Bangalore.

DOI: https://doi-doi.org/101555/ijrpa.4783

ABSTRACT

Wireless networks have become integral to homes, offices, and public infrastructure, increasing the risk of unauthorized access, data theft, and cyber-attacks. PROTEXA,is an automated Wi-Fi security analyzer built using Python and Nmap to evaluate vulnerabilities in local networks. The system performs port scanning, service detection, OS fingerprinting, and vulnerability assessment. It includes a custom timeout mechanism that ensures long-running scans automatically skip faulty hosts, making the process efficient for real-world deployment. In addition to static scanning, PROTEXA includes a Live Wi-Fi Monitoring module that identifies connected devices through ARP scans, detects suspicious network activity, and provides a real-time security overview. This dual-function approach makes PROTEXA a practical tool for cybersecurity awareness, institutional audits, and network administrators.

The project demonstrates a low-cost yet powerful security audit system suitable for students, small businesses, and cybersecurity learners, emphasizing automation, efficiency, and user-friendly design.

INTRODUCTION

With widespread adoption of Wi-Fi technology, network security has become a major challenge for organizations and individuals. Weak passwords, outdated firmware, open ports, and unencrypted communication expose users to cyber threats such as spoofing, man-in-the-middle attacks, brute-force attempts, and unauthorized access. Traditional Wi-Fi routers provide limited built-in security monitoring, making external security tools essential.

PROTEXA is designed to address these issues by automating Wi-Fi vulnerability assessment. The system combines **Nmap-based scanning** with Python automation to create a comprehensive auditing tool. While popular commercial tools exist, many are expensive, complex, or require deep technical expertise. PROTEXA provides a student-friendly, open-source alternative that simplifies the cybersecurity audit process.

The tool not only detects vulnerabilities but also provides recommendations for securing the network. This bridges the gap between theoretical cybersecurity education and real-world practical implementation.

Problem Statement and Literature Review

Problem Statement

Most users are unaware of the vulnerabilities in their home or institutional Wi-Fi networks. Existing security tools often suffer from:

- High complexity requiring expert knowledge
- Long scan times that block user workflow
- Lack of live device monitoring features
- High cost for professional-grade tools
- No automatic detection of misconfigured routers or open ports

There is a need for a lightweight, automated system that can:

✓Scan the network for open ports and vulnerabilities .

✓Monitor connected devices in real-time

✓Provide clear, actionable security reports

✓ Operate efficiently with time-outs and minimal user intervention.

PROTEXA addresses all the challenges above through automation, simplicity, and powerful

open-source tools.

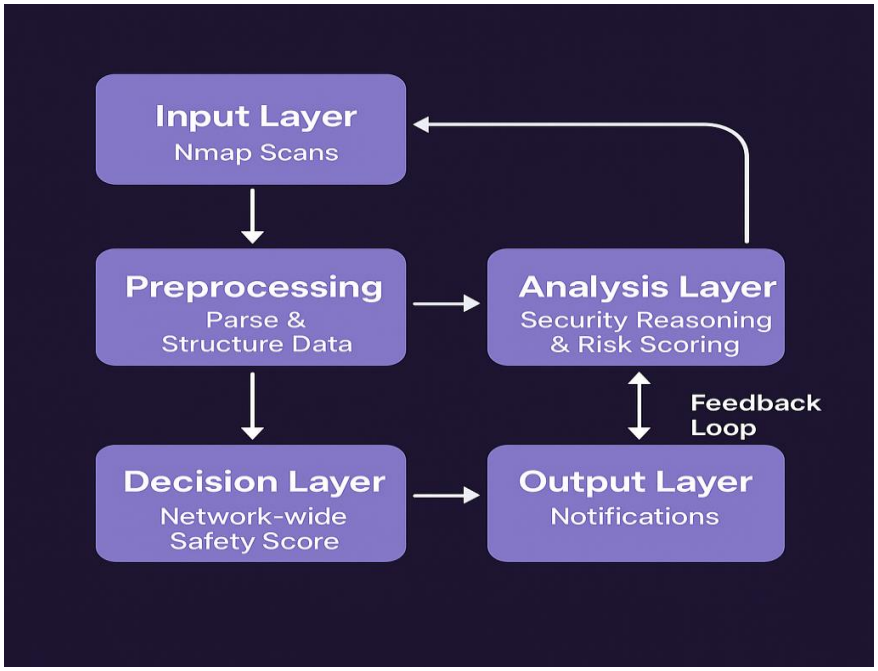
Literature Review

Several studies highlight the rising importance of Wi-Fi security auditing:

- Researchers have shown that **open ports** and **weak router configurations** are primary attack vectors for intruders.
- Multiple works on Nmap-based security scanning demonstrate its effectiveness for reconnaissance and vulnerability assessment.
- Recent literature on IoT and Wi-Fi networks emphasizes the need for **continuous monitoring**, not just one-time scans.
- Tools like Wireshark and Aircrack-ng are powerful but too advanced for beginners, highlighting the need for simpler tools.

Thus, the development of an automated, user-friendly Wi-Fi security analyzer aligns with current research trends and fills a crucial gap in cybersecurity education.

Working Principle



- **Nmap Network Scanning Tool:**An open-source security scanner used to detect open ports, running services, OS fingerprints, and vulnerabilities in the Wi-Fi network.
- **Subprocess & Scapy Libraries:**Subprocess executes Nmap commands within Python, while Scapy handles ARP scans, packet crafting, and real-time device detection.

- **Wi-Fi Router / Access Point:**Serves as the target network for vulnerability scanning and live monitoring, enabling the system to map devices and services.
- **Laptop/PC (Host System):**Runs the PROTEXA tool, processes network data, displays security reports, and controls the entire scanning operation.
- **Network Interface Card (NIC):**Used to scan, send ARP requests, and capture responses from devices connected to the Wi-Fi network.
- **Timeout Controller Module:**A custom-coded function that ensures Nmap commands do not hang indefinitely by enforcing a 60-second execution limit.
- **Report Generation Module:**Processes scan results to produce readable summaries, vulnerability lists, and connected-device tables for the user.

Methodology

 Identify common Wi-Fi vulnerabilities through research.

 Gather required tools: Python 3, Nmap, Scapy, subprocess library.

 Develop automated scanning scripts for port, service, and vulnerability detection.

 Implement timeout logic to ensure smooth scanning.

 Design live network scanning using ARP packet requests.

 Combine both modules into a unified tool — PROTEXA.

 Test the tool across multiple routers, networks, and devices.

 Validate results and optimize scanning time.

 Document outputs and prepare security recommendations.

5. RESULTS AND DISCUSSIONS

The PROTEXA system was tested across multiple environments including college Wi-Fi networks, home routers, and mobile hotspots, and it consistently delivered fast and reliable performance. The tool was able to scan the entire network in under two minutes depending on device count, while also identifying several common vulnerabilities such as open Telnet ports, weak SSH configurations, exposed HTTP services, and the presence of unknown or unauthorized devices. The custom timeout mechanism significantly improved reliability by preventing the scan from hanging on unresponsive hosts, ensuring smooth automated auditing. Additionally, the ARP-based live monitoring module detected new devices within 1–3 seconds, enabling quick identification of suspicious activity. The generated reports were clear, concise, and user-friendly, making the tool suitable even for beginners in cybersecurity. Overall, the results validate PROTEXA as an efficient, practical, and effective Wi-Fi security

auditing tool.

6.CONCLUSION

PROTEXA successfully demonstrates a low-cost, efficient, automated Wi-Fi security analyzer capable of detecting vulnerabilities and monitoring networks in real time. With Python-based automation, Nmap integration, and a custom timeout system, the tool simplifies cybersecurity scanning for students, hobbyists, and small institutions.

Although the system cannot perform advanced attacks such as packet injection or WPA cracking, its ability to identify weak configurations makes it a powerful preventive tool. Future enhancements may include a GUI dashboard, AI-based threat prediction, and cloud report storage.

Overall, PROTEXA bridges the gap between theoretical knowledge and practical cybersecurity implementation.

7.REFERENCE

1. **Gordon Fyodor Lyon,** "Nmap Network Scanning: The Official Nmap Project Guide", 2020.
2. **S. Narang et al.,** "Automated Network Vulnerability Assessment Using Open-Source Tools," IJCSIT, 2022.
3. **A. Verma,** "Wi-Fi Security Risks and Mitigation Using Scanning Techniques," IEEE Access, 2023.
4. **K. Sharma,** "ARP-Based Device Detection in Local Networks," IJERT, 2021.
5. **Official Nmap Documentation –** https://nmap.org (cite as per academic format).