iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78536

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Wi-Fi Network Packet-Port Vulnerability and Security Analyzer

G. Vijaya Lakshmi[1], B. Manoj Kumar[2], T. Chandra Sekhar[3], K. Raghavendhra Sai[4], A. Rakesh Kumar[5]
[1]*Assistant Professor, Computer Science And Engineering, Sanketika Vidya Parishad Engineering College, Vishakhapatnam, Andhra Pradesh, India*
[2, 3, 4,5]*B.Tech Final Semester, Bachelor of Technology, , Computer Science And Engineering, Sanketika Vidya Parishad Engineering College, Vishakhapatnam, Andhra Pradesh, India*

Abstract: ***Wireless networks are the primary gateways for modern digital communication, yet they remain susceptible to critical vulnerabilities due to weak encryption, exposed ports, and the lack of integrated monitoring. Existing security tools are often fragmented and command-line driven, creating a significant "expert-gap" that leaves administrators unable to visualize their risk posture effectively. To address these challenges, this project introduces an Integrated Wi-Fi Network Packet-Port Vulnerability and Security Analyzer. Developed using a Python-Flask framework, the system implements a synchronized, multi-layered diagnostic pipeline protected by a secure User Authentication and Login module. The backend utilizes Scapy for real-time ARP integrity monitoring and Nmap for granular service discovery. A key innovation is the Heuristic Rule-Based Audit engine, which cross-references discovered services against global CVE databases via RESTful APIs to provide live threat intelligence. To ensure proactive defense, the system features an Automated Email Alerting mechanism that triggers a critical notification to the administrator whenever the Network Health Score falls below a 50% threshold.***
The final implementation features a high-fidelity web dashboard that synthesizes complex telemetry into a quantifiable health score based on CVSS principles. By automating Security Audit Reports and providing structured Remediation Roadmaps, the project transforms raw network data into actionable security intelligence. This unified platform offers a proactive, scalable solution for enhancing wireless integrity in both residential and enterprise environments.
Keywords: Cybersecurity, Network Auditing, Packet Inspection, Port Scanning, Heuristic Analysis, Flask Framework.

I. INTRODUCTION

The rapid proliferation of wireless networking in both domestic and public environments has introduced significant security challenges, often leaving sensitive data exposed to sophisticated cyber threats [1][2][4]. Most home and small-office routers are configured for convenience rather than security, while public hotspots frequently lack the encryption necessary to protect users from intercepted traffic [2][5]. This project presents a comprehensive, intelligent network security probe designed to bridge the gap between complex industrial auditing tools and user-friendly consumer applications. It serves as an integrated diagnostic suite that audits the three fundamental layers of local area network security: the Physical/Wireless Layer, the Link Layer, and the Transport Layer .To ensure data integrity and restricted access, the system incorporates a secure User Authentication and Login module, ensuring that sensitive network telemetry is accessible only to authorized administrators. Unlike traditional scanners that merely list active connections, it utilizes a Heuristic Risk Engine to calculate a real-time "Network Health Score" based on vulnerability severity metrics inspired by industry standards such as CVSS [9]. A critical innovation of this system is its Automated Incident Response Layer; when the calculated health score falls below a critical threshold of 50%, the system immediately triggers an automated email alert to the administrator's verified address. By integrating with global vulnerability databases through a CVE Lookup Module, the system cross-references detected service versions with documented exploits [19][20], providing a professional-grade assessment of a network's threat posture. The final output is an actionable and exportable security audit and real-time notification suite that translates technical vulnerabilities into clear remediation roadmaps, enabling users to effectively harden their digital environments against modern cyber threats.

II. LITERATURE SURVEY

The academic and technical discourse surrounding wireless network security emphasizes the critical need for integrated auditing frameworks that address the multi-layered nature of modern cyber threats. Research by Masiukiewicz et al. [1] and Noor & Hassan [6] establishes that the proliferation of IEEE 802.11 networks has created a broad attack surface, ranging from physical layer

©IJRASET: All Rights are Reserved

vulnerabilities to complex link-layer interceptions. While standard encryption protocols exist, Mekhaznia & Zidani [4] argue that configuration oversights and legacy support often leave these networks susceptible to exploitation. This necessitates a transition from basic connectivity monitoring to deep-tier security probing that encompasses physical, link, and transport layer vulnerabilities.

A primary challenge identified in the literature is the "Expert-Gap" created by the fragmented nature of existing security tools. Sridaran & Budhrani [5] highlight that while utilities like Nmap [7] and Aircrack-ng [8] provide robust granular data, they operate as isolated silos. This decentralized approach requires human auditors to manually synthesize disparate terminal outputs into a cohesive security context. Simbaña et al. [3] propose that the solution lies in the development of practical vulnerability analysis toolkits that automate the reconnaissance process, thereby reducing the reliance on high-level command-line proficiency and making professional-grade auditing accessible to general administrators.

Furthermore, the integration of real-time threat intelligence has become a focal point for modern defensive research. Traditional scanning methodologies often rely on static, local definitions of risk which quickly become obsolete against evolving "Zero-Day" threats. According to Bheevgade et al. [2], the rise of public Wi-Fi infrastructure has heightened the necessity for automated cross-referencing with global repositories such as the National Vulnerability Database (NVD) [19] and CVE lists [20]. By aligning local telemetry with the Common Vulnerability Scoring System (CVSS) [9] and the OWISAM methodology [10], researchers argue that systems can produce standardized risk metrics. This theoretical shift from reactive logging to proactive, intelligence-driven remediation represents the current frontier in wireless security architecture.

III. EXISTING SYSTEM

The current landscape of wireless security assessment is defined by a decentralized collection of specialized utilities that operate in manual, disconnected phases[1],[6]. Methodologically, these tools span three operational layers: network discovery, traffic inspection, and active threat simulation. At the discovery level, engines like Nmap[7] provide granular service enumeration but lack user-centric risk interpretation. Deep traffic analysis is typically conducted via Wireshark [14] or Scapy [13] , while active penetration testing is relegated to frameworks such as WiFi-Pumpkin [16] and Aircrack-ng [8]. While technically robust, these tools function as isolated silos, requiring human auditors to manually aggregate disparate terminal outputs into a cohesive security context [5]. This results in a significant "expert-gap," where the deep technical granularity of the tools remains inaccessible to general administrators lacking extensive command-line proficiency [4].

A. Core Systemic Challenges

Despite their sophistication, existing frameworks face five primary challenges that hinder proactive security management:

1) Operational Complexity: A heavy reliance on command-line interfaces (CLI) necessitates high technical literacy to execute commands and parse raw data strings [4].

2) Lack of Modular Integration: The absence of a unified workflow forces users to transition between different environments for port scanning [7] and ARP monitoring [13], leading to fragmented oversight.

3) Visualization Deficit: Most utilities lack structured web dashboards, relying instead on raw log files which obscure real-time patterns and network risk postures [12].

4) Decoupled Intelligence: There is a critical absence of automated cross-referencing with global threat repositories; most tools fail to query the National Vulnerability Database[19] or CVE lists[20] automatically.

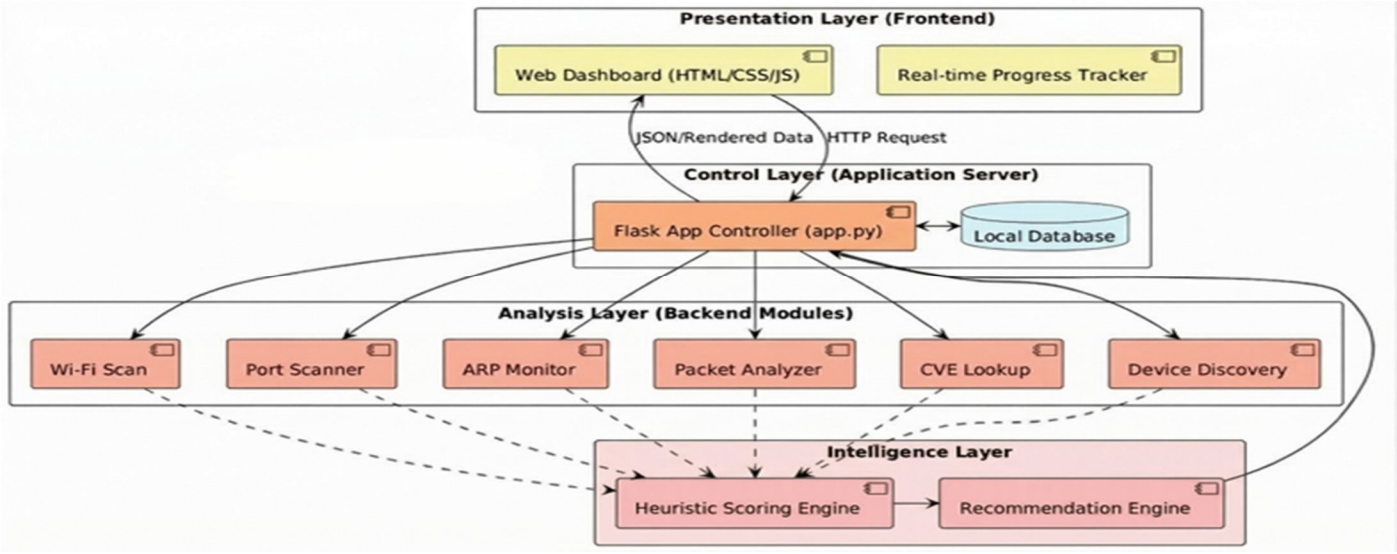
5) Passive Incident Response: Most existing frameworks function only as diagnostic tools, lacking automated alerting mechanisms (like SMTP notifications). This forces administrators to manually review logs rather than receiving real-time triggers when a security threshold is breached [12]

IV. PROPOSED SYSTEM

The proposed Wi-Fi Network Packet-Port Vulnerability and Security Analyzer is conceptualized as a "Unified Security Framework" designed to bridge the structural gap between complex network telemetry and actionable intelligence. Unlike fragmented utilities that require manual coordination [4], this system synchronizes discovery and threat intelligence into a cohesive diagnostic environment. The fundamental objective is to automate the transition from raw packet capture to risk mitigation using a modular architecture accessible to both expert and non-expert administrators [12]. To ensure secure data access and multi-user integrity, the framework incorporates a Robust User Authentication and Login System, restricting sensitive network telemetry to verified personnel To achieve this, the system utilizes a Three-Tier Architectural Model consisting of a Data Acquisition Layer, a Processing Layer, and a Presentation Layer.

The Data Acquisition Layer serves as the primary sensory organ, leveraging Scapy[13] and Nmap [7] for low-level packet sniffing and port sweeping. The Processing and Intelligence Layer acts as the central logic unit, cross-referencing fingerprinting data against the National Vulnerability Database[19] and CVE lists[20] via RESTful APIs. Finally, the Presentation Layer, developed using the Flask framework[12], synthesizes these diverse threat vectors into an intuitive web interface and a quantifiable "Network Health Score."

The core innovation of this framework is its synchronized 9-stage execution pipeline, ensuring a comprehensive wireless audit. The process initiates with environment mapping and active asset discovery to identify SSIDs and hardware standards[11], followed by port probing and service fingerprinting to determine open logical ports and software versions. For real-time integrity, the system executes ARP monitoring to detect Man-in-the-Middle (MITM) attempts[5] and Deep Packet Inspection (DPI) to flag unencrypted data leakage. The intelligence phase concludes with vulnerability correlation[20] and a proprietary Heuristic Risk Scoring algorithm, This intelligence layer is further enhanced by an Automated Email Alerting Mechanism, which serves as an active incident response trigger, dispatching critical security notifications to the administrator whenever the Network Health Score drops below the 50% safety threshold which uses weighted logic to ensure that critical threats—such as active spoofing—are prioritized over minor configuration issues[14]. The cycle concludes with data persistence in a local SQLite database[15] for automated report generation. To facilitate immediate risk mitigation, the framework includes an Integrated Defense Gateway that provides a direct interface for users to establish encrypted VPN tunnels, ensuring communication integrity immediately upon the discovery of a network vulnerability.



A. Advantages

The proposed framework introduces several distinct advantages over traditional, command-line-driven security utilities:

1) Actionable Remediation Roadmap: Beyond identifying flaws, the system provides structured guidance for network hardening, translating technical vulnerabilities into clear fix-actions.

2) Automated Intelligence Integration: Native integration with the NIST database[19] eliminates the manual labor involved in searching for exploits associated with specific software versions.

3) Historical Trend Analysis: Utilizing local persistence [15] enables a longitudinal view of network integrity, allowing users to track their security posture over time.

4) Performance Optimization: The analyzer employs "passive-active" scanning techniques, ensuring that comprehensive packet captures do not degrade the user's operational bandwidth.

5) Weighted Heuristic Scoring: By employing logic that prioritizes high-impact threats, the system provides a more realistic assessment of safety compared to simple arithmetic averages.

6) Proactive Incident Response: The integration of automated email alerts ensures that critical security breaches are communicated in real-time, allowing for immediate intervention without requiring the user to be actively monitoring the dashboard

7) Integrated Mitigation Gateway: Unlike standard scanning utilities that only identify flaws, this system offers a direct pathway to deploy encrypted VPN protocols, enabling users to secure their traffic and mask network identity with a single action.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

V. ALGORITHMS AND TECHNOLOGIES USED

The implementation of the system relies on a multi-stage logic flow to ensure data consistency and accurate risk quantification. This section details the Heuristic Scoring Algorithm and the technical stack utilized to bridge the gap between low-level network data and actionable security intelligence.

A. Weighted Heuristic Scoring Algorithm

The operational "brain" of the analyzer is a negative-weighting mathematical model designed to quantify network risk. Unlike systems that award points for security, this algorithm starts with a base health score ($S_{\{base\}} = 100$) and applies deductions based on identified vulnerabilities.

B. Mathematical Formula

The Final Health Score (H) is calculated as:

$$H = 100 - \Sigma(W_i * V_i)$$

Where:

- W_i represents the Severity Weight of a specific vulnerability.
- V_i represents the instance count or boolean presence of that vulnerability.

C. Standardized Weighting Logic

The system categorizes risks into tiers to ensure that critical threats are prioritized:

1) Critical Threats ($W = 40$): Active ARP spoofing or "OPEN" encryption standards. These represent high-impact faults allowing immediate data interception.
2) High-Risk Vulnerabilities ($W = 20$): Services with a CVSS score higher than 8.0 or the presence of insecure legacy protocols like Telnet and FTP.
3) Moderate Risks ($W=10$): Outdated service versions or unencrypted HTTP traffic.
4) Information Alerts ($W = 5$): Non-standard open ports with no documented CVEs.

The final score is normalized to a 0–100 range, where scores below 50 are classified as High Risk

D. Technologies Used

The system architecture is built upon a multi-tier stack designed to balance low-level network reconnaissance with professional-grade data visualization and automated incident response protocols. This structured approach ensures that high-fidelity security telemetry—harvested via raw socket operations—is seamlessly translated into an intuitive management interface. By decoupling Data Acquisition from Presentation, the framework maintains high operational performance while enabling event-driven alerting and real-time mitigation the moment a critical vulnerability is detected.

E. Backend and Core Logic

1) Python 3.x: Serves as the primary logic engine for orchestrating the synchronized 9-stage diagnostic pipeline. It leverages the Threading library for non-blocking background threat monitoring and the Subprocess module to facilitate low-level binary interfacing with Nmap and VPN utilities.
2) Flask Framework [12]: A lightweight WSGI micro-framework that functions as the middleware bridging the client-side interface with backend security scripts. It utilizes the Jinja2 templating engine for dynamic server-side rendering of real-time scan telemetry.
3) Scapy [13]: A sophisticated packet manipulation and sniffing library utilized for Deep Packet Inspection (DPI) and real-time ARP integrity monitoring to detect link-layer intercepted traffic.
4) Nmap (Network Mapper) [7]: Integrated via automated binary execution to perform high-resolution port auditing, service version detection, and remote OS fingerprinting.
5) SMTP & SMTPLIB: Implements the Simple Mail Transfer Protocol to establish encrypted connections with remote mail servers, enabling automated incident response via high-priority email alerts when the health score falls below the 50% threshold.

©IJRASET: All Rights are Reserved

F. Data Science and Intelligence Link

1) SQLite [15]: This is a lightweight, server-less database used to save every scan result. It allows the system to perform longitudinal trend analysis, which is a fancy way of saying it lets the user look back at past scans to see if their network security is getting better or worse over time.

2) Pandas & NumPy: These are powerful "Data Science" tools used to handle the heavy lifting. Specifically, they allow the system to quickly process large-scale security logs (like .csv files) during the audit phase, turning thousands of lines of raw data into simple, organized information.

3) RESTful API & CVSS [9]: Instead of relying on old, out-of-date information stored on your computer, the system uses APIs to "talk" to the internet in real-time. It fetches the latest threat data from global databases (NIST [19] and CVE [20]) to ensure your security score matches international industry standards.

4) Collections (Counter): This is a specialized tool used within the packet analyzer to "count" network traffic as it happens. It tracks exactly how many TCP vs. UDP packets are moving through the air, which is what creates the live charts on your dashboard.

G. Frontend Stack

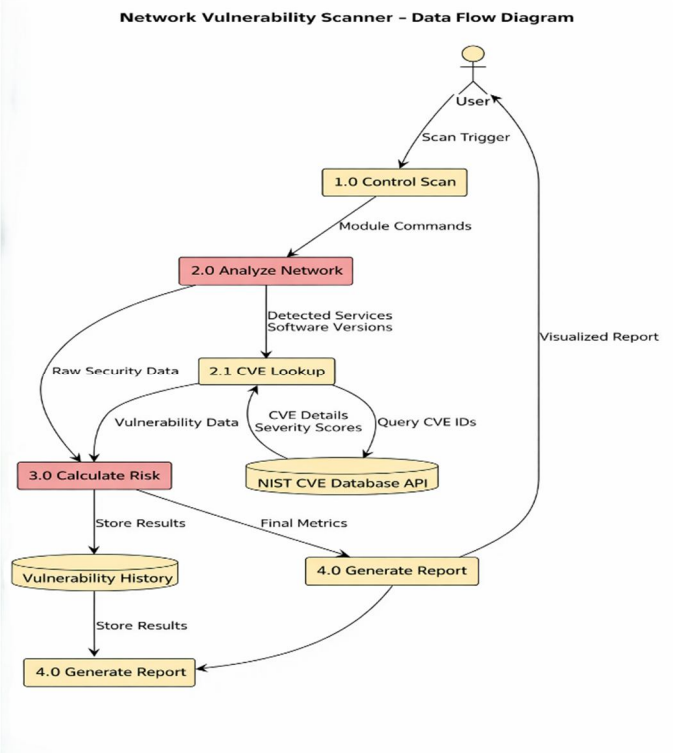
1) Tailwind CSS: A modern design framework used to create a "Glassmorphism" aesthetic. This provides a sleek, semi-transparent dark-mode dashboard that organizes complex security data into clean, readable sections, reducing visual clutter for the user.

2) JavaScript & Lucide-React: These tools manage the "live" feel of the interface. JavaScript allows the scan results to update instantly without refreshing the page, while Lucide provides high-quality icons (like shields and alerts) so users can understand threat levels at a glance.

3) HTML5 & CSS3: The fundamental building blocks used to create the "skeleton" and custom styling of the platform. They ensure the Security Audit Reports are structured logically and that critical alerts are clearly color-coded for easy identification.

VI. METHODOLOGY

The methodology of this project implements a multi-tier modular architecture designed to bridge the gap between low-level network telemetry and actionable security intelligence. The system follows a structured 9-stage execution pipeline, ensuring that data flows seamlessly from raw packet capture to a finalized security report.



A. Input

The Input phase serves as the primary handshake between the network administrator and the analytical backend. This stage is responsible for capturing the environmental parameters required to bound the scope of the security audit.

1) Scan Trigger: The process is initiated by the user through a "Scan Trigger" on the web-based dashboard. This event sends an asynchronous request to the Flask control layer (Process 1.0).

2) Environmental Parameters: The system requires specific inputs to interface with hardware, including the selection of the target Network Interface Card (NIC).

3) Administrative Authorization: To perform raw socket operations for packet sniffing (Scapy) and stealth port scanning (Nmap), the system must receive an "elevated privilege" input from the host operating system.

4) User Authentication Credentials: To secure the diagnostic environment, the initial input requires a verified username and password. This credential check ensures that only authorized administrators can trigger the 9-stage pipeline and access sensitive network telemetry

5) Subnet Mapping Input: The system automatically identifies the subnet mask and gateway IP to define the boundaries for the subsequent discovery and probing phases.

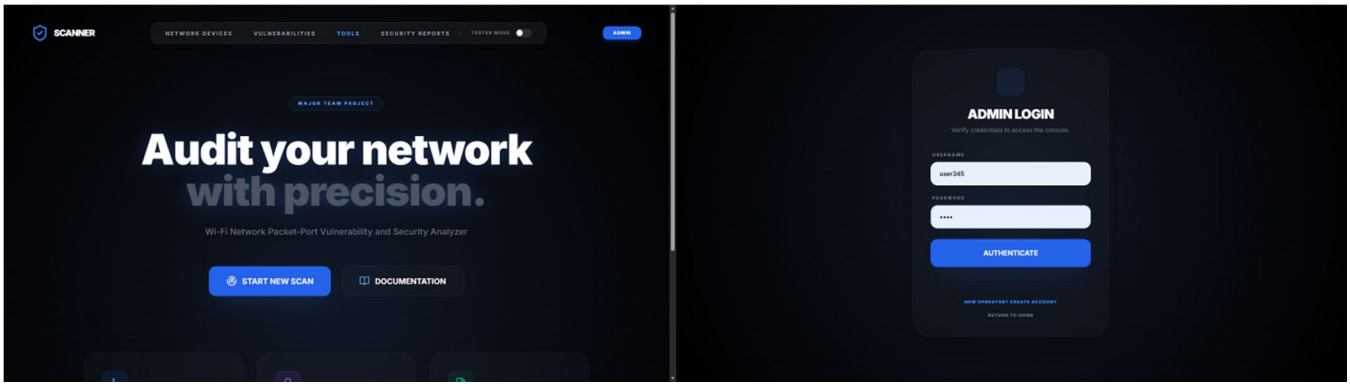
B. Process Initialization

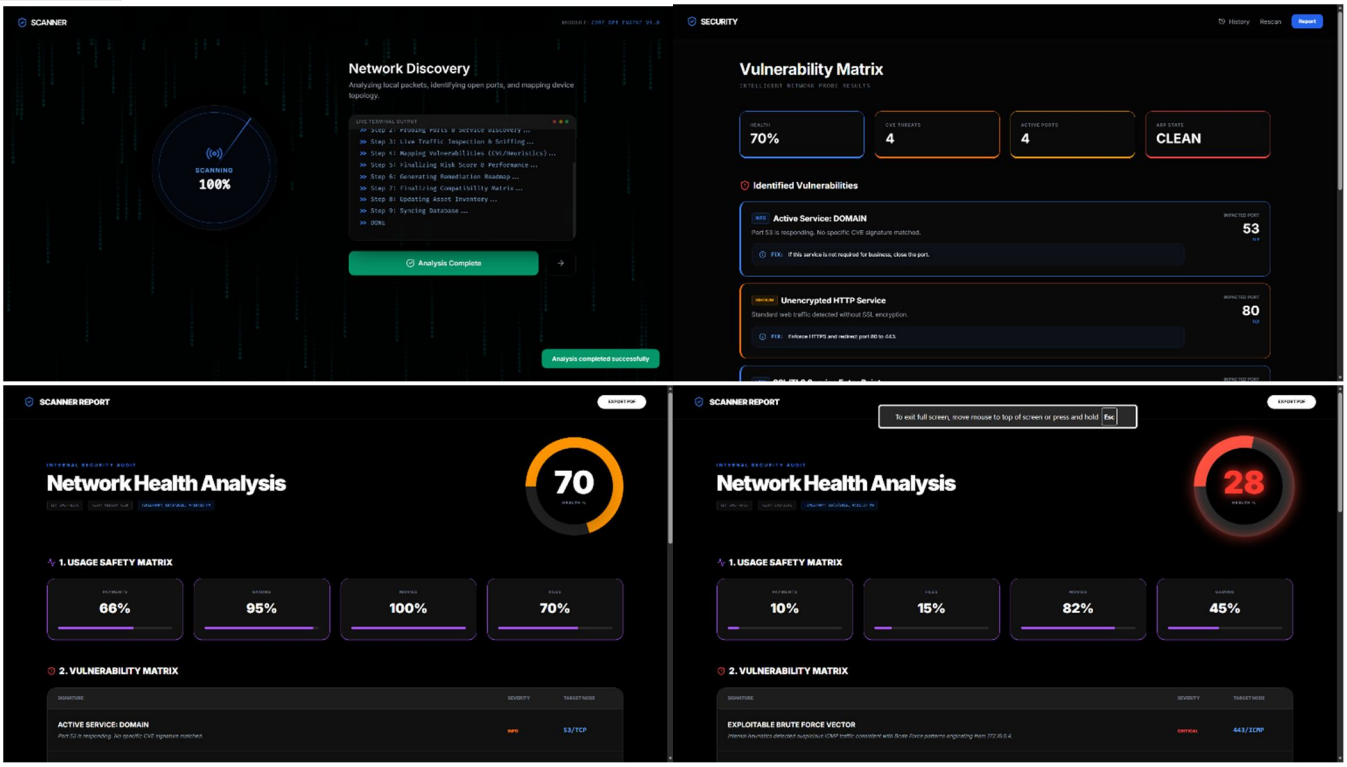
As shown in the Level 1 Data Flow Diagram, the Control Scan (1.0) process translates user inputs into specific Module Commands. These commands are passed to the Analyze Network (2.0) process, which orchestrates the backend diagnostic scripts. This stage ensures that all operational prerequisites are met before the system transitions into active data harvesting and risk calculation.

VII. RESULTS AND OUTCOME

Experimental trials confirm the system's ability to successfully synchronize its 9-stage pipeline to transform raw telemetry into actionable intelligence. The primary output, a quantifiable Network Health Score, utilizes a weighted heuristic engine to prioritize high-impact threats, such as ARP spoofing or deprecated encryption, over minor configuration alerts. In test scenarios, the system effectively identified a "Medium Risk" posture, specifically flagging exposed management interfaces and unencrypted services as critical entry points for potential exploitation. The implementation of a Secure User Authentication and Login system successfully protected these results, ensuring that the detected vulnerabilities and Network Health Scores were only accessible to verified administrators.

Beyond detection, the system provides behavioral insights via Deep Packet Inspection, visualizing the distribution of secure versus insecure traffic to highlight potential data leakage. This telemetry is synthesized into a Vulnerability Matrix and an automated Remediation Roadmap, providing administrators with a documented path for network hardening. By persisting these results into an SQLite database, the platform enables historical trend analysis for the longitudinal monitoring of network integrity. A critical success of the experimental trials was the validation of the Automated Email Alerting mechanism; in every test case where the health score fell below the 50% safety threshold, the system dispatched a real-time notification to the administrator, confirming its capability for proactive incident response





VIII. CONCLUSION

The design and implementation of the Security Core represent a significant advancement in localized network security auditing, successfully bridging the gap between expert-level penetration tools[8][16] and accessible management interfaces [12]. This research demonstrates that high-level web frameworks like Flask[12] can effectively orchestrate low-level primitives such as Scapy[13] and Nmap[7] to create a unified, high-performance defense mechanism. The implementation of a Secure User Authentication and Login module further strengthens this defense, ensuring that sensitive network telemetry and audit reports remain accessible only to authorized administrators.

The system's primary innovation is its synchronized 9-stage execution pipeline, which automates the transition from raw environmental reconnaissance to sophisticated threat correlation. Central to this success is the Heuristic Scoring Engine, which transforms disparate telemetry—including encryption standards[11],open port counts [7], and ARP integrity[13]into a singular, quantifiable Network Health Score based on CVSS standards[9]. By utilizing a RESTful API architecture, the analyzer ensures that vulnerability detection is grounded in real-time global intelligence from CVE databases [20] and the NVD[19] rather than static local definitions. A pivotal feature of this dynamic capability is the Automated Email Alerting mechanism, which acts as an active incident response trigger by dispatching real-time notifications whenever the Network Health Score drops below the 50% safety threshold. Ultimately, the project shifts the paradigm from reactive monitoring to proactive network defense by providing a structured Remediation Roadmap and a historical persistence layer via SQLite [15].

IX. FUTURE SCOPE

The proposed Security Core provides a solid framework for wireless network vulnerability assessment; however, several enhancements can further improve its capabilities. Future work may integrate Artificial Intelligence and Machine Learning techniques to enable anomaly-based detection of unknown or zero-day attacks using models such as Isolation Forest or K-Nearest Neighbors.

Additionally, migrating the system to a cloud-based architecture would allow centralized monitoring of multiple networks and enable real-time sharing of threat intelligence. The implementation of continuous real-time monitoring with instant alerts could further enhance network protection compared to the current scan-on-demand approach.

Another possible extension includes the development of a cross-platform mobile application for easier accessibility and administrative control. Finally, integrating scalable databases and big data analytics would support long-term vulnerability trend analysis and automated security reporting.

These improvements would transform the system into a more intelligent, scalable, and proactive wireless network security platform.

REFERENCES

The following references provide the academic and technical foundation for the design, implementation, and security analysis of the Security Core. These include peer-reviewed research papers on Wi-Fi vulnerabilities, official documentation for core networking tools, and industry-standard security methodologies.

Research Papers and Academic Journals

[1] Masiukiewicz, V. Tarykin, and V. Podvornyi, "Security threats in Wi-Fi networks," International Research Journal of Advanced Engineering and Science, vol. 1, no. 3, pp. 6-11, 2016. http://irjaes.com/wp-content/uploads/2020/10/IRJAES-V1N3P60Y16.pdf

[2] P. Bheevgade, C. Saha, R. Nath, S. Dabhade, H. Barot, and S. O. Junare, "The Rise of Public Wi-Fi and Threats," in Information Security, Privacy and Digital Forensics, S. J. Patel et al., Eds. Singapore: Springer Nature, 2024, pp. 175-189. https://www.researchgate.net/publication/375230379_The_Rise_of_Public_Wi-Fi_and_Threats

[3] S. Simbaña, G. López, C. Tipantuña, and F. Sánchez, "Vulnerability Analysis Toolkit for IEEE 802.11 Wireless Networks: A Practical Approach," in 2018 International Conference on Information Systems and Computer Science Vulnerability Analysis Toolkit for IEEE 802.11 Wireless Networks: A Practical Approach | IEEE Conference Publication | IEEE Xplore

[4] T. Mekhaznia and A. Zidani, "Wi-Fi security analysis," Procedia Computer Science, vol. 73, pp. 172-178, 2015. https://www.sciencedirect.com/science/article/pii/S1877050915034705

[5] R. Sridaran and R. Budhrani, "Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools," International Journal of Advanced Networking Applications (IJANA), pp. 137-150, Nov. 2014. https://www.researchgate.net/publication/273776388_Wireless_Local_Area_Networks_Threats_and_Their_Discovery_Using_WLANs_Scanning_Tools

[6] M. M. Noor and W. H. Hassan, "Current threats of wireless networks," in The Third International Conference on Digital Information Processing and Communications, 2013, pp. 704-713. https://www.sciencedirect.com/science/article/pii/S1877050917319853

Official Documentation and Technical Manuals

[7] G. F. Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.

[8] "Aircrack-ng Documentation," 2017. [Online]. Available: https://www.aircrack-ng.org/.

[9] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document," 2015. [Online]. Available: https://www.first.org/cvss/v3.0/specification-document.

[10] OWISAM, "OWISAM (Open Wireless Security Assessment Methodology)," Sep. 2013. [Online]. Available: https://www.owisam.org/.

[11] IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012.

Software Frameworks and Security Tools

[1] "Flask Documentation (v3.x)," Pallets Projects. [Online]. Available: https://flask.palletsprojects.com/.

[2] "Scapy Documentation: Packet Crafting and Sniffing," [Online]. Available: https://scapy.net/.

[3] "Wireshark User's Guide," Wireshark Foundation. [Online]. Available: https://www.wireshark.org/docs/.

[4] "SQLite Documentation," SQLite.org. [Online]. Available: https://www.sqlite.org/docs.html.

[5] "WiFi-Pumpkin: Framework for Rogue Wi-Fi Access Point Attack," Oct. 2017. [Online]. Available:https://github.com/P0cL4bs/WiFi-Pumpkin.

[6] "Fluxion: WiFi analyzer," Oct. 2017. [Online]. Available: https://github.com/wi-fi-analyzer/fluxion.

[7] "MITMf: Framework for Man-In-The-Middle attacks," Oct. 2017. [Online]. Available: https://github.com/byt3bl33d3r/MITMf.

Web Resources and Databases

[1] NIST, "National Vulnerability Database (NVD)," U.S. Department of Commerce. [Online]. Available: https://nvd.nist.gov/.

[2] MITRE, "CVE - Common Vulnerabilities and Exposures," [Online]. Available: https://cve.mitre.org/.

[3] "Kali Linux Wireless Penetration Testing Tools," Offensive Security. [Online]. Available: https://www.kali.org/tools/.

BIOGRAPHIES



Mrs.G.Vijaya Lakshmi is currently working as an Assistant Professor in the Department of Computer Science and engineering at Sanketika Vidya Parishad engineering college, Visakhapatnam. The institution is affiliated with Andhra University and accredited by NAAC. Her areas of interest include Machine Learning, Cybersecurity, and Network Security. She has guided several undergraduate projects related to data science and security applications



B. Manoj Kumar is a final-year B.Tech student in the Department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College, accredited with an 'A' grade by NAAC and affiliated with Andhra University. His interests include Cybersecurity and Network Security. He is working on his major project, Wi-Fi Network Packet-Port Vulnerability and Security Analyzer, focusing on Network Traffic Analysis, where he implemented Packet Sniffing and ARP Monitoring to detect unauthorized network interceptions and Man-in-the-Middle attacks. The project is carried out under the guidance of Mrs. G. Vijaya Lakshmi, Assistant Professor, SVPEC.



T. Chandra Sekhar is a final-year B.Tech student in the Department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College, accredited with an 'A' grade by NAAC and affiliated with Andhra University. His interests include Full-Stack Web Development and Artificial Intelligence. He is working on his major project, Wi-Fi Network Packet-Port Vulnerability and Security Analyzer, focusing on Backend Logic, where he engineered the Web Dashboard and the Automated Email Alerting system for real-time security notifications .The project is carried out under the guidance of Mrs. G. Vijaya Lakshmi, Assistant Professor, SVPEC.

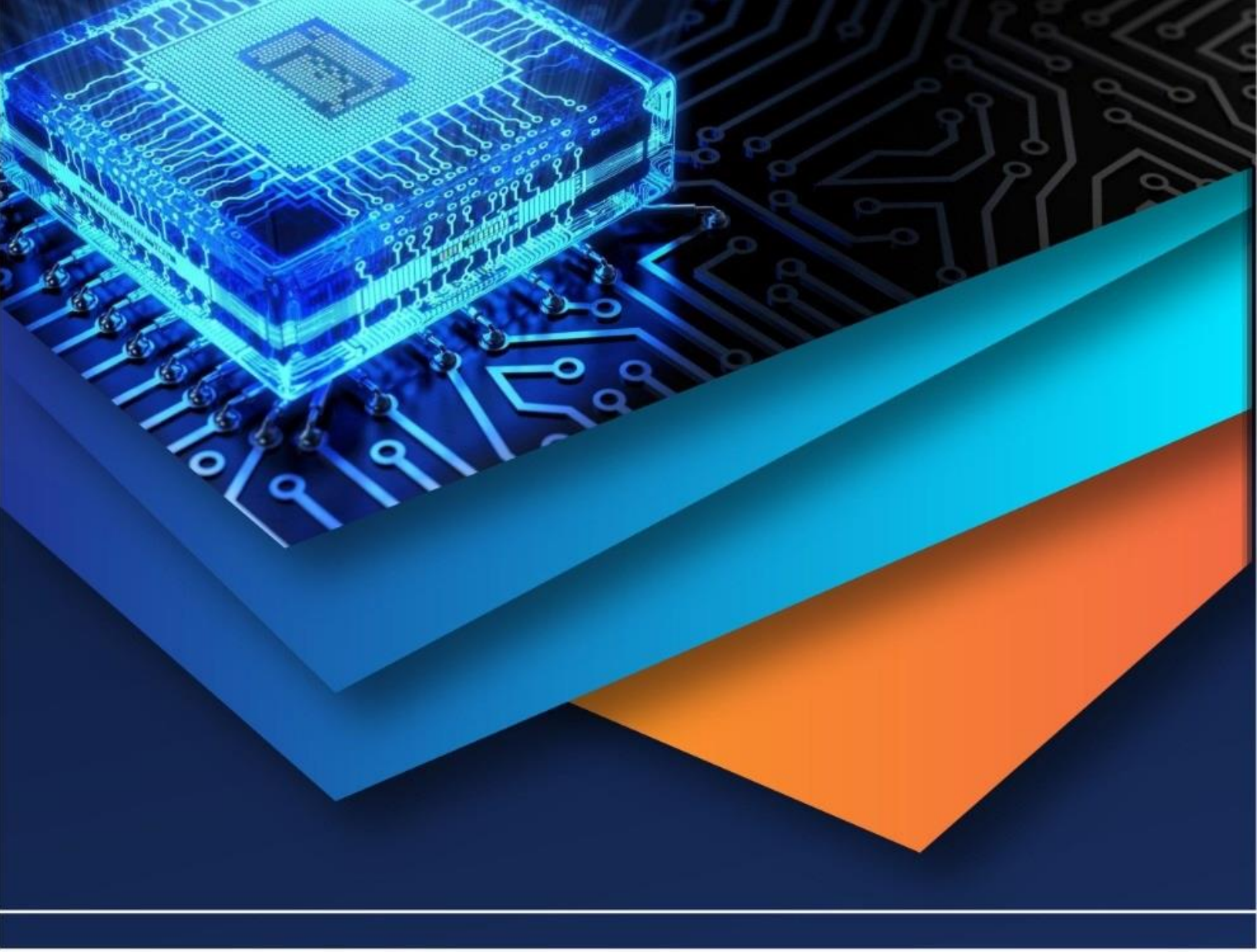


K. Raghavendhra Sai is a final-year B.Tech student in the Department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College, accredited with an 'A' grade by NAAC and affiliated with Andhra University. His interests include Database Management and SQL Optimization. He is working on his major project, Wi-Fi Network Packet-Port Vulnerability and Security Analyzer, focusing on Database Management, where he designed the Secure Login System and optimized the SQLite database for storing historical scan reports. The project is carried out under the guidance of Mrs. G. Vijaya Lakshmi, Assistant Professor, SVPEC.



A. Rakesh Kumar is a final-year B.Tech student in the Department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College, accredited with an 'A' grade by NAAC and affiliated with Andhra University. His interests include Data Science and Big Data Analytics. He is working on his major project, Wi-Fi Network Packet-Port Vulnerability and Security Analyzer, focusing on Threat Intelligence, where he integrated the CVE Vulnerability Database and developed the Heuristic Scoring Engine to calculate real-time network health .The project is carried out under the guidance of Mrs. G. Vijaya Lakshmi, Assistant Professor, SVPEC.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)