Abhinav Ugale, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

RUBYFI: The Wi-Fi Red Teaming Toolkit

Abhinav Ugale, Omkar Shinde, Manmeet Singh, Ms.Pradnya Patil
Dept. Computer Engineering Pillai HOC College of Engineering and Technology
(University of Mumbai) Rasayani, India

Abstract- Wi-Fi is now used everywhere, from our homes to public locations, and it connects lakhs of people. However, this ease comes with a major drawback. Most networks contain security flaws that attackers can easily exploit. These weaknesses can cause major problems such as data theft and invasion of privacy. To properly test for these dangers, one has to use many different and complicated command-line tools, which is not practical for everyone. To solve this, we have developed RubyFi, a complete Wi-Fi security testing toolkit. Our system brings all the necessary tools like aircrack-ng, reaver, and hashcat into a single, easy-to-use platform with both a graphical and command-line interface. RubyFi allows a user to perform a full range of tests, from capturing WPA/WPA2 handshakes for password cracking to launching Deauthentication and Evil Twin attacks. Importantly, we have also included modules to test for the latest WPA3 vulnerabilities, such as those found in the Dragonblood research, making it relevant for modern networks. Finally, RubyFi is an instructional tool that aims to make cybersecurity realistic. It makes ethical hacking easy, providing both students and security pros a straightforward way to find and understand Wi-Fi weaknesses. The main goal is to help people spot these security holes and learn how to fix them, leading to safer wireless networks for everyone.

Keywords: Aircrack-ng, Deauthentication, WPA/WPA2, Dragonblood.

I. INTRODUCTION

Wireless networks are now an important part of modern communication systems because they are flexible, easy to set up, and can support mobility. They are used a lot in homes, schools, businesses, and public places to give people easy access to the internet. Wireless communication, on the other hand, is more likely to be hacked than wired networks because it is sent over open radio frequencies. In today's connected world, wireless security is a big deal because of the risks of unauthorized access, data interception, and network disruption.

Several studies have highlighted that wireless networks are frequently targeted due to weaknesses in protocol implementation, configuration errors, and poor security practices. Research on wireless network security emphasizes that attackers can exploit these weaknesses to perform attacks such as eavesdropping, spoofing, and denial-of-service, even when encryption mechanisms are in place [1]. This indicates that relying solely on encryption standards is insufficient to ensure comprehensive wireless security.

This shows that encryption standards alone are not enough to make wireless networks completely safe. More research has been done on the weaknesses in common wireless security protocols like WPA and WPA2. Research on WPA2-PSK indicates that attackers can intercept the four-way handshake and execute offline dictionary attacks to retrieve network passwords, especially when weak passphrases are employed [2]. These results show that practical exploitation methods can weaken protocol-level security, which means that security checks need to be done all the time. Penetration testing has thus become an efficacious method for assessing the actual security of wireless networks.

Penetration testing uses ethical hacking tools to simulate authorized attacks. This helps find weaknesses, misconfigurations, and possible attack paths before they are used by bad people. Studies have demonstrated that penetration testing tools and frameworks can effectively evaluate wireless networks. This shows that relying on resilience by simulating real attack scenarios [3].

While current research has examined specific wireless attacks and testing tools, a more

comprehensive assessment of wireless network security utilizing ethical penetration testing methodologies is required. The goal of this study is to find weaknesses in wireless networks by using real-world penetration testing methods and to help make wireless networks more secure in the real world.

II. LITERATURE REVIEW

1.Penetration Testing for System Security: Methods and Practical Approaches.

Zhang et al. [1] suggest a thorough study of penetration testing as a moral and organized way to check the security of systems and networks. The study describes penetration testing as a controlled simulation of real-world cyberattacks that aims to find weaknesses before they are used by bad actors. The paper goes into detail about the different steps of penetration testing, such as reconnaissance, finding vulnerabilities, exploiting them, and reporting them. It stresses how important penetration testing is for modern security assessment. The authors talk about how penetration testing helps businesses figure out how real attacks work and how well their current security measures work across networked systems.

Advantages- Penetration testing provides an accurate assessment of a system's security by simulating an attacker's approach to identify vulnerabilities that could be exploited. It gives businesses actionable insights that help them prioritize security risks and improve their defenses.

Limitations- The study is mostly about general system and network security and doesn't go into much detail about specific wireless attack scenarios or Wi-Fi protocol weaknesses. It doesn't go into enough detail about wireless penetration testing tools and practical exploitation techniques, leaving a gap for more focused research on wireless network security.

2. The Evolution of Wireless Penetration Testing Tools: A Case Study of Aircrack-ng and Bettercap.

Alfarizy et al. [2] This paper explores the evolution of wireless penetration testing tools, with a particular focus on Aircrack-ng and Bettercap. The authors look at how wireless security testing has changed over time, from simple encryption cracking to more complex attack simulations that are used in modern ethical hacking. The research indicates that the two tools operate in distinct manners: Aircrack-ng primarily focuses on capturing Wi-Fi handshakes and decrypting passwords, whereas Bettercap is capable of facilitating more sophisticated attacks, such as establishing rogue access points, executing man-in-the-middle attacks, and manipulating traffic. The study shows that these tools are becoming more and more important for checking the security of wireless networks.

Advantages- The paper provides a clear comparison between traditional and modern wireless penetration testing tools, aiding security professionals in choosing the right tools based on their testing goals.

Limitations- The study mainly focuses on comparing and evolving tools, but it falls short in providing extensive real-world experimentation and thorough analysis of vulnerabilities in wireless protocols, such as WPA2 and WPA3.

3. Vulnerability Analysis of WPA Security Protocols.

Chaudhary et al.[3] This study provides a comprehensive analysis of security vulnerabilities that affect wireless security protocols, with a primary focus on WPA2 and WPA3. The authors talk about how flaws in the design and implementation of protocols can be used to carry out attacks like offline dictionary attacks, key reinstallation attacks, denial-of-service attacks, and man-in-the-middle attacks. The study also discusses the evolution of wireless security protocols from WEP to WPA3. It highlights the advancements in encryption and authentication; however, it also notes that actual implementations continue to exhibit security vulnerabilities.

Advantages- The study gives clear technical information about the weaknesses in WPA2 and WPA3 and helps us understand how modern wireless security protocols can be broken in real-world situations.

Limitations- The study mostly looks at protocol-level analysis and doesn't do a lot of hands-on

penetration testing with real-world wireless attack tools.

4. The Elusive Enigma: Unraveling Rogue Wi-Fi's Chessboard of Deception with Man-in-the-Middle Mastery and Rogue Access Point Intrigue.
Magno et al.[4] This study looks into the security risks that rogue Wi-Fi networks and man-in-the-middle (MitM) attacks pose in public and semi-public wireless settings. The paper discusses how hackers employ counterfeit access points that mimic legitimate networks to deceive individuals into connecting. This enables hackers to observe, alter, and capture network traffic. The study talks about different MitM methods, including fake captive portals, Wi-Fi eavesdropping, DNS spoofing, SSL/TLS stripping, and session hijacking. It also has fake network scenarios to show how users' private data can be stolen when they connect to bad wireless networks.
Advantages- It provides a clear explanation of prevalent rogue Wi-Fi and Man-in-the-Middle (MitM) attack techniques, as well as their implications for the security of user data.
Limitations- The discussion primarily focuses on attack scenarios and offers limited insight into methods for prevention or automatic detection.

5. From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake.
Vanhoef et al.[5] This study investigates security vulnerabilities in the WPA3 Dragonfly (SAE) handshake by scrutinizing side-channel attacks that may expose sensitive information during authentication. The authors show how timing and cache-based side-channel leaks can be used to carry out password partitioning attacks, which make WPA3 passwords less secure. The paper also talks about a formally verified way to implement the Dragonfly handshake that will make it less vulnerable to these kinds of attacks and stronger overall.

Advantages- The study goes into great detail about the technical flaws in the WPA3 handshake and suggests a verified implementation to make the protocol more secure.
Limitations- The research is predominantly theoretical, concentrating on cryptographic implementation aspects, with minimal discussion on practical wireless penetration testing scenarios.

6. Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators.
Alqahtani et al.[6] This work focuses on evaluating Wi-Fi security levels by applying penetration testing tools in a controlled organizational environment. The study demonstrates how commonly used ethical hacking tools are deployed to assess wireless network configurations, encryption strength, and susceptibility to attacks such as unauthorized access and traffic interception. The paper emphasizes the role of practical testing in identifying real-world weaknesses that are often overlooked during theoretical security assessments.
Advantages- Demonstrates practical application of penetration testing tools to assess real organizational Wi-Fi security.
Limitations- Limited to a specific environment and does not analyze advanced wireless attacks or newer security protocols in detail.

7. Enhancing Wireless Network Security via Ethical Hacking: Strategies and Best Practices.
Kumar et al.[7] This study explores the role of ethical hacking in improving wireless network security by actively identifying vulnerabilities before they can be exploited by malicious actors. The paper discusses prevalent techniques for compromising wireless networks and examines how ethical hacking tools and methodologies can be employed to evaluate the robustness of encryption, authentication protocols, and network configurations. It emphasizes the significance of employing ethical hacking not merely as a reactive measure to address security issues, but as a proactive strategy to safeguard your computer.

Advantages- Highlights ethical hacking as an effective approach for proactively improving wireless network security.
Limitations- The research is primarily theoretical and does not include thorough experimental validation through real-world wireless attack scenarios.

8. Exploring Wi-Fi WPA2-PSK Protocol Weaknesses.

Alhamry et al.[8] This study investigates the security weaknesses present in wireless networks that utilize WPA2-PSK. The paper clarifies how the WPA2-PSK authentication mechanism operates, focusing on the four-way handshake process, and demonstrates how attackers can exploit this to carry out offline dictionary attacks. It also discusses alternative methods of attack, such as deauthentication attacks, MAC address spoofing, ARP poisoning, and packet sniffing. Furthermore, it employs actual penetration testing tools to demonstrate that these vulnerabilities are indeed significant.

Advantages- It effectively elucidates the shortcomings of WPA2-PSK and demonstrates the application of penetration testing tools to execute actual attacks.
Limitations- It focuses solely on WPA2-PSK and does not consider newer protocols such as WPA3 or more sophisticated methods for safeguarding against attacks.

9. Penetration Testing: Wireless Network Attacks Methods on Kali Linux OS.

Ariyadi et al.[9] This study focuses on identifying and analyzing common wireless network attacks using the Kali Linux operating system. The paper discusses how Kali Linux serves as a comprehensive platform for evaluating wireless security, utilizing tools for packet capture, traffic analysis, authentication attacks, and denial-of-service attacks. To test the security of wireless networks, the authors show real-world attack methods like handshake capture, deauthentication attacks, MAC spoofing, and man-in-the-middle attacks. The study highlights the importance of practical testing to understand how adversaries take advantage of vulnerabilities in real-world Wi-Fi environments.

Advantages- It gives you hands-on experience with wireless attacks using Kali Linux and shows you how to do penetration testing in the real world.
Limitations- Limited focus on newer wireless security standards and lacks comparison with advanced or emerging attack methodologies.

10. Enhancing Wireless Network Security: An Exploration of Tools and Techniques.

Adelusi et al.[10] This paper examines various tools and techniques that can enhance the security of wireless networks by addressing prevalent threats and vulnerabilities. The paper discusses security tools such as encryption protocols, authentication methods, firewalls, and intrusion detection systems, examining their role in safeguarding wireless communication. It emphasizes that effective wireless security requires more than a single security measure; it necessitates a combination of technical controls, appropriate configuration, and ongoing surveillance.

Advantages- It gives a good overview of wireless security tools and methods and stresses the need for a layered security approach.
Limitations- The study is mostly descriptive and doesn't include any real-world wireless attacks or practical penetration testing experiments.

III. PROBLEM STATEMENT

Wi-Fi security auditing remains a challenging task due to the fragmented nature of existing tools. Security analysts often find themselves needing to manually integrate multiple command-line utilities, such as Aircrack-ng, Hashcat, and Reaver, to conduct a single test. This process is long and full of mistakes, making it hard to get started and making it much less efficient. Only highly trained experts can do effective wireless security testing. Because of this, many real-world weaknesses in popular protocols like WPA2 and WPA3 go unnoticed because routine and simple auditing isn't possible.

The project comes up with Rubify, a single, easy-to-use wireless security toolkit that brings together many auditing functions into one graphical interface. Rubify makes wireless security assessments easier for both learners and security professionals by hiding the complexity of the command line. This makes it useful for both educational purposes and important red-teaming activities.

IV. PROPOSED SYSTEM

Rubify is a single, easy-to-use Wi-Fi security auditing and red-teaming toolkit that makes it easier and faster to check the security of wireless networks. Rubify aims to address the shortcomings of current Wi-Fi auditing tools, which tend to be overly complex and fragmented. At present, security analysts must manually execute and manage several command-line utilities for each assessment. Rubify integrates these functionalities into a single platform, streamlining the process of conducting effective wireless security testing while reducing the need for manual effort.

Figure 1: RUBYFI Working Diagram

Rubify provides a unified graphical user interface that conceals the command-line operations occurring in the background during wireless penetration testing. Users can perform essential auditing functions such as wireless reconnaissance, capturing handshakes, auditing passwords, conducting deauthentication tests, and evaluating the security configurations of WPA, WPA2, and WPA3 using this interface. Rubify enables the evaluation of Wi-Fi security in a systematic and consistent manner, eliminating the necessity for extensive knowledge of command-line commands by integrating these functionalities into a single platform. The system is designed for use in both educational and professional settings. Rubify offers an accessible platform for learners and students to explore wireless security concepts and attack techniques in a secure and regulated environment. It provides security professionals and red-team members with an effective method for conducting practical wireless security assessments and identifying genuine vulnerabilities. In essence, Rubify aims to simplify, accelerate, and enhance wireless security auditing, thereby increasing the effectiveness of routine Wi-Fi security assessments.

V. METHODOLOGY

The Rubify system employs a modular and layered methodology to conduct wireless security audits that are efficient, ethical, and systematically organized. The methodology seeks to address the issues arising from disjointed wireless auditing tools by consolidating control, automating the execution of workflows, and enhancing user interaction with these tools. Rubify's core engine is intricately linked to every functional module, ensuring that all phases of wireless security assessment can interact seamlessly and operate efficiently.

The Rubify system operates on Kali Linux, a reliable and commonly utilized platform for assessing wireless security. Kali Linux is designed specifically for ethical hacking and penetration testing, providing all the necessary drivers, libraries, and system-level support required for wireless auditing. Rubify ensures the reliability and consistency of its security assessments by utilizing Kali Linux as the execution environment. This approach enables the use of industry-standard tools for wireless security.

A. User Interface and Access Control

The Rubify user interface serves as the primary means through which users engage with the system. The objective is to establish an intuitive and user-friendly platform that enables users to initiate wireless security assessments, select particular auditing modules, and observe the system's operations in real time. The interface simplifies the process of conducting wireless security audits for individuals with varying degrees of technical expertise by concealing low-level command-line operations. Access control mechanisms are integrated to ensure that only authorized users can utilize the system. This guarantees that all evaluations are conducted in a responsible and ethical manner.

B. System Workflow Management

Rubify employs a structured workflow that ensures wireless security assessments are conducted in a systematic and consistent manner. When a user initiates an audit, the system workflow manager ensures that the chosen modules operate in the correct sequence. This ensures that reconnaissance precedes authentication analysis, and that attack simulation occurs only after all essential data has been gathered. The workflow-based execution reduces mistakes made by people, makes things run more smoothly, and makes sure that all assessments are the same.

C. Wireless Reconnaissance Module

The wireless reconnaissance module's job is to collect important information about the wireless environment that is the target. This involves identifying nearby access points, monitoring which client devices are connected, and observing factors such as encryption standards and signal performance. During the reconnaissance phase, you get a basic idea of the network's layout and security. The information collected during this phase is utilized to determine the most effective testing methods while also identifying and eliminating unnecessary or ineffective tests.

D. Handshake Capture and Authentication Analysis

Authentication analysis is performed by evaluating handshake exchanges used in WPA, WPA2, and WPA3-secured networks. Rubify coordinates the capture and processing of authentication handshakes through its integrated auditing framework. This module helps assess the strength of authentication mechanisms and identify weaknesses caused by improper configuration or weak credential policies. By automating this process, Rubify ensures consistency and accuracy while reducing reliance on manual intervention.

E. Password Auditing and Credential Evaluation

The password auditing module evaluates the strength of wireless network credentials within a secure and controlled testing environment. Rubify analyzes authentication data that has been collected to identify passphrases that are either weak or easily guessable. The aim of this module is not to appropriate credentials, but rather to evaluate the robustness of passwords and highlight the risks associated with poor password practices. This assessment enables administrators to recognize the significance of effectively managing credentials within wireless settings.

F. Deauthentication and Availability Testing

Rubify has a deauthentication testing module that checks the strength and availability of wireless networks. This module replicates controlled disconnection scenarios to observe the responses of access points and connected devices when they are compelled to cease functioning. Availability testing can identify vulnerabilities in network stability and conditions that may lead to denial-of-service attacks. The findings from this module assist you in assessing the resilience of a wireless network against potential disruptions.

G. Rogue Access Point and MITM Evaluation

The rogue access point and man-in-the-middle evaluation module identifies potential threats associated with fraudulent wireless networks. Rubify examines the responses of devices and users to counterfeit networks that mimic legitimate ones. This assessment identifies vulnerabilities in network

authentication, user awareness, and access point validation. The module is especially useful in public and business settings where rogue Wi-Fi attacks happen a lot.

H. Tool Integration and Command Orchestration

Rubify integrates various wireless auditing tools via a unified integration layer. This layer manages the execution of commands, oversees parameters, and gathers output, all while ensuring that the process remains straightforward for the user. Rubify takes care of the internal orchestration of tools, so you don't have to chain them together by hand. This makes sure that each tool works in a controlled and coordinated environment. The proposed system's main contribution is this integration.

I. Logging and Monitoring Mechanism

A centralized logging system monitors and records all activities occurring during a wireless security assessment. Rubify monitors the status of the logs, identifies any vulnerabilities it detects, and assesses the system's responses throughout the auditing process. This logging feature ensures clarity and traceability, allowing users to review the steps and outcomes of the assessment. Logs can serve as a means of ensuring accountability and can be utilized for audits or more comprehensive analyses.

J. Result Analysis and Report Generation

The result analysis module processes the collected data to generate structured reports that illustrate the security level of the tested wireless network. These reports detail the identified vulnerabilities, the observed weaknesses, and the security insights derived from the assessment. The output is clear and comprehensible, making it suitable for both educational purposes and professional security assessments.

VI. CONCLUSION

This research presents Rubify, an all-encompassing toolkit for Wi-Fi security auditing and red-teaming, designed to address the intricacies and disjointed nature of existing wireless security assessment tools. Rubify makes it easier to check the security of wireless networks by combining several auditing and attack simulation functions into one easy-to-use graphical interface. It also keeps usage ethical and controlled. The proposed system facilitates a systematic assessment of the security mechanisms associated with WPA, WPA2, and WPA3 through coordinated reconnaissance, analysis of authentication processes, simulated controlled attacks, and comprehensive reporting. Through its modular architecture and centralized orchestration, Rubify reduces manual effort, lowers the barrier to entry for learners, and improves efficiency for security professionals. Overall, the system demonstrates that integrated and accessible auditing platforms can significantly enhance routine wireless security evaluation and contribute to stronger, more resilient wireless network defenses.

VII. RESULT ANALYSIS

Figure 2: Manage Interface

The Manage Interface screen allows the user to configure the wireless network adapter required for security assessment. Through this interface, Rubify detects the available wireless adapter and enables switching it into monitor mode using a graphical control. On-screen notifications indicate that monitor mode has been successfully activated, signifying that the system is prepared for wireless scanning and analysis. Additional options, such as disabling monitor mode and altering the MAC address, enhance the flexibility of ethical testing. This interface simplifies the process of configuring a wireless adapter, removing the necessity for manual command-line setup.

Figure 3: Scan network and target selection

The Scan Networks and Target Selection interface displays the wireless clients connected to the selected access point after the scanning process. The system lists detected clients along with key parameters such as MAC address, signal strength, and packet activity, allowing users to understand network participation in real time. Rubify enables the selection of a specific client for directed testing or the use of broadcast mode when individual client targeting is not required. This interface simplifies target identification and ensures that subsequent security assessments are performed in a controlled and precise manner.

Figure 4: Lauch Attack Menu

The Launch Attack Menu interface provides an overview of the various security tests available for the selected wireless network. Rubify displays crucial network details such as SSID, BSSID, channel, and encryption type once you select a target. This ensures that you have a comprehensive understanding before proceeding with any actions. Users have the ability to select from a range of auditing options available on the interface, including handshake capture, deauthentication testing, evil twin assessment, and WPS evaluation. This module simplifies decision-making by consolidating all supported attack simulations into a single menu. Additionally, it ensures that the transition from network discovery to security assessment is structured and efficient.

Figure 5: Deauthentication Attack Submenu

The Deauthentication Attack interface enables users to evaluate the selected wireless network in a controlled manner, assessing its stability and availability. The screen displays the specifics of the target network, including the SSID, BSSID, and operating channel, ensuring that all participants are informed about the forthcoming actions. Rubify has two testing modes: broadcast deauthentication, which disconnects all connected clients, and directed deauthentication, which disconnects just one client. This design facilitates precise measurement of the network's response to forced disconnection scenarios, thereby aiding in the ethical assessment of its resilience against availability-based attacks.

Figure 6: Client Selection for Directed Deauth

The Client Selection interface is used when performing directed deauthentication testing on a specific device connected to the target network. The screen lists all detected clients along with their MAC addresses, signal strength, and packet activity, enabling informed selection of an individual client. Rubify allows the user to either select a specific client or switch to broadcast mode, providing flexibility in testing. This interface supports precise and controlled evaluation of client-level network resilience during availability testing.

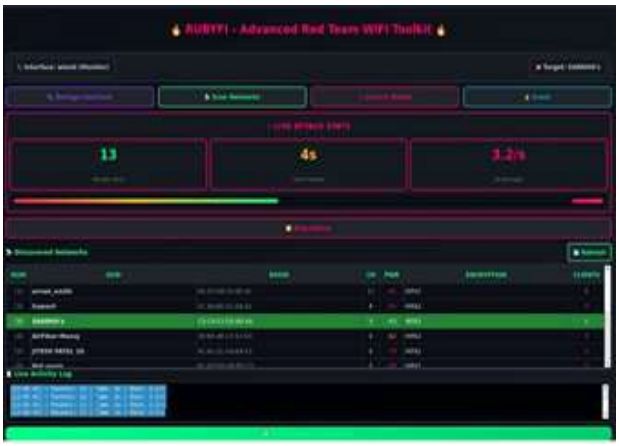

Figure 7: Deauth Attack Execution

The Deauthentication Attack Execution screen displays real-time feedback during the availability testing process. The interface presents live attack statistics such as packets transmitted, elapsed time, and attack rate, allowing the user to monitor execution progress clearly. A visual progress indicator and activity log further enhance transparency by showing ongoing system actions. This real-time monitoring helps evaluate how the target network responds to controlled deauthentication attempts and demonstrates Rubify's ability to provide immediate feedback during wireless security assessments.

For experienced users and those seeking backend control, the Rubify Command-Line Control Interface (CLI) provides an alternative method for engaging with text. The interface is organized and menu-driven, facilitating user management of wireless interfaces, scanning for and selecting target access points, initiating security assessments, and verifying passwords through straightforward numeric options.

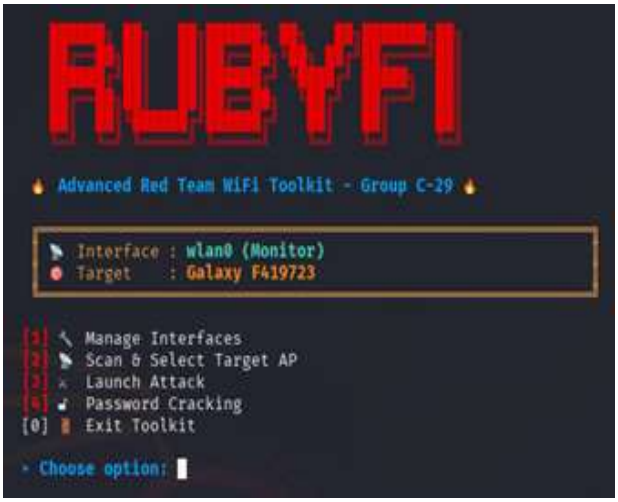

Figure 8: RUBYFI CLI

The active wireless interface and the selected target are clearly displayed, ensuring that the operation remains transparent. This CLI interface demonstrates the versatility of Rubify, as it operates seamlessly in both graphical and terminal modes within the Kali Linux environment. This adaptability enhances the toolkit's utility for a diverse array of users and testing scenarios.

Figure 9: Evil Twin Attack Active Indication

The Active screen of the Evil Twin Attack distinctly displays the ongoing assessment of the rogue access point. The interface displays system messages in real time, confirming the initiation of the simulated attack and the observation of client connection behavior. This status feedback informs the user about the current execution state and ensures that the assessment process remains transparent and trustworthy. The indication confirms that Rubify is capable of conducting controlled rogue access point testing in an ethical manner suitable for security auditing.

VIII. FUTURE SCOPE

Rubify excels at simplifying wireless security auditing by integrating various assessment features into a single platform. Nevertheless, there remains significant potential for enhancement moving forward. One approach to enhance the system involves incorporating sophisticated automation techniques that will minimize user input and expedite the assessment process. Employing machine learning to scrutinize data can assist in identifying attack patterns, categorizing vulnerabilities, and generating informed security recommendations based on the network's behavior. Rubify can also be updated in the future to work with new wireless standards and technologies, such as better analysis of WPA3 configurations and next-generation Wi-Fi protocols. Enhanced support for distributed and large-scale network environments could significantly increase its utility for conducting security audits at the enterprise level. The reporting module can be enhanced to generate reports that prioritize compliance and incorporate visual analytics.

Another potential enhancement involves enabling compatibility with various platforms and incorporating additional modules, thereby allowing integration with a broader range of security tools and cloud-based monitoring systems. These modifications would enhance Rubify's utility for professional red-teaming efforts while also ensuring it remains a valuable toolkit for wireless security auditing in both research and educational contexts.

REFERENCES

1. Wei Zhang, Ju Xing, Xiaoqi Li, "Penetration Testing for System Security: Methods and Practical Approaches," Published in IEEE, 2025.
2. Muhammad Fadilah Alfarizy, Mohamad Fadli Bin Zolkipli, "The Evolution of Wireless Penetration Testing Tools: A Case Study of Aircrack-ng and Bettercap," Published in Borneo International Journal, 2025.
3. Anurag Chaudhary, Krishan Kumar, "Vulnerability Analysis of WPA Security Protocols," Published in IEEE, 2024.
4. Eric B. Blancaflor, Frances Denielle C. Magno, Charles Ian S. Monteloyola, "The Elusive Enigma: Unraveling Rogue Wi-Fi's Chessboard of Deception with Man-in-the-Middle Mastery and Rogue Access Point Intrigue," Published on ResearchGate, 2024.
5. Salah Abdulghani Alabady, Mohammed A. M. Abdullah, Kaeed Ketab Kaeed, "Enhancing Wireless Security Via Ethical Hacking: Strategies and Best Practices," Published by Jomard Publishing, 2023.
6. Daniel De Almeida Braga, Natalia Kulatova, Mohamed Sabt, "From Dragonblood to Dragonstar: Side-channel Attacks on Formally Verified Implementation of WPA3 Dragonfly Handshake," Published in IEEE, 2023.
7. Tamsir Ariyadi, M. Rizky Pohan, "Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators," Published in JPPIPA, 2023.
8. Mohamed Alhamry, Dr. Alauddin Alomary, "Exploring Wi-Fi WPA2-PSK Protocol Weaknesses," Published in IEEE, 2022.
9. Renas Rajab Asaad, "Penetration Testing: Wireless Network Attacks Methods Using Kali Linux OS," Published on ResearchGate, 2021.
10. Thomas Ethan, Joshua Boluwatife Adelusi, "Enhancing Wireless Network Security: An Exploration of Tools and Techniques," Published on ResearchGate, 2020.