J-INTECH (Journal of Information and Technology)
Accredited Sinta 4 by the Ministry of Higher Education, Science and Technology
Decree of the Republic of Indonesia Number 10/C/C3/DT.05.00/2025
E-ISSN: 2580-720X || P-ISSN: 2303-1425

Implementation of ESP8266 Deauther Version 2 for Wireless Network Testing Against Deauthentication Attacks at PT Jaring Solusi Persada Tulungagung Branch

Diyah Kusuma Anggraini [1], Yayak Kartika Sari [2], Joko Iskandar [3]

[12.3]*Bhineka PGRI University, Faculty of Science and Technology, Informatics, 7 Mayor Sujadi Street, Manggisan, Plosokandang, Kedungwaru, Tulungagung Regency, East Java 66229, Indonesia*

Keywords
Access Point; Deauthentication; ESP8266 Deauther; Network Security; Quality of Services(QoS)

Corresponding Author:
diah96282@gmail.com

Abstract
The rapid advancement of wireless network technology and the Internet of Things (IoT) ecosystem in the industrial sector carries significant security risks, particularly regarding vulnerabilities within the management frame protocol. This study aims to evaluate the resilience of wireless network infrastructure against communication disruptions at the protocol level, specifically deauthentication attacks, at PT Jaring Solusi Persada (JSP) Tulungagung Branch. Applying a Research and Development (R&D) method with a Prototyping approach , empirical and real-time testing was conducted using a low-power ESP8266 Deauther Version 2 device as a penetration medium across 15 different access points (APs). Quality of Service (QoS) parameters, including throughput, latency, and packet loss, were measured using Wireshark software to analyze network performance degradation in detail. The experimental results reveal that deauthentication attacks inflict a highly destructive impact on vulnerable devices. Out of the 15 tested APs, 6 units (40%) consisting of consumer-grade devices (such as TP-Link, ZTE, and Totolink) were declared vulnerable because they did not support or activate the Management Frame Protection (MFP/IEEE 802.11w) feature. On these vulnerable devices, the attack successfully triggered complete client disconnections, a drastic 70% drop in throughput (from 567 kbps to 170 kbps), extreme latency spikes ranging from 100 to 300 ms, and a packet loss of 15%. Conversely, 9 AP units (60%), dominated by Ruijie Enterprise business-class devices, successfully withstood the attack and maintained stable network connections due to superior hardware specifications and better defense configurations. This study recommends upgrading network security standards to WPA3 and strictly enabling the Protected Management Frames (PMF) feature to ensure the company's operational continuity.

1. Introduction

The rapid advancement of information and communication technology in the digital era has brought fundamental changes to various aspects of human life, particularly in the management and protection of computer networks. The integration of wireless networks and the Internet of Things (IoT) ecosystem has now expanded into various strategic sectors, from industry and transportation to healthcare and public security systems.[1]. In general, this technology serves to connect physical entities with the digital world via the internet, allowing devices such as sensors and microcontrollers to operate and exchange data autonomously without requiring direct human intervention. The convenience offered by this system creates high efficiency, but on the other hand, heavy reliance on wireless connectivity also opens up significant security risks.[2]This study aims to evaluate the resilience of network infrastructure to communication intrusions at the protocol level, specifically deauthentication attacks, to provide a realistic picture of the often overlooked vulnerabilities in enterprise operational environments. The main motivation for this study stems from the fact that despite the implementation of modern security mechanisms such as firewalls and WPA2 or WPA3 encryption protocols, wireless networks still have weak points in the management framework.[3]A global security report shows that over 60% of security incidents on IoT devices are caused by weak network configurations and the use of unchanged default credentials. This issue was clearly found at PT. Jaring Solusi Persada (JSP) Tulungagung Branch, an ICT services company that relies heavily on stable Wi-Fi for internal coordination and customer service. The phenomenon of frequent sudden connection drops and signal fluctuations are early indications of potential vulnerabilities that need to be empirically tested using real-world attack methods, not just software simulations.[4].

A literature review of previous research reveals a variety of approaches to network security testing. Some studies use high-performance computing devices such as the Raspberry Pi or Kali Linux-based systems, which tend to be complex and impractical for rapid field testing.[5]Other studies have focused solely on defensive attack detection or theoretical simulations without involving physical hardware, often producing results that do not reflect real-world conditions. The novelty of this study lies in the use of the ESP8266 Deauther Version 2 as a testing medium. This device offers an efficient, power-efficient, portable solution capable of simulating deauthentication attacks directly and in real time without the need for an additional control computer.[6]. With its affordable cost yet strong penetration capabilities, this tool is highly relevant for mapping security risks in small and medium-sized industrial network infrastructures. The research method applied is Research and Development (R&D) with a Prototyping approach. This step begins with identifying problems at the research location, designing attack scenarios, and conducting live implementations on 15 different access points. Data analysis was performed using Quality of Service (QoS) parameters, including throughput, latency, and packet loss measurements, using Wireshark software to obtain accurate and detailed results.[7]This approach ensures that the research contribution is not limited to theory, but provides empirical data on the real-world impact of attacks on network performance in industrial environments. The results of this testing reveal important findings for information security management. The majority of tested devices exhibited a high level of vulnerability, with attacks successfully disabling connections and drastically degrading network performance. These findings underscore the urgency for organizations to begin adopting newer security technologies, such as the WPA3 standard and the Protected Management Frames (PMF) feature, to protect the integrity of their wireless communications.[8]Overall, this introduction leads the reader to understand that threats to wireless networks are no longer merely theoretical risks, but rather practical threats that can be addressed with simple tools but have a significant impact on the continuity of corporate operations. Thus, this paper provides a foundation for developing more effective mitigation strategies to address the dynamics of future cybersecurity threats.[9].

2. Research methods

Essentially, a research methodology serves as a systematic framework that guides researchers in solving problems or answering research questions through measurable and accountable procedures. In this network security study, the methodology encompasses technical steps ranging from hardware preparation and attack scenario design to data analysis techniques for evaluating the vulnerabilities of wireless systems at the research site. This approach is designed so that other researchers can replicate these tests with the same accuracy using predetermined tools and parameters.[10].

2.1 Place and Time of Research

The trial was conducted at the Tulungagung branch of PT. Persada Solutions Network (JSP). This location was chosen based on the company's urgent need for the stability of its fiber optic and wireless internet network infrastructure. Intensive field observations were conducted from October 22 to November 6, 2024, to map the network topology, identify access point locations, and measure signal strength at various test points.

2.2 Research Model and Development Procedures

This study applies a Research and Development (R&D) model using a Prototyping system development approach. The Prototyping method was chosen because of its iterative nature, allowing researchers to continuously evaluate and refine test equipment until optimal performance is achieved in simulating network disturbances.[11].

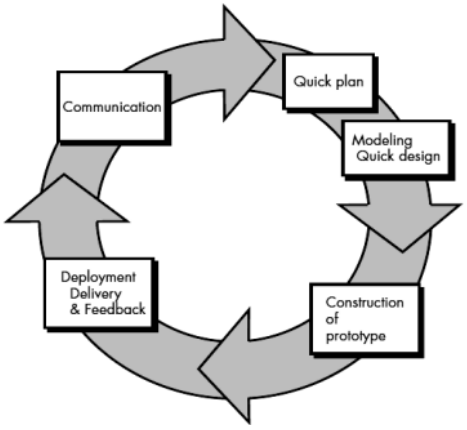

Figure1.Prototyping Approach Flow

The prototype creation stages applied in this research consist of the following five steps:

a) Initial Communication
   This stage involves the process of gathering requirements through direct communication between developers and users. The goal is to understand the users' problems, needs, and expectations regarding the system to be built.
b) Quick Plan
   Once requirements are obtained, developers develop an initial plan for the major features, system functions, and project constraints. This phase focuses on determining the scope and priorities of system development.
c) Rapid Design Modeling
   This phase produces a preliminary design of the system, including the user interface, data structures, and key workflows. This design is simple and serves as the basis for prototyping.
d) Prototype Making (Prototype Construction)
   Based on the initial design, developers build a prototype to demonstrate the system's basic form and function. This prototype is used to obtain direct feedback from users regarding the system's appearance and functionality.
e) Distribution, Delivery & Feedback
   The prototype is then handed over to users for testing and evaluation. Users provide feedback on the system's functionality, appearance, and performance. Based on this feedback, developers make improvements and refinements. This process is repeated until the system is deemed ready for full implementation.

2.3 Research Tools and Materials

To ensure replication of the study, the specifications of the equipment used are described in detail.

The main hardware includes:

- ESP8266 microcontroller: As an attack instrument that is tasked with scanning SSIDs and sending deauthentication packets independently (self-sufficiently).
- Lenovo Ideapad Slim Laptop: Serves as a control center to configure devices via Arduino IDE and run analysis applications.
- Target Devices: Includes 15 access point units of various models and security standards that have been tested for vulnerabilities.

Meanwhile, the software used consists of:

- Arduino IDE: Used for the compilation process and uploading source code to the microcontroller.
- Firmware Deauther V2: Core software that exploits a weakness in the IEEE 802.11 management frame protocol.
- Wireshark: A packet analysis tool for capturing traffic data in real-time and verifying the existence of remote frames.

2.4 Test Architecture Design (Rapid Design)

The Test Architecture Activity Diagram shows the flow of using the ESP8266 Deauther Version 2 as an instrument to simulate a deauthentication attack on a Wi-Fi network. This stage aims to systematically design a test scenario to ensure the attack process runs under control and is in accordance with the research objectives. The process begins by connecting the ESP8266 to a laptop via micro USB, followed by a user connection to the default SSID broadcast by the device. The Deauther web interface is accessed through a browser with the default IP address, enabling scanning of surrounding Wi-Fi networks to detect target SSIDs. Once detected, the user selects the SSID and executes a deauthentication attack against the access point. This design illustrates the communication flow between the user, the ESP8266, and the target access point as a tool for evaluating wireless network security.[12].

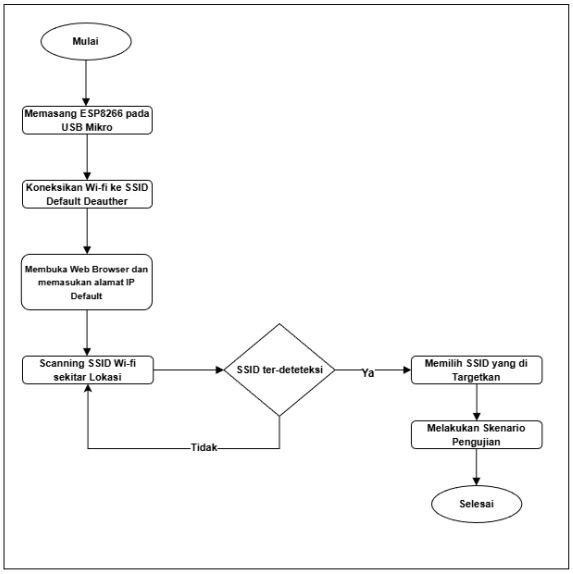

Figure 2.Test Architecture Activity Diagram

In the scenario planning stage of the test system and IoT network flow, as shown in Figure 2, testing was conducted using the Deauthentication Attack method against the access point to determine whether the Wi-Fi network being tested was vulnerable or not. The test system was designed to model the impact of

deauthentication attacks on the network quality of service (Quality of Service/QoS) on IoT devices, with the ESP8266 Deauther as the attack source and the monitoring laptop as a network parameter recorder and analyzer. The test flow included determining the test location, executing the attack according to the scenario, observing and interviewing users to validate whether the connection was lost or not, recording network activity, analyzing the causes of vulnerabilities or not from the hardware and software side of the access point, and documenting the occurrence of vulnerabilities [13].

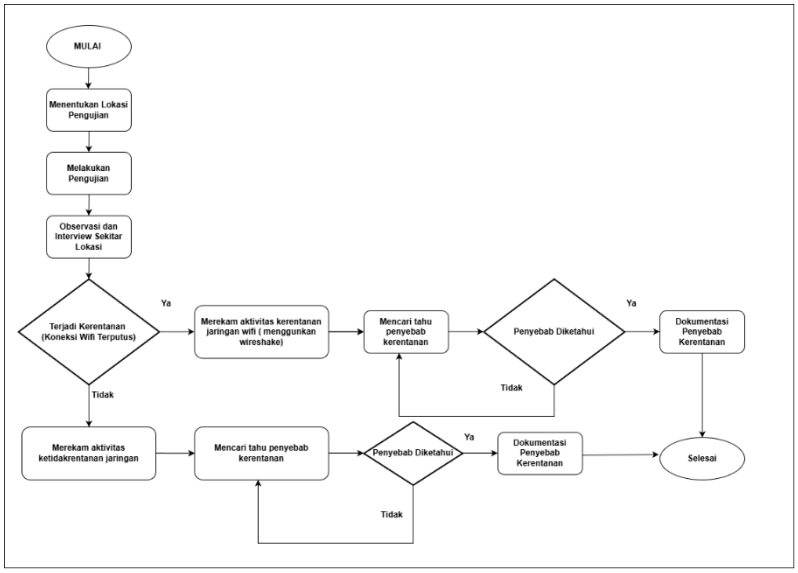

Figure 3. System Flow Planning Architecture and Test Network

2.5 Characteristics of Respondents and Research Objects

Given the technical-experimental nature of this research, the primary research object is network hardware infrastructure. The object characteristics include various types of access points operating at 2.4 GHz. From the perspective of human respondents, PT JSP network technicians served as key informants, providing operational validation regarding the impact of the attack on the end-user experience and overall system stability.

2.6 Data collection techniques

Data collection techniques were conducted through a combination of observation, interviews, and direct experiments. Primary data were obtained from the results of deauthentication attack simulations that recorded the direct impact on Quality of Service (QoS) parameters. QoS measurements were conducted using Wireshark software with packet capture and network traffic analysis methods under normal conditions and during attacks. The parameters described include throughput, latency, and packet loss on all 15 access points (APs) that were the object of the study. At each AP, the packet capture process was carried out for 60 seconds under normal conditions and 60 seconds under deauthentication attack conditions, with a minimum analysis threshold of 1000 packets sent in each test session. The client device used in the QoS measurements was a Lenovo Ideapad Slim laptop equipped with an IEEE 802.11n wireless network adapter at a frequency of 2.4 GHz. During the testing process, the ESP8266 Deauther device was placed at an average distance of approximately 3 meters from the target access point to maintain the stability of deauthentication packet delivery and minimize environmental interference. Each test on each access point was performed three times to ensure data consistency and reliability, and the final QoS results were calculated based on the average value of all tests performed. Secondary data was also collected through literature studies from journals and cybersecurity standard references such as NIST and ENISA to strengthen the theoretical foundation.[14].

2.7 Data Validity and Reliability

To ensure the validity of the results, the tests were performed repeatedly under varying network conditions. Data reliability was ensured through the use of industry-standard measurement tools such as Wireshark and iPerf3, which ensured an accurate and verifiable database for performance degradation measurements (such

as latency spikes of up to 300 ms or packet loss of 15%). The entire attack procedure was also documented in packet captures (pcap) and video to ensure transparency of the research results.

2.8 Attack execution procedure and parameter testing

Testing was conducted using the ESP8266 Deauther Version 2 on 15 access points (APs) at PT Jaring Solusi Persada, Tulungagung Branch. The Deauther V2 firmware was uploaded via the Arduino IDE and accessed via a web interface at the IP address 192.168.4.1. The ESP8266 scanned for SSIDs before executing a deauthentication attack by continuously sending deauthentication frames to the target access point. Quality of Service (QoS) measurements were performed using Wireshark under normal conditions and during the attack, measuring throughput, latency, and packet loss. Packet captures were performed for 60 seconds in each condition with a minimum threshold of 1,000 packets sent. Testing used a Lenovo Ideapad Slim laptop with an IEEE 802.11n 2.4 GHz adapter, with the ESP8266 placed approximately 3 meters from the target access point. The fifteen access points were tested three times to ensure the consistency and reliability of the research results.[15]. The calculation of throughput, latency, and packet loss parameters is done using the following QoS formula:

- Throughput
  Throughput is used to measure the speed at which data is successfully transmitted through the network during the testing process.
  $$Throughput = \frac{Data\ Amount}{TimeSpan(s)} \quad (1)$$
- Packet Loss
  Packet Loss is used to determine the percentage of data packets lost during the network transmission process.
  $$Packets\ Loss = \frac{Packets\ Send - Package\ Received}{Packets\ Send}\ x\ 100\% \quad (2)$$
- Latency
  Latency used to measure the delay that occurs when a packet is sent from the client to the access point.
  $$latency = \frac{Total\ Delay}{Number\ of\ Packages} \quad (3)$$

2.9 Data Analysis Techniques

The data obtained will be analyzed quantitatively. Researchers calculate the total percentage of vulnerabilities to determine the level of network security risk across all tested objects. The total percentage is calculated using the following formula:

- Calculation of the percentage of vulnerable devices

  $$\frac{Number\ of\ Vulnerable\ Devices}{Number\ of\ Devices\ Tested}\ x\ 100\% \quad (1)$$

- Calculation of the percentage of non-vulnerable devices

  $$\frac{Number\ of\ Devices\ Not\ Vulnerable}{Number\ of\ Devices\ Tested}\ x\ 100\% \quad (2)$$

3. Results and Discussion

3.1 Realization of Deauthentication Attack Testing Scheme

3.1.1 Hardware and software preparation

The initial stage includes preparing the ESP8266 device, data cables, and computer hardware used for the programming process. Additionally, firmware, or a program containing test functions according to the research scheme, is prepared.

3.1.2 Prototyping / Programming (Coding)

Before uploading the program, the first step is to write the program code that will be used to run the test scheme on the ESP8266 device. The code is written using the Arduino Integrated Development Environment (IDE) software, which serves as a tool for creating, editing, and managing programs on the microcontroller.

3.1.3 Programming Process Compiling device (compile)

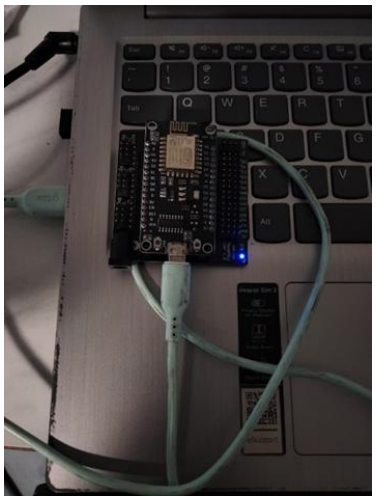

Figure 4.Compilation Device Programming Process

Figure 4 shows a test program uploaded to the ESP8266 memory via the Integrated Development Environment (IDE). At this stage, basic parameters are configured, such as selecting the board type, communication port, and network settings for the test object. Figure 4 shows the compilation process for connecting the Deauther device from a laptop to access the Deauther software home page.

Figure 5. Connect to Deauther Default SSID

After compiling to the ESP 8266, the SSID will appear, which is the main access point to the Deauther software home page. Figure 6 shows the process of connecting the Deauther device from a laptop to access the Deauther software home page.

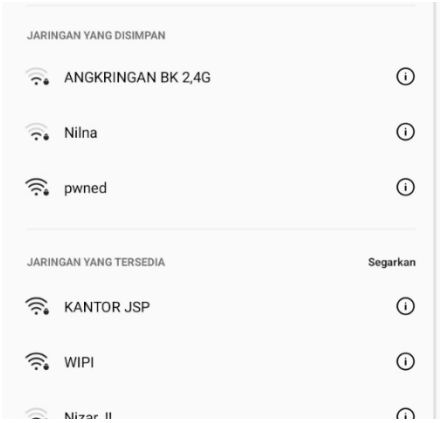

Figure 6.Wi-Fi Connection Status on Target Device

Figure 6 shows the Wi-Fi connection status on the target device before the deauthentication attack was executed. The image shows that the client device has successfully connected to the target Wi-Fi network with the status "Connected". This condition indicates that the network connection is in a normal and stable state before the attack testing process using ESP8266 Deauther Version 2. This view is used as an initial condition (baseline) to compare changes in the network connection after the attack is executed.

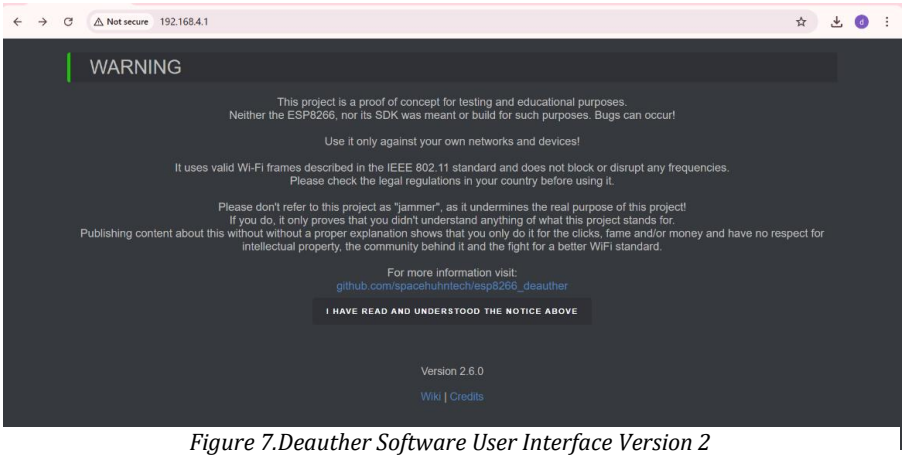

Figure 7.Deauther Software User Interface Version 2

Figure 7 shows the Deauther Version 2 web interface accessed through the default IP address 192.168.4.1. This interface is used to configure and execute deauthentication attacks using an ESP8266 device. Through this page, researchers can scan Wi-Fi networks, select a target access point, and invoke the "Deauth" feature to send deauthentication packets to the target device. This view demonstrates the control and monitoring process of the attacks carried out during the research.

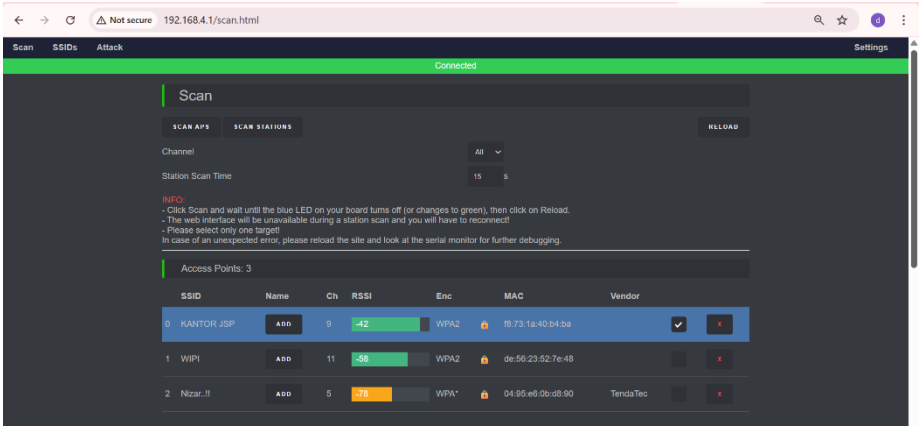

Figure 8. Scanning Target Wi-Fi SSID

Figure 8 shows the Wi-Fi SSID scanning process performed through the Deauther Version 2 web interface after successfully accessing the home page shown in Figure 7. At this stage, the ESP8266 device scans the surrounding Wi-Fi networks and displays available access points along with information such as SSID name, channel, signal strength (RSSI), encryption type, MAC address, and vendor. The displayed signal strength indicates the relative distance between the target network and the Deauther device used. Through this interface, researchers can select specific target access points to optimize the process of executing and monitoring deauthentication attacks.

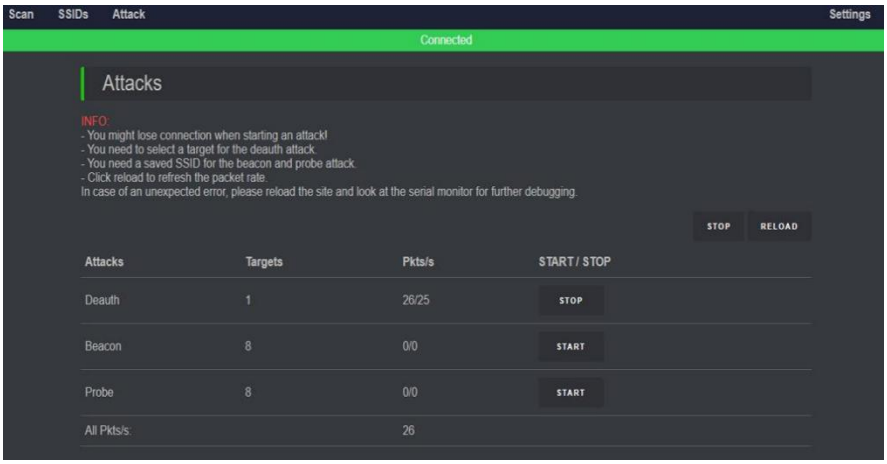

Figure 9. Running the Test

After scanning the Wi-Fi SSID to be attacked, then carry out the attack by pressing the Attack button in the menu at the top of the page, which is then continued in Figure 9, namely the process of carrying out the attack by pressing the Start button in the Deauth section. In this process, Deauther starts sending packets in the form of Deauthentication Frames to the target Wi-Fi network device. The result of this process will be considered successful if the target device experiences a disconnection from the Wi-Fi network, whereas if the network security on the device can handle this attack then nothing will happen to the target device's Wi-Fi network connection. This process can be stopped by pressing the Stop button in the Deauth section.

Figure 10. Test Response

Figure 10 shows the response from a target device connected to a Wi-Fi network. Figure 11 shows a target device attempting to reconnect to a Wi-Fi network that was disconnected by Deauther.

Figure 11. Final Response from Wi-Fi Target

Figure 11 shows the final response after the target device tries to reconnect to the previously connected Wi-Fi network, but the device is unable to reconnect to the Wi-Fi network, so it can be said that the Wi-Fi network device is vulnerable to Deauthentication Attack. The real impact of this attack on the stability of data transfer can be analyzed through the throughput parameters in Table 1 below:

Table 1. QoS Measurement Results on Vulnerable and Non-Vulnerable Access Points During Deauthentication Attacks

Parameter	Before Attack (Normal)	After the Attack (Deauthentication)
Throughput	567 kbps	170 kbps
Packet Loss	0%	15%
Latency	20,7ms	100-300 ms
Packets Send	1311	1000
Packets Received	1311	850

Based on the test results in Table 1, vulnerable access points experienced significant network performance degradation during the deauthentication attack. On TP-Link devices, throughput decreased from 567 kbps to 170 kbps, packet loss increased from 0% to 15%, and latency increased from 20.7 ms to 100–300 ms.

Furthermore, the number of received packets also decreased from 1,311 packets to 850 packets due to the deauthentication attack. In contrast, Ruijie Enterprise devices, as a non-vulnerable category, showed relatively small QoS changes and were still able to maintain network connection stability during the attack. These results indicate that non-vulnerable devices have better protection mechanisms against deauthentication attacks than vulnerable devices.[16].

Table 1 shows that vulnerable access points experienced significant network performance degradation during the deauthentication attack. On TP-Link devices, throughput decreased from 567 kbps to 170 kbps, packet loss increased from 0% to 15%, latency increased from 20.7 ms to 100–300 ms, and the number of received packets decreased from 1,311 to 850. These results indicate that the deauthentication attack disrupted network communications, reduced data transmission efficiency, and caused network instability due to repeated disconnections between clients and the access point. In contrast, Ruijie Enterprise devices, classified as non-vulnerable, experienced only relatively minor QoS changes and maintained a stable network connection throughout the attack. These results align with research by Fitrian et al. (2026), who found that WPA2-based networks without Protected Management Frames (PMF) experienced significant QoS degradation during deauthentication attacks, while WPA3 networks demonstrated greater resilience. Research by Asiana et al. (2025) also demonstrated increased latency and packet loss in a campus Wi-Fi environment during a simulated attack. Compared to previous studies, the industrial network environment at PT Jaring Solusi Persada showed a relatively comparable decrease in throughput and increase in packet loss, but experienced a higher increase in latency, reaching 300 ms. This difference is likely influenced by the type of device, network security configuration, and the more complex traffic conditions of an industrial network. This suggests that non-vulnerable devices have better protection mechanisms against deauthentication attacks than vulnerable devices. Table 1 shows a significant decrease in network performance due to the deauthentication attack. Throughput dropped from 567 kbps to 170 kbps (approximately 70%), indicating a significant reduction in data transmission speed caused by network interference. Packet loss increased from 0% to 15%, with 150 out of 1000 packets lost, due to repeated disconnections between the client and the access point.[17]. Meanwhile, latency increased from 20.7 ms to 100–300 ms, indicating delays caused by reconnection attempts and retransmissions.The results of the vulnerability level identification for each SSID are presented in Table 2 below:

Table 1. Deauthentication Attack Results Analysis

NO	Wi-Fi SSID Name	Hardware Type/Brand (AP)	Status
1	Solusi persada.net	Ruijie RG-AP820-L series device	Non Vulnerable
2	KANTOR JSP 5G	Ruijie RG-AP720-L enterprise AP	Non Vulnerable
3	Nilna	Ruijie RG-AP820-L wireless unit	Non Vulnerable
4	ANGKRINGAN BK 2.4G	Ruijie RG AP820-L Ruijie RG-AP820-L access device	Non Vulnerable
5	Nizar..!!	TP-Link TL-WR840N router device	Vulnerable
6	WIPI	TP-Link WR720N 150 Mbps router	Vulnerable
7	DAVA	TP-Link TL-WR840N wireless router	Vulnerable
8	KANTOR JSP	ZTE F609 GPON router	Vulnerable
9	Melody	Ruijie RG AP820-L Ruijie RG-AP820-L wireless access point	Non Vulnerable
10	GUDANG JSP	Ruijie RG AP820-L Ruijie RG-AP820-L enterprise AP unit	Non Vulnerable
11	Niken	Ruijie RG-AP820-L network access device	Non Vulnerable
12	RAHAYU.NET	Ruijie EW300-PRO wireless router	Vulnerable
13	JD	Totolink N200RE Totolink N200RE router device	Vulnerable
14	zidan	Ruijie RG AP820-L Ruijie RG-AP820-L access point unit	Non Vulnerable
15	AP.NET	Ruijie RG-AP820-L wireless AP device	Non Vulnerable

Based on the data in Table 2, it can be concluded that of the 15 Access Points tested, there is a dominance of Non-Vulnerable devices as many as 9 units (60%), most of which are Ruijie Enterprise series brands (RG AP820-L and RG AP720-L), showing good defense against deauthentication packets. In contrast, 6 units (40%) of devices were found to be Vulnerable, dominated by consumer category devices such as TP-Link, ZTE, and

Totolink, indicating that these devices have not activated or supported the Management Frame Protection (MFP) feature. This confirms a strong correlation between hardware specifications and network resilience, where business-class devices tend to be more stable in the face of forced disconnection attempts compared to standard home devices. To ensure that all test stages run consistently across the 15 access points, test scenarios were prepared that include various components and measurement parameters.[18]. Details of the test plan can be seen in Table 3 as follows:

Table 2. System Test Scenario Plan

Test Component	Testing Scenario	Measurable Parameter	Expect results
ESP8266 Deauther	Perform an attack on the target AP.	Number of deauth frames	Frame sent to AP
Wi-Fi Network	Observation of impact on clients	Client connection	Client connection lost.
Package Analysis	Frame detection via Wireshark	Frame deauthentication	The system detects the frame.
Network Performance	Measuring performance during attacks	Throughput & Latency	Performance degradation

Based on the test scenario plan presented in Table 3, it can be concluded that this test is comprehensively designed to evaluate the effectiveness and impact of deauthentication attacks using an ESP8266 Deauther device on a Wi-Fi network infrastructure. The main focus of this test includes validation of the device's functionality in sending attack packets, direct observation of user connectivity stability on the target network, and technical evidence through packet analysis using Wireshark software. Through measurable parameters such as the number of remote frames, client connection status, and network performance metrics such as throughput and latency, this scenario aims to demonstrate how interference at the wireless protocol layer can forcibly disconnect a client device from the access point. The expected results consistently show significant performance degradation and loss of service for legitimate users, thus validating the vulnerability of the 802.11 protocol to this type of attack. Overall, this table provides a systematic framework for documenting empirical evidence regarding network failure mechanisms under the stress of remote attacks, which can ultimately be used as a basis for evaluating more robust wireless intrusion defense or detection systems in the future.The real impact of the connection loss is visible in the Target Wi-Fi Final Result Response Image[19]. Then measure quantitatively through Quality of Service (QoS) parameters, with a comparison between normal conditions and conditions during an attack as listed in Table 4 below:

Table 3. Comparison of Quality of Service (QoS) Parameters

QoS parameters	Normal Condition (Not Attacking)	Conditions During Deauth Attack	Impact / Reject
Throughput	567 kbps	170 kbps	Decreased drastically (-70%)
Latency	20.7 ms	100 – 300 ms	Data delay spike
Packet Loss	0% (Stable)	15%	Significant data loss

Based on the data in Table 4, it can be concluded that the deauthentication attack using the ESP8266 had a very significant destructive impact on all Quality of Service (QoS) parameters on the tested Wi-Fi network. The most striking performance degradation was seen in the throughput value which dropped sharply by 70%, from the normal condition of 567 kbps to only 170 kbps, indicating a drastic narrowing of the data communication channel. In addition, this attack caused extreme network instability with a latency spike of up to 300 ms, or a more than tenfold increase from the normal condition of only 20.7 ms. The emergence of a packet loss value of 15% from the previous 0% (stable) also confirms that this attack not only slowed down the connection but also damaged the integrity of data transmission by causing the loss of information packets in the air. Technically, the combination of low throughput, high latency, and packet loss indicates that remote attacks regularly crippled

network efficiency, making internet services unreliable and very difficult for legitimate users to access during the attack. After identifying the technical impact on one network, testing was extended to several other devices to classify the level of infrastructure vulnerability, the results of which are summarized in Table 5 below:

Table 4. Device Vulnerability Classification Results (Access Points)

Device Category	Amount	Percentage	Security Status
Vulnerable	6Devices	40%	Disconnects completely during an attack
Not Vulnerable	9 Devices	60%	Connection remains stable during attack
Total Testing	15 Devices	100%	

Based on the data presented in Table 5, it can be concluded that the tested wireless network infrastructure exhibited varying levels of resilience to deauthentication attacks. Of the 15 Access Point (AP) devices tested, 6 devices, or 40%, were classified as Vulnerable, as the client connection was completely lost during the attack. This indicates that these devices likely lacked advanced wireless security mechanisms such as Management Frame Protection (MFP/802.11w), which is designed to validate the authenticity of management frames and mitigate deauthentication attacks. Conversely, 9 devices, or 60%, were categorized as Not Vulnerable, as the client devices maintained a stable connection throughout the simulated attack. This finding suggests that implementing stronger security configurations, firmware updates, or the use of more modern wireless hardware could significantly reduce the effectiveness of the ESP8266 Deauther attack. Overall, these classification results demonstrate that deauthentication attacks remain a real threat to wireless networks, especially for devices lacking modern security protections. These findings also emphasize the importance of improving wireless network security standards and regularly updating network device configurations to minimize potential vulnerabilities.[20].

4. Conclusion and Future Work

Based on penetration testing results using the ESP8266 Deauther Version 2 on 15 access points (APs) at PT Jaring Solusi Persada (JSP) Tulungagung Branch, it can be concluded that the wireless network infrastructure at the location still has critical security vulnerabilities. Six APs (40%), predominantly consumer-grade devices such as TP-Link, ZTE, and Totolink, were identified as vulnerable. When the attack was executed, client connections on these devices were completely disconnected because the devices did not support or enable the Management Frame Protection (MFP/802.11w) feature. This deauthentication attack was empirically proven to significantly reduce communication efficiency by reducing throughput by up to 70% (from 567 kbps to 170 kbps), triggering latency spikes of up to 100–300 ms, and causing packet loss of up to 15%. In contrast, nine APs (60%), mostly Ruijie Enterprise series, managed to maintain stable network connections during the attack due to their superior hardware specifications and stronger security configuration against deauthentication packets. These findings support the global IoT security benchmark presented in the Introduction, which states that over 60% of IoT security incidents are caused by weak configurations and inadequate protection mechanisms. This suggests that the wireless network vulnerabilities discovered at PT JSP reflect broader cybersecurity challenges worldwide. As a mitigation measure and recommendation to improve the resilience of PT JSP's network infrastructure in the future, it is strongly recommended that network administrators update security standards by adopting WPA3 encryption technology and enabling the Protected Management Frames (PMF/MFP) feature on all access points to validate the authenticity of management frames. Furthermore, reliance on standard consumer-grade hardware should be reduced and gradually replaced with business-grade devices, which are generally more resilient to forced disconnection attempts. For future research, researchers are encouraged to design active defense systems, such as implementing a Wireless Intrusion Detection System (WIDS) or Wireless Intrusion Prevention System (WIPS), capable of proactively monitoring and mitigating deauthentication attacks in real-time in industrial network environments.

5. Reference

[1] M. Chakroun, J. Sayah, C. Kallab, and S. El-haddad, “Internet of Things: Towards a Solid Ecosystem of Interconnected Things,” *Advances in Internet of Things*, vol. 12, no. 3, pp. 35–64, 2022, doi: 10.4236/ait.2022.123004.

[2] N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie, and T. Shongwe, “Internet of Things and Wireless Sensor Networks for Smart Agriculture Applications: A Survey,” *IEEE Access*, vol. 11, pp. 145813–145852, 2023, doi: 10.1109/ACCESS.2023.3346299.

[3] B. T. Hanggara, M. H. Nasrullah, and D. Pramono, “Analisis Perbandingan Performa Framework NestJS dan Lumen Pada Studi Kasus Aplikasi Berbasis REST API,” *J-INTECH (Journal of Innovation and Technology)*, vol. 12, no. 1, pp. 181–189, 2024, doi: 10.32664/j-intech.v12i1.1354

[4] R. A. Saputra, R. D. Ridwansyah, D. A. Erlangga, and E. Rilvani, “KEAMANAN SISTEM OPERASI DALAM ERA INTERNET OF THINGS,” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 2, pp. 1939–1944, 2025, doi: 10.36040/jati.v9i2.12837.

[5] M. Risal, andy lukman Affandy, and A. Ilham, “IMPLEMENTASI PRINTER SERVER WIRELESS FIDELITY BERBASIS RASBERRY PI PADA UNIVERSITAS HANDAYANI MAKASSAR,” *JURNAL IT (Media Informasi IT STMIK Handayani)*, vol. 15, no. 1, pp. 1–11, 2024.

[6] L. M. Z. Fikri, A. Z. M., and A. Zubaidi, “Analisis Keamanan Jaringan Wi-Fi Dengan Metode Deauthentication Attack Pada Access point Di Lingkungan Universitas Mataram,” *Jurnal Teknologi dan Sistem Informasi*, vol. 11, no. 2, pp. 75–84, 2023.

[7] Z. Alfian, A. Effendi, F. Priyogi, and R. N. Yatim, “Pengembangan Media Pembelajaran Logika Boolean Berbasis Web Menggunakan Pyodide Dengan Pendekatan Prototyping Bagi Mahasiswa Teknik Informatika,” *Journal of Informatics Management and Information Technology*, vol. 6, no. 1, pp. 19–29, 2026, doi: 10.47065/jimat.v6i1.941.

[8] H. P. Fitrian, E. Eriyana, H. M. Ibrahim, R. P. Rizqullah, and S. P. Meliansyah, “Security Evaluation of WPA2 vs WPA3 Wireless Network Against Deauthentication and Brute Force Attacks using Aircrack-ng,” *Jurnal Ilmiah Sistem Informasi (JUISI)*, vol. 5, no. 1, pp. 257–274, 2026, doi: 10.51903/gy968e07

[9] A. Irfan, A. Z. Nusri, Z. Rachmat, and S. Wulandari, “Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS),” *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI)*, vol. 7, no. 1, pp. 110–119, 2024, doi: 10.57093/jisti.v7i1.195.

[10] R. S. Pratikno, C. Trinata, and G. B. Hertantyo, "Kajian Literatur Analisis Keamanan Jaringan," *Pendas: Jurnal Ilmiah Pendidikan Dasar*, vol. 10, no. 2, pp. 361–370, 2025, doi: 10.23969/jp.v10i02.28330.

[11] Somantri, gina purnama Insany, and R. Ryansah, “Pengembangan Sistem Keamanan Kendaraan Bermotor Menggunakan Teknologi Fingerprint dengan Metode Prototype Berbasis Internet Of Things,” *G-Tech: Jurnal Teknologi Terapan*, vol. 8, no. 1, pp. 593–602, 2024, doi: 10.33379/gtech.v8i1.3879.

[12] M. S. Ariyanto, G. B. Hertantyo, and B. Hartati, “Serangan Deauthentication Attack Pada Wireless Access Point: Systematic Literature Review,” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, pp. 6606–6612, 2025, doi: 10.36040/jati.v9i4.13808.

[13] A. B. N. As-sajid and R. E. Putra, “Analisis dan Pengujian Dictionary Attack terhadap WPA3 Berbasis Script,” *JINACS (Journal of Informatics and Computer Science)*, vol. 5, no. 2, pp. 216–222, 2023. Doi: 10.26740/jinacs.v5n02.p216-222

[14] U. Sulung and M. Muspawi, “Memahami Sumber Data Penelitian: Primer, Sekunder, dan Tersier,” *EDU RESEARCH*, vol. 5, no. 3, pp. 110–116, 2024.

[15] K. P. Asiana, R. B. Huwae, and A. H. Jatmika, "Studi Eksperimen Keamanan Jaringan Wi-Fi Kampus: Analisis Kerentanan terhadap Serangan Evil Twin dan Deauthentication," *Edumatic: Jurnal Pendidikan Informatika*, vol. 9, no. 2, pp. 629–638, 2025, doi: 10.29408/edumatic.v9i2.31822.

[16] A. Pranandi, M. Nurdin, utari dwi F, and Y. Hermawan, "Serangan Phising Wifi Menggunakan ESP8266: Replikasi Jaringan untuk Penangkapan Informasi Otentikasi," *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis*, vol. 2, no. 7, pp. 638–649, 2024.

[17] Z. Alamin and M. Amirul, "Analisis Keamanan Jaringan pada Sistem Kendali Jarak Jauh untuk Infrastruktur Kritis (Network Security Analysis of Remote Control System for Critical Infrastructure)," *Jurnal Pengembangan Sains dan Teknologi*, vol. 1, no. 1, pp. 25–41, 2025, doi: 10.63866/jpst.v1i1.39.

[18] A. R. Manik, M. B. Akbar, and J. Purba, "Academic Portal with MFA (WhatsApp OTP via Fonnte), Role-Based Access Control, and Logging System for Network Monitoring," *Jurnal Ilmiah Sistem Informasi (JISI)*, vol. 4, no. 3, pp. 674–687, 2025, doi: 10.51903/qwz6pt87.

[19] Y. Farhan and A. S. Aziz, "Analisis Keamanan Jaringan Wi-Fi Pada SMKN 1 Kota Jantho Menggunakan Metode Vulnerability Assessment (Wi-Fi Network Security Analysis At SMKN 1 Kota Jantho Using The Vulnerability Assessment Method)," *Cyber Security dan Forensik Digital*, vol. 8, no. 2, pp. 1–10, 2025.

[20] T. Yusnanto, M. A. Muin, and S. Wahyudiono, "Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux," *Journal on Education*, vol. 4, no. 4, pp. 1470–1476, 2022, doi: 10.31004/joe.v4i4.2175.