Analysis of Wi-Fi Network Security Against Phishing and Distributed Denial of Service (DDoS) Attacks

Muhammad Taufik Rifaat[a,1], Amaliah Faradibah[a,2], Achmad Nuril Fauzi[b,3]

[a] *Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Jl. Urip Sumoharjo km.05, Makassar dan 90231, Indonesia*
[b] *Program Studi Teknik Elektro, Fakultas Teknik, Universitas Negeri Malang, Malang dan 65145, Indonesia*
[1] trifaat39@gmail.co; [2] amaliah.faradibah@umi.ac.id; [3] achmad.nuril.2405348@students.um.ac.id
**corresponding author*

ARTICLE INFORMATION

Received : 18 – 11 – 2024
Revised : 12 – 09 – 2025
Published : 29 – 10 – 2025

Keywords:
Distributed Denial Of Service (DDOS)
Phishing
Vulnerability Assessment
Fluxion

ABSTRACT

This study aims to analyze and identify vulnerabilities to Distributed Denial of Service (DDoS) and phishing attacks on FIKOM UMI's Wi-Fi with the access point SSID "UMI Connect," and to provide recommendations to FIKOM UMI. The method employed is Vulnerability Assessment using the Fluxion tool and a TP-Link wireless adapter. The findings reveal two types of vulnerabilities—packet injection and wireless hijacking—each with medium risk and medium confidence. These weaknesses reside at the SSID layer. Attackers can exploit them to disconnect clients from the network and subsequently perform phishing to obtain the access-point password of the targeted SSID. While some security components on the target access point are functioning properly, several areas still require improvement—specifically, unlimited packet rates per second passing through TCP/UDP data transmissions between users and the access point, which should be rate-limited.

I. Introduction

The Faculty of Computer Science (FIKOM) at Universitas Muslim Indonesia (UMI) operates a Wi-Fi network to support academic and non-academic activities across the FIKOM community. Approximately 500 FIKOM students require internet access for practicums, lectures, research, and other activities. The Wi-Fi network expands internet availability throughout the FIKOM area, making it easier for students to connect. Network management at FIKOM uses MikroTik devices—CCR1036-8G-2S+, version 6.49.7 (stable), with the device name MENARA CORE as the core router, and CRS328-24P-4S+, version 6.48.6 (long-term), named MikroTik-FIKOM. Wireless coverage is provided by Ubiquiti UniFi AP AC Pro access points at seven locations. Given the network's complexity and heavy utilization, security risks become increasingly significant. Phishing and Distributed Denial of Service (DDoS) attacks are among the threats faced. The security posture of FIKOM's Wi-Fi remains relatively passive, in part because it still relies on SHA-1 (Security Hash Algorithm 1) for encryption. Therefore, analyzing FIKOM UMI's Wi-Fi security against phishing and DDoS attacks is essential to protect the integrity and confidentiality of information.

Based on prior research, Wi-Fi network analyses against DDoS attacks have been conducted in university environments [1][2][3] and corporate environments [4]; studies have also examined vulnerabilities in academic information systems [5], phishing threats to online banking services [6], and network monitoring for DDoS attacks [7]. The Vulnerability Assessment method is among the most frequently used approaches for analyzing problems related to phishing and DDoS attacks. Consequently, further research applying the Vulnerability Assessment method is warranted.

In light of these issues, this study is titled "Analysis of FIKOM UMI's Wi-Fi Network Security Against Phishing and Distributed Denial of Service (DDoS) Attacks." Through these steps, FIKOM UMI can ensure that its Wi-Fi network serves not only as an efficient tool for education and research but also as robust protection against potential cyberattacks.

II. Method

Vulnerability assessment is the process used to analyze, identify, classify, and test points that could serve as The evaluation of network security using the Vulnerability Assessment method comprises several stages to discover exploitable gaps.:

A. Problem Identification

This stage is carried out by visiting FIKOM UMI directly and examining the constituent elements of the computer network on site.

B. Scenario

The scenario defines the structure, phases, and tool features to be used in the attacks, as well as the recommendations to be provided for the target system. The goal is to ensure that the planned steps and analyses match the specified requirements and function correctly.

C. Vulnerability Analysis

Needs analysis is the process of identifying and understanding what the researcher requires from the planned attack design in order to perform exploitation of the target.

D. Exploitation

Exploitation is the phase in which the planned attacks are implemented on the research target. The outcomes of this process are then analyzed. After implementation, testing is conducted to determine whether the target network's security meets the predefined quality standards. Testing is performed at the Faculty of Computer Science, Universitas Muslim Indonesia.

E. Report

In the reporting stage, all aspects of the research are documented comprehensively and clearly for the reader. The results serve as recommendations for stakeholders responsible for the target system.

F. Conclusion

The conclusion is a critical stage that summarizes the findings and their relevance to the research objectives. It includes the results of the analysis on the target system and enables the formulation of clear takeaways. The conclusion provides an overall picture of the research outcomes.

Figure 2. Research Stages

III. Results and Discussion

A. Results

1) Vulnerability Analysis

a. Network Scanning

At this stage, the target network was identified based on the SSID (network name), BSSID (router MAC address), the encryption type in use, and signal strength. As shown in Figure 3, the SSID "UMI Connect" was selected as the target by the researcher.

Figure 3. Network Scanning

b. Network Scanning

In this stage, a scan was performed to discover clients connected to the target network. The collected information includes the users' MAC addresses and signal strengths. User activity was also analyzed to determine when they are active and how frequently they connect to—or disconnect from—the network, as shown in Figure 4.

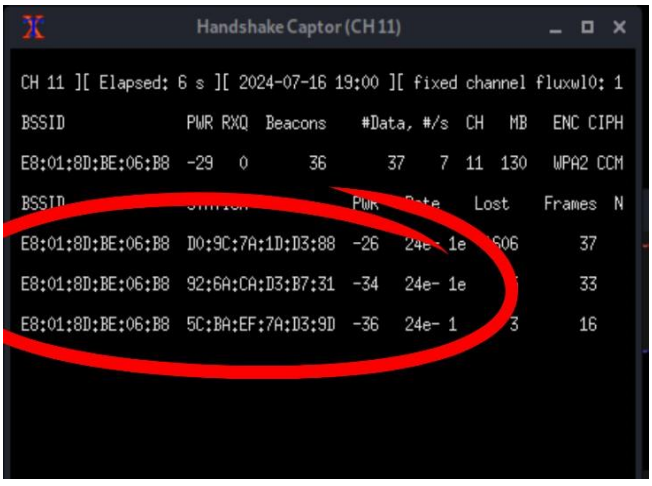

Figure 4. User Scanning

c. Network Scanning

Capturing the handshake is a crucial step when attacking Wi-Fi networks that use WPA/WPA2. The handshake occurs when a user attempts to connect to the Wi-Fi network. To capture it, the researcher forced connected users to disconnect and then reconnect by sending deauthentication

(deauth) packets to the user and the router. On the user interface in Figure 5, the target access point "UMI Connect" is shown under a Distributed Denial of Service (DDoS) attack.

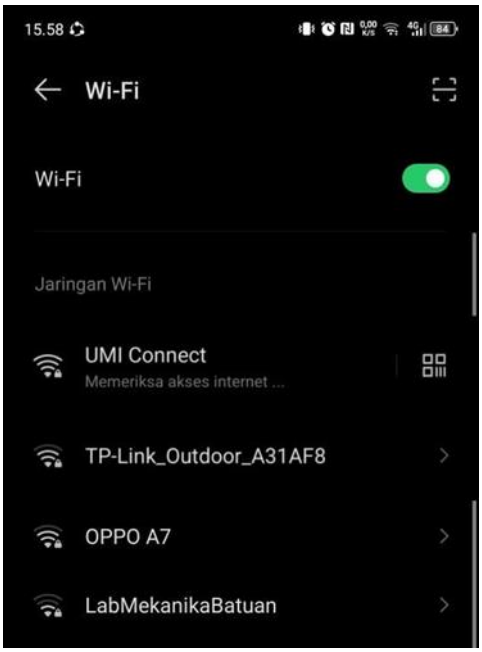

Figure 5. Target Access Point User View

In Figure 6, the researcher successfully obtained the encryption parameters needed to create a rogue access point, enabling the subsequent phishing attack stage.

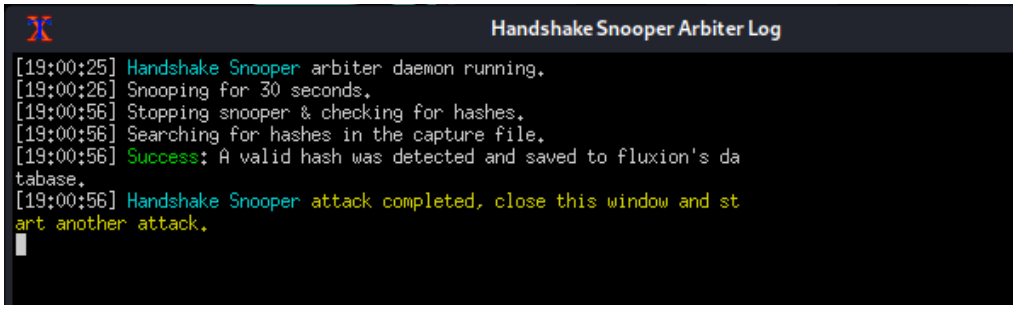

Figure 6. Encryption Capture

2) Exploitation

At this stage, a phishing attack was conducted after completing the vulnerability analysis.

First, the researcher selected a landing page to serve as the phishing medium, choosing from the options available in the Fluxion tool (see Figure 7).

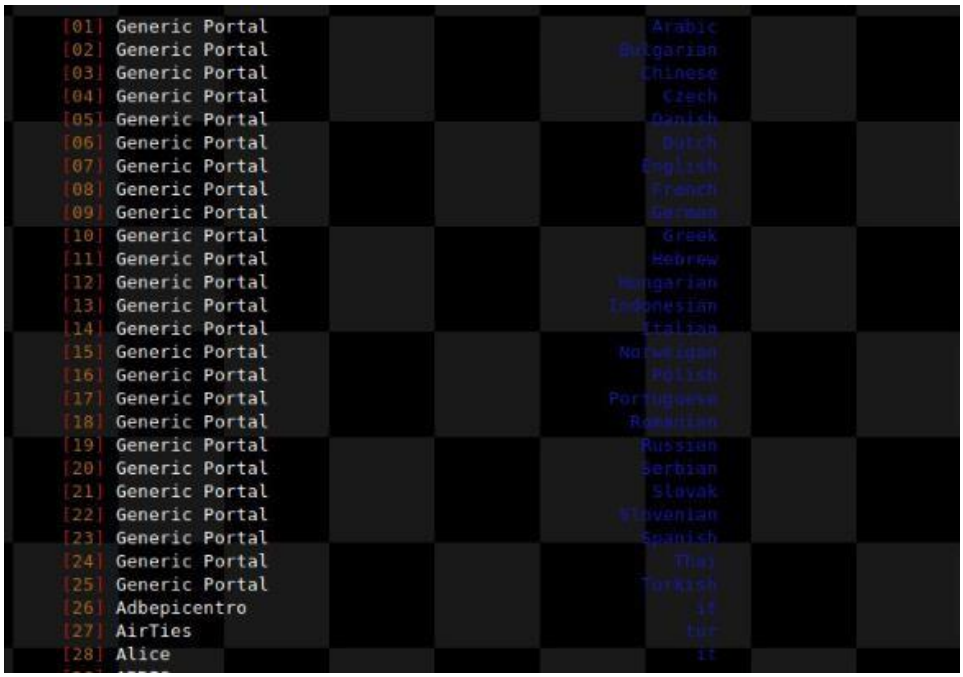

Figure 7. Phishing Landing-Page Options

Next, the researcher presented a fake access point to the victim while disabling the legitimate access point and activating the phishing landing page designed to capture the Wi-Fi password, as illustrated in Figures 8 and 9.

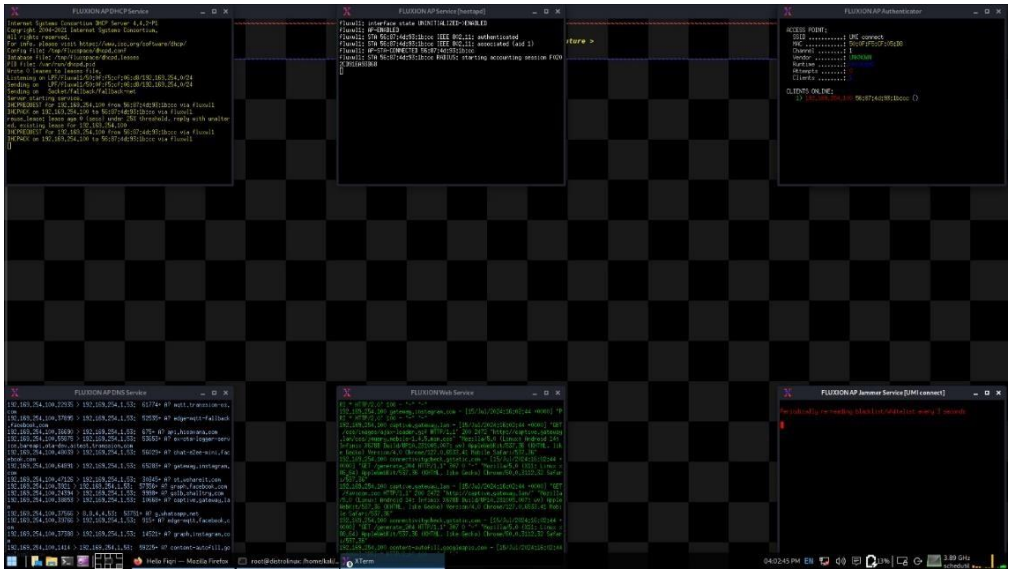

Figure 8. DDoS process steering users to the rogue access point

Rogue access point

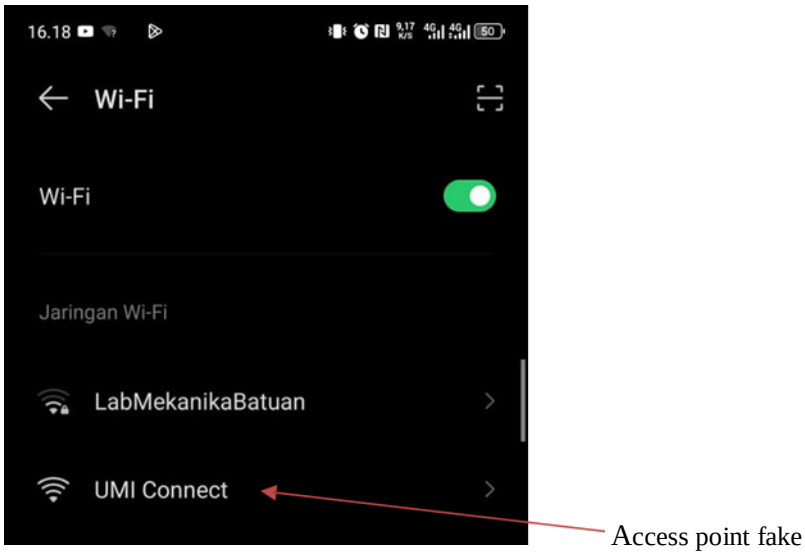

Figure 9. Rogue access point as displayed to the user

The victim then clicks the rogue access point, which redirects them to the phishing landing page prepared by the researcher (Figure 10). The user proceeds to enter the Wi-Fi password.

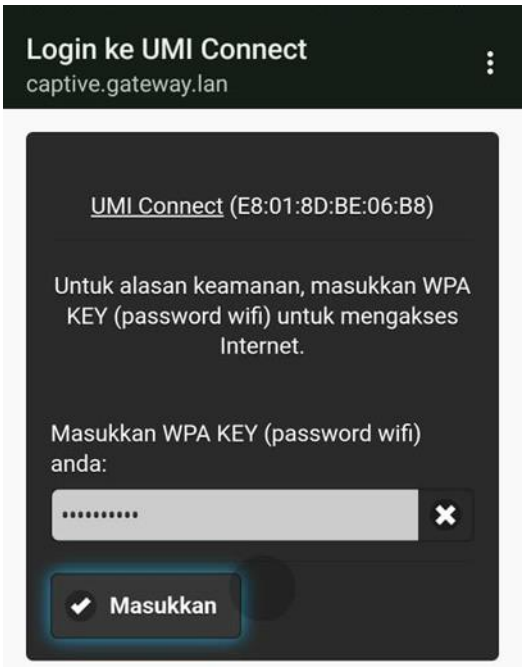

Figure 10. Phishing landing-page view

After the user submits the password on the landing page, the researcher receives the credentials in Fluxion's log output, i.e., the Wi-Fi password entered by the victim, as shown in Figure 11.

Figure 11. Log output from the rogue access point.

B. Discussion

This study was conducted over three days with three trials, each yielding different results depending on prevailing conditions, as summarized in Table 1.

Table 1. Summary of Attack Experiments

Date & Time	Result
10/7/2024	At the access-point location on the 1st floor of FIKOM UMI, the researcher successfully executed exploitation at 14:53 WITA, but only a DDoS attack. This was due to the large number of access points at other spots and high user mobility/volume, so only a small subset was affected. In addition, users were not lured into the phishing redirection.
12/7/2024	The second attempt was carried out at the 3rd-floor access-point location at 14:12 WITA, with results similar to the first trial. In this attempt, the researcher identified the cause: limitations of the equipment used during the attack and frequency support mismatches between the tool and the access point.
17-07-2024	After concluding the causes from the first two trials, the researcher performed exploitation at the 2nd-floor access-point location under conditions conducive to attack. The attack began at 17:00 WITA when the site was quiet. This ensured the prepared users could be detected as victims. Ultimately, the researcher successfully executed both DDoS and phishing attacks.

In this study, several users prepared as victims were used to target the access point. From the DDoS attack, the immediate impact on the access point was observed directly, followed by the phishing attack.

However, several constraints influenced the success rate of the attacks, as follows:

a) The wireless adapter used by the researcher supports monitoring only on the 2.4 GHz band.

b) The access point under attack was always shifted to 5 GHz; therefore, the DDoS did not fully exploit MAC addresses.

c) The number of target access points was large.

d) The researcher attacked a single target only due to limitations of the attack equipment.

e) The researcher had difficulty detecting which access point was being hit by the DDoS.

f) The attack is most effective when few users are on the access point and the user–AP distance is short.

Table 2 lists two vulnerability types—Packet Injection and Wireless Hijacked—with their respective risk and confidence levels.

Table 2. Vulnerability Summary.

Wi-Fi Network Vulnerabilities on UMI Connect	Vulnerability Location	Impact	Risk	Confidence
Packet Injection	SSID	Disconnects Wi-Fi network connections	Medium	Medium
Wireless Hijacked	SSID	Redirects users to a phishing landing page to	Medium	Medium

Wi-Fi Network Vulnerabilities on UMI Connect	Vulnerability Location	Impact	Risk	Confidence
		enter the Wi-Fi password		

For Packet Injection, the risk is medium because the limitations of the wireless adapter's supported frequencies affected attack performance. The likelihood of success is medium since the attacker must entice the prepared victim user, and a basic understanding of handshake capture is required.

For Wireless Hijacked, the risk is medium because it depends on the prior DDoS succeeding. The likelihood of success is medium due to possible incorrect password entries by users and a limited choice of landing-page options. Below is a brief explanation of recommendations for the identified vulnerabilities (see Table 3).

Table 3. Recommendation Summary.

No.	Vulnerability Type	Recommendation
1	Packet Injection	1) Configure the firewall to filter malicious traffic. 2) Implement rate limiting to cap the number of requests/packets allowed from a single IP within a given time window.
2	Wireless Hijacked	1) Use HTTPS (Hypertext Transfer Protocol Secure) to encrypt data between browser and server, making it harder for attackers to intercept session information. 2) Use WPA3 encryption; segregate guest and internal networks.

IV. Conclusion

The results indicate vulnerabilities on FIKOM UMI's Wi-Fi with the target access point UMI Connect, based on exploitation using the Fluxion tool—showing medium risk and medium confidence. This means some security components on the target access point function properly, but several items still require remediation, notably the absence of per-second packet rate limits on TCP/UDP data transmissions between users and the access point. There are also wireless-adapter limitations: it does not support 5 GHz, causing users to be shifted to 5 GHz (and vice versa). If the adapter is set to 5 GHz, users are shifted to 2.4 GHz.

Future studies of this type should use a wireless adapter that supports 2.4 GHz and 5 GHz in parallel. This will streamline the attack workflow in an experimental context, since user band-shifting will no longer hinder the flow of the test procedure..

References

[1] E. Pratama, "Wardriving Jaringan WIFI Serta Menganalisa Qos Pada Jaringan Internet Universitas Sriwijaya Yang Tidak Terenkripsi Keamanannya," vol. 1, no. 2, pp. 11–18, 2024.

[2] R. Anugerah Julyan Rahmat, N. Fahriani, S. Jl Raya Sutorejo No, D. Sutorejo, K. Mulyorejo, and J. Timur, "Deteksi Serangan DDoS Dan Sniffing Pada Jaringan Wireless Di Lab Informatika Um Surabaya Dengan Metode Vulnerability Assessment," vol. 2, no. 1, pp. 88–96, 2023.

[3] A. Y. Suharmanto, A. S. M. Lumenta, X. B. N. Najoan, T. Elektro, U. Sam, and R. Manado, "Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi," J. Tek. Inform., vol. 13, no. 3, pp. 1–10, 2018.

[4] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "Pendeteksi Serangan DDoS (Distributed Denial Of Service) Menggunakan Honeypot Di PT. Torini Jaya Abadi," J. Sist. Inf. dan Inform., vol. 2, no. 2, pp. 64–80, 2019, doi: 10.47080/simika.v2i2.606.

[5] E. Irawadi Alwi and L. Budi Ilmawan, "Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment," 2021.

[6] Amin Muftiadi, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking," Hexatech J. Ilm. Tek., vol. 1, no. 2, pp. 60–65, 2022.

[7] A. Hamzah, S. Juli, I. Ismail, L. Meisaroh, S. Si, and M. Si, "Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix dan Web Web Application Firewall di PT PLN (Persero) Transmisi Jawa Bagian Tengah," e-Proceeding Appl. Sci., vol. 5, no. 3, pp. 2378–2384, 2019