e-ISSN: 3108-9828 | p-ISSN: 3109-3981
Volume 3 No 1 May 2026 | Page: 20–28
DOI: https://doi.org/10.64803/jocsaic.v3i1.173

Journal of Computer Science Artificial Intelligence and Communications

Journal Homepage: https://journals.raskhamedia.or.id/index.php/jocsaic

Wireless Network Security Analysis Using the Penetration Testing Method in a Campus Environment

Abil Alwi Prayoga[1*], Siti Khodijah[2]

[1,2]Sains Komputasi dan Kecerdasan Digital, Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, Indonesia
Author(s) Email: [1*]abilabil1752@gmail.com, [2]sitikhodija31@gmail.com

ARTICLE INFO

Article history:

Received May 17, 2026
Revised May 25, 2026
Accepted May 29, 2026
Publish May 31, 2026

ABSTRACT

The rapid development of information technology has increased the utilization of wireless networks in higher education environments to support academic activities, administrative services, and digital communication. However, the widespread use of wireless networks also introduces various cybersecurity risks due to the open nature of wireless communication media. This study aims to analyze the security level of campus wireless networks using the penetration testing method to identify vulnerabilities and evaluate existing security mechanisms. The research applies a systematic penetration testing approach consisting of several stages, including information gathering, scanning, vulnerability assessment, exploitation testing, and reporting. The testing process focuses on analyzing wireless configurations, authentication mechanisms, encryption implementation, and potential unauthorized access risks. The results indicate that although the campus wireless network has implemented security protocols such as WPA/WPA2 and encryption mechanisms, several vulnerabilities remain, particularly related to weak password policies, limited access control, and insufficient network monitoring. Based on the vulnerability assessment, improvements are recommended through the implementation of stronger authentication methods, enhanced password management policies, continuous network monitoring, and periodic security evaluations. This research demonstrates that penetration testing is an effective method for identifying security weaknesses and improving wireless network protection. The findings are expected to provide valuable insights for educational institutions in developing more secure, reliable, and sustainable wireless network infrastructures.

Keywords:

Wireless Network Security, Penetration Testing, Cybersecurity, Vulnerability Assessment, Campus Network

Corresponding Author:
Abil Alwi Prayoga,
Sains Komputasi dan Kecerdasan Digital, Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, Indonesia
Medan, Indonesia
Email: abilabil1752@gmail.com

DOI: https://doi.org/10.64803/jocsaic.v3i1.173

1. INTRODUCTION

The rapid advancement of information technology has driven educational institutions to adopt computer network infrastructure as a key component in supporting academic and administrative activities[1]. Modern higher education environments rely heavily on network connectivity for a wide range of functions, including digital learning, access to academic information systems, online library services, internal communication, and the use of various internet-based applications. Wireless networks or Wireless Local Area Networks (WLANs) are widely implemented on campuses because they offer users flexible access without the constraints of physical cabling[2]. However, the increased use of wireless networks also introduces new challenges, particularly regarding information security[3].

Wireless networks differ from wired networks in that they utilize radio waves an open transmission medium as the communication channel[4]. Consequently, data transmitted over the network is more susceptible to interception by unauthorized parties if security systems are not properly designed and configured[5]. Threats such as unauthorized access, packet sniffing, man-in-the-middle attacks, brute-force attacks, and the exploitation of network device configuration vulnerabilities pose risks that can compromise the confidentiality, integrity, and availability of information. In higher education environments, where the user base is large and diverse comprising students, faculty, administrative staff, and personal devices (Bring Your Own Device/BYOD) wireless network security risks become increasingly complex[6].

Network security is a crucial aspect of information technology management, as disruptions to network systems can hinder an institution's academic and operational processes[7]. Based on information security concepts, three primary aspects must be addressed: confidentiality, integrity, and availability. Confidentiality ensures that information is accessible only to authorized parties; integrity guarantees that data remains unaltered without authorization; and availability ensures that network services are usable when needed[8]. Failure to uphold these three aspects can lead to data breaches, unauthorized access, and significant losses for educational institutions.

One approach for identifying and evaluating wireless network security levels is penetration testing[9]. Penetration testing is a security assessment method that involves simulating attacks on a network system to identify security vulnerabilities before malicious actors can exploit them. Unlike passive security testing, which relies solely on monitoring, penetration testing actively attempts to exploit system weaknesses using specific techniques and tools, allowing network administrators to determine the system's vulnerability level[10].

In practice, penetration testing on wireless networks involves several stages: reconnaissance, scanning, vulnerability assessment, exploitation, and reporting. The reconnaissance stage gathers initial information about the network infrastructure, such as identifying access points, encryption types, and the devices in use. Next, the scanning stage identifies potential security vulnerabilities within the network. Once weaknesses are identified, the exploitation stage involves simulating attacks on the system such as testing authentication strength and wireless protocol security[11]. Finally, the results of this entire process are analyzed and compiled into a report detailing risk levels and recommendations for improving network security[12].

Previous studies indicate that wireless networks in educational institutions still face various security issues[13]. Factors such as improper device configuration, weak passwords, and suboptimal implementation of security standards are primary causes of vulnerabilities. Furthermore, the increasing sophistication of cyber-attack technologies necessitates periodic evaluations of network security systems. Consequently, security testing via penetration testing serves as a preventive measure that can assist organizations in strengthening their network defense systems.

Campus environments are critical subjects for wireless network security analysis due to their dynamic user characteristics. A vast number of devices connect to the campus network daily, each with varying levels of security[14]. This situation heightens the risk of security threats, particularly if user access management and network configuration are not optimally handled. Regular security evaluations enable IT administrators to assess the network's actual state and implement appropriate mitigation measures. This study aims to analyze wireless network security within a campus environment using penetration testing[15]. The analysis involves identifying potential vulnerabilities, testing the security of authentication systems, and evaluating existing protection mechanisms. The findings are expected to provide an overview of the wireless network's security posture and offer strategic recommendations for enhancing the security of the campus network infrastructure.

This research contributes not only by identifying technical weaknesses but also by providing a security evaluation approach that educational institutions can adopt to improve their readiness against cyber threats. The study offers campus network administrators a reference for strengthening security systemsnsuch as optimizing device configurations, implementing the latest wireless security standards, managing user access rights, and establishing continuous network monitoring. Ultimately, robust wireless network security supports the creation of a secure, effective, and trustworthy digital academic environment.

2. RESEARCH METHODOLOGY

2.1 Research Type and Approach

This study employs a quantitative approach with an experimental research method to analyze the security level of wireless networks in a campus environment. This approach was selected because the research focuses on measuring, identifying, and evaluating security vulnerabilities based on direct testing activities conducted on the wireless network infrastructure. The method applied in this research is penetration testing, which is a security testing approach that simulates cyber attacks against a system to identify potential vulnerabilities before they are exploited by unauthorized

DOI: https://doi.org/10.64803/jocsaic.v3i1.173

parties. The penetration testing process is conducted in a controlled environment to ensure that the testing activities do not disrupt network services and academic operations. The results obtained from the penetration testing process are analyzed to determine the level of security risks and to provide recommendations for improving the security of the campus wireless network infrastructure.

2.2 Research Stages

The research stages are carried out systematically to obtain accurate results regarding wireless network security conditions. The research process adopts the penetration testing framework consisting of several phases, including information gathering, scanning, vulnerability assessment, exploitation, and reporting.

Each stage has a specific purpose in identifying and evaluating vulnerabilities within the wireless network system.

The research workflow is illustrated in Figure 1.

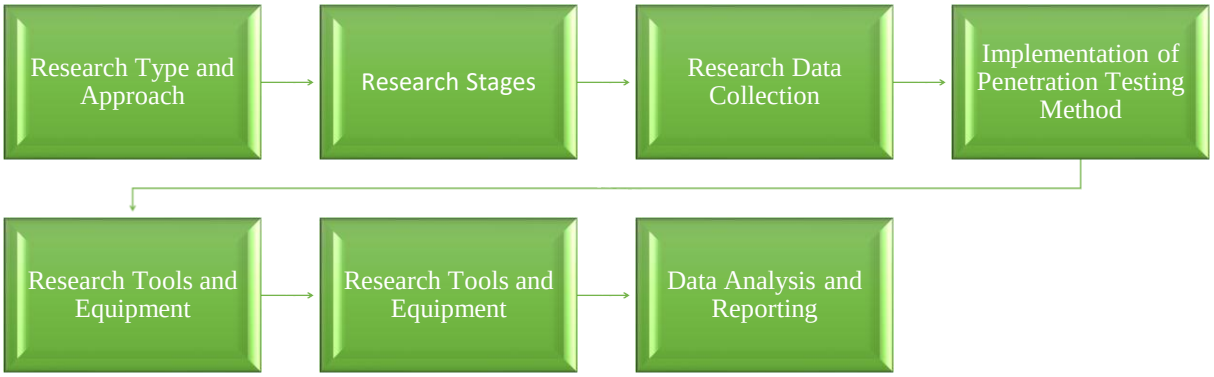

Figure 1. Research Methodology Workflow

Figure 1 Description:

Figure 1 illustrates the research workflow, starting from identifying security issues in wireless networks, collecting network information, conducting penetration testing, analyzing vulnerabilities, and producing recommendations to improve network security.

2.3 Research Data Collection

Data collection was conducted through direct observation of the wireless network infrastructure implemented in the campus environment. The collected data includes information related to network devices, wireless security configurations, authentication mechanisms, and network conditions during the testing process.

In addition, documentation methods were used to obtain supporting information, such as network topology, access point specifications, and existing security policies implemented by network administrators.

The collected data serves as the initial reference for designing penetration testing scenarios and determining the appropriate testing parameters.

The initial wireless network parameters observed in this research are presented in Table 1.

Table 1. Wireless Network Data Collection Parameters

No	Parameter	Description
1	SSID Name	Wireless network identification name tested
2	Security Type	Security protocols such as WPA/WPA2/WPA3
3	Encryption Type	Encryption algorithm implemented in the network
4	Access Point	Wireless device providing network services
5	Number of Users	Number of connected devices on the network
6	IP Address	Network addressing information used during testing

Table 1 Description:

Table 1 presents the parameters collected during the initial observation phase before conducting wireless network security testing.

2.4 Implementation of Penetration Testing Method

The penetration testing method in this research is implemented through several testing phases to identify security weaknesses in the campus wireless network. Each phase is performed using security analysis tools that support network evaluation activities.

The penetration testing stages used in this study are explained as follows:

a. Information Gathering
The information gathering stage is conducted to collect initial information regarding the wireless network under investigation. The collected information includes SSID identification, wireless channel, security protocol, encryption method, and connected devices.This stage aims to understand the characteristics and configuration of the wireless network before conducting further security testing.

b. Scanning
The scanning stage is performed to map the wireless network and identify active devices connected to the infrastructure. This process aims to discover access points, IP addresses, open ports, and potential weaknesses in available network services.Several tools are used during this stage, including Wireshark, Nmap, and Aircrack-ng, which assist in network traffic analysis, device identification, and wireless security evaluation.

c. Vulnerability Assessment
The vulnerability assessment stage is conducted to evaluate security weaknesses based on the scanning results. The analysis focuses on wireless configuration, authentication mechanisms, encryption implementation, and possible vulnerabilities that may threaten network security.The identified vulnerabilities are categorized based on their risk levels, including low, medium, and high-risk vulnerabilities. This classification helps determine the priority of security improvements required.

d. Exploitation Testing
The exploitation stage involves performing controlled attack simulations against the identified vulnerabilities. This process aims to determine whether the discovered weaknesses can actually be exploited by unauthorized users.The testing scenarios include password strength evaluation, wireless authentication testing, and packet analysis to determine whether transmitted data can be accessed without proper authorization.

2.5 Research Tools and Equipment

This research utilizes several hardware and software components to support wireless network penetration testing activities. The tools used are selected based on their ability to perform security analysis and vulnerability identification.

The research equipment is presented in Table 2.

Table 2. Research Tools and Equipment

No	Tools/Equipment	Function
1	Testing Laptop	Main device for conducting security analysis
2	Kali Linux	Operating system for penetration testing activities
3	Wireshark	Network packet analysis and traffic monitoring
4	Nmap	Network scanning and device identification
5	Aircrack-ng	Wireless security testing and password analysis
6	Campus Router/Access Point	Wireless network object being tested

Table 2 Description:

Table 2 describes the hardware and software tools used during the penetration testing process to support wireless network security analysis.

2.6 Research Tools and Equipment

The testing scenario is designed based on potential threats that may occur in a campus wireless network environment. The evaluation focuses on identifying vulnerabilities that can potentially compromise network confidentiality, integrity, and availability. The testing parameters include authentication security, encryption strength, access control mechanisms, and possible unauthorized access attempts.

The vulnerability assessment results are evaluated based on the severity level of the identified weaknesses. The evaluation criteria are shown in Table 3.

DOI: https://doi.org/10.64803/jocsaic.v3i1.173

Table 3. Vulnerability Risk Classification

Risk Level	Description
Low	Vulnerability has minimal impact and requires limited improvement
Medium	Vulnerability may affect network security under certain conditions
High	Vulnerability can significantly compromise network security

Table 3 Description:

Table 3 explains the classification used to determine the severity level of vulnerabilities discovered during penetration testing.

2.7 Data Analysis and Reporting

The final stage of this research involves analyzing the results obtained from penetration testing activities. Data collected from scanning, vulnerability assessment, and exploitation testing are evaluated to determine the current security condition of the campus wireless network. The analysis results are presented in the form of identified vulnerabilities, risk levels, attack scenarios, and recommended security improvements. The recommendations may include strengthening wireless configurations, implementing stronger authentication mechanisms, updating network devices, and applying continuous network monitoring systems.Through this research methodology, the study is expected to provide a comprehensive overview of wireless network security conditions in the campus environment and contribute to improving cybersecurity readiness against potential network threats.

3. RESULT AND DISCUSSION

3.1 Overview of Wireless Network Security Testing Results

The security analysis of the campus wireless network was conducted using the penetration testing method to identify potential vulnerabilities and evaluate the level of security implemented in the network infrastructure. The testing process was carried out through several stages, including information gathering, network scanning, vulnerability assessment, and controlled exploitation testing. The results obtained from the testing process provide an overview of the current security condition of the wireless network, particularly regarding authentication mechanisms, encryption implementation, access control, and potential weaknesses that could be exploited by unauthorized users.

The analysis showed that the wireless network infrastructure had implemented basic security mechanisms; however, several security weaknesses were still identified. These weaknesses were mainly related to password strength, configuration settings, network exposure, and insufficient monitoring mechanisms. The penetration testing results indicate that wireless networks in academic environments require continuous security evaluation because the large number of users and various connected devices increase the possibility of security incidents.

The overall testing process is illustrated in Figure 2.

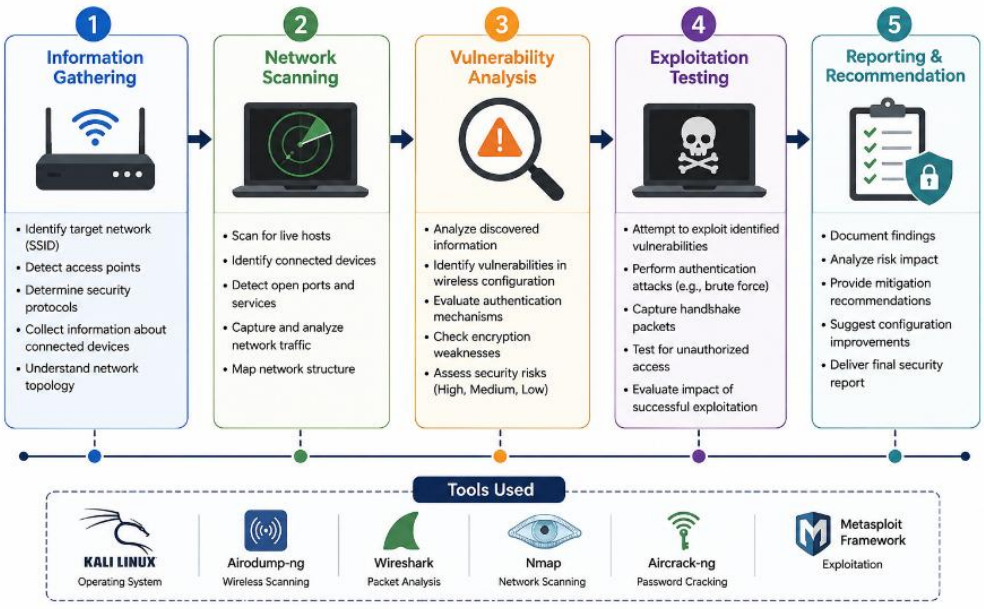

Figure 2. Wireless Network Penetration Testing Process

Figure 2 Description:

Figure 2 illustrates the penetration testing workflow used in this research, starting from information collection, vulnerability identification, exploitation testing, and security improvement recommendations.

3.2 Information Gathering Results

The first stage of penetration testing was information gathering, which aimed to obtain initial information regarding the wireless network environment. At this stage, several parameters were identified, including SSID name, wireless security protocol, encryption type, access point information, and connected devices.

The information gathering process is important because it provides an understanding of the network structure before conducting deeper security testing. Through this stage, researchers can determine possible attack vectors that may exist in the wireless infrastructure.

The results of information gathering are presented in Table 4.

Table 4. Information Gathering Results of Wireless Network

No	Testing Parameter	Result	Analysis
1	SSID Detection	Successfully identified	Wireless network can be detected publicly
2	Security Protocol	WPA/WPA2	Security mechanism has been implemented
3	Encryption Type	AES	Provides adequate data protection
4	Access Point Identification	Successfully detected	Device information is exposed
5	Connected Client Detection	Successfully identified	User activity can be monitored

Table 4 Description:

Table 4 presents the results obtained during the information gathering stage, including detected network information and initial security analysis. Based on Table 4, the wireless network has implemented encryption-based security mechanisms. However, the visibility of SSID and access point information indicates that attackers can still obtain basic network information. Although SSID visibility itself does not represent a direct vulnerability, exposed network information may assist attackers during reconnaissance activities.

3.3 Network Scanning Results

The scanning stage was performed to identify active devices, network services, and possible security weaknesses. Network scanning provides important information regarding the internal condition of the wireless infrastructure.The scanning process used network analysis tools to identify connected devices and analyze communication activities within the wireless network.

The scanning results are shown in Table 5.

Table 5. Network Scanning Results

No	Scanning Activity	Result	Security Impact
1	Active Device Detection	Several connected devices identified	Medium risk
2	IP Address Identification	Successfully obtained	Potential information disclosure
3	Network Traffic Monitoring	Communication packets detected	Requires encryption protection
4	Open Service Detection	Several services identified	Requires configuration review

Table 5 Description:

Table 5 shows the results of network scanning activities used to identify active devices, network information, and possible security risks. The scanning results indicate that network information can be obtained through monitoring activities. This condition is common in wireless networks because communication occurs through radio signals that can be captured within transmission coverage areas. Although encrypted communication reduces the possibility of direct data leakage, improper configuration may still create opportunities for attackers to perform packet analysis or unauthorized access attempts.

3.4 Vulnerability Assessment Results

The vulnerability assessment stage was conducted to analyze weaknesses identified during previous testing phases. The evaluation focused on authentication mechanisms, password security, encryption configuration, and access control

implementation.The identified vulnerabilities were classified based on risk severity levels to determine their impact on network security.

The vulnerability assessment results are presented in Table 6.

Table 6. Identified Wireless Network Vulnerabilities

No	Vulnerability	Risk Level	Description
1	Weak Password Policy	High	Weak passwords increase the possibility of brute force attacks
2	Open SSID Broadcasting	Low	Network information can be identified easily
3	Limited Access Monitoring	Medium	Suspicious activities may not be detected quickly
4	Outdated Configuration	Medium	Older configurations may contain security weaknesses
5	Lack of Periodic Security Testing	High	Vulnerabilities may remain undetected

Table 6 Description:

Table 6 presents identified vulnerabilities, their risk levels, and explanations regarding their potential impact on wireless network security.Based on the assessment results, password management becomes one of the most significant security factors. Weak passwords can increase the possibility of unauthorized access through brute force attacks. Therefore, implementing stronger password policies is essential, including password complexity requirements and periodic password changes.

Another important finding is the lack of periodic security evaluation. Without regular penetration testing activities, newly emerging vulnerabilities may remain unnoticed. Therefore, security testing should become part of routine network maintenance activities.

3.5 Exploitation Testing Results

The exploitation testing stage was performed to simulate possible attacks against the identified vulnerabilities. The purpose of this stage was not to damage the network system but to evaluate whether existing weaknesses could be exploited by unauthorized users. Several attack scenarios were tested, including authentication testing, packet analysis, and unauthorized access simulation.

The exploitation testing results are shown in Table 7.

Table 7. Exploitation Testing Results

No	Testing Scenario	Result	Security Evaluation
1	Password Strength Testing	Vulnerable under weak password conditions	Requires stronger password policy
2	Packet Capture Analysis	Network traffic successfully observed	Requires secure communication
3	Unauthorized Access Simulation	Access prevention partially effective	Additional authentication recommended
4	Encryption Testing	Encryption function works properly	Security level considered adequate

Table 7 Description:

Table 7 describes the exploitation testing scenarios and evaluates the effectiveness of current wireless security mechanisms. The results show that encryption mechanisms provide sufficient protection against direct data interception. However, security weaknesses may still occur due to human factors, particularly weak password usage and improper user management. This finding confirms that technical security mechanisms alone are insufficient without proper security awareness among network users.

3.6 Overall Security Risk Analysis

Based on the results from all penetration testing stages, the overall security condition of the campus wireless network can be categorized as moderate security level. The network has implemented fundamental security mechanisms; however, several improvements are required to reduce potential risks.

The overall risk evaluation is summarized in Figure 3.

DOI: https://doi.org/10.64803/jocsaic.v3i1.173

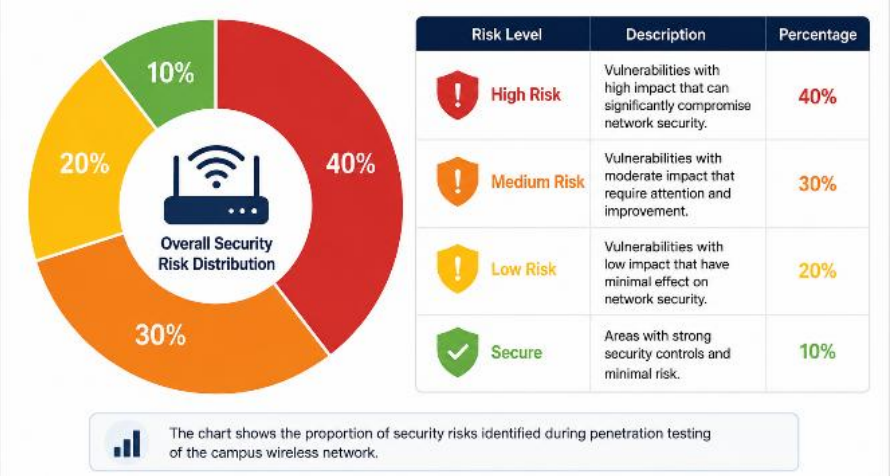

Figure 3. Wireless Network Security Risk Distribution

Figure 3 Description:

Figure 3 illustrates the distribution of security risks identified during penetration testing. High-risk findings require immediate attention, while medium and low risks require continuous improvement. The dominance of high and medium-risk findings indicates that wireless network security requires continuous improvement. In a campus environment, where many users connect daily, security weaknesses can become significant threats if not properly managed.

3.7 Discussion of Research Findings

The findings of this study demonstrate that penetration testing is an effective approach for evaluating wireless network security in educational environments. Through systematic testing, vulnerabilities that are difficult to identify through normal monitoring activities can be discovered.The results support previous studies indicating that wireless networks in educational institutions face significant security challenges due to high user mobility, increasing device connectivity, and diverse user behavior.

One of the main findings is that authentication security plays an important role in protecting wireless infrastructure. Although WPA/WPA2 encryption provides protection against unauthorized access, weak authentication credentials can reduce the effectiveness of the security mechanism. Furthermore, the research highlights the importance of implementing layered security approaches. Network security should not depend only on encryption but also involve access management, user awareness, monitoring systems, and regular security assessment.

The implementation of periodic penetration testing can help administrators identify weaknesses before they are exploited by attackers. Additionally, recommendations such as implementing stronger authentication methods, updating network devices, and applying security monitoring systems can significantly improve wireless network resilience.

4. CONCLUSIONS

This study has successfully analyzed the security level of campus wireless networks using the penetration testing method. The research was conducted through several testing stages, including information gathering, network scanning, vulnerability assessment, exploitation testing, and security evaluation. The results indicate that the wireless network infrastructure has implemented fundamental security mechanisms, particularly through the use of wireless encryption protocols such as WPA/WPA2. However, the analysis also reveals several security weaknesses that may potentially increase the risk of unauthorized access and cyber threats. The vulnerability assessment results show that several factors require improvement, including password management policies, access control mechanisms, network monitoring systems, and periodic security evaluation. Weak authentication credentials were identified as one of the main risks because they may allow attackers to perform brute force attacks and gain unauthorized access to network resources. In addition, the limited implementation of continuous security monitoring may cause suspicious activities to remain undetected for a longer period. The penetration testing approach proved to be an effective method for identifying security gaps within wireless network infrastructure. By conducting controlled attack simulations, administrators can understand potential threats and evaluate the effectiveness of existing security controls before actual attacks occur. The findings of this research emphasize that wireless network security cannot rely only on encryption mechanisms but must also involve a comprehensive security strategy, including stronger authentication, regular vulnerability assessments, updated network configurations, and increased user awareness regarding cybersecurity practices. Overall, the campus wireless network can be categorized as having an adequate but improvable security level. Continuous improvement efforts are required to maintain confidentiality, integrity, and availability of network services. The implementation of periodic penetration

testing and proactive security management is recommended to ensure that the wireless network remains resilient against evolving cyber threats and can continue supporting academic activities in a secure and reliable manner.

REFERENCES

[1] U. Ibrahim, "The Role of Cloud Computing in Transforming ICT Infrastructure in Educational Institutions," *Int. J. Appl. Sci. Res.*, vol. 2, no. 2, pp. 213–226, 2024, doi: https://doi.org/10.59890/ijasr.v2i2.1333.

[2] R. Rawi, M. R. M. Isa, M. N. Ismail, A. A. B. Sajak, and A. Mustafa, "Preliminary study: The Readiness of WLAN Infrastructure at Malaysian Higher Education Institutes to Support Smart Campus Initiative," *Int. J. Informatics Vis.*, vol. 7, no. 3, pp. 945–951, 2023, doi: https://doi.org/10.30630/joiv.7.3.1242.

[3] A. Alhammadi *et al.*, "Artificial Intelligence in 6G Wireless Networks: Opportunities, Applications, and Challenges," *Int. J. Intell. Syst.*, vol. 2024, no. 1, p. 8845070, 2024, doi: https://doi.org/10.1155/2024/8845070.

[4] S. Franjic, "Wireless Technology is Easy to Use," *Trends J. Sci. Res.*, vol. 1, no. 1, pp. 22–28, 2022, doi: https://doi.org/10.31586/ijmebac.2022.294.

[5] N. O. Miracle, "The Importance of Network Security in Protecting Sensitive Data and Information," *Int. J. Res. Innov. Appl. Sci.*, vol. IX, no. VI, pp. 259–270, 2024, doi: https://doi.org/10.51584/ijrias.2024.906024.

[6] R. Palanisamy, A. A. Norman, and L. Mat Kiah, "BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts," *J. Organ. Comput. Electron. Commer.*, vol. 31, no. 4, pp. 320–342, 2021, doi: https://doi.org/10.1080/10919392.2022.2028530.

[7] M. Babbar and T. Gupta, "Response of educational institutions to COVID-19 pandemic: An inter-country comparison," *Policy Futur. Educ.*, vol. 20, no. 4, pp. 469–491, 2022, doi: https://doi.org/10.1177/14782103211021937.

[8] I. Bala, I. A. Pindoo, M. M. Mijwil, M. Abotaleb, and W. Yundong, "Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence," *Jordan Med. J.*, vol. 58, no. 2, pp. 250–270, 2024, doi: https://doi.org/10.35516/jmj.v58i2.2527.

[9] D. N. Astrida, A. R. Saputra, and A. I. Assaufi, "Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)," *Sinkron*, vol. 7, no. 1, pp. 147–154, 2022, doi: https://doi.org/10.33395/sinkron.v7i1.11249.

[10] O. R. Arogundade, "Network Security Concepts, Dangers, and Defense Best Practical," *Comput. Eng. Intell. Syst.*, vol. 14, no. 2, 2023, doi: 10.7176/ceis/14-2-03.

[11] J. Softić and Z. Vejzović, "Impact of Vulnerability Assesment and Penetration Testing (VAPT) on Operating System Security," in *2023 22nd International Symposium INFOTEH-JAHORINA, INFOTEH 2023*, IEEE, 2023, pp. 1–6. doi: https://doi.org/10.1109/INFOTEH57020.2023.10094095.

[12] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," *J. Comput. Inf. Syst.*, vol. 66, no. 1, pp. 123–150, 2026, doi: https://doi.org/10.1080/08874417.2024.2329985.

[13] A. Arina, "Analysis of IoT security issues used in Higher Education Institutions," *Int. J. Math. Comput. Res.*, vol. 09, no. 05, pp. 2277–2286, 2021, doi: 10.47191/ijmcr/v9i5.01.

[14] K. N. Ohei and R. Brink, "The Effectiveness of Wi-Fi-Network Technology on Campuses and Residences for an Improved Learning Experience and Engagement," *Mousaion South African J. Inf. Stud.*, vol. 39, no. 1, 2021, doi: https://doi.org/10.25159/2663-659x/7842.

[15] C. Adu-Boahene, S. N. Nikoi, and A. Nsiah-Konadu, "Campus Network and Systems Security Assessment Using Penetration Testing: The Case of the University of Education Winneba, Kumasi," *Asian J. Res. Comput. Sci.*, vol. 12, no. 1, pp. 7–25, 2021, doi: https://doi.org/10.9734/ajrcos/2021/v12i130273.