|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 6| No. 3|Oct|Year 2025|
This is an Open Access article, published by Institute of Information Technology and Social Science (IITSS), Indonesia

Application of Hardening for WLAN Security Optimization in the IT Services Division at PT PUSRI

Muhammad Reihan Pratama[1*]

Abstract

Computer networks typically use two primary transmission methods: wired and wireless networks, commonly referred to as Wireless Local Area Networks (WLANs). In WLAN implementations, the standard security mechanism frequently adopted is Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK), which relies on an SSID and password. Despite this security mechanism, criminal activities such as unauthorized access and network intrusions continue to occur. Therefore, it is essential to enhance network security to ensure that WLAN environments remain secure and capable of minimizing potential risks to users. This study aims to improve and optimize WLAN network security by conducting vulnerability scanning using Nessus to assess existing security conditions, followed by the implementation of hardening techniques to strengthen and obscure vulnerabilities. Hardening includes several approaches such as applying raw firewalls and firewall filters, restricting ports and services, disabling unnecessary services, disabling the MikroTik Neighbor Discovery Protocol (MNDP), and implementing port knocking as an additional layer of protection. The findings indicate that applying vulnerability scanning alongside a structured hardening strategy significantly minimizes identified risks and enhances the overall resilience of the WLAN network against intrusions and security threats.

Keywords

Firewall, Hardening, MikroTik, Port, Vulnerability Scanning

Article History
Received 30 July 2025
Accepted 21 October 2025

How to Cite

Triwulanda, A. (2025). IoT-Based Server Room Temperature and Humidity Monitoring. ***Jurnal Jaringan Komputer dan Keamanan,*** *6*(3), 123-130.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: 211220003@student.binadarma.ac.id

Introduction

The rapid advancement of information and communication technology has significantly transformed various sectors of modern society. Government agencies, private companies, and educational institutions increasingly rely on technological systems to support administrative operations, data exchange, and decision-making processes (Irsan, 2023). Among these technological developments, computer networking has undergone substantial growth, particularly in data transmission systems. Computer networks generally utilize two main types of transmission media—wired and wireless. Wireless Local Area Networks (WLANs) have become especially prominent due to their ability to connect multiple devices within the same environment, enabling seamless communication and efficient resource sharing (Saraun, Lumenta, & Sengkey, 2021). Such capabilities support collaborative workflows and enhance organizational productivity (Simanjuntak et al., 2019).

WLAN technology operates using electromagnetic waves as the medium for transmitting data, thus eliminating the need for physical cabling. This wireless communication model is widely implemented in residences, schools, laboratories, offices, and other limited areas due to its practicality and ease of installation (Ryansyah & Irawan, 2023). WLAN provides high flexibility, particularly for mobile device users such as laptops and smartphones, who require uninterrupted movement within the coverage area. Wi-Fi, the most common implementation of WLAN, allows users to connect to the internet or internal networks through routers or access points, making it a fundamental component of modern digital infrastructure (Firmansyah, Purnama, & Astuti, 2021).

To ensure the security of WLAN environments, WPA2-PSK is widely adopted as a standard encryption protocol. WPA2-PSK utilizes the Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) to secure user authentication and data transmission (Michael, Ruslianto, & Hidayati, 2021). However, despite its encryption capabilities, WLAN networks remain vulnerable to various cybersecurity threats, including unauthorized access, brute-force attacks, and service disruptions. As Umar and Marsaid (2023) emphasize, security gaps in wireless networks can lead to significant risks such as unauthorized penetration, data leakage, or compromised network performance, underscoring the necessity of enhanced protective measures.

To evaluate these potential security weaknesses, this study employs the Nessus vulnerability scanner—a widely recognized tool for assessing cybersecurity risks within network environments. The initial scanning results identified seven open ports: FTP (21), SSH (22), Telnet (23), DNS (53 TCP/UDP), HTTP (80), HTTP-alternative (8080), and MikroTik Neighbor Discovery Protocol (5678). These findings were categorized into medium-, low-, and informational-level vulnerabilities based on standard risk classifications (Farismana & Pramadhana, 2023). The identification of open ports and service exposures highlights the potential avenues through which attackers may gain unauthorized access or exploit system vulnerabilities.

To mitigate these risks, the research implements a series of hardening techniques on a MikroTik router—an essential step in strengthening WLAN security and reducing the attack surface. Router hardening involves the application of specific security measures, such as configuring firewall rules, disabling unnecessary services, closing unneeded ports, and limiting access to critical features (Kamilah & Hendrawan, 2019). Additional protective strategies include concealing system vulnerabilities, blocking suspicious login attempts, disabling the MNDP service to reduce exposure to reconnaissance, and applying port knocking mechanisms to protect the SSH service from unauthorized access (Wiryadinata, 2022). These combined techniques aim to provide layered security that is more resilient against common attack vectors targeting WLAN infrastructures.

Through the integration of vulnerability assessment and targeted hardening strategies, this study seeks to strengthen the overall robustness of the WLAN environment. By systematically reducing risk exposure and enhancing network defense mechanisms, organizations can better safeguard their digital assets, ensure uninterrupted network availability, and maintain secure communication channels. Ultimately, this research contributes to improving WLAN security practices in institutional environments and highlights the importance of proactive cybersecurity management in an increasingly interconnected world.

Methodology

This study applies action research, a methodological approach used to identify problems, develop solutions, and evaluate outcomes within a specific context (Makmur, Siaulhak, & Jasman, 2023). Action research enables the researcher to assess the effectiveness of vulnerability scanning and hardening techniques in optimizing WLAN security. The method consists of five stages:

Diagnosing

Identifying security weaknesses through initial vulnerability scanning using Nessus (Kurnia, 2020). Initial vulnerability scanning was conducted using Nessus by selecting New Scan, targeting IP address 192.168.1.36, and choosing the Port Scan (common ports) option. The scan revealed vulnerabilities categorized into Medium, Low, and Info levels.

Table 1. Initial Vulnerability Scan Results

No	Category	Title	Family	Port/Service
1	Medium	Unencrypted Telnet Server Misconfiguration		23/Telnet
2	Low	SSH Multiple Issue Misconfiguration		22/SSH
3	Info	MikroTik Neighbor Discovery Protocol Detection	Service Detection	5678/MNDP
4	Info	MikroTik RouterOS Detection	Service Detection	80/WWW
5	Info	SSH Multiple Issue	Service Detection	22/SSH
6	Info	Nessus SYN Scanner	Port Scanner	21/22/23/53/80/8080
7	Info	Service Detection	Service Detection	21/22/23/80

No	Category	Title	Family	Port/Service
8	Info	DNS Server Detection	DNS	53/TCP/UDP
9	Info	FTP Server Detection	Service Detection	21/FTP
10	Info	SSH Protocol Version Supported	General	22/SSH
11	Info	Telnet Server Detection	Service Detection	23/Telnet

The analysis showed seven open ports that posed security threats. These vulnerabilities required systematic mitigation through hardening.

Action Planning

Developing a hardening strategy to address the vulnerabilities identified. Based on the scan results, a comprehensive hardening strategy was developed:

1. Restrict access to ports 21 (FTP), 22 (SSH), and 80 (HTTP) for authorized networks only (192.168.10.0/24).
2. Secure DNS port 53 (TCP/UDP) using firewall raw and filter rules to mitigate DNS flooding (Bahri, 2024).
3. Disable Telnet (23) and HTTP alternative port (8080).
4. Disable the MNDP service (5678) to prevent router information disclosure (Jawad, Amalia, & Nadzarudien, 2023).
5. Implement port knocking to protect SSH access (Wiryadinata, 2022).

Table 2. Hardening Actions for Identified Ports

No	Port	Hardening Action
1	21, 22, 80	Firewall filter rules, access restrictions
2	53 TCP/UDP	Firewall raw + filter protection
3	23, 8080	Disable services using Tarpit
4	5678 (MNDP)	Disable MNDP
5	22 (SSH)	Implement Port Knocking

Action Taking

Implementing firewall rules, disabling services, applying port restrictions, turning off MNDP, and executing port knocking.

Evaluating

Re-scanning the WLAN environment to evaluate the effectiveness of the hardening framework.

Learning

Analyzing improvements and comparing system security before and after hardening.

Results

Hardening Implementation (Action Taking)

Network vulnerabilities identified during the examination phase are summarized in Table.

1. Firewall Filter for Ports 21, 22, and 80
   Firewall filters were configured to permit access only from the 192.168.10.0/24 network. Unauthorized IP addresses attempting to access these services were blocked.
2. Firewall Raw and Filter on DNS Port 53
   Firewall raw rules detected abnormal TCP packets directed to port 53, adding suspicious IPs into a flooding list for automatic blocking. Similarly, UDP packets exceeding 100 requests per second were flagged and dropped.
3. Disabling Telnet (23) and HTTP Alternative (8080)
   Telnet was disabled due to its unencrypted communication risks. Port 8080 was disabled because port 80 was already serving as the primary web service.
4. Disabling MikroTik Neighbor Discovery Protocol (5678)
   MNDP was disabled on all interfaces to prevent unauthorized identification of the router by devices on the same network segment.
5. Implementing Port Knocking
   Two-step port knocking was implemented:
   - Step 1: Knock on port 5555
   - Step 2: Knock on port 22 (SSH)

Only clients performing sequential knocking were granted access.

Evaluation of Hardening

After hardening, a second vulnerability scan was performed.

Table 3. Post-Hardening Scan Results

No	Category	Title	Family	Port
1	Info	DNS Server Detection	DNS	53/TCP/UDP
2	Info	MikroTik RouterOS Detection	Service Detection	80/TCP
3	Info	Nessus Scan Information	Settings	-

Only two open ports remained (53 and 80), both of which were secured through restrictions and firewall rules.

Learning

Before hardening, the network exhibited:

- 7 open ports
- 1 medium vulnerability
- 3 low vulnerabilities
- 9 informational risks

After hardening:

- Only 2 ports remained open
- No medium or low vulnerabilities
- Only informational items detected
- Improved router confidentiality
- Enhanced resilience against intrusion and service exploitation

Discussion

The results of the hardening implementation demonstrate a significant improvement in the security posture of the WLAN infrastructure. Prior to the hardening process, the initial vulnerability assessment identified seven open ports, including FTP (21), SSH (22), Telnet (23), DNS (53 TCP/UDP), HTTP (80), HTTP alternative (8080), and MikroTik Neighbor Discovery Protocol (5678). These services are commonly associated with security weaknesses, especially when left exposed without proper filtering (Farismana & Pramadhana, 2023). The presence of medium- and low-level vulnerabilities also highlighted the router's susceptibility to reconnaissance, brute-force attempts, and unauthorized exploitation, substantiating the need for a robust hardening strategy. As pointed out by Umar & Marsaid (2023), such vulnerabilities in wireless networks can facilitate unauthorized access or data leakage if not mitigated effectively.

The implementation of firewall filtering on critical ports (21, 22, and 80) proved to be an effective defense mechanism. By restricting access exclusively to the 192.168.10.0/24 internal network, the system successfully prevented unsolicited connection attempts originating from outside the trusted network segment. Similar approaches have been widely recommended in MikroTik security best practices, where access limitation and source-IP verification play crucial roles in preventing brute-force attacks and credential theft (Kamilah & Hendrawan, 2019). This selective access filtering not only reduced exposure to external threats but also enhanced control over administrative traffic, thereby strengthening the confidentiality of sensitive router configurations.

Further improvements were achieved through the application of raw firewall rules on DNS port 53. Raw tables allowed early packet detection before connection tracking, enabling faster and more efficient handling of abnormal traffic patterns. By automatically identifying suspicious TCP packets and rate-limiting excessive UDP requests exceeding 100 queries per second, the router showed increased resilience against potential DNS flooding attempts—a common technique used in network-based denial-of-service attacks. This aligns with the recommendation of Wiryadinata (2022), who notes that proactive filtering and traffic-limiting measures are crucial for mitigating the initial stages of network reconnaissance and flooding scenarios.

Disabling unnecessary services such as Telnet (23), the HTTP alternative (8080), and MikroTik's Neighbor Discovery Protocol (5678) further minimized the router's attack surface. Telnet is widely recognized as an insecure protocol due to its plaintext authentication, making it highly susceptible to interception (Michael, Ruslianto, & Hidayati, 2021). Likewise, disabling MNDP effectively prevented unauthorized users on the same subnet from identifying the router type and version—information often exploited during targeted attacks. These actions are consistent with established hardening principles, which emphasize the removal of non-essential services to reduce potential exploitation paths (Kamilah & Hendrawan, 2019).

The implementation of port knocking added another layer of security, especially for SSH access. By requiring clients to perform a two-step sequential port knock (ports 5555 and 22), the SSH service became completely invisible to unauthorized hosts. Such techniques are effective in concealing administrative services from direct scanning, thereby preventing automated attacks such as dictionary-based or brute-force login attempts. This supports the view of cybersecurity researchers that multi-stage authentication mechanisms greatly enhance router confidentiality and limit unauthorized access attempts (Umar & Marsaid, 2023).

The post-hardening vulnerability scan validates the effectiveness of the implemented techniques. Only two open ports remained—DNS (53) and HTTP (80)—both of which were protected through tailored firewall rules and access restrictions. Notably, medium- and low-level vulnerabilities were completely eliminated, resulting in only informational findings. In practical terms, this signifies improved router confidentiality, reduced exposure to external threats, and enhanced security resiliency. These outcomes demonstrate that systematic hardening and proper firewall configuration significantly strengthen WLAN infrastructure against scanning, intrusion, and exploitation attempts, aligning with established cybersecurity frameworks and previous studies (Farismana & Pramadhana, 2023). The improved security posture ensures a safer network environment and minimizes the risk of unauthorized access, confirming the effectiveness of the implemented hardening measures.

Conclusion and Recommendations

The vulnerability assessment using Nessus successfully identified several weaknesses in the WLAN network, including open ports and potential service exploits. The implementation of hardening measures firewall rules, service restrictions, MNDP deactivation, disabling insecure ports, and port knocking proved effective in minimizing vulnerabilities. The WLAN security posture improved significantly, resulting in greater stability, reduced exploitability, and overall stronger protection against network threats.

Disclosure Statement

The authors declare no conflict of interest in conducting this study.

Acknowledgments

The authors express their gratitude to Universitas Bina Darma and the IT Services Division of PT PUSRI for providing the facilities and environment necessary to conduct this research.

References

Bahri, S. (2024). Securing network devices from DDoS attacks using Firewall-RAW features on MikroTik routers. KAKIFIKOM, 06(01), 1–6.

Farismana, R., & Pramadhana, D. (2023). Vulnerability assessment for analyzing security levels. Jurnal, 3(1).

Firmansyah, P., Purnama, R. A., & Astuti, R. D. (2021). Optimization of wireless security using MAC address filtering. Jurnal, 15(1), 25–33.

Irsan. (2023). Wireless LAN security using MAC address filtering at SDN Kunciran 8. Jurnal, 1(6), 1536–1540.

Jawad, F., Amalia, R. A., & Nadzarudien, T. S. (2023). Security optimization and network monitoring at DPRD Bekasi Office. Jurnal, 3(2), 184–189.

Kamilah, I., & Hendrawan, A. H. (2019). Vulnerability analysis of attendance server in Informatics Laboratory. Prosiding Semnastek, 16, 1–9.

Kurnia, D. (2020). Analysis of DHCP starvation attack on MikroTik RouterOS. Core IT, 8(5), 12–17.

Makmur, A., Siaulhak, S., & Jasman, I. (2023). Bandwidth management optimization using action research at Palopo City Communication and Informatics Office. INTECOMS, 6(2), 910–917.

Michael, Ruslianto, I., & Hidayati, R. (2021). Comparison analysis of WPA2-PSK and captive portal security in public wireless networks. Jurnal Komputer dan Aplikasi, 09(01), 108–118.

Muin Abdul, M., Kapti, & Yusnanto, T. (2020). Campus website security vulnerability analysis using Nessus. International Journal of Computer and Information System, 03(02).

Ryansyah, E., & Irawan, A. S. Y. (2023). Systematic literature review: Misuse of public Wi-Fi in Indonesia. JITEK, 3(1), 1–13.

Santoso, H. (2020). Implementation of firewall and web filtering on MikroTik RouterOS for healthy and safe internet. Jurnal Teknik Informatika Atmaluhur, 3(1), 82.

Saraun, A., Lumenta, A. S. M., & Sengkey, D. F. (2021). Analysis of WLAN security at Minahasa Regency Educational Affairs Office. Jurnal Teknik Informatika, 17(1), 565–572.

Simanjuntak, P., et al. (2019). LAN usage analysis at PT USDA Seroja. CBIS Journal, 06(01), 23–28.

Umar, R., & Marsaid, A. P. (2023). LAN network security analysis against DDoS threats using penetration testing. Jurnal Riset Komputer, 10(1), 2407–389.

Wiryadinata, R. (2022). Design of SSH port security using port knocking. Jurnal, 5(1), 28–33.

Yudi Mulyanto, M., Julkarnain, & Afahar, A. J. (2021). Implementation of port knocking for network security at SMKN 1 Sumbawa Besar. Jurnal Informatika Teknologi dan Sains, 3(2), 326–335.

Biographical Notes

MUHAMMAD REIHAN PRATAMA is a student in the Computer Engineering Study Program, Faculty of Vocational Studies, Universitas Bina Darma. His research interests include network security, wireless technologies, and vulnerability assessment.