WIRELESS NETWORK SECURITY USING WIRELESS INTRUSION DETECTION SYSTEM

Zahrina Amalia[1]

[1] *Universitas Teknokrat Indonesia, Jl. Zainal Abidin Pagaralam No.9-11 Labuhan Ratu, Bandar Lampung, Indonesia*

Article Information

Received: 15-11-2023
Revised: 30-11-2023
Published: 15-12-2023

Keywords
intruction detection system (IDS),denial of service (DOS),brute force attack,intrusion attack

Correspondence Email:
zahrina_amalia@teknokrat.ac.id

Abstract

Wireless network security is becoming increasingly important in the era of rapidly developing information technology. In an effort to protect wireless networks from attacks and threats, the use of a wireless intrusion detection system (Wireless Intrusion Detection System) has become an effective solution. This journal aims to examine the application of the Wireless Intrusion Detection System in improving wireless network security. WIDS is a system used to detect intrusions on wireless networks. This system can identify attacks such as denial of service (DoS) attacks, brute force attacks, and intrusion attacks. With WIDS, network administrators can take appropriate action to overcome these attacks and maintain the integrity of the wireless network..

1. Introduction

Implementing information systems is an obligation for individuals and organizations/companies. Although the convenience of the system is highly appreciated, there are risks that can threaten the integrity of the system, potentially causing loss of data or information, and even disrupting the running of business processes within an organization or company. Therefore, at Sumbawa University of Technology, a place that is currently widely used in Indonesia for goods delivery and money transfer services, there are still many features that are implemented online.Currently, technological developments are taking place very quickly, especially with the presence of very sophisticated internet facilities. However, it needs to be acknowledged that internet use also carries a number of risks and losses. One example is potential threats originating from irresponsible parties, generally known as hackers. Therefore, a network administrator must ensure that the computer network system remains safe and protected from possible attacks by hackers(Purnama et al., 2023).

In the modern era like today, human involvement with technology has become inevitable. Technology plays an important role in simplifying various aspects of our lives, especially in the use of wireless networks. However, without implementing a proper authentication method such as WPE or Captive Portal, the risk of easy access from outsiders to the wireless network increases, while managing the bandwidth of each user becomes inefficient resulting in competition in bandwidth usage between users. At this stage, to overcome this problem and determine the access speed after logging in, the router will limit the speed based on bandwidth configuration rules that match the user's hotspot profile(Prasetyo et al., 2023). This is done to optimize

wireless network management and prevent unnecessary competition in bandwidth usage, by effectively capturing login access.The need for monitoring and protecting the system is crucial considering the high number of internet users in Indonesia. According to a report by the National Cyber Security Operations Center (Pusopskamsinas) of the National Cyber and Crypto Agency (BSSN), it was recorded that during the period from January 1 to April 12 2023, 88,414,926 cyber attacks had occurred. In the report, it was revealed that the most common attack pattern was trojan activity with a percentage reaching 56%, while information gathering activities reached 43%.Computer networks are a crucial element in this modern era. Through computer networks, connectivity between devices can be realized through the use of LAN (Local Area Networks) and WAN (Wide Area Networks)(Parga Zen et al., 2023). The existence of a computer network allows interaction and exchange of information between devices. Considering that we now continually depend on computer networks to carry out various computing activities, it is important for us to understand why computer networks have such a significant role today. To see the development of computer networks(Aprianto, 2023).

Server security is a critical element that needs to be given serious attention in the context of computer networks. Nearly all information stored in various institutions or organizations, including commercial companies, universities, government agencies, and private individuals, can be accessed by users from various locations and whenever needed(Esabella & Bella Fitriana, 2023).

1.1 Literature Review

This article discusses network security analysis with a focus on implementing the Snort Intrusion Detection System (IDS) together with ACID (Analysis Console for Intrusion Databases) on the Ubuntu Server platform. This article also explains that using tools such as Snort IDS, ACID, and Ntop can help monitor and analyze network traffic, detect potential attacks, and provide protection against security threats.refers to related literature and research, including analysis and implementation of IDS using Snort on cloud servers.Additionally, the article discusses the use of tools such as Hping, Nmap, Nessus, and Ethereum for internet network security analysis. This provides an additional layer of comprehensive understanding and management of network security (Ruruh Wuryani,Indah Fenrian,Dicky Surya Dwi Putra,Desiyanna Lasut,Susanto Hariyanto).

This article discusses the design and implementation of an Intrusion Detection System (IDS) using Debian 7 and Snort with a focus on detecting DoS (Denial of Service) and SQL Injection attacks. IDS operates by analyzing network traffic to identify suspicious or unauthorized patterns or behavior within the network.Apart from discussing the implementation of Snort, the article also covers the use of the LOIC application as an example of an attack, explains the Wireless Access Point (WAP/AP), and describes the NDLC (Network Development Life Cycle) method in designing computer networks.Test results show that IDS successfully detected DoS and SQL Injection attacks, and was able to block the attacker's IP using a firewall(Muhammad Aprianto).

The article explores the creation of a webbased Computer Based Test (CBT) application integrated with a wireless network and its influence on student learning results. The study aims to deploy a wireless network utilizing MikroTik RouterBoard devices and the Sahabat Siswa (SaSis) platform for real-time exam results and analysis. The System Development Life Cycle (SDLC) methodology is employed, utilizing a prototype model for the development process (Juni Agung,Prasetyo Rufi,Yoso Wiyarno).

The article explores the creation of a webbased Computer Based Test (CBT) application integrated with a wireless network and its influence on student learning results. The study aims to deploy a wireless network utilizing MikroTik RouterBoard devices and the Sahabat Siswa (SaSis) platform for real-time exam results and analysis. The System Development Life Cycle (SDLC) methodology is employed, utilizing a prototype model for the development process. Overall, the article provides a comprehensive overview of the development and implementation of a web-based CBT application with a wireless network, as well as the validation and testing processes. It also highlights the positive impact of the application on student learning outcomes (Satria Galang Saputra, Bita Parga Zen, Abdurahman).

This journal discusses wireless network security evaluation by applying the Penetration Testing Execution Standard (PTES) method at the Kalisapu Village Hall Office. Test results show that although the wireless network security system is quite reliable, there is a need for improvements to strengthen security and reduce the risk of cybercrime. Research methods include steps such as pre-interaction, information gathering, threat modeling, and vulnerability analysis. This study focuses on analyzing network security in a cafe and measures to protect it from attacks, such as port scanning and service attacks. The research methodology includes qualitative research methods and the SPDLC process (Yunanri W,Yuliadi , Shinta Esabella,Yasinta Bella Fitriana).

This article discusses the implementation of the Snort Intrusion Detection System (IDS) as a Security System by utilizing WhatsApp and Telegram as a means of notification. IDS plays a role in identifying and detecting potential attacks on the network, but some IDS experience limitations in providing notification to administrators when an attack occurs. Therefore, this research proposes the use of WhatsApp and Telegram as notification media to increase the effectiveness of the network security system. The network development method used is the Network Development Life Cycle (NDLC) which consists of six stages, with an emphasis on the implementation stage. At the implementation stage, the network topology and security system design is carried out on a small scale between the server and the attack. Furthermore, prototype and implementation simulations were carried out to ensure that the IDS Snort system could operate properly when facing attacks and was able to provide notifications via the WhatsApp and Telegram applications. The research results show that IDS Snort successfully detects attacks and sends notifications via WhatsApp and Telegram, confirming the system's feasibility in providing effective warnings (Tommy Purnama, Yusuf Muhyidin, Dayan Singasatia).

2. Research Methods

Methods for improving wireless network security involve the use of Wireless Intrusion Detection Systems (WIDS) as a proactive way to detect and address potential threats to data integrity and confidentiality. In the initial stages, the focus is on reviewing and identifying weaknesses in the wireless network. This involves checking security configurations, identifying weak points, and assessing possible risks.After identifying weaknesses, the next step is to implement a Wireless Intrusion Detection System (WIDS). WIDS is designed to monitor and analyze wireless network traffic, detecting suspicious patterns or unauthorized behavior. Selecting a WIDS that suits the network needs and user environment is key.In the configuration stage, the method will include strict security policies and adjust WIDS parameters according to network characteristics. This involves establishing detection rules, configuring sensitivity, and customizing notifications for rapid response to detected threats.

Next, implementing mitigation measures is an important part. If WIDS detects a threat or suspicious activity, this method will provide guidance for taking appropriate action, such as isolating the infected device or enabling additional authentication mechanisms. Additionally, this method involves user training and awareness to reduce the risk of potential attacks.

In the evaluation phase, this method will continuously monitor the effectiveness of WIDS and analyze detection reports to evaluate the overall security of the wireless network. Regular updates to WIDS policies and configurations will also be integrated in accordance with new developments in security threats and wireless intrusion detection technology.Thus, wireless network security methods using Wireless Intrusion Detection Systems (WIDS) include steps from identifying weaknesses, implementing WIDS, parameter configuration, threat mitigation, to continuous evaluation. It provides a comprehensive approach to strengthening the security and resilience of wireless networks in the face of evolving threats.

3. Result and Discussion

The method to enhance the security of wireless networks by involving Wireless Intrusion Detection System (WIDS) has yielded significant results. The initial stage of this method is focused on reviewing and identifying vulnerabilities in wireless networks, providing a profound understanding of weak points and potential risks that may arise. The subsequent implementation of WIDS allows the system to actively monitor and analyze

wireless network traffic, detecting suspicious patterns or unauthorized behaviors. The method also emphasizes careful configuration and the enforcement of strict security policies, including the establishment of detection rules, sensitivity configuration, and notification adjustments. Consequently, the response to detected threats can be significantly improved.

The implementation of mitigation measures becomes a crucial step in maintaining network security, offering guidance on taking appropriate actions when WIDS detects threats or suspicious activities, such as isolating infected devices and activating additional authentication mechanisms. User awareness takes center stage in reducing the risk of potential attacks, with the method including training and user awareness to ensure that they understand their roles in maintaining security and identifying suspicious activities.

4. Conclusions

Based on the search results, it can be concluded that the use of the Wireless Intrusion Detection System (WIDS) is an effective solution in improving wireless network security. WIDS can identify attacks such as denial of service (DoS) attacks, brute force attacks, and intrusion attacks on wireless networks. With WIDS, network administrators can take appropriate action to protect the network and sensitive data sent over the wireless network.

Be sure to implement WIDS in your wireless network to detect and protect the network from potentially damaging attacks. By enabling WIDS, you can proactively identify attacks and take appropriate action. Perform active monitoring of reports and alerts generated by WIDS. This will help you detect attacks quickly and take appropriate action to protect your wireless network. Consider combining WIDS with other security technologies such as firewalls and encryption to provide a stronger layer of protection for your wireless network.

5. References

Aprianto, M. (2023). Desain Dan Implementasi Intrusion Detection System Menggunakan Debian 7 Dan Snort. Teknologipintar.Org, 3(3), 1–20. www.aprianto.com,

Esabella, S., & Bella Fitriana, Y. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC). Media Online, 4(1), 634–641. https://doi.org/10.30865/klik.v4i1.1157

Parga Zen, B., Satria Galang Saputra, & Abdurahman. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). Jurnal Sistem Informasi Galuh, 1(2), 43–51. https://doi.org/10.25157/jsig.v1i2.3152

Prasetyo, J. A., Rufi'i, R., & Wiyarno, Y. (2023). Pengembangan Aplikasi Computer Based Test (Cbt) Berbasis Web Dengan Jaringan Nirkabel (Wireless Network) Pada Hasil Belajar. JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), 8(3), 1010–1021. https://doi.org/10.29100/jipi.v8i3.4379

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. Jurnal Teknologi Informasi Dan Komunikasi, 14(2), 358–369. https://doi.org/10.51903/jtikp.v14i2.726