JOURNAL OF DATA SCIENCE | Vol.2024:41
eISSN:2805-5160

Data Security Analysis with Advanced Firewall Filtering at PT PUSRI

Misinem [1], Muhammad Ari Januarta [2], Tamsir Aryadi [3], Ahmad Qudri [4], Nurul Adha Oktarini Saputri [5]

[1,2,3,4,5] Faculty of Vocational, Universitas Bina Darma, Palembang, Indonesia

[*]**Email:** misinem@binadarma.ac.id

Abstract

Data and network security analysis are essential for ensuring the integrity, confidentiality, and availability of organizational data. Among the various threats, sniffing attacks—where malicious actors intercept and monitor data transmitted over a network—pose a significant risk to data security. This study analyzes the network security performance of the IT Service Department of PT—Palembang, focusing on the impact of sniffing attacks and the effectiveness of countermeasures. The research involves a comprehensive evaluation of the existing security infrastructure, testing for vulnerabilities to sniffing attacks, and implementing advanced security mechanisms. These mechanisms include encryption protocols, network segmentation, and intrusion detection systems. The analysis assesses the performance of these countermeasures in mitigating risks and enhancing overall network security. Findings from this study reveal that the proper implementation of security mechanisms significantly reduces the risk of sniffing attacks. Encryption ensures the confidentiality of transmitted data, network segmentation limits unauthorized access, and intrusion detection systems provide real-time threat identification. Additionally, the research highlights the importance of proactive measures, such as training IT staff on security best practices and implementing enhanced real-time monitoring systems. This study not only evaluates the technical aspects of network security but also provides actionable recommendations for sustainable improvements. By addressing both current vulnerabilities and future preparedness, the analysis underscores the critical role of a multi-layered security approach in safeguarding organizational data

Keywords

Network security, Sniffing attacks, Encryption, Network segmentation, Intrusion Detection

Introduction

The advancement of information technology is currently accelerating, and this technology has become a common thing among the public. Technology constantly evolves, making it easier for institutions that rely on networks to work. Therefore, tools that support this development are needed, such as a stable internet. However, security issues are often a significant concern and

Submission: 24 July 2024; **Acceptance:** 28 October 2024

should be checked regularly. The processed data information is valuable to the recipient because it provides total value in accuracy, timeliness, and relevance (Amarudin, 2018).

The Internet is a communication network that connects millions of people separated by distance and time around the world. It is a public and global network that provides a direct connection to anyone through a Local Area Network (LAN) and an Internet Service Provider (ISP) (Andriani et al., 2022). Network security must be developed and maintained so that no one breaks into data on the server. The usefulness of network security stems from the need to protect data. The leading cause of data loss and corruption is that some parties must be authorized to access or change the data. data use (Arini et al., 2023, Ariyadi et al., 2024).

PT. Pupuk Sriwidjaja Palembang is one of the largest factories on the island of Sumatra. Currently, the company produces Ammonia, Urea, and NPK. The leading equipment they use has functions to support various aspects of performance, including computers and networks (Fatimah et al., 2022). Sniffing is a cybercrime by monitoring or capturing data packets that pass through a particular network. This crime aims to steal personal data, such as passwords, account information, and others (Hae, 2021 & Kurniawan, 2021).

Sniffing occurs when data is transmitted between a client and a server (or vice versa), where an unauthorized party obtains someone else's username and password, intentionally or unintentionally. The perpetrator can use the victim's account to commit fraudulent acts or damage/delete the victim's data. Therefore, when you send or receive data over an internet connection, you must remain aware of the potential for insecure transmission processes or sniffers trying to steal data (Maslan, 2020).

One method to protect data from sniffing attacks is using IPSec Tunnel through a VPN implemented with authentication and encryption. IPSec has an Internet Key Exchange (IKE) that serves as a mechanism to form an IPSec tunnel (Novriansyah et al., 2021). Before this tunnel is formed, peering is carried out by negotiating the security methods used by the initiator and responder (Nugraha, 2022)

Methodology

Researchers Use Experimen Methods; Experimen Methods are the process of testing and evaluating various aspects of a network, such as performance, reliability, and security. The following are the stages of the research carried out.

Figure 1. Research Stages

a. Initial Stage

At this stage, the researcher prepares equipment for research in the IT Services Department of PT. Pusri Palembang, To Sniff by Installing Software to be Used, Which includes Ettercap, Wireshark, and Software that is also needed, namely N-MaP and Installed on Laptop Hardware that is connected to the network of the IT Service Department of PT. Pusri Palembang.

b. Topology Design

At this stage, the researcher will create a topology that will be used in this research by conducting a test of the network and analysis of the attack, as well as applying the security of the existing firewall network on microtia to improve protection against sniffing attacks.

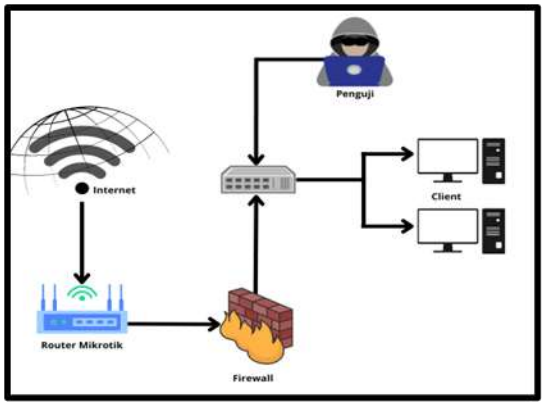

Figure 2. Star Topology

c. Analysis

At the analysis stage, the researcher analyzes the problems in the Object of study, namely the network and the phenomenon occurring. Besides analysis, network security and strategy implementation security to prevent attacks on the network.

d. Testing

The researcher conducted a test on the IT service department PT network. Pusri Palembang has been connected, and based on the data obtained later, these problems will get results based on the testing process.

e. Result

The results of testing attacks on the network will be known type attacks that can compromise the IT services department PT network. Pusri Palembang and Producing Solutions in Overcoming Problems This is by implementing more effective network security.

Results and Discussion

The implementation is conducted, the results are collected, and the discussions are done, as explained in this part.

Results

1. Microtic Display
   a. The login is displayed on the web microtic browser in the early stages.

Figure 3. Microtic Login Web View in Browser

   b. At this stage, sniffing attacks are tested without a firewall and by scanning Nmap (network mapper).

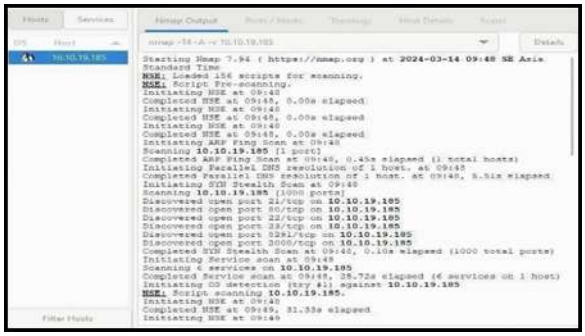

Figure 4. Scanning Using Zenmap Tools

   c. At this stage, network capture is carried out using Wireshark tools.

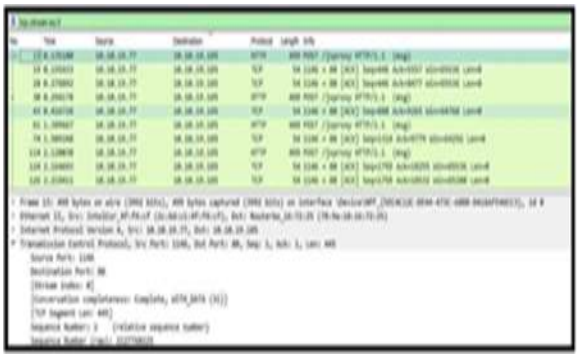

Figure 5. Wireshark Network Capture

2. Layer 7 protocol firewall configuration
   a. A layer seven protocol will be configured in the next stage to prevent attacks on Winbox microtic access.

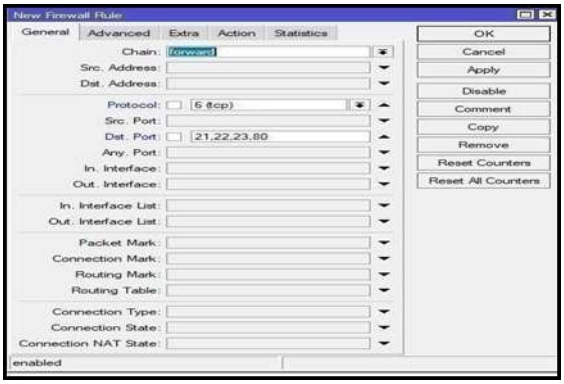

Figure 6. Firewall Rules

   b. Then go to the layer seven protocol menu and select the + button, then enter the domain name www.mikrotik.co.id and regexp +(Mikrotik.co.id)$.

Figure 7. Firewall Layer 7

   c. Next, enter the action menu and the drop command, click apply, and ok.

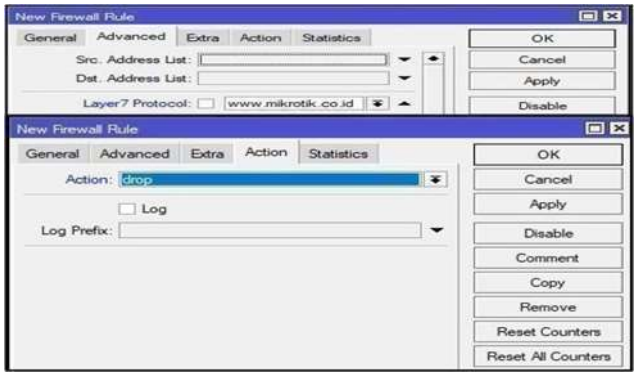

Figure 8. Action Drop Display

Discussion

The security configuration of the MikroTik firewall system was undertaken in two phases: vulnerability testing and implementing a Layer 7 protocol firewall. These steps aimed to enhance the system's defenses against sniffing attacks and unauthorized access.

Phase 1: Vulnerability Testing

The process began by accessing the MikroTik login interface via a web browser, replicating an initial user interaction point to identify potential vulnerabilities. Sniffing attacks were simulated using **Nmap** and **Zenmap** tools to scan the network for open ports and security gaps. These tools provided detailed insights into the system's exposure to external threats by mapping the network and analyzing potential entry points.

Additionally, **Wireshark**, a network protocol analyzer, was employed to capture and study data packets during transmission. This analysis revealed areas of susceptibility where malicious actors could potentially intercept sensitive information. The findings underscored the need for advanced protective measures to secure the system's infrastructure.

Phase 2: Layer 7 Protocol Firewall Configuration

To address the vulnerabilities discovered during testing, a Layer 7 protocol firewall was configured. This advanced security measure filters traffic based on application-layer data, providing enhanced protection against targeted attacks. The process began by accessing the firewall rules menu, where specific parameters were defined to block unauthorized access.

Domain-specific filtering was implemented by inputting www.mikrotik.co.id into the Layer 7 protocol settings and creating a regular expression (regexp) pattern to identify and manage traffic associated with this domain. This approach allowed the system to validate legitimate traffic while blocking malicious attempts. Finally, the action menu was configured with a "drop" command to terminate unauthorized traffic. Once implemented, the system was retested to ensure the effectiveness of these new security rules.

Insights and Effectiveness

The introduction of the Layer 7 protocol firewall significantly improved the security of the MikroTik system. By filtering traffic at the application layer, the system gained the ability to prevent specific types of malicious traffic that traditional firewalls might overlook. Using domain-based rules enhanced precision in blocking unauthorized access, while the "drop" action successfully prevented harmful data packets from reaching their target.

The testing tools, Zenmap and Wireshark, were instrumental in identifying vulnerabilities, allowing for a tailored approach to mitigation. However, the effectiveness of these measures hinges on the accurate definition and regular updating of firewall rules to counter new and evolving threats.

Recommendations

While the current configuration provides robust protection, additional measures could enhance the system's security. Regularly updating firewall rules, employing SSL/TLS encryption for data transmission, and implementing multi-factor authentication (MFA) is essential to safeguard against evolving attack methods. Additionally, real-time monitoring and alert systems can help promptly identify and respond to suspicious activities.

In summary, the combination of thorough vulnerability testing and the strategic implementation of a Layer 7 protocol firewall has strengthened the MikroTik system's defenses against sniffing attacks and unauthorized access. These measures establish a solid foundation for future scalability and ongoing improvements in network security.

Conclusions

This study highlights the critical importance of robust network security measures in mitigating the risk of sniffing attacks, particularly within the IT Service Department of PT Pusri Palembang. The research successfully identified and addressed potential weaknesses in the organization's network infrastructure through a systematic approach encompassing vulnerability testing and the implementation of advanced security mechanisms.

The vulnerability assessment phase, conducted using tools such as Nmap, Zenmap, and Wireshark, revealed areas of susceptibility to sniffing attacks, particularly in the absence of adequate firewalls. The subsequent implementation of a Layer 7 protocol firewall proved effective in addressing these vulnerabilities by filtering traffic at the application layer and blocking unauthorized access through domain-specific rules and the "drop" command.

The results demonstrate that the Layer 7 protocol firewall significantly enhances the system's ability to prevent sniffing attacks and ensures the secure transmission of sensitive data. However, the study also underscores the necessity of regular updates to firewall rules and the adoption of complementary measures such as encryption, multi-factor authentication, and real-time network monitoring to maintain robust security in the face of evolving threats.

This research provides a practical and scalable framework for improving network security, offering valuable insights for organizations facing similar challenges. The findings reinforce the need for continuous investment in security infrastructure and training for IT Staff to safeguard the integrity, confidentiality, and availability of organizational data.

References

Amarudin, A. (2018). Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode PortKnocking. Prosiding Semnastek.

Andriani, R., Wulandari, D. S., & Margianti, R. S. (2022). Rekam medis elektronik sebagai pendukung manajemen pelayanan pasien di RS Universitas Gadjah Mada. Jurnal Ilmiah Perekam Dan Informasi Kesehatan Imelda (JIPIKI), 7(1), 96-107.

Arini, A., Arsalan, M. L., & Sukmana, H. T. Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus: Pt. Akurat. Co). Cyber Security dan Forensik Digital, 6(2), 30-38.

Ariyadi, T., Irwansyah, I., & Mubarok, M. S. H. (2024). Analisis Keamanan Jaringan Wifi Mahasiswa UBD Dari Serangan Packet Sniffing. JURNAL ILMIAH INFORMATIKA, 12(01), 53-58.

Fatimah, F., Mary, T., & Pernanda, A. Y. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat. JURTEII: Jurnal Teknologi Informasi, 1(2), 7-11.

Hae, Y. (2021). Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8(4), 2095-2105.

Kurniawan, R. (2021). Analisis Keamanan Fasilitas Jaringan (Wifi) Terhadap Serangan Packet Sniffing Pada Protocol Http Dan Https (Doctoral dissertation, Universitas Islam Riau).

Maslan, A. (2020). KEAMANAN JARINGAN DARI SERANGAN PAKET DATA SNIFFING DI PTRADEN SYAID KANTOR POS PIAYU KOTA BATAM. Computer and Science Industrial Engineering (COMASIE), 3(5), 107-117.

Novriansyah, M. F., Nugraha, Y., Wiguna, H., Ernesto, A., Sulasikin, A., Nasution, B. I., ... & Suherman, A. L. (2021, October). The Impact of Large-Scale Social Restriction and Odd-Even Policies During COVID-19 Pandemic to Traffic Congestion and Air Pollution in Jakarta. In 2021 International Conference on Artificial Intelligence and Big Data Analytics (pp. 1-6). IEEE.

Nugraha, A. D., Husaini, H., & Anwar, A. (2022). Analisis Keamanan Data Dalam Jaringan Terhadap Kegiatan Sniffing Menggunakan Serangan Man In The Midle Attack. Jurnal Teknologi Rekayasa Informasi dan Komputer, 5(2).