|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 6| No. 3|Oct|Year 2025|

Network Security Implementation Against Sniffing Attacks in the IT Services Department of PT Pupuk Sriwidjaja (PUSRI) Palembang

Ardiansyah[1*]

Abstract

Network security is a crucial aspect of maintaining data integrity, confidentiality, and availability within organizations. Sniffing attacks, in which an attacker intercepts and monitors data transmitted over a network, pose a significant threat to data protection. This study aims to analyze the performance of the network security system of the IT Services Department at PT Pupuk Sriwidjaja (PUSRI) Palembang against sniffing threats. The research includes evaluating existing security systems, testing potential sniffing attacks, and implementing and analyzing the effectiveness of various security mechanisms such as encryption, network segmentation, and intrusion detection. The results indicate that appropriate security mechanisms substantially reduce the risk of sniffing attacks. This study also provides recommendations for further improvements, including staff training on cybersecurity best practices and strengthening real-time network monitoring.

Keywords

Network Security, Sniffing Attacks, Encryption, Segmentation, Pt Pupuk Sriwidjaja

Article History

Received 03 August 2025
Accepted 26 October 2025

How to Cite

Ardiansyah. (2025). Network Security Implementation Against Sniffing Attacks in the IT Services Department of PT Pupuk Sriwidjaja (PUSRI) Palembang. ***Jurnal Jaringan Komputer dan Keamanan****, 6*(3), 100-105.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: ardi10062@gmail.com

Introduction

The rapid advancement of information technology continues to shape and influence organizational operations in various sectors. Modern organizations increasingly depend on computer networks to facilitate administrative processes, internal communication, and data exchange. As operational activities rely heavily on stable internet connectivity, ensuring network reliability and protection becomes a fundamental requirement. Network security measures must be implemented and continuously monitored to prevent misuse of network resources, unauthorized access, and data breaches that may compromise organizational stability and trust (Tekino, 2020). Without structured security controls, organizations face heightened vulnerability to cyber threats that can disrupt operations and cause significant financial and reputational damage.

The internet functions as a global communication platform that connects millions of users worldwide. As a public and interconnected network, it supports various services accessed through Local Area Networks (LANs) and Internet Service Providers (ISPs). While the internet enables flexible data transmission and remote collaboration, its open nature also introduces significant security risks. Data stored and transmitted across networks must be safeguarded through robust security infrastructures to prevent interception, tampering, or unauthorized retrieval. Ensuring the confidentiality, integrity, and availability of information has therefore become a priority for organizations that manage sensitive and mission-critical operations.

PT Pupuk Sriwidjaja Palembang, one of the largest fertilizer manufacturers in Sumatra, relies extensively on computerized systems to support its production and administrative activities. As a company producing Ammonia, Urea, and NPK fertilizers, its operational processes depend on accurate information flow and timely access to digital resources. Consequently, securing its internal network infrastructure is essential for supporting reliable communication between departments, maintaining production continuity, and protecting strategic corporate information. Any disruption in network performance may impede internal workflows and adversely impact the company's operational efficiency.

One notable cyber threat that organizations must anticipate is sniffing, a technique used by attackers to intercept and monitor data packets transmitted across a network. Sniffing attacks aim to capture sensitive information such as login credentials, session tokens, or personal data, which may then be exploited for unauthorized access or malicious activities (Pos et al., 2020). When data travels between a client and a server, attackers positioned within the network path can capture unencrypted traffic, making systems vulnerable to identity theft, unauthorized system access, or further exploitation. This highlights the importance of adopting encrypted communication mechanisms to prevent attackers from accessing readable data.

To counter sniffing attacks, organizations can implement IPSec VPN tunnels, which protect data through authentication and encryption processes. IPSec technology uses the Internet Key Exchange (IKE) protocol to negotiate security parameters before establishing a secure communication tunnel. This approach ensures that data transmitted across the network remains confidential and protected from eavesdropping. IPSec VPNs provide secure connections for remote and internal communication, making them an effective method to

preserve data integrity and prevent unauthorized interception. Such encryption-based safeguards are particularly important for companies that depend on secure remote access and inter-branch communication.

Previous studies have demonstrated the effectiveness of VPN technology in enhancing network security. Research by Supriyono, Widjaya, and Suparmi (2013) successfully implemented VPNs to secure data communication between the head office and branch offices at PT Mega Besar Alami, showing improved confidentiality and secure access across the organization. Another study by Sugiyatno and Dina Atika (2018) evaluated SSTP VPN security using Raspberry Pi and concluded that PPTP VPNs are resistant to sniffing-based interception attempts. These findings reinforce the value of VPN solutions as protective mechanisms against network-based attacks. Building on these insights, the present study explores the implementation of an IPSec VPN tunnel to protect organizational data and strengthen network security within PT Pupuk Sriwidjaja Palembang.

Methodology

Research Location and Duration

The research was conducted at the IT Services Department of PT Pupuk Sriwidjaja (PUSRI) Palembang.The study took place from January 4, 2024, to March 28, 2024, during the internship period of the researchers.

Data Collection Methods

Data collection was carried out to obtain complete, clear, and detailed information required for the research.

Observation Method

Researchers identified issues related to data transmission in the IT Services Department and observed packet interactions using Wireshark.

Interview Method

Interviews were conducted with employees of the IT Services Department to obtain insights related to network security issues and the research topic.

Literature Review

Relevant theories were collected from books, journals, articles, and various online sources.

Research Stages

1. Initial Stage: Preparing sniffing tools such as Ettercap, Wireshark, and Nmap.
2. Design Stage: Designing network topology and analyzing potential sniffing attacks.
3. Analysis Stage: Conducting network vulnerability analysis based on real-time conditions.
4. Testing Stage: Executing sniffing tests to identify vulnerabilities in the IT Services network.
5. Results Stage: Identifying attack types and determining effective security solutions.

Results

Sniffing Activity Before Firewall Implementation

Activity	Software	Status	Result
Port Scanning	Zenmap	Successful	Discovered open ports: 21, 22, 23, 80
Credential Theft (MikroTik)	Wireshark	Successful	Captured MikroTik WebFig username and password
ARP Poisoning	Ettercap	Successful	Extracted sensitive login credentials

These results indicate that prior to firewall implementation, attackers could easily access open ports and intercept sensitive information such as login credentials.

Sniffing Activity After Firewall Implementation

Activity	Software	Status	Result
Port Scanning	Zenmap	Failed	Firewall blocked TCP ports, preventing discovery of open ports
Credential Theft (MikroTik)	Wireshark	Failed	WebFig access was blocked by administrators
ARP Poisoning	Ettercap	Failed	Firewall prevented access to sensitive data

Results

The results of the pre-implementation tests clearly demonstrate that the network environment at PT Pupuk Sriwidjaja (PUSRI) Palembang was highly vulnerable to sniffing-based cyberattacks. Tools such as Zenmap, Wireshark, and Ettercap were able to perform port scanning, credential interception, and ARP poisoning with complete success. The discovery of open ports (21, 22, 23, and 80) reflects a weak perimeter defense, as these commonly targeted service ports are often exploited by attackers to gain entry into internal systems. This condition is consistent with Pos et al. (2020), who emphasize that unprotected network traffic allows attackers to easily capture sensitive information and compromise system integrity.

The successful retrieval of MikroTik WebFig credentials via Wireshark further confirms the absence of encryption and secure authentication mechanisms prior to the firewall and IPSec VPN implementation. Credential theft poses a severe risk because attackers can use intercepted usernames and passwords to infiltrate administrative interfaces, modify configurations, or escalate privileges. These findings align with Tekino (2020), who notes that unsecured communication channels expose organizations to the threat of unauthorized access

and data breaches. Similarly, the success of ARP poisoning attacks using Ettercap indicates that internal LAN communication was not protected by proper network segmentation or packet filtering.

Following the deployment of the IPSec VPN and firewall system, the network exhibited significantly improved resistance to sniffing and interception attempts. Port scanning using Zenmap failed due to the firewall's ability to block external probing and conceal open ports from unauthorized scanning attempts. This is consistent with the security architecture described by Supriyono, Widjaya, and Suparmi (2013), who found that VPN-based tunneling and filtering mechanisms reduce external visibility of network services. By preventing port enumeration, the firewall effectively reduces the reconnaissance phase of cyberattacks, limiting the attacker's ability to identify potential entry points.

Credential theft attempts after implementation were also unsuccessful. Wireshark was unable to capture MikroTik WebFig login information because access to the WebFig interface was restricted and protected via firewall rules. Moreover, IPSec encryption ensured that communication between client and server was unreadable when intercepted, fulfilling the confidentiality principles highlighted by J. Safira, Hanafi, and Munawar (2021). This demonstrates that encrypted communication tunnels not only protect data in transit but also minimize the risk of credential exposure through packet sniffing.

The failure of ARP poisoning attacks after security hardening reflects the effectiveness of enforced firewall rules, improved interface filtering, and the encapsulation of traffic within secure VPN tunnels. These enhancements disrupt the ability of attackers to inject spoofed ARP packets or position themselves as intermediaries in the communication flow. This finding supports Sugiyatno and Atika (2018), who concluded that VPN-protected networks exhibit strong resistance to sniffing-based interception and man-in-the-middle attacks. As a result, attackers are unable to manipulate local traffic or extract sensitive information from compromised ARP tables.

Overall, the comparison between pre- and post-implementation network conditions demonstrates a substantial improvement in security posture. IPSec VPN successfully encrypts data flows and authenticates communicating entities, while firewall filtering enhances perimeter protection and mitigates internal threats. These combined mechanisms significantly limit the attack surface, prevent reconnaissance activities, and protect critical credentials from unauthorized access. Although the results are promising, further enhancements—such as intrusion detection systems (IDS), continuous log monitoring, and multi-layered segmentation—are recommended to reinforce long-term resilience and adapt to evolving cyber threat landscapes.

Conclusion and Recommendations

The implementation of IPSec VPN and firewall mechanisms at the IT Services Department of PT Pupuk Sriwidjaja (PUSRI) Palembang successfully improved network security. These security enhancements significantly reduced the success rate of sniffing attacks and prevented unauthorized access and credential theft.

Disclosure Statement

The authors declare no conflicts of interest.

Acknowledgments

The authors express gratitude to PT Pupuk Sriwidjaja (PUSRI) Palembang and Universitas Bina Darma for providing facilities and support throughout this study.

References

Supriyono, H., Widjaya, J. A., & Suparmi, A. (2013). Implementation of Virtual Private Network (VPN) to secure data communication at PT Mega Besar Alami.

Sugiyatno, & Atika, D. (2018). Security testing of SSTP VPN using Raspberry Pi.

Pos, et al. (2020). Sniffing attack mechanisms and prevention strategies.

Tekino. (2020). Information security and data protection.

Kumar, A., & Lee, B. (2021). Analysis of packet sniffing attacks and detection techniques: A systematic review. Journal of Network Security and Applications, 9(2), 55–68. https://doi.org/10.5121/jnsa.2021.9204

Alshamrani, A., Myneni, S., Chowdhury, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851–1877. https://doi.org/10.1109/COMST.2018.2890071

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson Education.

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. National Institute of Standards and Technology.

Shirey, R. (2007). Internet Security Glossary, Version 2. RFC 4949. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC4949

Biographical Notes

MUHAMAD ARY JANUARTA is a student in the Computer Engineering Program at Universitas Bina Darma specializing in cybersecurity research.