ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

Cyber Attack Simulation and Detection in a Segmented WAN–LAN–DMZ Network

S. Sangamithra[1]; Ajaay Pranav O. B.[2]; Bharath J. B.[3]; Sanjeevi K. S.[4]

[1]Assistant Professor, Dept. of Computer Science Engineering, K.L.N College of Engineering, Tamil Nadu, India
[2,3,4]Student, Dept. of Computer Science Engineering, K.L.N College of Engineering, Tamil Nadu, India

Publication Date: 2026/04/03

Abstract: The growing complexity of cyber threats has revealed critical limitations in traditional network security mechanisms. This paper presents a framework for simulating and detecting cyber-attacks using a segmented WAN DMZ LAN architecture. A virtual environment is developed with a vulnerable DMZ server and protected LAN system. A pfSense firewall and Suricata IDS are used to monitor and detect attacks. Results show improved detection and isolation of threats using segmentation and monitoring.

Keywords: *Network Security, DMZ, Firewall, IDS, Cyber Attack Simulation, pfsense, Suricata*.

How to Cite: S. Sangamithra; Ajaay Pranav O. B.; Bharath J. B.; Sanjeevi K. S. (2026) Cyber Attack Simulation and Detection in a Segmented WAN–LAN–DMZ Network. *International Journal of Innovative Science and Research Technology*, 11(3), 2983-2991. https://doi.org/10.38124/ijisrt/26mar1610

I. INTRODUCTION

Modern organizations increasingly depend on interconnected digital infrastructures, making them more vulnerable to advanced and persistent cyber threats. Conventional security measures, including standalone firewalls and signature-based intrusion detection systems, are often inadequate in defending against complex, multi-stage attack scenarios.

To strengthen network security, segmentation techniques such as the implementation of a Demilitarized Zone (DMZ) are widely adopted. This approach isolates externally accessible services from critical internal systems, thereby reducing the risk of direct compromise. However, purely theoretical approaches do not provide sufficient insight into how attackers identify vulnerabilities, exploit systems, and move across network boundaries. A practical and experimental setup is essential to understand these attack dynamics and evaluate the effectiveness of defensive mechanisms.

In this context, the present work introduces a controlled cyber-attack simulation framework that combines network segmentation, firewall policy enforcement, and intrusion detection capabilities. The primary goal is to emulate realistic attack scenarios and systematically analyze system behavior using collected log data, enabling a deeper understanding of both attack methodologies and defensive responses.

- *Objective and Scope of the Project*

The main objective of this project is to develop a structured and secure network environment that supports the simulation and analysis of cyber-attacks. The system is designed using a segmented architecture consisting of WAN, DMZ, and LAN zones, enabling the study of attack progression across different network layers.

Another objective is to implement a multihomed firewall using pfSense to enforce traffic control policies between network segments. This ensures that only authorized communication is permitted while preventing direct access to internal systems. Additionally, an Intrusion Detection System (IDS) is incorporated to monitor network traffic and identify suspicious or malicious activities.

The project also aims to simulate real-world attack scenarios such as network scanning, vulnerability exploitation, and unauthorized access attempts. These simulations help in understanding attacker behavior and evaluating the effectiveness of security controls. Logs generated from the firewall, IDS, and endpoint systems are analyzed to identify potential indicators of compromise and reconstruct the sequence of events during an attack.

The scope of this work is limited to a virtualized network environment focused on network-level attack simulation and detection. Advanced enterprise-level integrations and large-scale deployments are not included. However, the proposed framework provides a strong foundation for practical cybersecurity learning and can be extended to support more advanced security implementations.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

II. SYSTEM MODULES

The proposed system is composed of multiple interconnected modules that collectively simulate cyber-attacks and detect malicious activities within a segmented network environment. Each module performs a specific function, contributing to the overall operation of the system.

- *Network Segmentation Module*

This module is responsible for dividing the network into distinct zones, namely WAN, DMZ, and LAN. Each segment represents a different level of trust and accessibility within the network. The WAN acts as the external network where potential attackers originate, while the DMZ hosts publicly accessible services such as the web server. The LAN contains internal systems that require strict protection. By isolating these segments, the module ensures that a compromise in one zone does not directly impact other parts of the network.

- *Firewall Management Module*

The firewall management module implements traffic control policies using a multihomed firewall configuration. The pfSense firewall is configured with multiple interfaces to connect the WAN, DMZ, and LAN networks. This module defines and enforces rules that regulate communication between different segments. It allows only necessary traffic, such as web access to the DMZ, while blocking unauthorized attempts to access the LAN. In addition, it records network activities in the form of logs, which are essential for further analysis.

- *Attack Simulation Module*

This module is responsible for generating controlled cyber-attack scenarios within the virtual environment. An attacker system is used to perform various activities such as network scanning, vulnerability probing, and exploitation attempts. These simulated attacks replicate real-world attacker behavior and are directed primarily toward the DMZ server. The purpose of this module is to evaluate how the system responds to different types of threats and to study the progression of attacks across network layers.

- *Intrusion Detection Module*

The intrusion detection module continuously monitors network traffic to identify suspicious or malicious activities. It utilizes an Intrusion Detection System (IDS), such as Suricata, to analyze packets based on predefined signatures and behavioral patterns. When potential threats are detected, alerts are generated with relevant details including source, destination, and type of attack. This module plays a crucial role in providing visibility into network activities and identifying ongoing attacks in real time.

- *Log Collection and Analysis Module*

This module gathers logs from multiple sources, including the firewall, IDS, web server, and endpoint systems. These logs contain detailed information about network traffic, system events, and detected threats. The collected data is analyzed to identify patterns, trace attacker activities, and determine indicators of compromise. By correlating logs from different components, this module helps reconstruct the sequence of events during an attack and evaluate the effectiveness of security mechanisms.

- *Reporting Module*

The reporting module presents the findings obtained from log analysis in a structured format. It summarizes detected attacks, system responses, and overall network behavior during the simulation. The module provides insights into how the attack was executed, how it was detected, and which security controls were effective. This information is useful for understanding system performance and improving future security strategies.

III. LITERATURE REVIEW

- *"Survey on Intrusion Detection Systems in Software-Defined Networking," 2025.*

This study presents a detailed analysis of intrusion detection mechanisms used in modern network environments. It highlights the role of Intrusion Detection Systems (IDS) in continuously monitoring network traffic and identifying malicious activities in real time. The paper discusses various detection techniques and their effectiveness; however, it mainly focuses on theoretical analysis and lacks practical implementation in a segmented network environment.

- *Lorenzo Diana, Pierpaolo Dini, Davide Paolini, "Overview on Intrusion Detection Systems for Computer Network Security," March 2025.*

This paper provides a comprehensive overview of intrusion detection systems, including signature-based and anomaly-based detection techniques. It explains how IDS monitors network traffic and identifies malicious patterns. While the study highlights detection accuracy and methodologies, it lacks practical implementation in a real-time segmented network environment.

- *Cyber Attack Simulation and Detection in a Segmented LAN–DMZ Network, Project Work, 2026.*

This work focuses on designing a segmented network architecture using WAN, DMZ, and LAN zones combined with a multihomed firewall and intrusion detection system. It includes real-world attack simulations such as port scanning, brute force, and denial-of-service attacks. The system also performs log analysis using firewall and IDS data. However, the implementation has limited focus on advanced attack correlation and automated response mechanisms.

- *William Stallings, "Network Security Essentials: Applications and Standards," Pearson Education, 2017.*

This book explains fundamental concepts of network security, including layered defense mechanisms, firewall policies, and intrusion detection systems. It emphasizes the importance of combining multiple security controls to protect network infrastructure. Although it provides strong theoretical knowledge, it does not include practical simulation or real-time attack analysis.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

IV. EXISTING SYSTEM

The existing system, as described in the base survey study, focuses on the analysis of intrusion detection mechanisms in modern network environments. It explains how Intrusion Detection Systems (IDS) monitor network traffic and detect malicious activities using techniques such as signature-based and anomaly-based detection. The study also highlights different types of IDS and their role in improving network security, providing a strong theoretical foundation.

However, the system is primarily limited to a conceptual approach and does not include practical implementation in a real or simulated network environment. It does not demonstrate how these detection techniques operate within a segmented architecture such as WAN–DMZ–LAN, which is essential for analyzing real-world security scenarios.

In addition, the system does not support cyber-attack simulation or real-time log analysis. It lacks mechanisms to evaluate system performance under actual attack conditions and does not provide insights into attack progression across network layers. Therefore, further extension into a practical framework is required for comprehensive security analysis.

➢ *Proposed System*

The proposed system extends the existing theoretical approach by implementing a practical cyber-attack simulation and detection framework within a segmented WAN–DMZ–LAN architecture. A multihomed pfSense firewall is configured to enforce strict traffic control between network zones, while an Intrusion Detection System (IDS) such as Suricata is integrated to monitor network activity and identify potential threats in real time.

The system incorporates an attacker environment to simulate real-world cyber-attacks, including network scanning, vulnerability exploitation, and unauthorized access attempts. These attacks are primarily directed toward the DMZ server, allowing analysis of how threats interact with segmented networks. Firewall rules and IDS alerts are used to observe and evaluate system responses under controlled attack conditions.

In addition, the system performs log collection and analysis from multiple sources, including firewall logs, IDS alerts, and host system events. This enables tracking of the complete attack lifecycle, from initial access to attempted lateral movement and data exfiltration. By combining practical implementation with real-time monitoring, the proposed system provides a more comprehensive and realistic approach to network security analysis.

V. SYSTEM ARCHITECTURE

The proposed system is built on a segmented network model comprising three distinct zones: Wide Area Network (WAN), Demilitarized Zone (DMZ), and Local Area Network (LAN). These segments are interconnected through a multihomed pfSense firewall, which functions as the central security layer responsible for managing and filtering traffic across the network.

The WAN represents the external environment where the attacker system is deployed, simulating real-world threat conditions. The DMZ serves as an intermediary zone that hosts a vulnerable web server, allowing controlled access from external sources while isolating internal systems. The LAN contains a Windows 11 workstation that represents critical internal assets requiring strong protection against unauthorized access.

The pfSense firewall is configured with dedicated interfaces for each network segment and applies strict access control policies to regulate communication. It permits only necessary traffic, such as web requests from the WAN to the DMZ, while preventing direct connectivity to the LAN. In addition, the system integrates the Suricata Intrusion Detection System (IDS) to continuously inspect network traffic and identify suspicious activities, including scanning attempts and intrusion behavior.

During operation, the attacker initiates various attack techniques from the WAN targeting the DMZ server. In the event of a compromise, attempts to access internal resources are restricted by firewall rules, thereby preventing lateral movement into the LAN. Simultaneously, logs generated by the firewall, IDS, and endpoint systems are collected and analyzed to trace attack patterns and evaluate the overall effectiveness of the security framework.

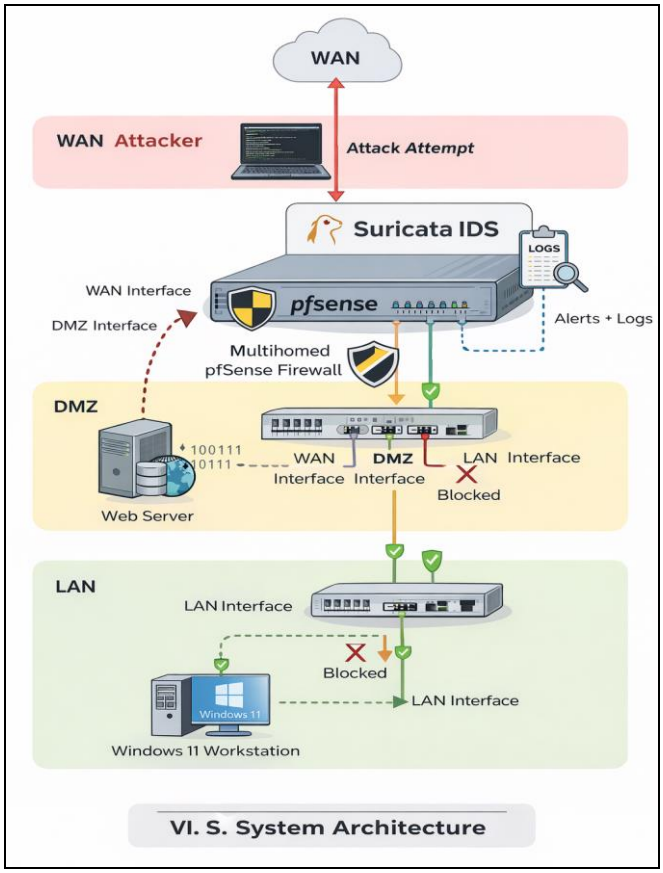

Fig 1 Architecture Diagram

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

VI. RESULTS AND DISCUSSION

The proposed system was implemented in a virtualized WAN–DMZ–LAN environment using pfSense firewall and Suricata IDS. Various cyber-attack scenarios were performed to evaluate system performance, including network scanning, SQL injection, and command injection attacks. The results obtained from firewall logs, IDS alerts, and application responses demonstrate the effectiveness of the system in detecting and controlling malicious activities.

Fig 2 pfSense WAN Firewall Rules Configuration

The firewall rules configured on the WAN interface allow only specific traffic such as HTTP access to the DMZ server while blocking unauthorized connections. This ensures controlled exposure of services and prevents direct access to internal network resources.

Fig 3 pfSense Interface Configuration

This figure illustrates the configuration of firewall rules on the WAN interface, where controlled access is provided to the DMZ server while blocking unauthorized inbound traffic. The rule set ensures that only specific services such as HTTP are permitted, thereby reducing the attack surface and enforcing strict perimeter security.

Proper segmentation of the network enables isolation between external, intermediate, and internal zones, forming the foundation for secure communication.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

Fig 4 Command Injection Attack Result

The figure demonstrates a successful command injection attack on the DVWA application hosted in the DMZ. The attacker is able to execute system-level commands, confirming the presence of vulnerabilities in the web application.

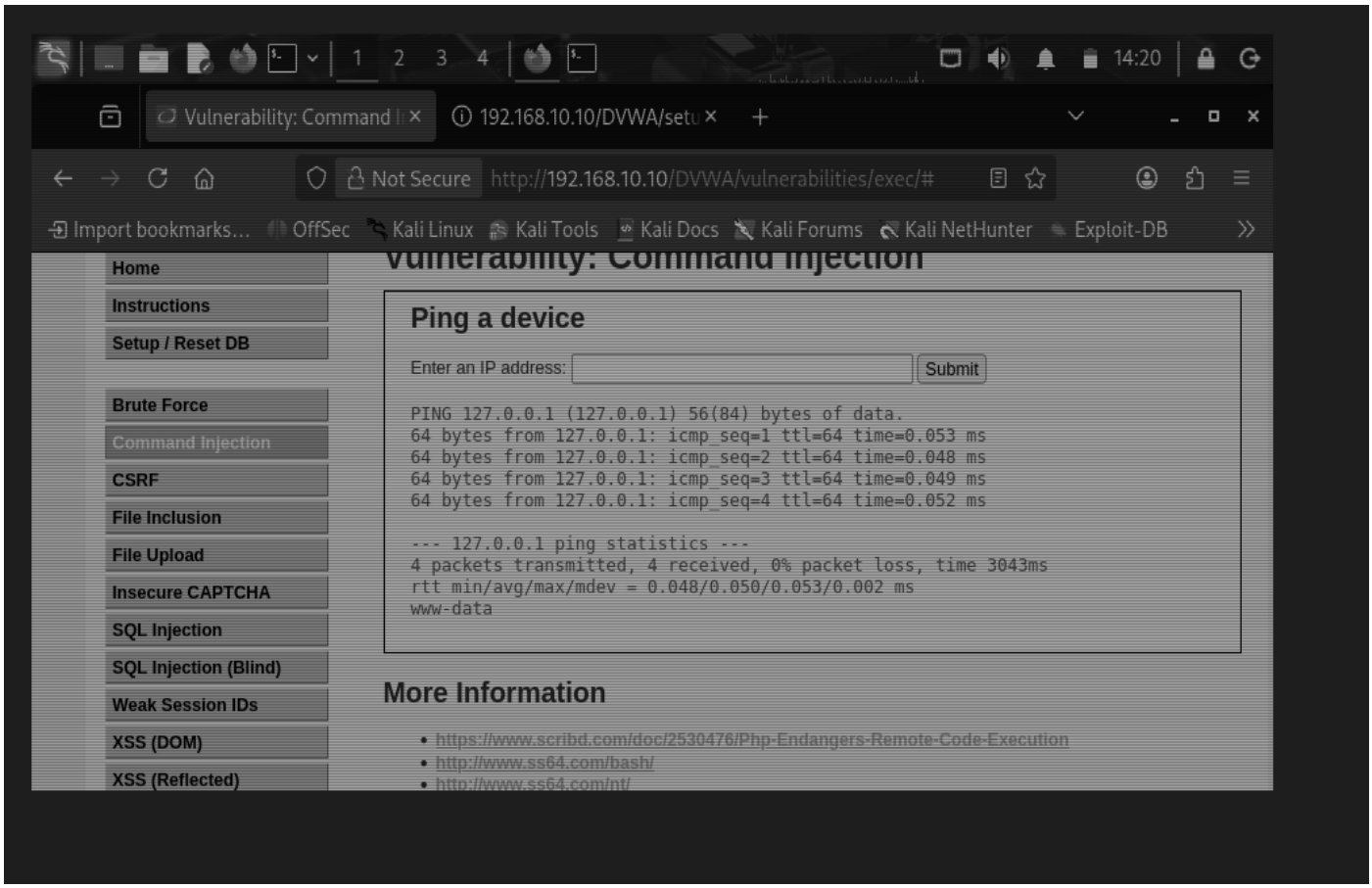

Fig 5 Command Injection Output Analysis

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

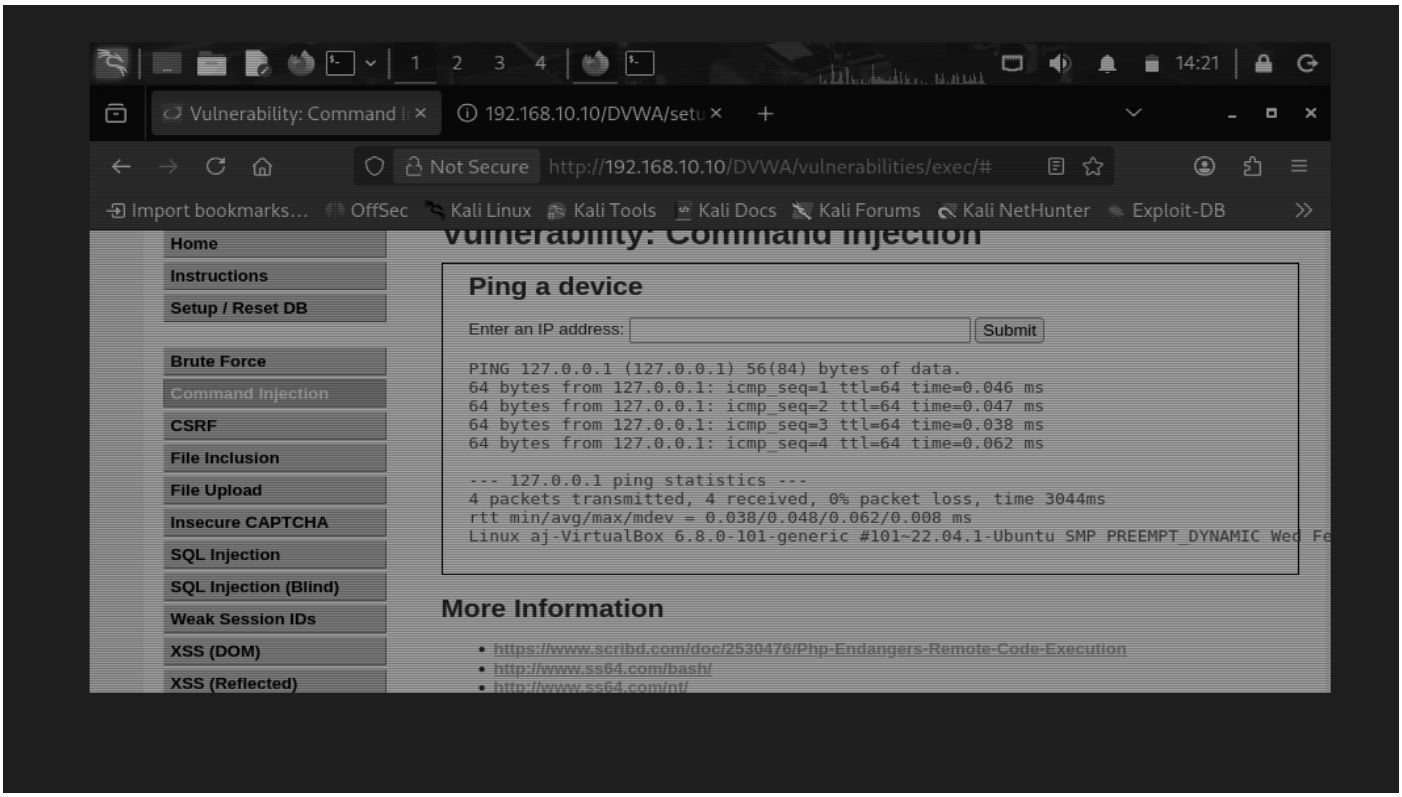

Fig 5 Command Injection Output Analysis

This figure shows detailed system responses obtained from the command injection attack, including system-level information. The output confirms that the attacker has gained partial control over the server, emphasizing the importance of secure coding practices and input sanitization.

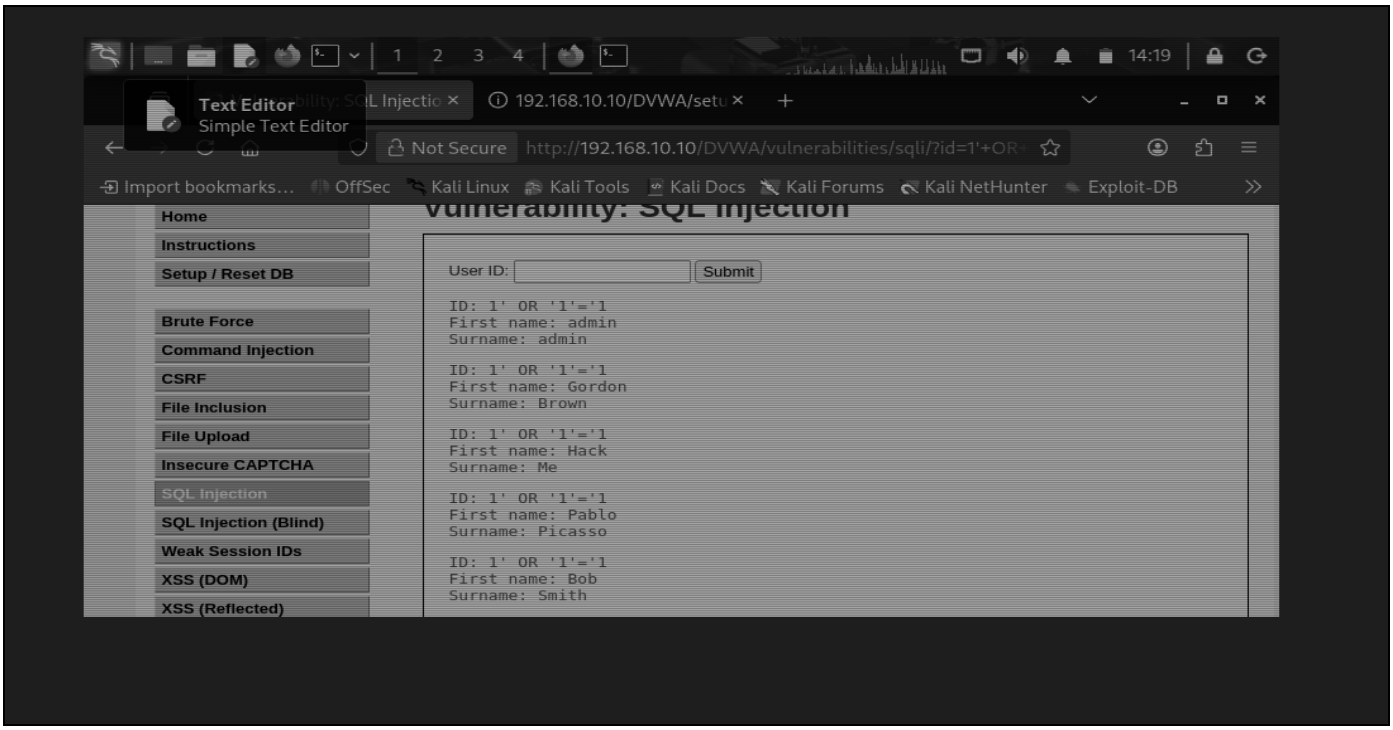

Fig 7 SQL Injection Attack Result

The figure presents the output of a SQL injection attack, where unauthorized database information is retrieved by manipulating input queries. This confirms the presence of exploitable database vulnerabilities and demonstrates how attackers can bypass authentication mechanisms.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

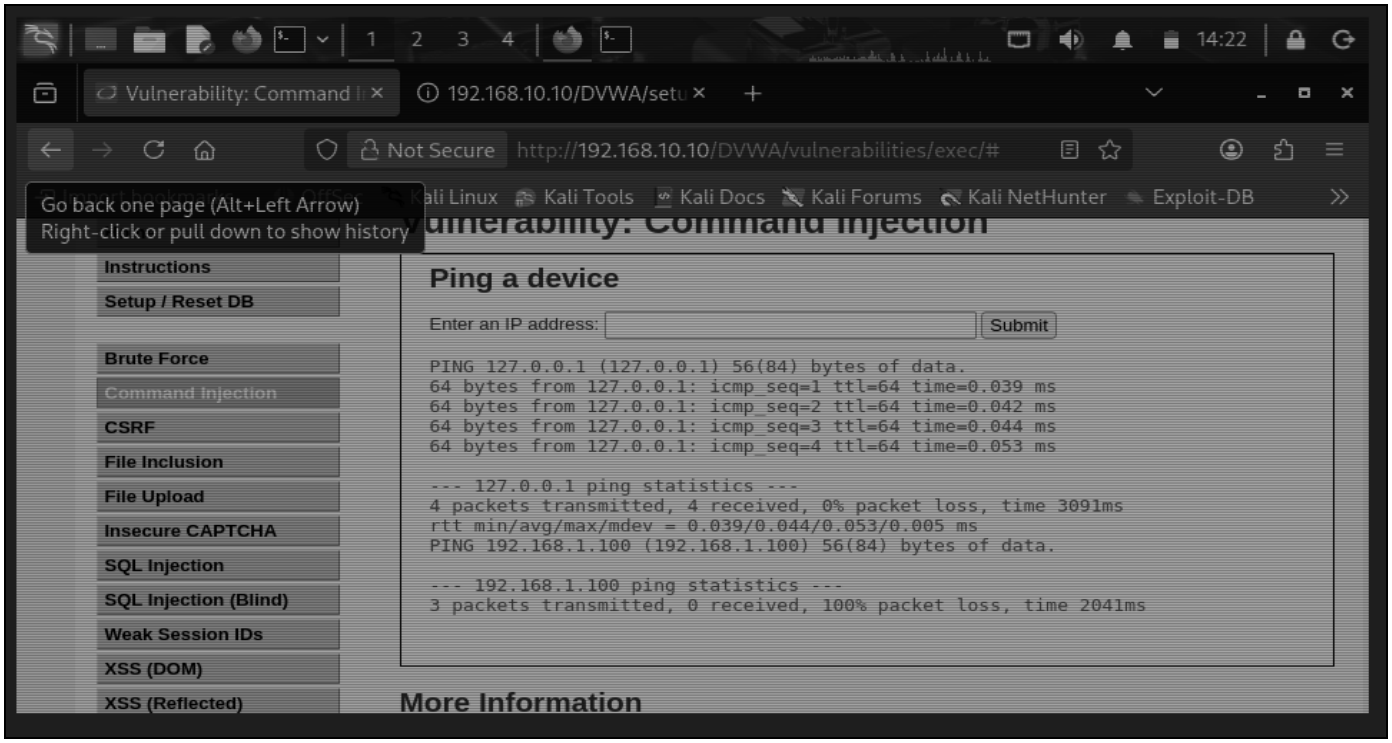

Fig 8 Blocked Lateral Movement to LAN

The figure illustrates failed attempts to access the LAN from the compromised DMZ server. The firewall effectively blocks these requests, demonstrating the strength of network segmentation in preventing lateral movement and protecting internal resources.

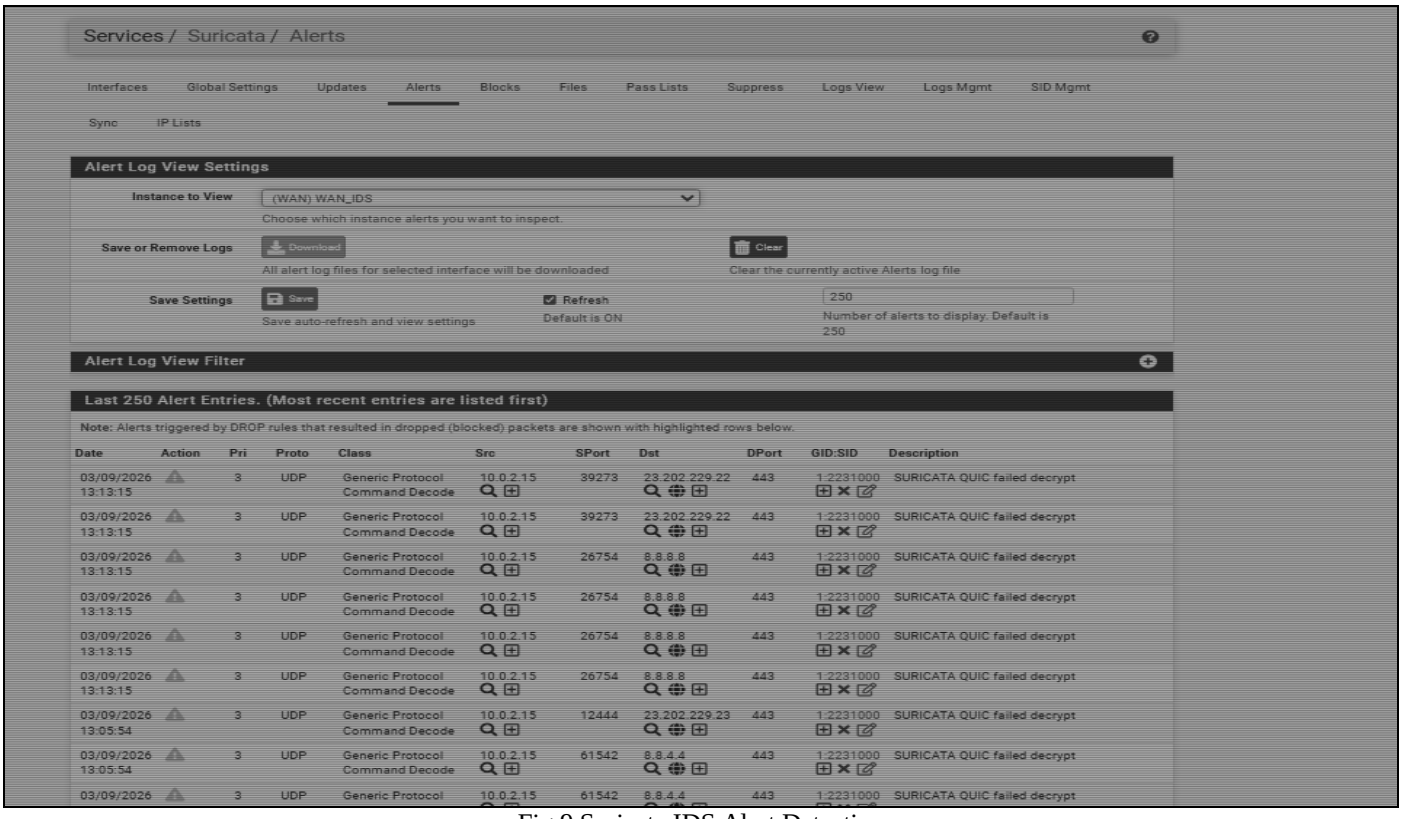

Fig 9 Suricata IDS Alert Detection

This figure displays alerts generated by the Suricata Intrusion Detection System in response to suspicious traffic. The alerts include detailed parameters such as source IP, destination IP, and protocol, enabling real-time identification of potential threats.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

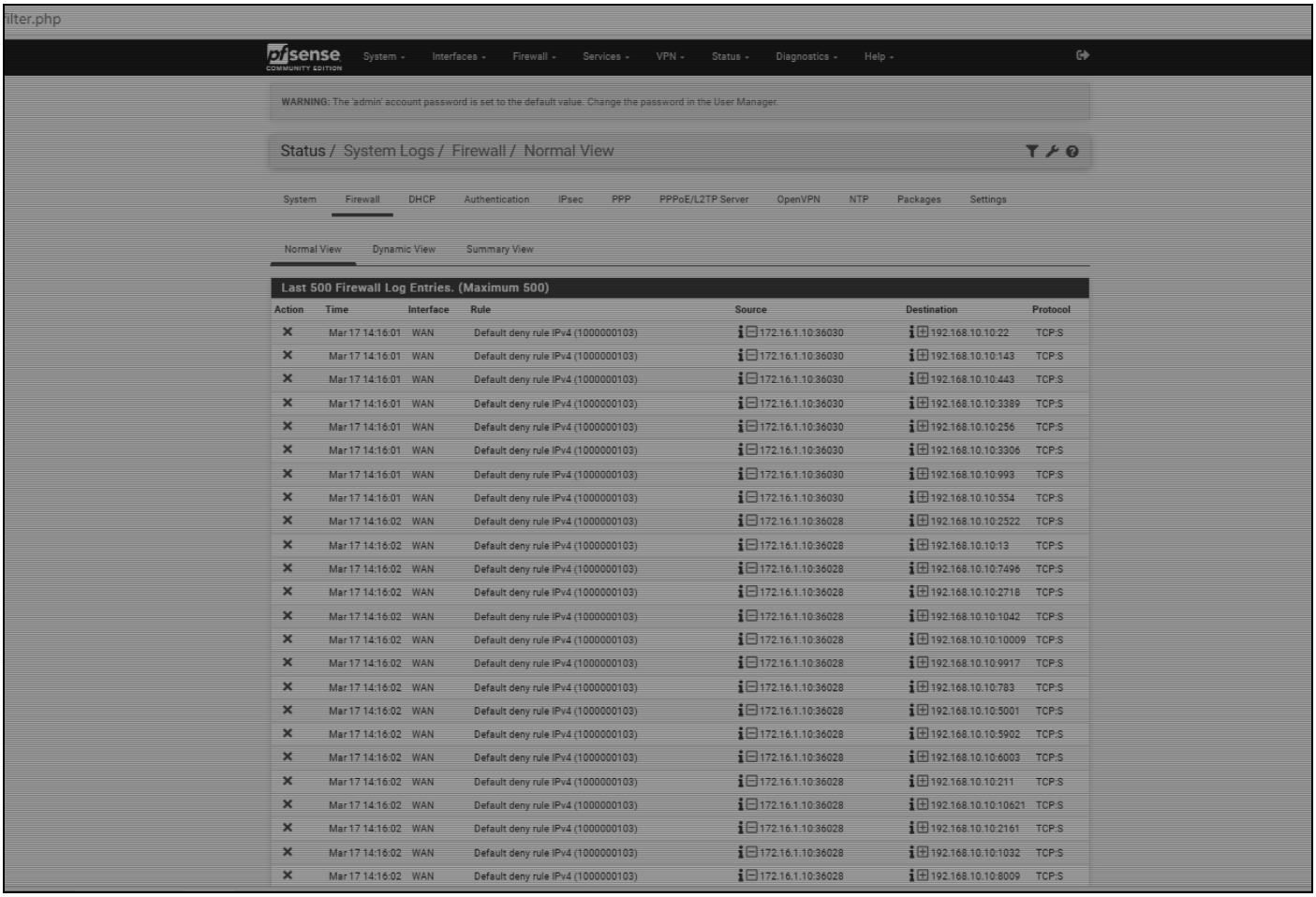

Fig 10 pfSense Firewall Traffic Logs

The figure shows firewall log entries capturing both permitted and denied traffic. These logs provide valuable insights into network activity, allowing administrators to trace attack patterns and verify the effectiveness of implemented security policies.

Overall, the results confirm that the proposed system not only detects multiple types of cyber-attacks but also effectively restricts unauthorized access through firewall enforcement and network segmentation. The integration of IDS and logging mechanisms enables comprehensive monitoring and analysis of security events.

VII. CONCLUSION

This work presents a practical framework for cyber-attack simulation and detection using a segmented WAN–DMZ–LAN network architecture. The system integrates a multihomed pfSense firewall with a Suricata Intrusion Detection System to monitor, detect, and control malicious activities across network segments. By implementing real-world attack scenarios such as SQL injection and command injection, the study demonstrates how vulnerabilities can be exploited in a controlled environment.

The results confirm that network segmentation, combined with strict firewall rules, effectively prevents unauthorized access to internal systems, even when the DMZ server is compromised. In addition, the IDS successfully detects suspicious traffic and generates alerts, while firewall logs provide detailed insights into network behavior. This combination enables comprehensive monitoring and analysis of cyber-attacks.

Overall, the proposed system provides a realistic and effective approach to understanding attack techniques and evaluating network security mechanisms. It highlights the importance of layered security, continuous monitoring, and log analysis in protecting modern network infrastructures.

REFERENCES

[1]. “Survey on Intrusion Detection Systems in Software-Defined Networking,” 2025.
[2]. L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computer Network Security", 2025.
[3]. W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson Education, 2017.
[4]. A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur, and J. Srivastava, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection," *SIAM International Conference on Data Mining*, 2003, pp. 25–36, doi: 10.1137/1.9781611972733.3.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1610

[5]. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, 2010, pp. 305–316, doi: 10.1109/SP.2010.25.
[6]. S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," *Technical Report No. 99-15*, Chalmers University, 2000.
[7]. S. Kumar and E. H. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection," *Proceedings of the 17th National Computer Security Conference*, 1994.
[8]. J. Zhang, M. Zulkernine, and A. Haque, "Random-Forests-Based Network Intrusion Detection Systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 38, no. 5, pp. 649–659, 2008, doi: 10.1109/TSMCB.2008.2001303.
[9]. Digininja, "Damn Vulnerable Web Application (DVWA)," [Online]. Available: http://www.dvwa.co.uk/.
[10]. The pfSense Project, "pfSense Documentation," [Online]. Available: https://www.pfsense.org/.
[11]. Open Information Security Foundation, "Suricata IDS Documentation," [Online] Available: https://suricata.io/.