PROJECT REPORT

Submitted By:

Fatima Munir

Shumaq Shoaib

Executive Summary

This report documents the integration of pfSense, Snort, and Wazuh to establish a layered intrusion detection and security monitoring solution. The goal was to design and validate a secure network architecture capable of detecting, blocking, and centrally monitoring malicious activity. The resulting system improves visibility, threat detection, and incident response capabilities.

Introduction

Modern networks face increasingly sophisticated cyber threats. To address these challenges, this project focuses on integrating three key components: - **pfSense:** Provides firewall and routing functionality. - **Snort:** Delivers intrusion detection and prevention. - **Wazuh:** Offers centralized log management and SIEM capabilities.

The integration demonstrates a cost-effective, open-source security solution suitable for academic and organizational environments.

System Architecture

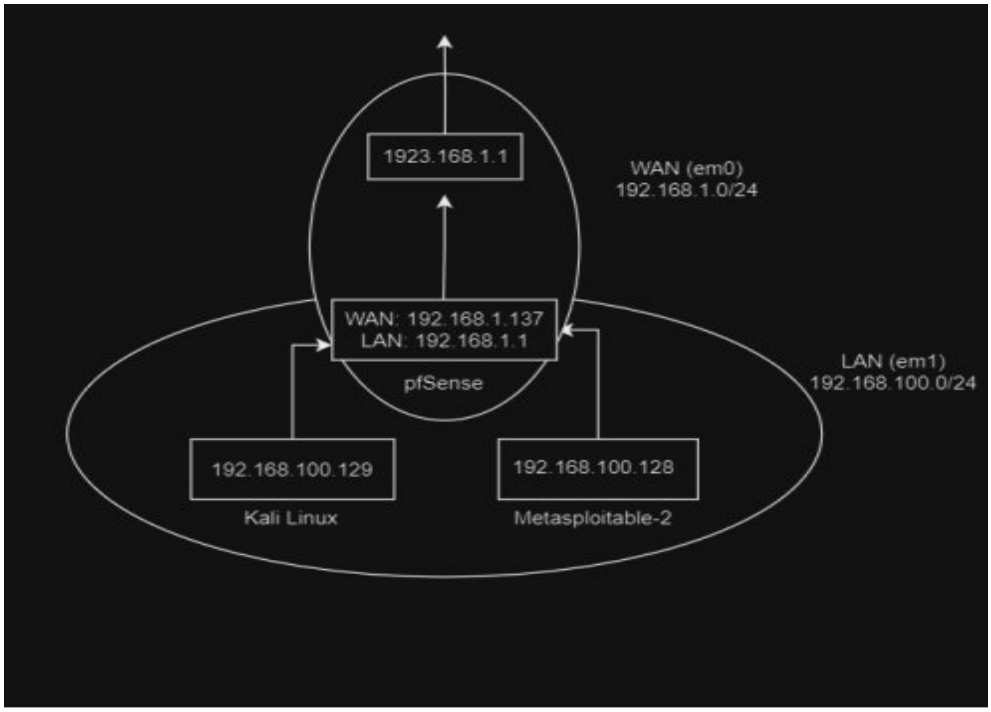
The network was set up using virtualized components:

a. **pfSense:** Configured with two adapters: Host-Only (internal network) and NAT (external network).

b. **Metasploitable-2:** Simulates a vulnerable internal host.

c. **Kali Linux:** Acts as an attacker and monitoring host.

Both internal hosts used pfSense as their default gateway. The topology ensures all traffic flows through pfSense for inspection.



Implementation Methodology

pfSense Configuration

- Installed pfSense with Auto (ZFS) partitioning and RAID 1+0.
- Configured LAN and WAN interfaces and verified IP assignments.
- Accessed pfSense web interface to:
    - Change default admin password.
    - Configure firewall rules, including blocking ICMP traffic on LAN.
    - Verified rule functionality via diagnostics and ping tests.

Snort Deployment

- Installed Snort package through pfSense.
- Configured rules using VRT/community sets via OinkCode.
- Monitored WAN interface with:
    - Preset botnet detection rules.
    - Automatic rule updates every 7 days.
    - Custom ICMP detection rule.
- Verified Snort operation by generating ICMP traffic and observing alerts.

Wazuh SIEM Integration

- Enabled SSH on pfSense.
- Installed Wazuh agent on pfSense after editing pkg.conf and configuring ossec.conf.
- Set up Wazuh manager on Ubuntu server following official documentation.
- Verified agent-server communication; logs and alerts appeared in Wazuh dashboard.

Testing and Validation

- Tested firewall ICMP blocking rules using ping requests.
- Verified Snort alerts for ICMP traffic.
- Validated Wazuh receiving and displaying Snort and pfSense logs in real-time.

Results and Discussion

The integrated setup provided:

1. Multi-layer defense with firewall, IDS/IPS, and SIEM.
2. Centralized monitoring of alerts.
3. Verified detection of malicious traffic and visibility into network activities.

Conclusion

The integration of pfSense, Snort, and Wazuh delivers a robust, open-source security solution. pfSense offers firewall and routing controls, Snort adds intrusion detection and prevention, and Wazuh centralizes monitoring and incident response. This architecture strengthens the network’s security posture

References

[1] pfSense Documentation: https://docs.netgate.com/pfsense/en/latest/
[2] Snort Documentation: https://www.snort.org/documents
[3] Wazuh Documentation: https://documentation.wazuh.com/current/quickstart.html