INSTITUTE FOR ADVANCED COMPUTING
AND
SOFTWARE DEVELOPMENT,
AKURDI, PUNE

DOCUMENTATION ON

"ENTERPRISE NETWORK DEFENSE & SECURE APPLICATION MONITORING''

PG-DITISS August 2025

SUBMITTED BY:

GROUP NO: 08

KUNJAN SHARMA (258418)

ROHIT GAJRE (258429)

MS. RUTUJA KULKARNI
PROJECT GUIDE

MR. ANIL SHARMA
CENTRE CO-ORDINATOR

ABSTRACT

Modern enterprises face increasingly sophisticated cyber threats such as distributed denial-of-service attacks, reconnaissance scans, malware propagation, and web application exploits. Traditional perimeter-based security approaches are no longer sufficient to protect critical assets deployed across complex networks.

This project presents the design and implementation of a **secure enterprise network defense architecture** based on **Network Defense Concepts (NDC)** and layered security principles. The architecture uses network segmentation through DMZ and internal zones, intrusion detection using Suricata, centralized monitoring through Wazuh SIEM, firewall enforcement, encryption, and controlled access between network segments.

A multi-tier password storage web application is deployed where the frontend server resides in the DMZ and remains internet-facing, while backend databases are placed in a protected internal network with no direct external connectivity. This design minimizes attack surface and mirrors real-world enterprise infrastructure.

Suricata is configured as a Network Intrusion Detection System (IDS) to detect reconnaissance scans, DoS/DDoS patterns, and OWASP Top 10 web attacks such as SQL injection and cross-site scripting. Wazuh collects logs from servers and IDS sensors, correlates security events, and provides Security Operations Center (SOC) style visibility through dashboards and alerts.

The project emphasizes **detection, monitoring, and response** rather than pure prevention, aligning with modern cyber-defense strategies adopted by large enterprises. The implementation demonstrates how layered security, network zoning, and centralized visibility can effectively defend enterprise environments against real-world cyber threats.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Sr. No.	Abbreviation	Full-Form
1.	IDS	Intrusion Detection System
2.	SIEM	Security Information and Event Management
3.	DMZ	Demilitarized Zone
4.	SOC	Security Operations Center
5.	NDC	Network Defense Concepts
6.	DoS	Denial of Service
7.	DDoS	Distributed Denial of Service
8.	OWASP	Open Web Application Security Project
9.	SQLi	SQL Injection
10.	XSS	Cross Site Scripting

LIST OF FIGURES

1. INTRODUCTION

With rapid digital transformation, enterprises increasingly depend on web-based services, cloud platforms, and interconnected digital infrastructures to support business operations. While these technologies improve efficiency and scalability, they also expand the organizational attack surface. Public-facing applications, misconfigured network services, outdated systems, and insecure coding practices create opportunities for adversaries to compromise systems, disrupt services, and steal sensitive information. As a result, securing enterprise networks has become a critical concern for modern organizations.

Cyber-attacks today typically follow a multi-stage lifecycle rather than isolated events. Adversaries begin with reconnaissance activities such as port scanning and service enumeration, followed by exploitation of discovered vulnerabilities. Successful compromise may then lead to privilege escalation, lateral movement across network segments, persistence mechanisms, and eventual data exfiltration or service disruption. Traditional perimeter-focused security approaches are often insufficient against such advanced threats, emphasizing the necessity for layered and continuously monitored defense strategies.

Network Defense Concepts (NDC) advocate a defense-in-depth methodology that combines multiple security controls across different layers of the infrastructure. These include network segmentation, strict access control, intrusion detection systems, centralized log monitoring, and structured incident response mechanisms. When deployed together, these measures significantly reduce the likelihood of successful attacks and enable earlier detection of malicious activity.

This project applies NDC principles to design and implement a secure enterprise laboratory network that reflects real-world production environments. The architecture incorporates a DMZ-based deployment for public-facing web applications and a protected internal network for sensitive database systems. Network intrusion detection is provided through Suricata IDS, while centralized event correlation and visualization are achieved using the Wazuh SIEM platform. Firewall enforcement and encrypted communication channels further strengthen the security posture by restricting inter-zone traffic and protecting data in transit.

1.1 Problem Statement

Traditional enterprise networks often depend primarily on perimeter firewalls to block unauthorized external access, while internal systems remain insufficiently monitored and loosely segmented. Such architectures are increasingly ineffective against modern cyber threats that exploit compromised endpoints to move laterally within networks, perform internal reconnaissance, and target application-layer vulnerabilities. The lack of visibility inside network boundaries allows attackers to operate undetected for extended periods, increasing the potential impact of breaches.

Several critical challenges arise from these traditional designs. Organizations frequently fail to implement proper separation between public-facing services and sensitive internal resources, exposing critical assets if perimeter defenses are bypassed. The absence of centralized logging and event correlation makes it difficult for security teams to identify coordinated attacks occurring across multiple systems. Limited monitoring of east–west traffic within internal networks further restricts detection of lateral movement and insider threats. Additionally, delayed alerting mechanisms and the lack of Security Operations Center–style investigation capabilities hinder timely incident response and root-cause analysis.

This project addresses these limitations by implementing a comprehensive network defense architecture based on Network Defense Concepts. The proposed solution introduces multi-zone network segmentation to isolate critical systems, deploys network-based intrusion detection sensors for continuous traffic inspection, and centralizes log collection through a SIEM platform. Security alerts are correlated to enable faster detection and prioritization of incidents, while SOC-style dashboards and workflows are demonstrated to support effective monitoring and investigation. Through this approach, the project seeks to enhance enterprise visibility, detection capability, and response readiness against real-world cyber threats.

2. LITERATURE SURVEY

Enterprise network-security strategies have progressively evolved from traditional perimeter-centric models toward defense-in-depth architectures that employ multiple, layered security controls. Demilitarized Zone (DMZ) networks have long been adopted to separate internet-facing services from sensitive internal systems, thereby reducing direct exposure of critical assets and limiting the impact of perimeter breaches.

Intrusion Detection Systems (IDS) such as Snort and Suricata play a crucial role in monitoring network traffic for malicious signatures and anomalous behaviors. Among these, Suricata has gained prominence due to its multi-threaded packet-processing capabilities, deep protocol inspection features, and support for comprehensive rule sets such as Emerging Threats. These characteristics enable real-time detection of reconnaissance scans, denial-of-service patterns, and web-application attacks at the network layer.

Security Information and Event Management (SIEM) platforms—including Splunk, the ELK stack, and Wazuh—provide centralized log aggregation, correlation, and visualization across diverse systems. Wazuh, in particular, has emerged as a popular open-source SIEM/XDR solution that combines host-based intrusion detection, vulnerability assessment, file-integrity monitoring, and automated response mechanisms. Such platforms allow security teams to analyze events holistically rather than in isolation, significantly improving situational awareness.

Research conducted by the OWASP Foundation, particularly through the OWASP Top 10 project, identifies the most prevalent web-application vulnerabilities exploited in real-world environments, including SQL injection, broken authentication mechanisms, and cross-site scripting. These vulnerabilities continue to represent a substantial portion of enterprise security incidents, emphasizing the need for layered monitoring and detection controls beyond simple firewall filtering.

Despite the availability of these technologies, many organizations struggle to integrate them into a unified and operationally efficient security architecture. IDS sensors, SIEM platforms, firewall policies, and segmentation controls are often deployed in isolation, reducing their overall effectiveness. .

3. METHODOLOGY

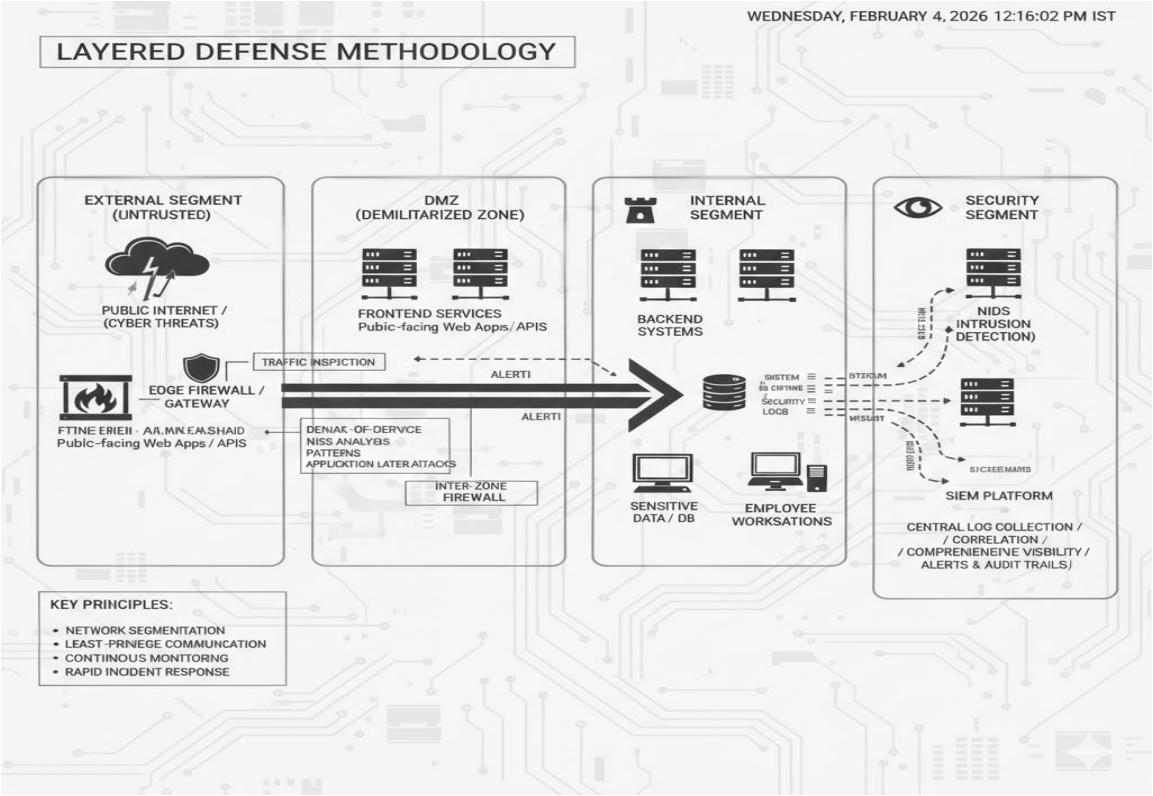


Figure 1: Layered Defense Methodology

The project follows a layered defense methodology based on Network Defense Concepts to secure enterprise infrastructure against modern cyber threats. The network is divided into multiple zones—external, DMZ, internal, and security segments—to isolate public-facing services from critical backend systems and limit lateral movement in case of compromise.

Network-based Intrusion Detection Systems inspect traffic between zones to identify reconnaissance activity, denial-of-service attempts, and application-layer attacks. System, application, and security logs are centrally collected and correlated through a SIEM platform, providing comprehensive visibility across the environment.

Secure deployment practices place frontend services in the DMZ and sensitive data within the internal network, enforcing least-privilege communication between tiers. Continuous monitoring through dashboards, alerts, and audit trails enables security teams to quickly detect suspicious activity and respond to incidents.

3.1. SYSTEM ARCHITECTURE

The proposed secure enterprise defense architecture is organized into four primary network zones to enforce isolation and defense-in-depth principles. The **External Network** represents the internet and attacker-simulation environment used for testing reconnaissance and exploitation attempts. The **DMZ Network** hosts the web frontend server and is intentionally exposed to external access while being strictly separated from internal resources. The **Internal Network** contains the database server, which stores sensitive information and has no direct connectivity to the internet. The **Security Zone** houses the Suricata Intrusion Detection System and the Wazuh SIEM platform, responsible for monitoring, logging, and analysis.

Firewalls positioned between each zone enforce strict allow-list–based access-control policies. Only explicitly authorized traffic—such as HTTP/HTTPS connections from the external network to the DMZ and database queries from the DMZ to the internal network—is permitted, while all other communication paths are denied by default. This approach minimizes the attack surface and limits lateral movement if a system becomes compromised.

Suricata is deployed as a passive network sensor by connecting it to mirrored network interfaces that capture traffic flowing between the DMZ and internal segments. The IDS inspects packet payloads and protocol behavior to detect reconnaissance scans, denial-of-service attempts, and web-application attacks, generating alerts for suspicious activity in real time.

Wazuh agents are installed on the web server, database server, and IDS sensor to forward operating-system logs, application events, and security alerts to the central Wazuh manager. The SIEM correlates these inputs to create consolidated incident views and presents them through SOC-style dashboards for analyst investigation.

All communication between components—including agent-to-manager telemetry, backend application connections, and administrative access—is protected using Transport Layer Security (TLS). Encryption ensures confidentiality and integrity of sensitive data traversing the network and prevents interception or tampering by unauthorized parties.

4. REQUIREMENT SPECIFICATION

4.1. SOFTWARE REQUIREMENTS

- Ubuntu Server 22.04
- Apache
- MySQL
- Suricata IDS
- Wazuh SIEM
- iptables
- OpenSSL
- Kali Linux (attack simulation tools)

4.2. HARDWARE REQUIREMENTS

- Quad-core processor
- 16 GB RAM minimum
- 100 GB storage
- Multiple VMs for segmentation
- VMware

5. WORKING

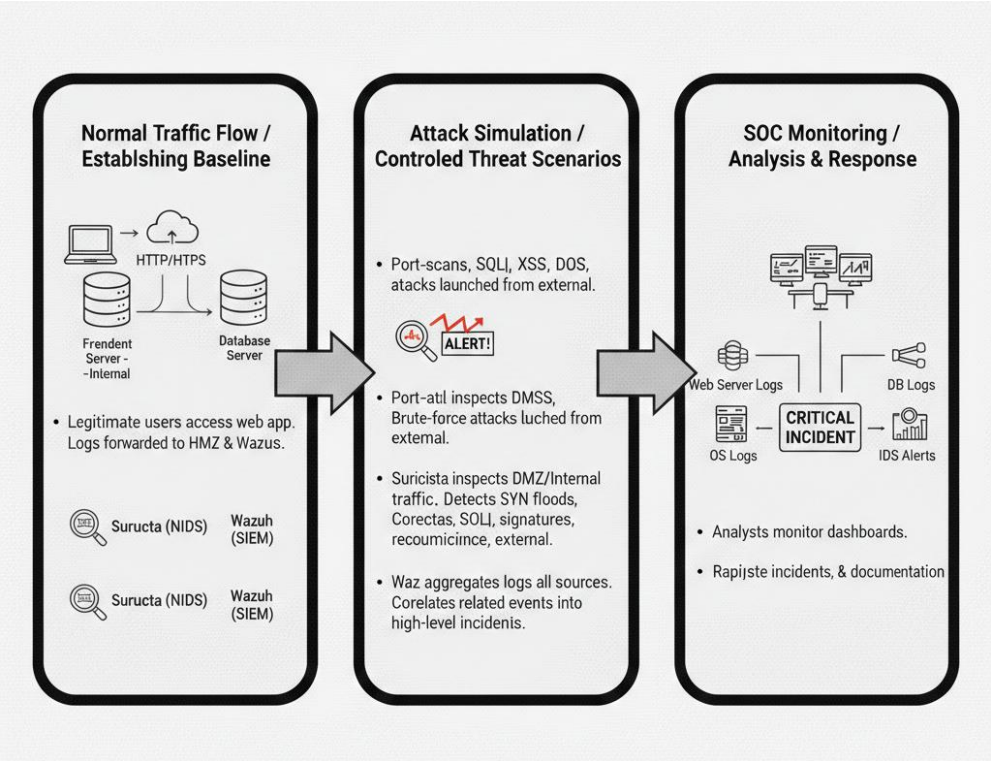


Figure 2: Work Flow

Phase 1: Normal Traffic Flow

During normal operations, legitimate users access the web application hosted in the DMZ over HTTP and HTTPS protocols. The frontend server communicates with the internal database server only through firewall-approved ports, ensuring controlled backend connectivity. Network traffic and system logs are simultaneously forwarded to Suricata and Wazuh to establish a baseline of expected behavior.

Phase 2 – Attack Simulation

Controlled attacks are launched from an external attacker machine to evaluate the resilience of the architecture. These include port-scanning activities, SQL injection attempts, cross-site scripting payloads, denial-of-service traffic, and brute-force login attempts. The scenarios are designed to realistically represent common enterprise threat patterns.

Phase 3 – Detection

Suricata continuously inspects packets flowing through the DMZ and internal network segments to identify malicious activity. It detects SYN flood patterns, SQL injection signatures, reconnaissance scans, and malformed requests at the network layer. Generated alerts provide immediate visibility into potential security incidents

Phase 4 – Correlation

Wazuh aggregates logs from the web server, database server, IDS sensors, and operating systems across all zones. Related events are correlated into higher-level incidents, reducing noise and highlighting coordinated attack behavior. Centralized alerting and severity classification support efficient incident triage.

Phase 5 – SOC Monitoring

Security analysts observe dashboards, timelines, and threat-visualization panels through the SIEM interface. Detected incidents are investigated using packet data and log trails to determine impact and root cause. The SOC-style monitoring workflow enables rapid response, documentation, and escalation when required.

6. IMPLEMENTATION

The laboratory environment was implemented using multiple virtual machines to accurately simulate a real-world enterprise network. Separate systems were deployed for the DMZ web server, internal database server, Suricata IDS sensor, Wazuh SIEM manager, and an attacker simulation machine. Each virtual machine was installed with a hardened Linux operating system and connected to isolated virtual networks representing the external, DMZ, internal, and security zones. Static IP addressing was used to maintain consistent routing and monitoring across all components.

Firewall controls were enforced at network boundaries using Linux-based filtering mechanisms such as **iptables** or **nftables** with a default-deny policy. Only essential communication paths were permitted, including inbound HTTP and HTTPS traffic from the internet to the DMZ web server and database connections from the DMZ to the internal server on a specific port. Outbound connections from the internal network to the internet were completely blocked to prevent data exfiltration and unauthorized command-and-control traffic.

Suricata was deployed as a passive network intrusion detection sensor by attaching it to mirrored network interfaces so that it could inspect traffic flowing between the network zones without affecting performance. The IDS was configured with the **Emerging Threats** ruleset to detect common reconnaissance scans, denial-of-service patterns, and web-application attacks. In addition to these default signatures, custom detection rules were created to identify SQL injection strings, cross-site scripting payloads, and anomalous HTTP requests targeting the deployed application.

The Wazuh platform was implemented using a centralized manager and distributed agent model. Wazuh agents were installed on every host—including the DMZ server, database server, and IDS sensor—to collect operating-system logs, web-server access records, authentication events, and file-integrity information. File Integrity Monitoring was enabled on sensitive directories, and active response modules were configured to automatically block malicious IP addresses or terminate suspicious processes when high-severity alerts were generated.

Secure communication between all servers and security components was ensured through the use of **Transport Layer Security (TLS)** encryption. Digital certificates were generated and deployed for Wazuh agent-to-manager communication, web-server HTTPS traffic, and backend database connections. This prevented interception or manipulation of sensitive data and ensured confidentiality and integrity of both application traffic and security telemetry across the enterprise network.

Figure 3:SQL Injection

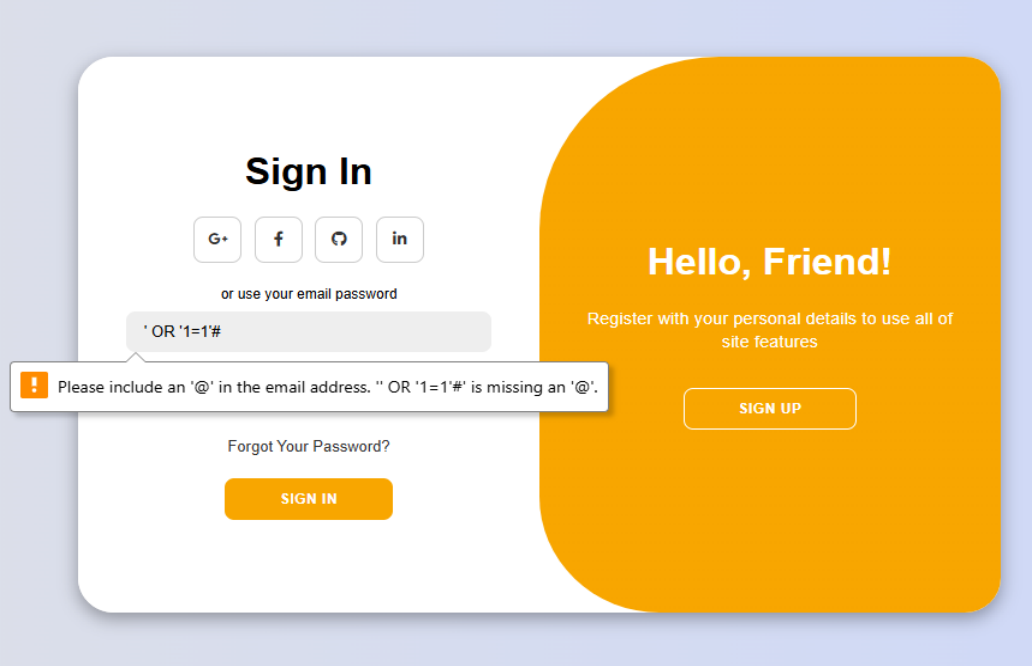


Figure 4: DataBase

```
MariaDB [user_db]> select * from users;
+----+--------+----------------+--------------------------------------------------------------+
| id | name   | email          | password                                                     |
+----+--------+----------------+--------------------------------------------------------------+
|  1 | Kunjan | kunj@gmail.com  | $2y$10$zzhJcqH.vvjsPYQ/E4q6h.2o0lGDE46XY1A/EAxDy1YckBI.XOyzW |
|  2 | Rohit  | rohit@gmail.com | $2y$10$0UgHEp8Javi8VsK3X9w6AuuG0mGaOqiX6ayDLLSZT2M/ZjJThOtzq |
+----+--------+----------------+--------------------------------------------------------------+
2 rows in set (0.000 sec)
```

Figure 5: Wazuh Dashboard

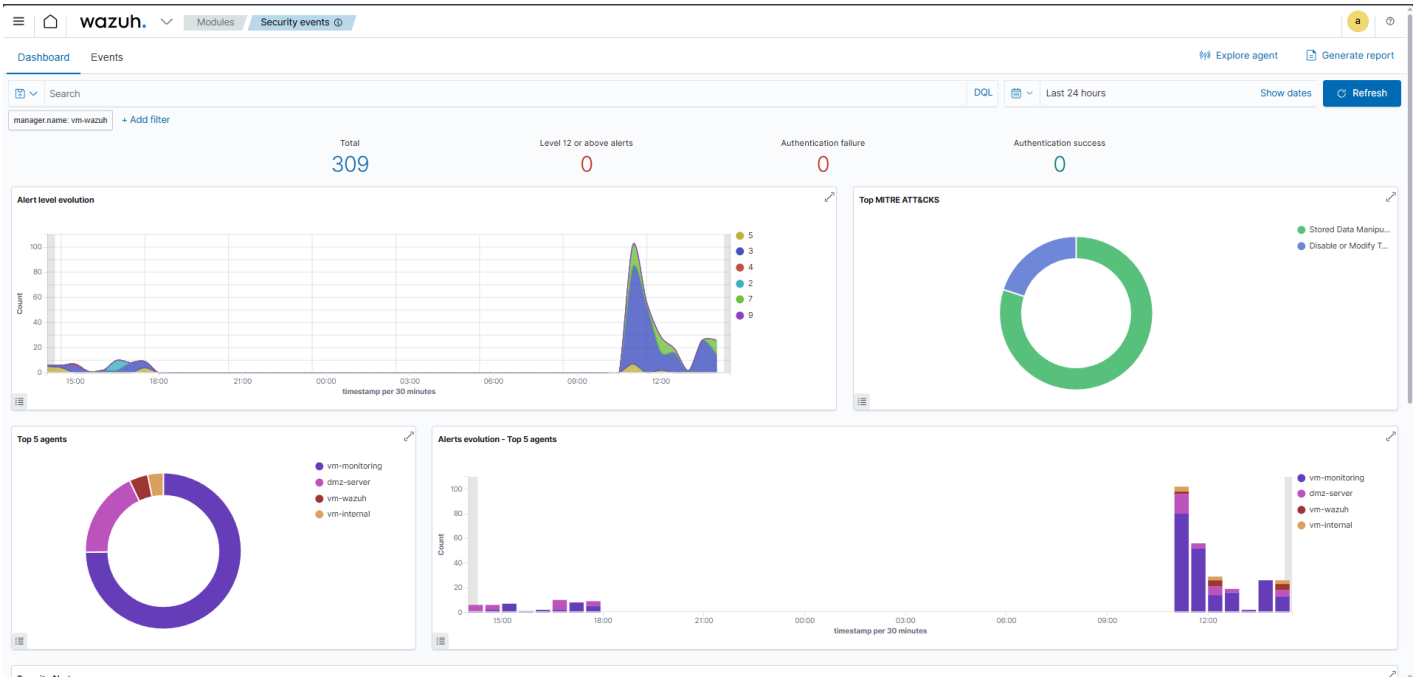


Figure 6: Alerts

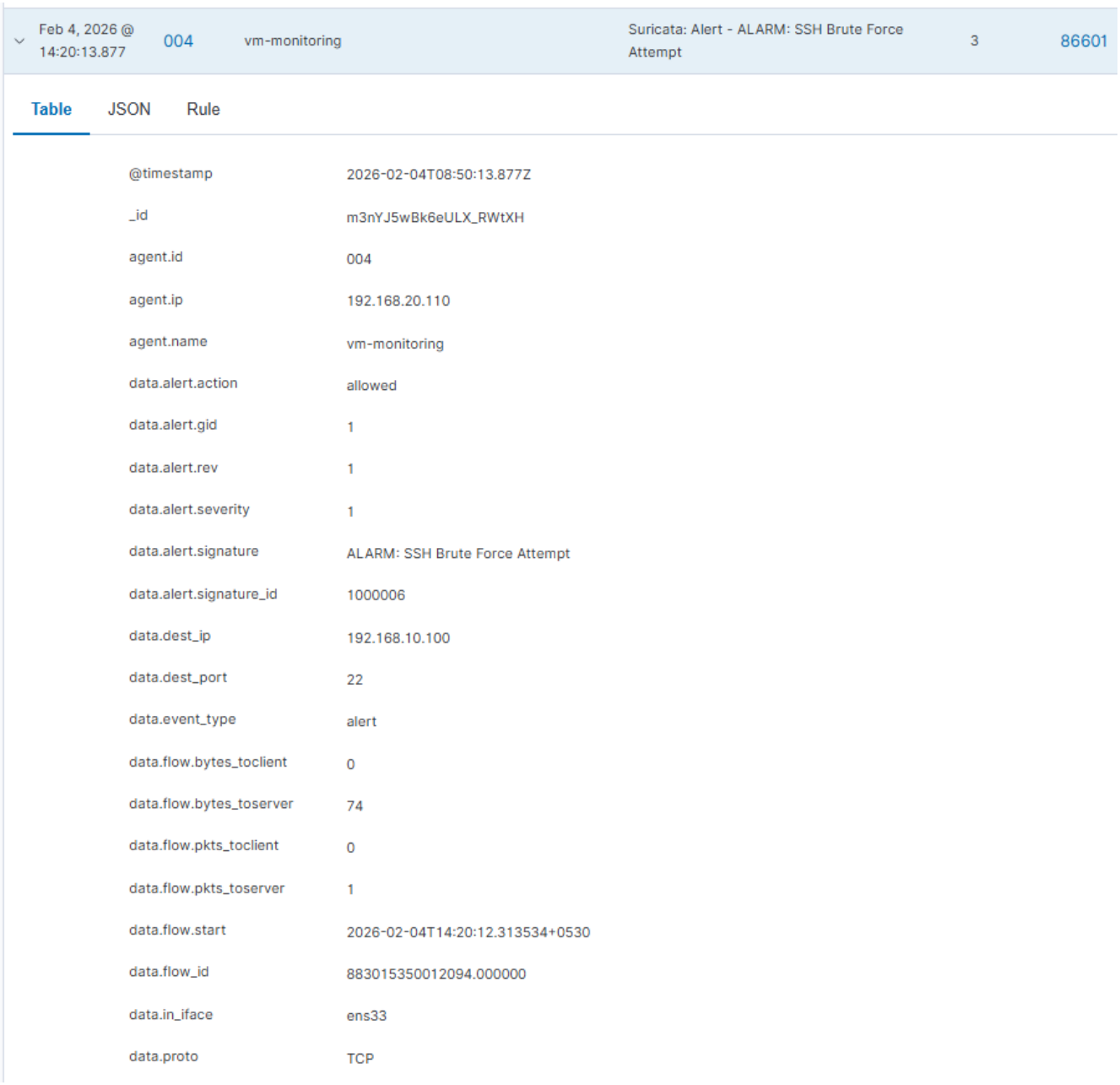
Feb 4, 2026 @ 14:20:13.877	004	vm-monitoring	Suricata: Alert - ALARM: SSH Brute Force Attempt	3	86601
Feb 4, 2026 @ 14:20:13.874	004	vm-monitoring	Suricata: Alert - ALARM: Nmap Scan Detected	3	86601
Feb 4, 2026 @ 14:15:29.810	004	vm-monitoring	Host-based anomaly detection event (rootcheck).	7	510
Feb 4, 2026 @ 14:15:29.768	004	vm-monitoring	Host-based anomaly detection event (rootcheck).	7	510
Feb 4, 2026 @ 14:15:29.449	001	dmz-server	Listened ports status (netstat) changed (new port opened or closed).	7	533
Feb 4, 2026 @ 14:15:29.374	001	dmz-server	Listened ports status (netstat) changed (new port opened or closed).	7	533

Figure 7: Bruteforce Attack

```
┌──(kali㉿kali)-[~]
└─$ hydra -l shuhari -P /usr/share/wordlists/rockyou.txt ssh://192.168.10.100
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-04 14:21:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.resto
re
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.10.100:22/
[ERROR] could not connect to ssh://192.168.10.100:22 - Connection refused
```

Figure 8:Bruteforce Alert in Wazuh



\

Figure 9: Fail2ban

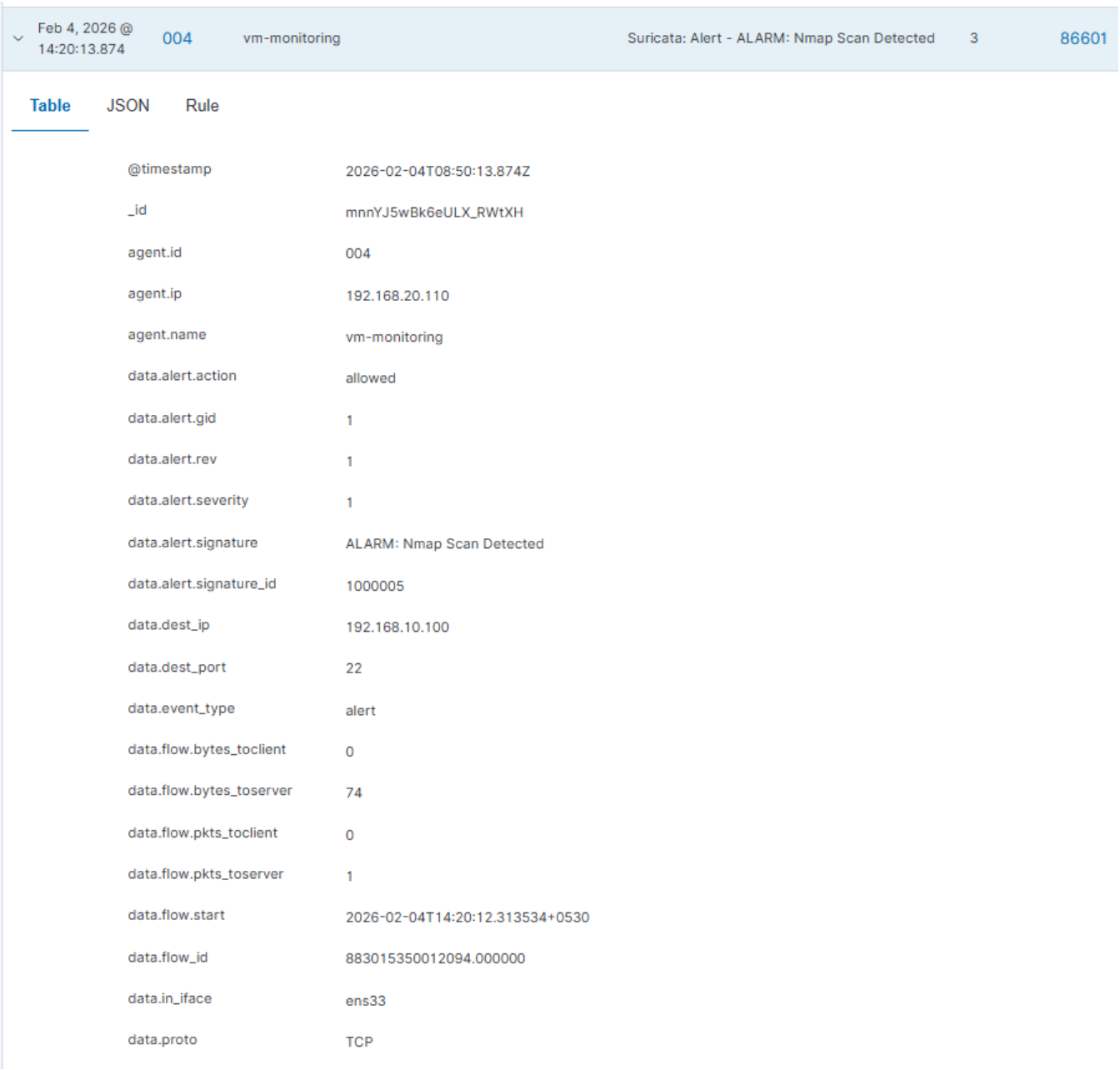
```
shuhari@dmz-server:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     14
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.10.133
```

Figure 10:Nmap Scanning

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.100
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-04 14:19 IST
Nmap scan report for 192.168.10.100
Host is up (0.00069s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:CC:B9:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```

Figure 11: Nmap Alert in Wazuh



7. APPLICATIONS

The proposed secure enterprise network defense architecture can be extensively utilized in **Security Operations Center (SOC) training laboratories**, where analysts gain practical experience in monitoring real-time dashboards, correlating alerts from multiple security controls, and responding to simulated cyberattacks. By recreating realistic attack scenarios such as reconnaissance scans, web-application exploitation, and denial-of-service attempts, the environment enables trainees to understand detection workflows and escalation procedures followed in professional SOC operations. It also serves as an effective platform for **network-defense demonstrations**, allowing instructors and security teams to visually explain layered-security concepts including DMZ deployment, firewall segmentation, intrusion-detection monitoring, and centralized log collection.

The environment further supports **incident-response exercises**, enabling teams to rehearse the full lifecycle of an incident—from initial detection and containment to forensic investigation and recovery. Security practitioners can analyze packet captures, review correlated SIEM alerts, and practice isolating compromised hosts using firewall or active-response mechanisms. In academic institutions and professional training programs, the project functions as a comprehensive platform for **cybersecurity education**, offering students hands-on exposure to enterprise-grade tools such as Suricata and Wazuh while reinforcing theoretical concepts such as defense-in-depth, network zoning, and secure system design.

In addition, the architecture is well suited for **blue-team simulations and compliance-auditing laboratories**, where defensive teams can evaluate detection coverage against known attack techniques and frameworks such as MITRE ATT&CK. Auditors and security assessors can verify logging completeness, access-control enforcement, encryption of sensitive communications, and network-isolation policies in a controlled environment. These capabilities make the proposed system valuable not only for training and experimentation but also for validating organizational security controls and improving overall enterprise cyber-resilience.

8. ADVANTAGES & DISADVANTAGES

Advantages

a) Defense-in-Depth
The architecture applies layered security controls including network segmentation, firewall enforcement, intrusion detection, encryption, and centralized monitoring, reducing the impact of any single point of failure.

b) Real Enterprise-Like Design
The use of DMZ and internal network separation closely resembles production enterprise environments, making the project suitable for realistic security testing and training.

c) SOC Visibility
Centralized logging and correlation through Wazuh provide Security Operations Center–style dashboards and alerts, enabling rapid detection and investigation of incidents.

d) Open-Source Tools
The solution relies on widely adopted open-source platforms such as Suricata and Wazuh, lowering deployment cost while maintaining professional-grade capabilities.

e) Detection of Multiple Attack Classes
The IDS and SIEM combination enables identification of reconnaissance scans, DoS traffic, and OWASP Top 10 web attacks across different layers of the network.

f) Modular and Extensible
Each component can be independently upgraded or replaced, allowing easy integration of additional sensors, automation scripts, or threat-intelligence feeds.

Disadvantages

a) Complex Setup
Deploying multiple network zones, IDS sensors, and SIEM agents requires careful planning and configuration, which may be challenging for beginners.

b) High VM Resource Usage
Running several virtual machines and real-time packet inspection consumes significant CPU, memory, and storage resources.

c) Rule Tuning Required
IDS signatures and SIEM correlation rules must be continuously adjusted to minimize noise and adapt to changing threat patterns.

d) False Positives
Signature-based detection may occasionally flag legitimate traffic as malicious, requiring analyst verification.

e) Maintenance Overhead
Regular updates of operating systems, detection rules, certificates, and log pipelines are necessary to maintain effectiveness and security.

9. CONCLUSION

This project successfully demonstrates the practical implementation of Network Defense Concepts using open-source security technologies to protect enterprise infrastructures. By integrating network segmentation, strict firewall enforcement, intrusion detection through Suricata, and centralized event correlation using the Wazuh SIEM platform, the proposed system delivers enhanced visibility into malicious activities targeting both publicly exposed web applications and protected internal servers.

The architecture closely mirrors real-world Security Operations Center environments and emphasizes a detection-centric security strategy rather than relying solely on preventive controls at the perimeter. Experimental results and simulated attack scenarios highlight how layered defenses combined with continuous monitoring significantly improve an organization's ability to rapidly identify threats, analyze attack patterns, and initiate appropriate response actions.

Future enhancements to the system may include integration with Security Orchestration, Automation, and Response platforms to automate incident handling and containment procedures. Additional improvements could involve incorporating external threat-intelligence feeds for enriched alert context, deploying automated blocking mechanisms at network boundaries, and applying machine-learning-based anomaly-detection techniques to complement signature-based detection. These advancements would further strengthen the resilience and operational maturity of the proposed enterprise cyber-defense architecture.

10. REFERENCES

1. **Suricata User Guide** – Official documentation for Suricata IDS/NIDS, including installation, configuration, and rules.
   Available at: https://docs.suricata.io/
2. **Suricata Official Documentation Hub** – Main Suricata docs and quick-start pages maintained by the Open Information Security Foundation.
   Available at: https://suricata.io/documentation/
3. **Wazuh SIEM Documentation – Network IDS Integration** – Guide on integrating Suricata with Wazuh for centralized log and alert analysis.
   Available at: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html
4. **OWASP Top Ten Web Application Security Risks** – Official project page summarizing the most critical web application vulnerabilities.
   Available at: https://owasp.org/www-project-top-ten/
5. **NIST Cybersecurity Framework & Guidelines** – U.S. National Institute of Standards and Technology foundational cybersecurity guidelines (NIST publications).
   Available at: https://www.nist.gov/cyberframework (and related publications such as NIST SP 800-53).
6. **Emerging Threats Ruleset for Suricata** – Rules repository and downloads for open Suricata signatures used for threat detection.
   Available at: https://rules.emergingthreats.net/open/ (Suricata rules download site)
7. **Linux / Netfilter Firewall Documentation** – Official documentation for Linux firewall tools such as iptables/nftables.
   Available at: https://www.netfilter.org/ and man pages for *iptables* / *nftables*.
8. **MITRE ATT&CK Framework** – Authoritative threat-taxonomy and behavioral modeling framework for cyber adversary tactics and techniques.
   Available at: https://attack.mitre.org/
9. **ISO/IEC 27001 Information Security Management Standard** – International standard for establishing, implementing, maintaining, and improving an ISMS (may require purchase).
   Available at: https://www.iso.org/standard/27001.html