WEST UNIVERSITY OF TIMIŞOARA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
BACHELOR STUDY PROGRAM: COMPUTER SCIENCE IN ENGLISH

BACHELOR THESIS

SUPERVISOR:
Lect. Dr. Cira Cristian

GRADUATE:
Farkas Andrei

TIMIŞOARA
2025

WEST UNIVERSITY OF TIMIŞOARA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
BACHELOR STUDY PROGRAM: COMPUTER SCIENCE IN ENGLISH

SIEM Based Thread Detection and Response for Enterprise Infrastructures

SUPERVISOR:
Lect. Dr. Cira Cristian

GRADUATE:
Farkas Andrei

TIMIŞOARA
2025

Abstract

This thesis describes how to use open source security tools and virtualization technologies to develop and implement a complete enterprise cybersecurity infrastructure. The project shows how to build a multitier network architecture using the GNS3 virtualization platform that includes automated incident response capabilities, centralized security monitoring, and sophisticated threat detection.

The network is separated into four security zones, each connected by a centralised pfSense firewall. The LAN zone (192.168.1.0/24) maintains internal systems and attack testing, while the Management zone (192.168.2.0/24) separates the SIEM infrastructure for security reasons. The DMZ zone (192.168.3.0/24) contains web services that need internet access, but the VPN zone (192.168.4.0/24) mimics distant connections and external dangers. To make things more realistic, pfSense connects to an OSPF router (10.10.10.2) for dynamic routing and to the internet using NAT1.

In this project, an open-source SIEM platform is used to collect logs, detect threats in real time, and automatically trigger response actions. Built around the MITRE ATT&CK framework, custom detection rules were developed to provide deeper visibility into attacker behaviour. These rules help identify common techniques such as network reconnaissance (T1046), brute-force password guessing (T1110.001), and denial-of-service attacks (T1499.001).

This project uses well-known security tools to simulate a number of realistic attacks. Network scans were conducted using Nmap, brute-force login attempts were tried using Hydra, common web vulnerabilities were examined using Nikto, and denial-of-service attacks were simulated using hping3. These tests were conducted to demonstrate how the system responds to actual threats in practice and to verify that the detection rules function as expected.

Key achievements include successful detection of all simulated attacks, automated IP blocking for identified threats, integration of host-based and network-based monitoring, and creation of a reproducible blueprint for security operations training. The project proves that enterprise-grade security capabilities can be implemented using exclusively open-source tools, making advanced security operations accessible for education and small organizations.

Keywords: Cybersecurity, SIEM, Network Security, Threat Detection, Wazuh, pfSense, GNS3, MITRE ATT&CK, Incident Response, Open Source Security

Contents

List of Figures

Chapter 1

Introduction and State of the Art

Modern cybersecurity challenges demand monitoring solutions that provide real-time visibility across complex organisational networks. As traditional perimeter-based defences fall short against increasingly sophisticated attackers, organisations must adopt integrated strategies that combine network segmentation, centralised monitoring, and automated threat detection. This chapter lays the foundation for building a virtualised cybersecurity environment using open-source technologies. The sections that follow outline the current threat landscape, define the research objectives, explore the development of security monitoring systems, and present the implementation methodology that guided this project.

1.1 Motivation and Research Context

Cybersecurity has become a critical concern for modern enterprises due to the increasing complexity of digital infrastructures and the evolving sophistication of cyber threats. Organizations require secure, segmented network architectures capable of monitoring, detecting, and responding to a wide variety of attacks in real time. However, practical hands-on environments for cybersecurity training and validation remain scarce and expensive.

Traditional perimeter-based defences are no longer sufficient to tackle the complex and dynamic assault strategies present in the new threat landscape. Monitoring systems that provide awareness across many network zones and possible attack surfaces are necessary to combat Advanced Persistent Threats[1] (APTs), insider attacks, and zero-day vulnerabilities[2]. In this regard, obtaining complete security awareness and efficient threat detection now heavily relies on Security Information and Event Management[3] (SIEM) systems.[16].

[1]APT: Advanced Persistent Threat refers to prolonged and targeted cyberattacks where attackers gain access to networks and remain undetected for extended periods.

[2]Zero-day exploits: Attacks that take advantage of previously unknown vulnerabilities in software or systems before developers have had time to create and distribute security patches.

[3]SIEM: Security Information and Event Management systems that aggregate and analyze security data from multiple sources to provide real-time threat detection and response capabilities.

1.2 Problem Statement and Research Objectives

This thesis uses virtualised environments[4] and open-source technologies to mimic a realistic enterprise-level cybersecurity architecture. The configuration is intended to provide complete security monitoring capabilities while remaining usable and accessible for research and educational purposes.

This research tackles several important challenges in both cybersecurity education and practical implementation. First, the high cost of commercial security tools creates a barrier for smaller organisations and academic institutions that want to deploy full-scale monitoring solutions. Second, the complexity of modern enterprise security architectures makes it difficult to understand how different components work together and how effective they are against specific attack types. Third, the lack of realistic environments for simulating attacks limits both the validation of security setups and the hands-on training of future security professionals.

The infrastructure development objectives include:

1. Support for segmented, zone-based network design[5] that mirrors enterprise architectures

2. Integration of a central security gateway using pfSense[6] [8] for traffic control and monitoring

3. Implementation of secure remote access through VPN[7] infrastructure [10]

4. Deployment of a centralized SIEM platform using Wazuh[8] for comprehensive security monitoring

5. Realistic attack simulation and validation of detection capabilities across multiple threat vectors

1.3 Project Scope and Implementation Strategy

The scope of this thesis covers the full lifecycle of building a cybersecurity infrastructure — from the initial network design to simulating attacks and refining the response mechanisms. The focus is on practical, hands-on implementation using widely adopted tools and methods that reflect real-world enterprise environments.

[4]Virtual environments: Simulated computing environments that run on physical hardware but operate as separate, isolated systems, enabling multiple operating systems and applications to run on a single physical machine.

[5]Zone-based network design: A network architecture approach that divides the network into distinct security zones, each with specific security policies and access controls based on the sensitivity and function of the systems within that zone.

[6]pfSense: An open-source firewall and router platform based on FreeBSD that provides enterprise-grade networking and security features including packet filtering, traffic shaping, and VPN capabilities.

[7]VPN: Virtual Private Network technology that creates encrypted tunnels for secure remote access to organizational networks over public internet connections.

[8]Wazuh: An open-source security monitoring platform that provides intrusion detection, compliance monitoring, and incident response capabilities based on the OSSEC framework.

Using open-source technologies that offer enterprise-level capabilities while yet being appropriate for educational usage, this project adopts a practical implementation strategy. GNS3[9][4] for simulating network environments, Kali Linux[10][9] for carrying out attack scenarios, pfSense for firewall administration and routing, and Wazuh for security monitoring and event correlation are important components.

Realistic assault scenarios that mirror prevalent threat patterns in actual business settings are the methodology's main focus. Among the simulated attacks are denial-of-service efforts using hping3[11][12], network reconnaissance using Nmap[12][5], web application vulnerability scans using Nikto[13][2], and brute-force credential attacks[14] using Hydra[15][15].

1.4 Cybersecurity Challenges in Enterprise Networks

Due in large part to their dispersed architecture, dependence on cloud services, and the explosive expansion of mobile and Internet of Things devices, modern corporate networks face an ever-increasing array of security concerns. Once the cornerstone of network security, perimeter-based defences are no longer effective against sophisticated attacks that use trusted connections, encrypted channels, and genuine credentials to pass unnoticed across systems.

Modern businesses now have an attack surface that extends well beyond conventional network borders. Attackers can take advantage of the many possible access points that are introduced by cloud platforms, remote work arrangements, and third-party integrations. Multiple attack routes are frequently combined by advanced threats, making detection and response much more difficult.

Lateral movement[16] inside networks, when hackers use compromised credentials to access further systems and increase their privileges. Polymorphic malware and zero-day vulnerabilities are challenging for standard signature-based detection techniques to address since they are constantly evolving to evade detection. The volume

[9]GNS3: Graphical Network Simulator that enables complex network topologies using real network operating systems in virtual environments without requiring physical hardware.

[10]Kali Linux: A Debian-based Linux distribution specifically designed for penetration testing and security auditing, containing hundreds of security tools for testing network security, web applications, and system vulnerabilities.

[11]hping3: Network tool able to send custom TCP/IP packets and was designed as a command line oriented TCP/IP packet assembler/analyzer for network testing and security auditing.

[12]Nmap: Network exploration tool and security scanner used for network discovery and security auditing, capable of determining what hosts are available on the network and what services they offer.

[13]Nikto: Open source web server vulnerability scanner that performs comprehensive tests against web servers for multiple security issues including dangerous files, outdated server software, and security misconfigurations.

[14]Credential attacks: Attempts to gain unauthorized access to systems by obtaining or guessing user credentials such as usernames and passwords through various methods including brute force, dictionary attacks, or social engineering.

[15]Hydra: A parallelized login cracker that supports numerous protocols and is commonly used for testing authentication security through dictionary and brute-force attacks.

[16]Lateral movement: The techniques that attackers use to progressively move through a network in search of key assets and data after gaining initial access.

of security events generated by modern infrastructure usually overwhelms security staff, leading to alert fatigue and the neglect of critical circumstances.

1.5 Security Information and Event Management Evolution

From simple log gathering tools to sophisticated security orchestration systems that integrate threat information, behavioural analysis, and automatic reaction mechanisms, SIEM platforms have evolved. In addition to assisting compliance initiatives and facilitating efficient forensic investigations, contemporary systems provide centralised visibility across hybrid cloud infrastructures.

Modern SIEM platforms go far beyond traditional log collection and correlation. Advanced solutions now integrate machine learning for anomaly detection, user and entity behaviour analytics (UEBA)[17] to uncover insider threats, and threat intelligence feeds to provide context for analysing security events. These features allow security teams to detect complex attack patterns that would be missed by conventional, signature-based methods.

This project utilizes Wazuh, an open-source SIEM platform that builds upon the OSSEC[18] foundation while providing modern capabilities including real-time rule-based and behavior-based detection, comprehensive dashboard visualizations with alert correlation, integration with threat intelligence sources, and support for automated response mechanisms including file integrity monitoring, rootkit detection, and active response capabilities [16].

1.6 MITRE ATT&CK Framework Integration

The MITRE ATT&CK framework [7] provides a standardized taxonomy of known attacker techniques and tactics that has become the industry standard for threat modeling and security analysis. The framework organizes adversary behavior into tactics that represent the technical goals of attacks and techniques that describe how attackers achieve those goals.

To guarantee organised detection and transparent reporting, every custom detection rule in this project is purposefully in line with certain methods from the MITRE ATT&CK architecture. T1190 (Exploit Public-Facing Application) is used to gain initial access through vulnerable web applications; T1099.001 (Endpoint Denial of Service) targets system availability; T1110.001 (Brute Force: Password Guessing) targets credential-based attacks; and T1046 (Network Service Scanning) is used for reconnaissance.

Threat intelligence feeds can be integrated, SOC-style monitoring logic is strengthened, security event traceability is improved, and compliance with security frameworks that use the MITRE ATT&CK model for threat analysis and control validation is supported.

[17]UEBA: User and Entity Behavior Analytics is a cybersecurity solution that uses machine learning to detect threats by identifying unusual behavior patterns.

[18]OSSEC: Open Source Security Event Correlator, a host-based intrusion detection system that provides log analysis and integrity checking.

1.7 Open-Source Security Tooling Landscape

The ecosystem for open-source security has developed to provide strong tools that are comparable to proprietary solutions in terms of both capability and versatility. What distinguishes them is the degree of personalisation and transparency they offer, which are particularly advantageous in research and educational settings. As the foundation of the simulated company environment in this project, these tools demonstrate the practical potential of open-source technology in creating dependable and efficient cybersecurity infrastructure.

A diverse range of open-source technologies are used in this project to develop and test the cybersecurity infrastructure. Without the need of actual hardware, GNS3 makes it possible to build and simulate intricate network topologies completely in a virtual environment. With hundreds of security testing tools bundled into a single, specially designed distribution, Kali Linux serves as the main platform for attack simulation. With a web-based interface and an adaptable plugin system that enables a variety of configurations, pfSense equips the setup with enterprise-grade firewall and routing capabilities.

Wazuh provides the centralized SIEM platform with agent-based monitoring, real-time correlation, and web-based dashboards. OpenVPN enables encrypted remote tunnel access for external attack simulation. The attack simulation toolkit includes Hydra for credential attacks, Nmap for network discovery and scanning, Nikto for web vulnerability assessment, hping3 for denial of service and flood traffic generation, and DVWA [11] for vulnerable web application testing.

Additional infrastructure components include FRR[3], which is integrated into the environment to enable dynamic OSPF routing. This addition allows for realistic enterprise-grade routing behaviour and supports automatic network convergence, effectively mirroring the functionality found in production networks.

1.8 Thesis Structure and Methodology

From the early thoughts and network architecture to the practical implementation and attack simulation to the final analysis and future enhancements, this thesis is organised into eight chapters, each of which builds on the one before it. The approach combines theoretical underpinnings with hands-on, real-world implementation in order to foster a strong grasp of business cybersecurity as well as the abilities required to construct and evaluate such systems.

The project's practical aspects—how the system was put into place, tested, and improved—are covered in the next chapters. In Chapter 2, the general architecture is presented, along with the design choices that shaped the network's structure. The implementation of the fundamental network infrastructure, including interface configuration, routing configuration, and access control rules, is covered in Chapter 3. The deployment of the SIEM platform is the main topic of Chapter 4, which also describes how agents were set up and placed throughout the network.

Advanced threat detection is covered in Chapter 5, with a particular emphasis on developing unique detection criteria that are in line with the MITRE ATT&CK methodology. A series of realistic assault scenarios are described in Chapter 6 to evaluate the system's capacity to recognise and react to various threats. In order to decrease reaction time, Chapter 7 presents active defence strategies and automated

incident response procedures. Chapter 8 concludes with an evaluation of the results, an assessment of the implementation's overall efficacy, and recommendations for future development.

The project uses an iterative methodology in which testing, assessment, and improvement come after each stage of execution. The system's ability to accurately identify and react to actual threats is enhanced by this cycle of development and validation. In order to give readers the information and practical skills necessary for contemporary cybersecurity employment, the aim is to meaningfully blend theory and practice.

1.9 Related Work

The development of practical cybersecurity training environments and SIEM-based monitoring systems has been an active area of research, with several notable contributions addressing similar challenges to those tackled in this thesis.

Scarfone and Mell [13] provided foundational guidance on intrusion detection and prevention systems, establishing principles that remain relevant for modern SIEM deployments. Their work emphasized the importance of multi-layered detection approaches, which aligns with our multi-agent monitoring strategy.

In the realm of educational cybersecurity environments, Whitman and Mattord [17] explored the challenges of creating realistic training scenarios for cybersecurity education. Their research highlighted the gap between theoretical knowledge and practical skills, supporting the need for hands-on laboratory environments like the one developed in this thesis.

More recently, Heartfield et al. [6] conducted a comprehensive analysis of cybersecurity training platforms, identifying key requirements for effective security education tools. Their taxonomy emphasizes the importance of realistic attack simulation and comprehensive monitoring capabilities, both central features of our implementation.

The integration of open-source tools for enterprise security monitoring has been examined by Casey et al. [1], who demonstrated the viability of open-source solutions in professional security operations. Their work provides empirical evidence supporting the approach taken in this thesis, where enterprise-grade capabilities are achieved through careful integration of open-source components.

Regarding SIEM platform effectiveness, Silberschatz et al. [14] discussed the challenges of correlation and analysis in large-scale monitoring systems. Their findings inform our three-agent deployment strategy, which balances comprehensive coverage with manageable complexity.

While these studies provide valuable insights, most focus on either theoretical frameworks or single-tool implementations. This thesis contributes to the field by demonstrating a complete, integrated approach that combines network segmentation, multi-agent monitoring, and automated response capabilities using exclusively open-source technologies, while maintaining educational accessibility and practical effectiveness.

Chapter 2

System Design and Implementation

Developing an effective cybersecurity infrastructure involves thoughtful planning of the network architecture, strategic placement of monitoring systems, and the implementation of robust security controls capable of detecting and responding to a wide range of threats. This chapter presents the design and deployment of a virtualised enterprise cybersecurity environment that combines realistic network segmentation with extensive monitoring capabilities. The sections that follow explore the overall network architecture, outline the design of the security zones, assess the monitoring deployment strategy, and highlight the core security principles that underpin this multi-layered defence approach.

2.1 Network Architecture Overview

This project utilised the GNS3 simulation platform[4] to construct the enterprise cybersecurity infrastructure, which allows for the realistic simulation of routers, firewalls, and virtual machines without requiring physical hardware. The architecture, which is separated into multiple security zones, represents a contemporary enterprise network. Every zone is made to carry out particular operational tasks while maintaining complete isolation and permitting efficient environmental monitoring.

Each of the network's four main segments represents a different security zone that is commonly found in business settings. The distinct operating requirements and threat profiles connected to various infrastructure components are reflected in the customised security rules and monitoring configurations that are put up in these zones.

Centralised switching is the foundation of the system, and pfSense[8] is the primary routing and security enforcement component. The architecture of this design is modelled by that of real enterprise networks, with a central firewall linked to multiple network switches. Apart from offering Layer 2 connectivity within each security zone, these switches maintain zone isolation and provide comprehensive traffic monitoring across the whole environment.

Figure 2.1 shows the entire network topology with monitoring agents placed strategically throughout various security zones. The central pfSense firewall with certain interface configurations (em0-em5) that offer routing and security policy enforcement is shown in the topology. Four dedicated switches that offer extensive

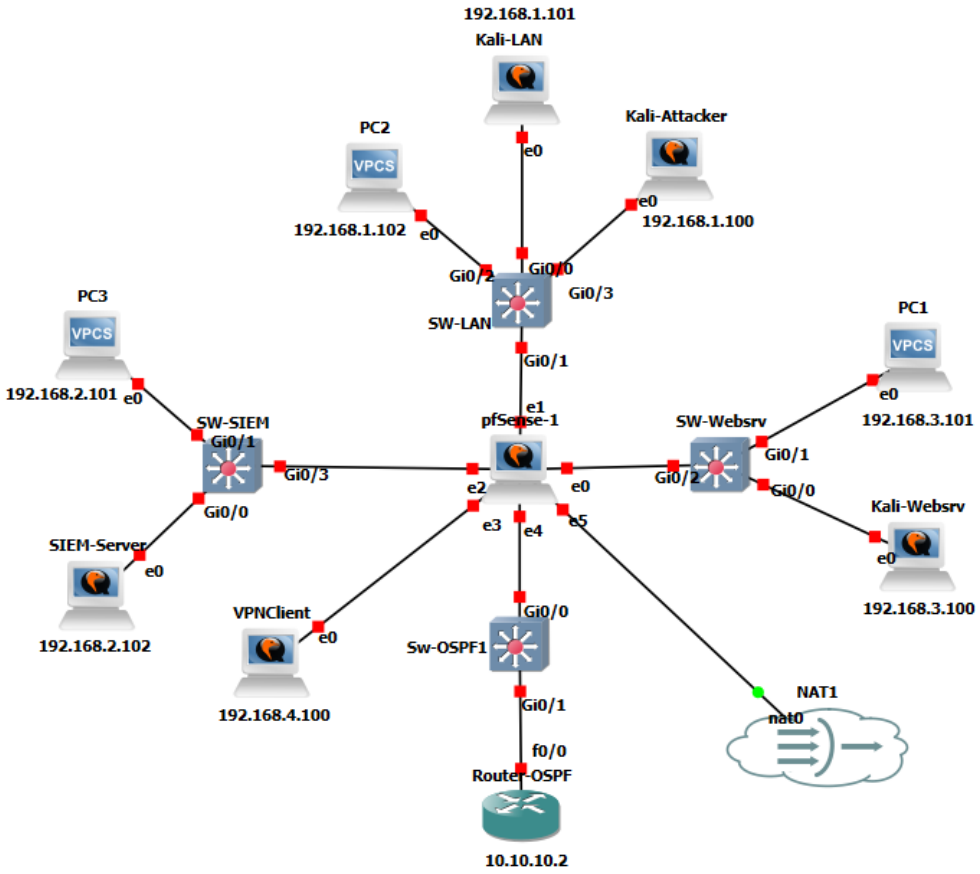

Figure 2.1: Complete network topology with multi-zone infrastructure

monitoring and security testing capabilities are part of the topology, which serves various security zones.

2.2 Network Zones and System Architecture

The LAN zone (192.168.1.0/24) serves as the primary internal user network where employee workstations and internal systems operate. SW-LAN connects internal systems including Kali-LAN and Kali-Attacker for comprehensive attack simulation while representing the traditional corporate network where business operations occur and users access organizational resources.

The Management zone (192.168.2.0/24) hosts critical infrastructure components including the SIEM platform and network management systems. SW-SIEM provides management network connectivity for the SIEM-SERVER infrastructure while representing the secure management network commonly isolated in enterprise environments to protect critical infrastructure from general network traffic.

The DMZ zone (192.168.3.0/24) exposes public-facing services including web servers and applications that require internet accessibility. SW-Websrv supports the DMZ environment hosting Kali-Websrv with DVWA[1] [11] deployment while implementing the classic demilitarized zone concept where public services operate

[1]DVWA: Damn Vulnerable Web Application is a PHP/MySQL web application designed to be vulnerable for security testing and education purposes.

with restricted access to internal networks.

Through secure tunnels, the VPN zone (192.168.4.0/24) replicates connections from outside attackers and supports encrypted remote access architecture. The VPN zone maintains the proper security protections while offering expedited connectivity for VPN Client operations and external attack simulation by connecting directly to pfSense without the need for intermediate switching.

Host Name	IP Address	Zone	Purpose	Wazuh Agent
Kali-LAN	192.168.1.103	LAN	Monitored internal system, attack target	Yes (kali-lan)
Kali-Attacker	192.168.1.102	LAN	Unmonitored attack source	No
SIEM-SERVER	192.168.2.102	Management	Wazuh manager and web UI	Manager
Kali-WebSrv	192.168.3.100	DMZ	DVWA web server with monitoring	Yes (Websrv)
VPN Client	192.168.4.101	VPN	External attacker simulation	Yes (VPN)
Router-OSPF	10.10.10.2	External	Dynamic routing infrastructure	No

Table 2.1: System architecture with IP addressing and monitoring coverage

The layout of the IP addressing scheme is shown in Table 2.1, which reserves lower address ranges for critical infrastructure components and uses DHCP[2] to allocate dynamic ranges to client systems. Critical systems that need constant addressing, including monitoring endpoints and core services, are assigned static IP addresses in order to provide dependable administrative access and precise correlation of security incidents.

2.3 Strategic Monitoring Architecture

Correlating attack patterns and defensive actions is made possible by the monitoring architecture's deliberate three-agent deployment, which offers thorough visibility across several network zones. While reflecting many system types frequently encountered in business contexts, each monitored system plays a distinct function in the overall security monitoring approach.

In addition to facilitating advanced correlation analysis, the three-agent monitoring approach offers several viewpoints on security incidents and attack trends. The standard internal endpoint that needs defence against both external threats and lateral movement situations is represented by Kali-LAN. Network activity, file system modifications, authentication events, and system-level security events that point to compromise or malicious behaviour are all tracked by this system.

Kali-WebSrv provides specialized monitoring for web application security in the DMZ environment. This system focuses on HTTP request analysis, web application attack detection, database interaction monitoring, and file integrity verification for web content. The positioning in the DMZ makes it an ideal target for external attacks while providing comprehensive visibility into web-based threat vectors and application-layer security events.

VPN Client offers unique visibility into external attack patterns by monitoring the activities of systems that connect through VPN infrastructure. This agent

[2]DHCP: Dynamic Host Configuration Protocol provides automated IP address assignment and network configuration for client systems, eliminating the need for manual IP configuration.

detects attack tool usage, monitors outbound connections that may indicate attack activities, and correlates VPN connection events with suspicious behaviors to identify external threat actors leveraging legitimate remote access infrastructure.

In order to simulate actual attack scenarios in which the source system functions outside of organisational control, Kali-Attacker is purposefully left unmonitored. By carefully monitoring target systems and network infrastructure components, this design decision produces realistic testing settings where assaults come from systems without security monitoring and are identified.

2.4 Network Services Implementation

All network zones may automatically issue IP addresses thanks to centralised DHCP services, which also keep the right reservations for important systems. Plug-and-play connectivity for testing systems is made possible by the setup, which also supports thorough security correlation and guarantees constant addressing for monitored infrastructure.

```
# DHCP scope configuration for LAN zone
interface em1 {
    range 192.168.1.100 192.168.1.150;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8, 1.1.1.1;
    default-lease-time 86400;
}

# Management zone DHCP configuration
interface em2 {
    range 192.168.2.100 192.168.2.150;
    option routers 192.168.2.1;
    option domain-name-servers 8.8.8.8, 1.1.1.1;
}
```

Listing 2.1: DHCP configuration for comprehensive zone coverage

Listing 2.1 illustrates how the DHCP configuration stores fixed addresses for essential infrastructure elements that need consistent connectivity while automating IP address issuance. For trustworthy external name resolution, DNS services are set up using safe upstream resolvers, namely Cloudflare DNS (1.1.1.1) and Google DNS (8.8.8.8). For internal systems, local DNS resolution is offered concurrently. Additionally, DNS query logging is included in the setup to facilitate security analysis, and the danger of DNS-based attacks is reduced by using trustworthy resolvers with validation procedures.

By integrating with Router-OSPF, the OSPF implementation offers enterprise-grade dynamic routing, facilitating realistic routing protocol behaviour and automated network convergence. This setup supports automated failover and scalable network extension while showcasing sophisticated networking ideas.

```
router ospf
  router-id 10.10.10.1
  network 192.168.1.0/24 area 0.0.0.0
  network 192.168.2.0/24 area 0.0.0.0
  network 192.168.3.0/24 area 0.0.0.0
  network 192.168.4.0/24 area 0.0.0.0
```

```
7   redistribute connected
```

Listing 2.2: OSPF configuration for dynamic routing across all zones

The OSPF setup creates neighbour connections between pfSense and Router-OSPF, allowing route exchange and network redundancy features, as seen in Listing 2.2. With all networks participating in the OSPF domain, Area 0 acts as the backbone area, facilitating speedy convergence during network topology changes and providing optimal routing efficiency and easy management.

2.5 Security Design Principles

The infrastructure design implements defense-in-depth principles that provide multiple layers of security control and monitoring while maintaining the operational flexibility necessary for comprehensive security testing and validation. The design balances realistic security implementation with the requirements of an educational and testing environment.

The main security control approach is zone isolation, which forbids direct connection across network zones without firewall mediation and explicit policy authorisation. While permitting controlled testing scenarios and proper administrative access requirements necessary for thorough security validation, this architecture inhibits lateral movement across zones.

Comprehensive monitoring coverage provides multiple detection perspectives through strategic agent placement across different network zones and system types. The monitoring architecture captures attack activities from both source and target perspectives, enabling comprehensive threat correlation and analysis that would be impossible with single-point monitoring solutions or traditional perimeter-based security approaches.

Attack pattern correlation capabilities enable the detection of sophisticated multi-stage attacks that span multiple network zones and time periods. The multi-agent deployment supports correlation of reconnaissance activities with subsequent exploitation attempts, identification of lateral movement patterns across network boundaries, and attribution of attack activities to specific threat actors or attack campaigns.

The centralised SIEM platform collects, correlates, and analyses all security events from throughout the infrastructure thanks to central monitoring integration. In addition to offering thorough forensic analysis and compliance reporting requirements that show security efficacy and educational value, this method offers unified threat detection and response capabilities.

By using rule-based blocking and response methods that stop attacks from getting worse and lessen the effect of successful exploits, automated response capabilities offer instant threat containment. While offering thorough audit trails and manual override possibilities for complicated cases demanding human judgement and analysis, the response system functions autonomously.

Chapter 3

VPN Infrastructure and Remote Access Security

Remote access has become a critical requirement for modern organisations, but it also introduces security challenges that must be carefully addressed through proper implementation and monitoring. This chapter focuses on the deployment and security of VPN infrastructure within the cybersecurity environment, highlighting how encrypted remote access can serve as both a legitimate business necessity and a potential entry point for attackers. The sections that follow detail the OpenVPN server setup, client certificate management, deployment procedures, security monitoring techniques, and realistic attack simulations used to evaluate the effectiveness of VPN-based threat detection mechanisms.

3.1 OpenVPN Server Configuration

Secure remote access is made possible by the Virtual Private Network implementation, which also uses encrypted tunnels to simulate realistic external attacks. The combination of OpenVPN[1] [10] with pfSense results in a complete remote access solution that accommodates both valid connectivity and security testing situations.

Utilising the pfSense integrated wizard, the OpenVPN server setup streamlines certificate administration and configuration. The deployment establishes a strong PKI PKI: Public Key Infrastructure offers the structure for creating, distributing, and managing digital certificates in secure communications. infrastructure with local Certificate Authority[2] features that facilitate scalable client certificate creation and revocation management.

The whole server setup procedure, including SSL/TLS encryption parameters and network assignment choices, is illustrated via the pfSense OpenVPN configuration interface. SSL/TLS encryption with industry-standard cyphers, UDP transport on port 1194 for best performance, tunnel subnet allocation from 10.8.0.0/24 range, DNS push configuration that points clients to secure resolvers, and thorough logging for connection monitoring and security analysis are some of the server configuration parameters.

[1]OpenVPN: Open-source VPN solution that provides secure point-to-point or site-to-site connections using SSL/TLS for encryption and authentication.

[2]CA: Certificate Authority is a reliable organisation that issues digital certificates to confirm the legitimacy of entities in a public key infrastructure.

```
# OpenVPN server configuration
port 1194
proto udp
dev tun
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 1.1.1.1"
cipher AES-256-CBC
auth SHA256
tls-auth ta.key 0
comp-lzo
keepalive 10 120
```

Listing 3.1: OpenVPN server configuration parameters for secure remote access

The configuration shown in Listing 3.1 establishes the core OpenVPN server parameters that ensure secure and reliable VPN connectivity. The server utilizes AES-256-CBC encryption for data protection and SHA256 authentication for message integrity verification.

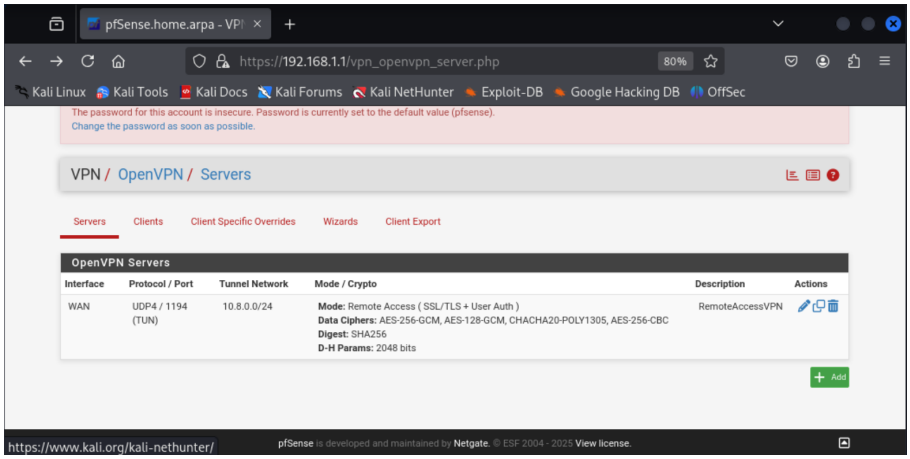

Figure 3.1: pfSense OpenVPN server configuration interface

Figure 3.1 shows the pfSense web interface providing an intuitive configuration platform for OpenVPN server deployment. The interface enables administrators to configure encryption parameters, network settings, and client access controls through a centralized management interface.

3.2 Client Configuration and Certificate Management

VPN client configuration emphasizes security through proper certificate implementation while maintaining usability for testing scenarios. The certificate generation process creates unique client credentials that enable individual client identification and access control through the centralized authentication infrastructure.

Client certificates are created using the pfSense Certificate Manager, which generates RSA keys, appropriate subject alternate names for client identification, and

exportable formats that support a variety of client platforms. The certificate distribution procedure offers automatic client configuration generation with embedded certificates and keys for easier deployment.

The OpenVPN client configuration's structure demonstrates the breadth of security procedures needed to set up safe VPN connectivity. To guarantee a self-contained and dependable setup, every configuration file has all required encryption parameters and authentication credentials incorporated directly within the file.

```
# OpenVPN client configuration
client
dev tun
proto udp
remote 192.168.4.1 1194
resolv-retry infinite
nobind
cipher AES-256-CBC
auth SHA256
verb 3

<ca>
-----BEGIN CERTIFICATE-----
[Certificate Authority]
-----END CERTIFICATE-----
</ca>

<cert>
-----BEGIN CERTIFICATE-----
[Client Certificate]
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
[Private Key]
-----END PRIVATE KEY-----
</key>
```

Listing 3.2: OpenVPN client configuration file structure with embedded certificates

The configuration structure shown in Listing 3.2 includes placeholders for the actual certificate content. In a production deployment, the Certificate Authority certificate, client certificate, and client private key would be embedded directly within these sections, creating a self-contained configuration file that requires no external certificate files.

Configuration validation testing, connectivity verification methods, and troubleshooting instructions for typical connection problems are all part of the client deployment process. While preserving business continuity for authorised users, certificate revocation features offer security controls for compromised or terminated client access.

3.3 VPN Client Deployment and Testing

The VPN Client system deployment offers a framework for simulating realistic attacks over encrypted tunnels and illustrates external connectivity scenarios. Legit-

imate remote access capabilities and security testing features that verify detection and response procedures are both prioritised in the client configuration.

VPN client system preparation entails numerous critical procedures to ensure secure and functional interaction with the total network. This comprises installing the OpenVPN client software, deploying the required certificates and configuration files, configuring the network interface to accommodate VPN tunnel access, and changing the routing table to route traffic through the encrypted channel. The final setup enables the system to replicate both legitimate user access and adversary behaviour, enabling for realistic testing of the monitoring infrastructure in a variety of threat scenarios.

Successful tunnel formation and network connectivity validation are demonstrated by the VPN connection establishing procedure. Routing configuration for internal network access, IP address assignment from the VPN subnet range, tunnel encryption negotiation, and certificate validation are all steps in the connection establishment process.

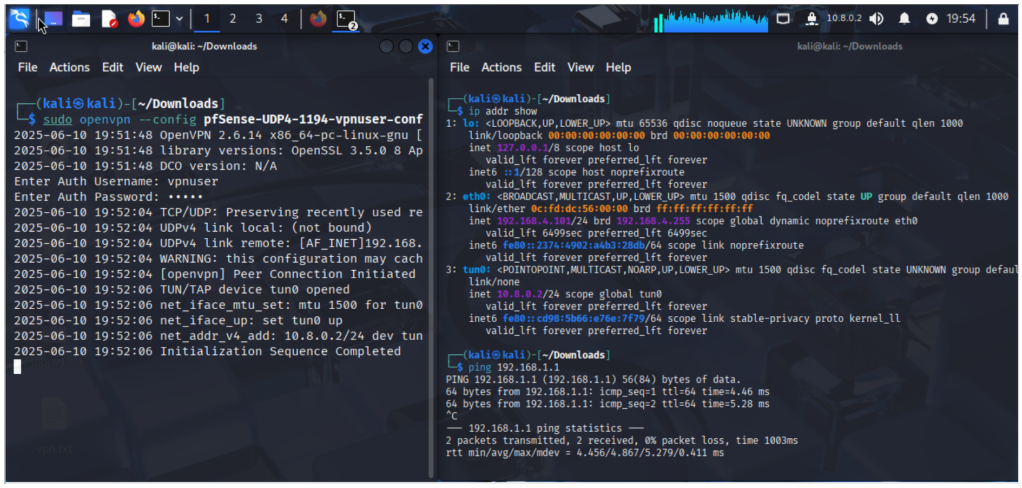

Figure 3.2: VPN Client connection establishment

Figure 3.2 displays the connection logs, which clearly illustrate what occurs when a user connects to the VPN. The system goes through the entire setup procedure, handling the SSL/TLS security handshake first, then creating the tunnel interface and assigning the client an IP address. Clients can safely connect to the internal network and receive IP addresses in the 10.8.0.0/24 range when everything is operating as it should. Both standard user access and our security testing trials run well with this configuration.

3.4 VPN Security Monitoring and Attack Detection

Monitoring VPN infrastructure gives insight into connection trends and any security risks that take use of remote access features. The monitoring approach preserves genuine user privacy and operational efficiency by combining behavioural analysis and connection recording to detect suspect activity.

Connection event monitoring captures tunnel establishment and termination events, authentication success and failure patterns, data transfer volume and timing analysis, and client IP address tracking for geographic correlation. The monitoring infrastructure integrates with the Wazuh SIEM platform to provide centralized analysis and correlation with other security events across the multi-zone infrastructure.

VPN-specific threat detection tools detect credential abuse attempts utilising VPN access, data exfiltration activities using encrypted channels, lateral movement patterns after successful VPN authentication, and reconnaissance activities using tunnel connections. In addition to supporting incident response and forensic analysis needs, these detection capabilities offer thorough insight into VPN-based threat situations.

The following monitoring configuration demonstrates the comprehensive VPN logging and analysis capabilities implemented through system-level monitoring and iptables integration.

```
# Monitor OpenVPN connections and authentication events
tail -f /var/log/openvpn.log | grep -E "CONNECTED|DISCONNECTED|
    AUTH"

# Check active VPN sessions and connection status
cat /var/run/openvpn-status.log

# Monitor VPN client network activities
sudo iptables -A OUTPUT -o tun+ -j LOG --log-prefix "
    VPN_TRAFFIC: "

# Analyze VPN connection patterns
grep "CONNECTED" /var/log/openvpn.log | awk '{print $1, $2, $NF
    }'
```

Listing 3.3: VPN connection monitoring and traffic analysis configuration

This monitoring configuration provides comprehensive visibility into VPN operations, enabling security analysts to track connection patterns, identify suspicious activities, and correlate VPN events with other security incidents detected across the infrastructure.

3.5 Attack Simulation Through VPN Infrastructure

Attack models based on VPNs show genuine external threat patterns and evaluate the efficacy of security monitoring across encrypted communication channels. The attack simulation mimics real threat actor behaviours by doing reconnaissance, exploitation, and lateral movement tasks using authentic VPN connectivity.

Attack scenarios include network reconnaissance through encrypted tunnels using standard scanning tools, credential-based attacks targeting internal systems from external IP ranges, web application exploitation through VPN-sourced traffic, and cross-zone attack patterns that leverage VPN access for multi-stage operations. These scenarios test detection capabilities while providing realistic threat simulation for security validation.

The VPN Client serves as both a legitimate remote access demonstration and an external attack platform, enabling comprehensive security testing that validates monitoring effectiveness across different threat vectors. The dual-purpose configuration allows security analysts to observe how external threats might leverage VPN infrastructure while testing the effectiveness of detection and response mechanisms.

Attack correlation capabilities identify patterns that span VPN connections and internal network activities, providing comprehensive threat detection that addresses sophisticated attack campaigns. The multi-agent monitoring architecture enables correlation of VPN connection events with subsequent attack activities, demonstrating the advanced detection capabilities achieved through strategic monitoring placement.

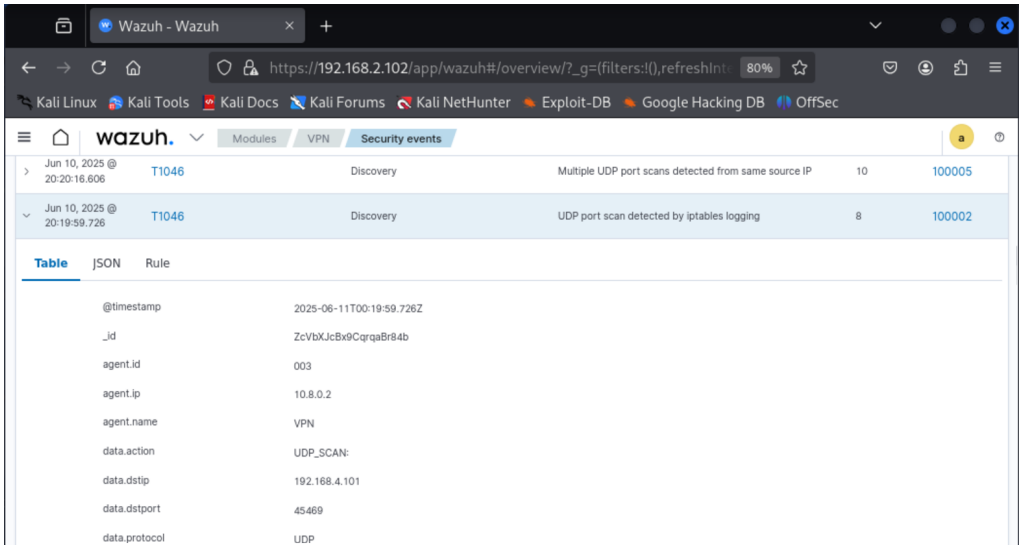

Figure 3.3: VPN-based attack detection and correlation

The dashboard interface for Figure 3.3 shows the extensive correlation capabilities that allow security analysts to spot threat trends across internal network activity and VPN connections. This gives insight into advanced threats that use reputable remote access infrastructure to launch attacks and move laterally.

Chapter 4

Wazuh SIEM Platform Deployment and Configuration

Effective cybersecurity monitoring requires a centralized platform capable of collecting, analyzing, and correlating security events from across the entire network infrastructure. This chapter details the deployment and configuration of the Wazuh SIEM platform as the cornerstone of the security monitoring architecture. The following sections examine the installation process, explore the strategic multi-agent deployment approach, detail the integration of various log sources, and discuss the configuration of dashboards and alert management systems that provide comprehensive visibility into security events across all network zones.

4.1 SIEM Infrastructure Installation

As the centralised security monitoring solution, Wazuh [16] is used in the Security Information and Event Management platform deployment to offer extensive log aggregation, threat detection, and incident response capabilities throughout the multi-zone architecture. Installing Wazuh on the specialised SIEM-SERVER lays the groundwork for enterprise-level security monitoring while preserving the open-source accessibility that is crucial for learning settings.

The installation process deploys multiple integrated components that work together to provide complete SIEM functionality. The Wazuh manager serves as the central correlation engine and agent communication hub. Elasticsearch provides high-performance data storage and indexing capabilities. Kibana delivers comprehensive web-based dashboards and visualization capabilities.

To guarantee correct component integration and setup, the Wazuh installation makes use of the official automated installer script. For complete SIEM capability, the installation script sets up all essential dependencies, security certificates, and inter-component connections.

```
# Download and execute Wazuh all-in-one installer
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
chmod +x wazuh-install.sh
sudo bash wazuh-install.sh -a

# Verify installation status and service health
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-indexer
```

```
sudo systemctl status filebeat

# Check Wazuh manager configuration
sudo /var/ossec/bin/wazuh-control status
```

Listing 4.1: Wazuh SIEM platform installation using official automated installer

The streamlined deployment process, shown in Listing 4.1, shows how each SIEM component is automatically configured via a set of installation instructions. Immediately upon installation, verification commands are run to confirm that the setup was successful and to demonstrate that all services are up and running and properly integrated.

The installation immediately sets up database indices for effective data storage, configures SSL certificates for safe connections, generates default user accounts with the necessary rights, and initialises dashboard templates for instant security monitoring. To guarantee peak performance under anticipated monitoring loads, post-installation optimisation entails memory allocation tweaking, log retention policy setting, and integration testing.

4.2 Multi-Agent Deployment Strategy

A strategic three-agent deployment is used in the monitoring architecture to enable advanced threat analysis and attack correlation while offering thorough visibility across several network zones. Depending on its network location and the kinds of security events that are most pertinent to its zone, each agent has a distinct monitoring function.

Considerations for agent deployment include cross-zone threat detection correlation capabilities, log source variety and security event kinds, system resource availability and performance effect, network zone coverage requirements, and integration complexity and maintenance needs. The three-agent approach strikes a compromise between thorough coverage, resource usage, and operational effectiveness.

Kali-LAN agent deployment focuses on internal network monitoring including authentication events, system integrity verification, network activity analysis, and process monitoring for malicious software detection. This agent represents typical endpoint monitoring in enterprise environments where internal systems require protection from both external attacks and insider threats.

The agent installation and registration process demonstrates the streamlined deployment methodology that enables rapid monitoring expansion across the infrastructure. Each agent requires proper registration with the central manager to establish secure communications and begin log forwarding.

```
# Download and install Wazuh agent package
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent
    /wazuh-agent_4.7.0-1_amd64.deb
sudo dpkg -i wazuh-agent_4.7.0-1_amd64.deb

# Register agent with manager using automatic authentication
sudo /var/ossec/bin/agent-auth -m 192.168.2.102 -A kali-lan

# Configure manager IP address
```

```
echo "WAZUH_MANAGER='192.168.2.102'" | sudo tee /var/ossec/etc/
    ossec-init.conf

# Start agent services and enable automatic startup
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Listing 4.2: Wazuh agent installation and secure registration with central manager

The installation procedure outlined in Listing 4.2 configures automated service startup to provide continuous monitoring coverage while establishing secure connections between agents and the central management. Individualised monitoring and correlation throughout the infrastructure are made possible by the registration procedure, which generates distinct agent identities.

Kali-Websrv agent configuration emphasizes web application security monitoring through Apache log analysis, HTTP request examination for attack patterns, database interaction monitoring, and file integrity verification for web content. This agent provides specialized DMZ monitoring that addresses web-based attack vectors and application-layer security threats.

VPN Client agent setup provides external attack perspective monitoring through VPN connection event tracking, outbound traffic analysis for attack tool usage, tunnel activity correlation with suspicious behaviors, and cross-zone attack pattern identification. This unique monitoring perspective enables detection of external threats that leverage VPN infrastructure for attack delivery.

4.3 Log Source Configuration and Integration

While maximising efficiency and reducing false positive alarms, thorough log source setup guarantees full insight into security-relevant events across all monitored systems. By emphasising log sources that offer actionable security insight over extensive but noisy logging, the configuration method prioritises quality over quantity.

Universal log sources monitored across all agents include system authentication logs for login analysis, kernel messages for low-level security events, system logs for general operational monitoring, and custom iptables logs with attack detection prefixes. These sources provide foundational security monitoring capabilities that apply across different system types and network zones.

The thorough log source integration that permits multifaceted security monitoring across various system contexts is illustrated by the Wazuh agent configuration file structure. For appropriate event extraction and correlation, a certain parser setup is needed for each log source.

```
<ossec_config>
  <!-- System authentication monitoring -->
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/auth.log</location>
  </localfile>

  <!-- System operations and security events -->
  <localfile>
    <log_format>syslog</log_format>
```

```
    <location>/var/log/syslog</location>
  </localfile>

  <!-- Kernel security events and attack detection -->
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

  <!-- Apache web server access monitoring -->
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>
```

Listing 4.3: Wazuh agent comprehensive log source configuration for multi-zone monitoring

This setup, which is displayed in Listing 4.3, gives an example of the multi-source monitoring technique that records security events from web server activity, kernel operations, and authentication systems. Through the integration of several log sources, thorough threat detection across many attack vectors and system components is made possible.

Specialized log sources provide zone-specific monitoring capabilities tailored to the security requirements and threat vectors most relevant to each network zone. Web server monitoring includes Apache access and error logs for HTTP attack detection, PHP error logs for application vulnerability exploitation, and database logs for SQL injection and data access monitoring.

Real-time detection of unauthorised changes to important system files, configuration adjustments, and content alterations is made possible via file integrity monitoring. System folders, application files, and configuration files are all included in the monitoring setup, but regularly changing files that may provide an excessive number of false positive alarms are not.

4.4 Dashboard Configuration and Alert Management

The Wazuh web interface provides centralized security monitoring and management capabilities through comprehensive dashboards that integrate data from all monitored agents. Dashboard configuration emphasizes actionable security intelligence presentation while supporting both real-time monitoring and historical analysis requirements.

Attack pattern visualisation with geographic and temporal correlation, MITRE ATT&CK technique mapping for threat intelligence integration, agent status monitoring with connectivity and performance metrics, real-time alert feeds with severity-based filtering, and customised dashboards for particular attack types and security scenarios are the main dashboard components.

The thorough monitoring coverage made possible by the three-agent deployment technique is displayed in the Wazuh dashboard interface. The interface allows drill-

down analysis for in-depth incident investigation while offering real-time access into security events across all monitored zones.

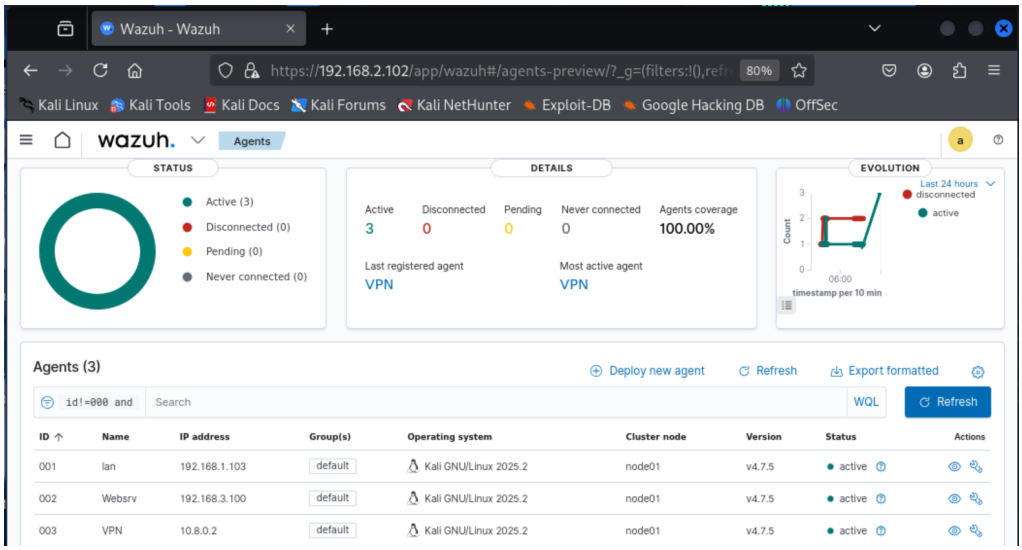

Figure 4.1: Wazuh multi-agent monitoring dashboard

Figure 4.1 displays the dashboard interface that gives security analysts thorough insight into the multi-zone architecture and facilitates the quick detection of attack patterns and security events. While alert correlation capabilities detect complex assault operations, agent status monitoring guarantees ongoing coverage.

Alert management features include correlation rules for grouping relevant events, alerting systems for important security events, retention policies for compliance and forensic investigation, and severity-based prioritisation for efficient incident response. To properly handle various security event types, the setup offers both automatic response integration and human investigation procedures.

Drill-down capabilities for in-depth event analysis, export capability for reporting and compliance documentation, the ability to create bespoke visualisations for particular monitoring requirements, and connection APIs for access to other security tools are all examples of advanced dashboard features. These features enable all-encompassing security operations while preserving the adaptability required for various organisational needs and changing threat environments.

The extensive implementation of the SIEM platform shows how well open-source security monitoring solutions work in business settings and lays the groundwork for enhanced threat detection and incident response capabilities. Sophisticated attack correlation is made possible by the multi-agent architecture, which also preserves the affordability and usability necessary for research and educational applications.

Chapter 5

MITRE ATT&CK Integration and Custom Detection Rules

For threat detection to be effective, standardised frameworks and well designed detection algorithms that can correctly detect intricate attack patterns while lowering false positives are essential. The process of creating unique detection rules suited to certain threat situations is described in this chapter, which focusses on the integration of the Wazuh SIEM platform with the MITRE ATT&CK architecture. The subsequent sections address the application of industry-standard threat classification, the development of targeted rules for various attack vectors, the creation of detection capabilities tailored to a VPN, and the methods of optimisation and validation employed to guarantee consistent and dependable security monitoring.

5.1 MITRE ATT&CK Framework Implementation

Standardised classification and analysis of adversary tactics and methods seen in actual cyberattacks are provided via the MITRE ATT&CK framework [7]. Structured threat detection and analysis that is in line with industry-standard threat intelligence and incident response techniques utilised throughout business security operations is made possible by the integration of this framework into the Wazuh SIEM platform.

The execution of the framework concentrates on particular strategies and tactics that are detectable and successfully mimicked in the infrastructure environment. The chosen methods illustrate real-world threat situations that security professionals face in business settings and serve as representative attack vectors that offer useful instructional value.

Network Discovery (T1046) represents systematic reconnaissance activities that attackers use to identify potential targets and attack vectors. Port scanning and network enumeration activities generate specific network traffic patterns that can be detected through firewall logging and correlation analysis. The detection implementation identifies scanning behaviors while distinguishing between malicious reconnaissance and legitimate network management activities.

Brute Force attacks (T1110.001) target authentication systems to gain unauthorized access through systematic password enumeration. These attacks gener-

ate distinctive authentication failure patterns that enable behavioral detection and automated response activation. The implementation detects various brute force techniques while providing graduated response mechanisms that balance security effectiveness with operational continuity.

Network Denial of Service (T1499.001) attacks target system availability through resource exhaustion and service disruption. These attacks generate network traffic patterns that can be identified through volume analysis and connection monitoring. The detection implementation provides early warning capabilities while supporting immediate response measures to minimize service impact.

The MITRE ATT&CK integration enhances threat intelligence capabilities by providing standardized attack categorization that supports incident response coordination, threat hunting activities, compliance reporting requirements, and threat intelligence sharing with external organizations and security communities.

5.2 Custom Detection Rule Development

Custom detection rules minimise false positive alarms, which may overload security analysts and diminish the efficacy of monitoring, while providing focused identification of certain attack patterns and suspicious behaviours. The process of developing rules prioritises accuracy and dependability while retaining sensitivity to identify complex attack variants and evasion strategies.

The rule development methodology comprises threshold tuning to balance detection sensitivity with false positive rates, correlation logic development for multi-event attack patterns, baseline establishment for typical system and network activities, and threat pattern analysis to find distinctive signatures and behaviours. To guarantee detection efficacy in a variety of attack scenarios, every rule is put through extensive testing and validation.

Rule categorization aligns with the MITRE ATT&CK framework to provide standardized threat intelligence integration while supporting incident response workflows and threat hunting activities. The categorization enables security analysts to understand attack context and relationships while supporting strategic threat analysis and defensive planning activities.

The comprehensive custom rule implementation demonstrates targeted detection capabilities for the primary attack vectors simulated within the infrastructure environment while providing practical examples of detection logic development and optimization.

5.2.1 Network Discovery Detection Rules

Network reconnaissance detection identifies systematic scanning activities that indicate potential attack preparation or intelligence gathering activities. The detection logic analyzes firewall logs and kernel messages to identify scanning patterns while distinguishing between malicious reconnaissance and legitimate network operations.

```
<!-- TCP Port Scan Detection - T1046 -->
<rule id="100001" level="8">
  <if_sid>99000</if_sid>
  <match>TCP_SCAN</match>
```

```
  <description>TCP port scan detected from $(srcip)</
   description>
  <mitre>
    <id>T1046</id>
  </mitre>
  <group>reconnaissance,mitre_discovery</group>
</rule>

<!-- Multiple TCP Scans -->
<rule id="100004" level="10">
  <if_matched_sid>100001</if_matched_sid>
  <same_source_ip />
  <description>Multiple TCP port scans from same source: $(
   srcip)</description>
  <frequency>10</frequency>
  <timeframe>300</timeframe>
  <mitre>
    <id>T1046</id>
  </mitre>
  <group>reconnaissance,mitre_discovery</group>
</rule>

<!-- Advanced Scanning -->
<rule id="100005" level="9">
  <if_sid>99000</if_sid>
  <match>STEALTH_SCAN|SYN_SCAN|FIN_SCAN</match>
  <description>Advanced scanning technique detected from $(
   srcip)</description>
  <mitre>
    <id>T1046</id>
  </mitre>
  <group>reconnaissance,mitre_discovery</group>
</rule>
```

Listing 5.1: Network scanning detection rules with MITRE ATT&CK integration and adaptive thresholds

The detection rules displayed in Listing 5.1 offer thorough coverage of network reconnaissance operations and use graduated severity levels that correspond to the threat intensity and sophistication of attacks. Frequency-based correlation indicates systematic scanning campaigns, and individual scan detection gives reconnaissance operations baseline monitoring.

The MITRE ATT&CK technique mapping enables standardized threat categorization while supporting threat intelligence correlation and incident response coordination. The technique identification assists security analysts in understanding attack context and planning appropriate response measures.

5.2.2 Brute Force Attack Detection Rules

Authentication attack detection identifies systematic credential enumeration activities that target user accounts and system access controls. The detection logic analyzes authentication logs to identify failure patterns while accounting for legitimate authentication errors and temporary account issues.

```
<!-- SSH Authentication Failure -->
<rule id="100006" level="5">
```

```
3   <if_sid>5700</if_sid>
4   <match>authentication failure|Failed password</match>
5   <description>SSH authentication failure for user $(user) from
      $(srcip)</description>
6   <mitre>
7     <id>T1110.001</id>
8   </mitre>
9   <group>authentication_failed,mitre_credential_access</group>
10 </rule>
11
12 <!-- SSH Brute Force Treshold Excedeed -->
13 <rule id="100007" level="12">
14   <if_matched_sid>100006</if_matched_sid>
15   <same_source_ip />
16   <description>SSH brute force attack detected from $(srcip)</
      description>
17   <frequency>8</frequency>
18   <timeframe>180</timeframe>
19   <mitre>
20     <id>T1110.001</id>
21   </mitre>
22   <group>authentication_failed,mitre_credential_access</group>
23 </rule>
24
25 <!-- Multiple User Brute Force Attack -->
26 <rule id="100008" level="11">
27   <if_matched_sid>100006</if_matched_sid>
28   <same_source_ip />
29   <different_user />
30   <description>Multiple user brute force attack from $(srcip)</
      description>
31   <frequency>5</frequency>
32   <timeframe>300</timeframe>
33   <mitre>
34     <id>T1110.001</id>
35   </mitre>
36   <group>authentication_failed,mitre_credential_access</group>
37 </rule>
```

Listing 5.2: SSH brute force detection with behavioral analysis and automated response integration

Listing 5.2 displays the brute force detection rules, which employ advanced behavioural analysis to differentiate between isolated authentication failures and coordinated attack operations. assaults against several accounts are detected by multi-user detection, whereas assaults against individual user accounts are the subject of threshold-based detection.

The severity levels serve as suitable triggers for automatic response systems while reflecting the possible effect and intensity of the assault. While lower-severity warnings provide inquiry and trend analysis for security operations planning, high-severity alerts initiate quick reaction steps.

5.2.3 Web Application Attack Detection

Attack patterns that target database levels and HTTP services are detected by web application security monitoring. While taking into consideration valid application

use and automated scanning operations, the detection logic examines web server logs and application replies to spot exploitation attempts.

```
<!-- SQL Injection Detection -->
<rule id="100031" level="9">
  <if_sid>31100</if_sid>
  <match> UNION | union |SELECT|INSERT|UPDATE|DELETE|DROP</
   match>
  <regex>(\%27)|(\textquotesingle)|(\-\-)|(\%23)|(#)</regex>
  <description>SQL injection attempt detected from $(srcip)</
   description>
  <mitre>
    <id>T1190</id>
  </mitre>
  <group>web_attack,mitre_initial_access</group>
</rule>

<!-- Cross-Site Scripting (XSS) -->
<rule id="100032" level="8">
  <if_sid>31100</if_sid>
  <match>script|javascript|onerror|onload|onclick</match>
  <regex>&lt;script|javascript:|vbscript:|onload=|onerror=</
   regex>
  <description>XSS attack attempt detected from $(srcip)</
   description>
  <mitre>
    <id>T1059.007</id>
  </mitre>
  <group>web_attack,mitre_execution</group>
</rule>

<!-- Web Vulnerability Scanner -->
<rule id="100034" level="7">
  <if_sid>31100</if_sid>
  <match>nikto|nessus|acunetix|burp|sqlmap|w3af</match>
  <description>Web vulnerability scanner detected: $(user_agent
   )</description>
  <mitre>
    <id>T1046</id>
  </mitre>
  <group>web_attack,mitre_discovery</group>
</rule>
```

Listing 5.3: Web application attack detection with SQL injection and XSS pattern recognition

The Listing 5.3 web application detection rules encompass all the primary attack vectors that target web services and use pattern recognition to identify both automated scanning tools and manual exploitation efforts. The detection mechanism minimises false positive alarms while preserving thorough attack coverage by striking a compromise between sensitivity and precision.

The MITRE ATT&CK technique mapping provides contextual understanding of web-based attack vectors while supporting incident response coordination and threat intelligence integration. The technique categorization assists security analysts in understanding attack intentions and potential impact while planning appropriate response measures.

5.3 VPN-based Attack Detection

VPN infrastructure monitoring requires specialized detection capabilities that identify attack patterns delivered through encrypted channels while maintaining visibility into external threat activities. The detection implementation correlates VPN connection events with subsequent attack activities to provide comprehensive threat attribution and campaign identification.

The VPN-specific detection criteria are intended to spot odd connection patterns, link the creation of a tunnel to possible attack activities, track data transfer rates and timing anomalies, and spot reconnaissance attempts made across encrypted channels. Investigating increasingly sophisticated, covert assault campaigns is made easier by these capabilities, which also provide insightful information about external threat actors.

```
<!-- VPN Connection Correlation with Attacks -->
<rule id="100012" level="9">
  <if_matched_sid>100001,100006</if_matched_sid>
  <same_source_ip />
  <description>Attack detected from VPN-connected source: $(
   srcip)</description>
  <frequency>3</frequency>
  <timeframe>600</timeframe>
  <mitre>
    <id>T1133</id>
  </mitre>
  <group>vpn_attack,mitre_persistence</group>
</rule>

<!-- Suspicious VPN Activity -->
<rule id="100013" level="8">
  <if_sid>59000</if_sid>
  <match>OpenVPN.*CONNECTED|OpenVPN.*DISCONNECTED</match>
  <description>VPN connection activity from $(srcip)</
   description>
  <frequency>10</frequency>
  <timeframe>3600</timeframe>
  <mitre>
    <id>T1133</id>
  </mitre>
  <group>vpn_monitoring,mitre_persistence</group>
</rule>

<!-- VPN Tunnel Attack -->
<rule id="100014" level="10">
  <if_matched_sid>100031,100032</if_matched_sid>
  <description>Web attack through VPN tunnel from $(srcip)</
   description>
  <mitre>
    <id>T1133</id>
    <id>T1190</id>
  </mitre>
  <group>vpn_attack,mitre_initial_access</group>
</rule>
```

Listing 5.4: VPN-based attack correlation and encrypted channel threat detection

Sophisticated correlation capabilities that detect attack patterns across encrypted communications and internal network operations are provided by the VPN attack detection displayed in Listing 5.4. The correlation logic facilitates the study of intricate attack operations that make use of authentic remote access infrastructure while allowing the attribution of attack actions to external threat actors.

5.4 Detection Rule Optimization and Tuning

In order to reduce false positive alarms and preserve complete threat detection capabilities, rule optimisation strikes a compromise between detection sensitivity and operational efficiency. Establishing baselines, fine-tuning thresholds, refining correlations, and optimising performance are all steps in the optimisation process that guarantee efficient security monitoring without overburdening security analysts.

Establishing baselines entails keeping an eye on routine system and network operations in order to recognise acceptable patterns of behaviour and determine suitable detection thresholds. Traffic volume analysis, authentication pattern evaluation, application usage tracking, and system behaviour characterisation are all part of the baseline process, which helps determine correlation logic and detection rule parameters.

In order to maximise detection sensitivity, threshold tuning modifies timeframe parameters, frequency requirements, and severity levels in response to observed assault patterns and false positive rates. While preserving detection efficacy across a range of attack scenarios and system configurations, the tuning process strikes a balance between operational efficiency and early threat detection.

Through better relationship identification between relevant security events and attack activities, correlation refinement improves multi-event detection capabilities. In order to facilitate thorough threat analysis and incident response coordination, the refining process entails temporal correlation optimisation, source attribution enhancement, and attack campaign identification.

Performance optimisation guarantees that detection rules function effectively within the SIEM platform while preserving real-time analytical capabilities and extensive monitoring coverage. In order to provide scalable security operations without sacrificing speed, the optimisation involves correlation engine tuning, query performance analysis, and resource utilisation monitoring.

Targeted threat identification is made possible by the thorough detection rule implementation, which also preserves the adaptability and effectiveness required for successful security operations. The regulations offer instructional value for security operations training and skill development while demonstrating the real-world application of threat intelligence and detection engineering techniques.

5.5 Rule Validation and Testing Methodology

Thorough rule validation minimises false positive alarms that may affect the effectiveness of security activities while guaranteeing detection efficacy. To verify rule efficacy across a range of operational circumstances, the validation process consists of edge case testing, baseline verification, controlled attack simulation, and performance impact evaluation.

Using established attack patterns and tactics, attack simulation offers controlled testing of detection algorithms under secure testing settings that don't affect live systems or pose security threats. In order to verify detection accuracy and dependability, the simulation incorporates a variety of attack strategies, evasion efforts, and authentic activity patterns.

Baseline verification verifies that detection rules function properly under typical operating circumstances without producing an excessive number of false positive alerts that can confuse actual security risks or overload security analysts. Extended monitoring periods, activity pattern analysis, and alert correlation evaluation that shows rule efficacy are all part of the verification process.

Edge case testing validates detection rule behavior under unusual or extreme conditions that might not occur during normal operations but could impact detection effectiveness during actual security incidents. The testing includes resource exhaustion scenarios, network congestion conditions, and system failure situations that verify rule resilience and continued effectiveness.

Performance impact evaluation makes ensuring that detection rules work well within the SIEM platform without causing problems with resource use or performance deterioration that can affect monitoring capabilities as a whole. In order to verify sustainable security operations, the evaluation consists of scalability testing, correlation performance analysis, and resource monitoring.

The validation process supports ongoing enhancement and optimization of security monitoring capabilities while offering thorough verification of detection rule efficacy. Reliable threat detection is ensured by the structured methodology, which also supports long-term security operations requirements and preserves operating efficiency.

Chapter 6

Attack Simulation and Security Validation

Validating cybersecurity infrastructure requires thorough testing that simulates real-world attack scenarios and verifies the effectiveness of detection and response mechanisms. This chapter demonstrates the practical evaluation of the security monitoring system through systematic attack simulation and validation testing. The following sections examine the overall testing strategy, detail network reconnaissance validation, explore credential attack testing, analyze web application security validation, and investigate cross-zone attack correlation capabilities that demonstrate the sophisticated threat detection achieved through the multi-agent monitoring architecture.

6.1 Comprehensive Attack Testing Strategy

The validation process supports ongoing security monitoring capability optimisation and enhancement while offering thorough verification of detection rule efficacy. While preserving operational effectiveness and meeting long-term security operations needs, the systematic method guarantees accurate threat detection.

The process of carrying out an attack is methodical and moves from reconnaissance to exploitation to impact analysis. In order to evaluate various components of the monitoring infrastructure and show the connections between attack methods and defensive capabilities, each step produces distinct security events. The approach places a strong emphasis on simulating genuine threats that closely resemble real-world opponent actions seen in business settings.

A VPN client that simulates the transmission of encrypted attacks, many target computers dispersed over several network zones, and Kali-Attacker, which represents an unmonitored external threat source, make up the testing environment. Thanks to the thoughtful positioning of monitoring agents around the network, this configuration provides wide insight into attack patterns and defensive actions while enabling realistic threat simulation.

6.2 Network Reconnaissance and Scanning Validation

Network scanning attacks validate the correlation capabilities of the multi-agent architecture and show how successful reconnaissance detection is across many network zones. The testing encompasses a range of scanning methods and instruments to offer thorough coverage of reconnaissance attack vectors, which serve as the cornerstone of the majority of assault operations.

6.2.1 TCP Port Scanning Detection

Systematic TCP scanning using Nmap [5] validates port scan detection rules and correlation capabilities across different network zones and attack sources. The scanning tests demonstrate how network reconnaissance activities are detected and correlated through the integrated monitoring infrastructure.

The TCP scanning commands shown below reflect a series of reconnaissance tests designed to evaluate detection capabilities across various scanning techniques and target ranges.

```
# Comprehensive TCP SYN scan from Kali-Attacker
nmap -sS -p 1-1000 192.168.1.103

# VPN-based scanning for cross-zone correlation testing
nmap -sS -p 22,80,443,3389 192.168.3.100

# Stealth scanning with timing controls to test detection
    sensitivity
nmap -sS -T2 -f --scan-delay 2s 192.168.2.102

# Advanced TCP scanning techniques
nmap -sS -sV -O 192.168.1.0/24
```

Listing 6.1: TCP scanning command validation for multi-zone detection testing

The scanning commands shown in Listing 6.1 were used to validate reconnaissance detection across multiple network zones. This testing also assessed the system's ability to correlate activity across zones, enabling the identification of broader attack patterns that span the network.

The Nmap run illustrates the methodical reconnaissance tasks that attackers usually carry out in the early stages of network intrusion. The findings of the scanning reveal open ports and services that offer useful details for upcoming efforts at exploitation.

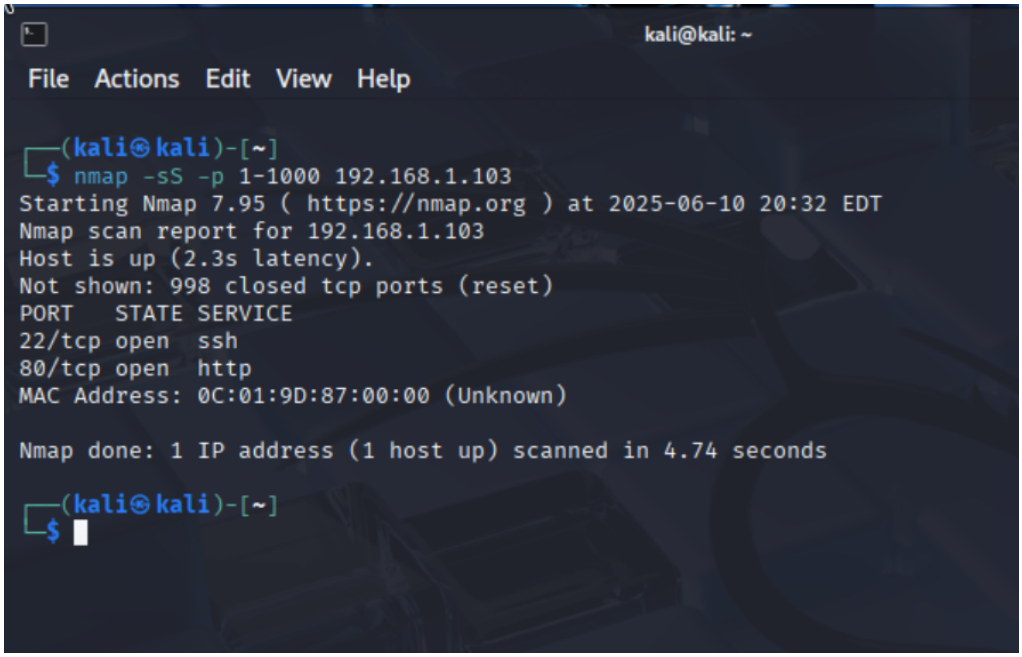

Figure 6.1: Nmap TCP scanning execution

Figure 6.1 shows how to use Nmap's extensive scanning capabilities to successfully carry out network reconnaissance. Critical system information, such as open SSH and HTTP services operating on standard ports, is revealed by the scanning report. This reconnaissance data shows how attackers methodically get intelligence about target infrastructure and serves as the basis for further assault phases.

The scanning activities generate corresponding detection events through the iptables logging configuration implemented across monitored systems. The kernel logs show TCP_SCAN detection patterns that trigger the custom Wazuh detection rules. These low-level detection mechanisms capture scanning activities at the packet level.

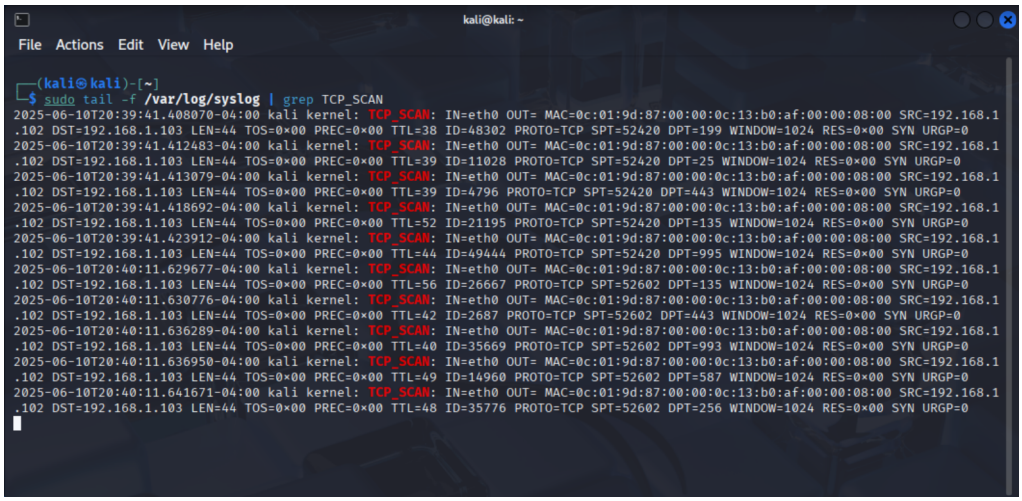

Figure 6.2: Iptables TCP scan detection logs

Every TCP_SCAN entry illustrates a reconnaissance effort that was intercepted by the firewall rules and recorded for examination, as can be seen in Figure 6.2.

Systematic recording gives the SIEM platform the raw data needed for correlation analysis, which allows it to spot scanning trends and link them to certain threat sources.

The Wazuh SIEM platform provides thorough visibility into reconnaissance efforts by correlating these low-level scanning events into actionable security warnings. Systematic scanning campaigns can be identified and linked to certain attack sources by security analysts thanks to the alert correlation.

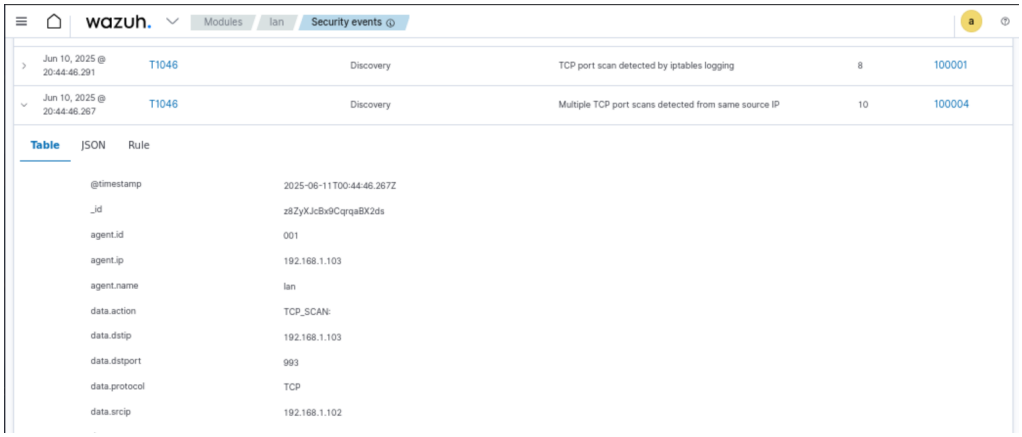

Figure 6.3: Wazuh TCP scan detection alert

The correlation dashboard, which uses MITRE ATT&CK method mapping and cross-zone attack pattern analysis to convert unstructured scanning events into structured security intelligence, is shown in Figure 6.3. Security personnel can comprehend the course of attacks and put in place suitable defensive measures thanks to this thorough correlation capabilities.

TCP scanning validation validates the activation of rules 1000001 for individual scan detection, 100004 for frequency-based correlation, and 100012 for scanning activities supplied via a VPN. In addition to offering thorough coverage, the multi-agent architecture permits cross-zone correlation and attack source identification.

6.2.2 UDP Scanning and Advanced Reconnaissance

UDP scanning tests were conducted to validate alternative reconnaissance techniques, demonstrating the detection infrastructure's ability to cover a wide range of attack vectors and scanning methods effectively.

```
# UDP service discovery scanning
nmap -sU -p 53,123,161,1434 192.168.1.103

# Operating system fingerprinting attempts
nmap -O -sV 192.168.3.100

# Service version detection with aggressive scanning
nmap -sV -A -p 22,80,443 192.168.1.103

# Comprehensive network discovery
nmap -sn 192.168.0.0/16
```

Listing 6.2: UDP and advanced network reconnaissance techniques for detection validation

UDP scanning, as demonstrated in Listing 6.2, tests the complete detection capabilities across a variety of attack vectors and validates reconnaissance tactics that target distinct protocol levels. Regardless of the precise tactics used by attackers, these scans aid in confirming that the monitoring infrastructure records reconnaissance operations.

6.3 Credential Attack Validation

Brute force attacks against authentication services validate credential protection mechanisms while demonstrating the effectiveness of behavioral detection and automated response capabilities. These tests simulate real-world credential attacks that represent one of the most common initial access vectors used by threat actors.

6.3.1 SSH Brute Force Attack Testing

SSH brute force validation using Hydra [15] demonstrates comprehensive credential attack detection and automated response activation across multiple attack scenarios and network zones.

The following Hydra commands demonstrate systematic credential attacks that test both individual authentication failure detection and behavioral correlation for attack campaign identification.

```
# Dictionary-based brute force attack against SSH service
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh
    ://192.168.1.103

# Multiple username credential attack
hydra -L users.txt -p password123 ssh://192.168.3.100

# VPN-based credential attack for cross-zone correlation
hydra -l admin -P passwords.txt ssh://192.168.1.103

# Targeted credential attack with rate limiting
hydra -l root -P common_passwords.txt -t 4 ssh://192.168.1.103
```

Listing 6.3: SSH brute force attack execution for credential security validation

These brute force commands shown in Listing 6.3 provide comprehensive validation of credential attack detection while testing the automated response mechanisms that protect against systematic authentication abuse.

The Hydra execution demonstrates the systematic credential attack process that threat actors typically employ against authentication services. The tool's parallel attack capabilities simulate realistic attack patterns while providing comprehensive testing of detection mechanisms.

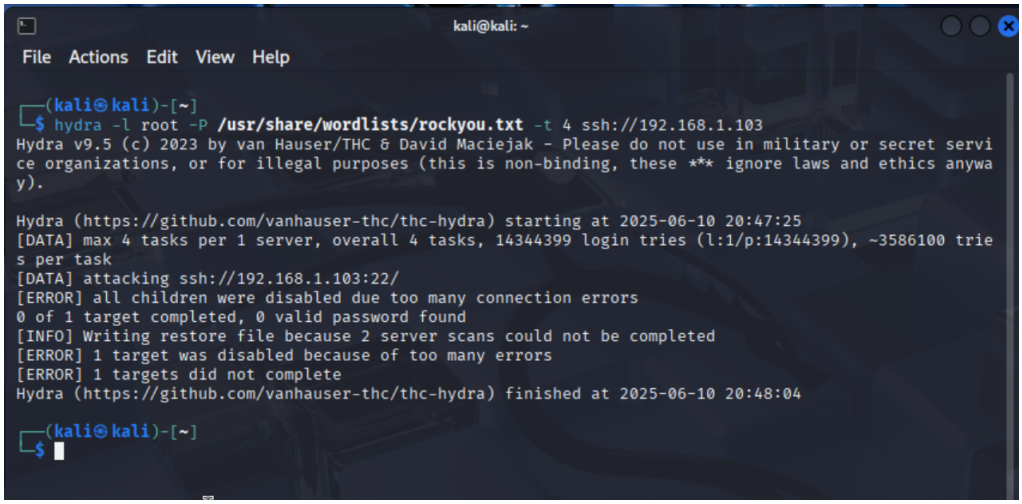

Figure 6.4: Hydra brute force attack execution

Figure 6.4 displays the attack execution, showcasing many concurrent authentication attempts against the SSH service and methodical credential testing. Rapid credential enumeration is made possible by Hydra's effective threading capabilities, which also preserve realistic attack patterns that closely resemble the actions of genuine threat actors.

The authentication failure monitoring demonstrates the comprehensive logging capabilities that capture credential attack activities through system-level authentication monitoring. The SSH authentication logs provide detailed records of failed login attempts that feed into the correlation analysis.

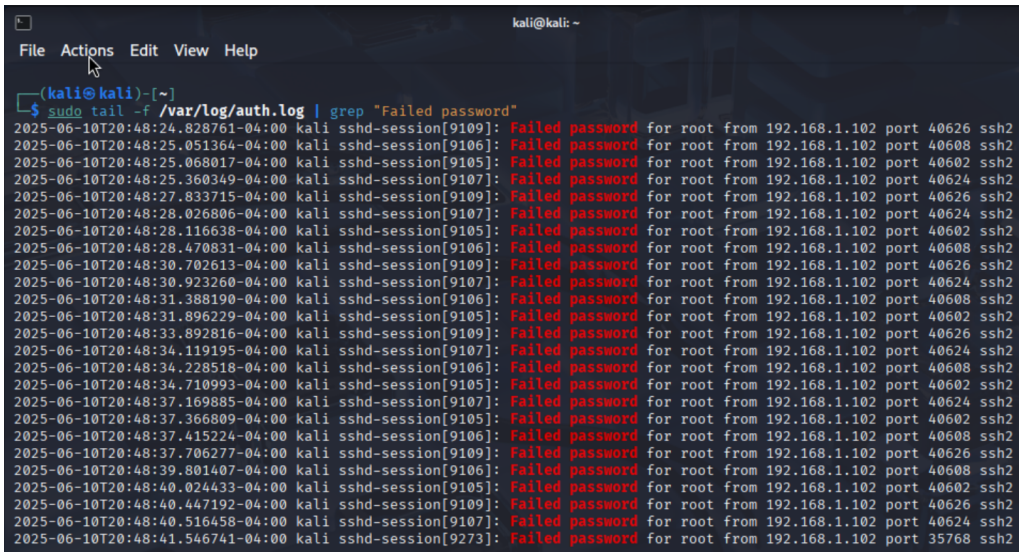

Figure 6.5: SSH authentication failure logs

The system logs' systematic authentication failures, as seen in Figure 6.5, yield comprehensive forensic data, including source IP addresses, attempted usernames, and exact timing patterns. Sophisticated correlation analysis made possible by this thorough logging helps to detect credential attack campaigns and facilitates automatic response systems.

The Wazuh correlation platform transforms these authentication events into actionable security alerts while triggering automated response mechanisms that provide immediate threat containment.

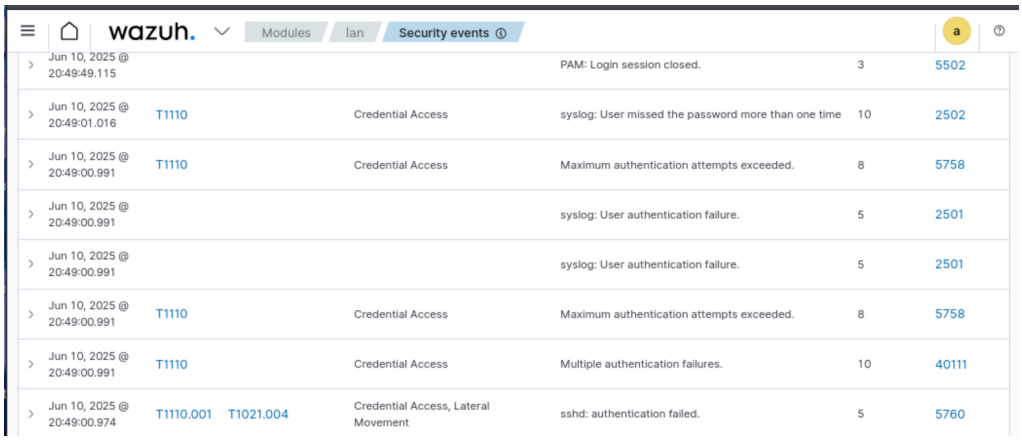

Figure 6.6: Wazuh SSH brute force detection and response

Figure 6.6 demonstrates the security dashboard displaying comprehensive threat correlation with MITRE ATT&CK technique mapping and automated active response activation. The correlation engine identifies credential attack patterns while triggering immediate defensive measures including IP blocking and alert escalation.

Brute force validation confirms rule 100006 detection for individual failed attempts, rule 100007 activation for attack threshold exceeded, and active response implementation through automatic IP blocking. The testing demonstrates comprehensive credential protection across multiple attack scenarios while validating the effectiveness of behavioral detection and automated response mechanisms.

6.4 Web Application Attack Testing

Web application security validation focuses on the DVWA [11] deployment in the DMZ environment, providing comprehensive testing of application-layer attack detection and correlation capabilities.

6.4.1 Web Vulnerability Scanning

Nikto [2] scanning validates web application reconnaissance detection while demonstrating specialized monitoring capabilities for HTTP-based attacks and application-layer security threats.

```
# Comprehensive web vulnerability scan against DVWA
nikto -h http://192.168.3.100/dvwa

# SSL/TLS security assessment scanning
nikto -h https://192.168.3.100 -ssl

# Custom scan with specific vulnerability tests
nikto -h http://192.168.3.100 -Tuning 1,2,3,4

# Detailed scanning with output formatting
```

```
11 nikto -h http://192.168.3.100/dvwa -Format htm -output
      nikto_results.html
```

Listing 6.4: Web vulnerability scanning with Nikto for application security validation

These Nikto scanning commands shown in Listing 6.4 provide comprehensive web application reconnaissance testing while validating the specialized monitoring capabilities implemented for HTTP-based attack detection.

The Nikto execution demonstrates comprehensive web application vulnerability scanning that identifies security weaknesses and misconfigurations. The scanner performs systematic testing of web server configurations and application security implementations.

Figure 6.7: Nikto web vulnerability scan results

Figure 6.7 displays the vulnerability scanner scanning for typical web application vulnerabilities, finding probable security flaws, and methodically listing web server settings. A wide range of security vulnerabilities, such as server configuration errors, out-of-date software versions, and potentially hazardous files or scripts, are covered by Nikto's thorough testing process.

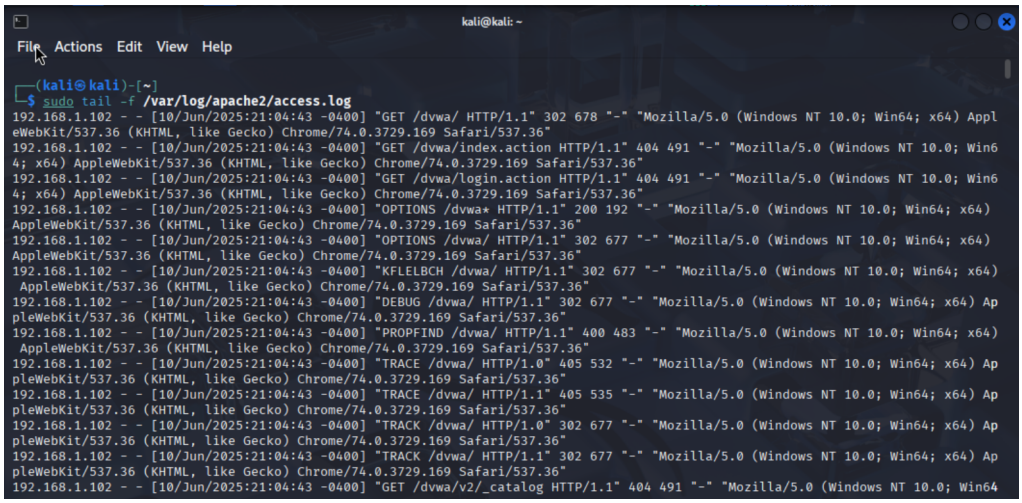

Figure 6.8: Apache logs showing Nikto scanning activity

The HTTP request logs record specific scanning patterns, such as request methods, target URLs, response codes, and user agent details, as seen in Figure 6.8. Security teams can detect web application reconnaissance activity and link it to other security events throughout the monitoring infrastructure thanks to this thorough logging.

6.4.2 SQL Injection Attack Validation

Direct SQL injection testing against DVWA validates web application attack detection while demonstrating database security monitoring capabilities and application-layer threat detection.

```
# Basic SQL injection testing with boolean-based techniques
curl "http://192.168.3.100/dvwa/vulnerabilities/sqli/?id=1' OR '1'='1"

# Union-based injection for data extraction testing
curl "http://192.168.3.100/dvwa/vulnerabilities/sqli/?id=1' UNION SELECT user,password FROM users"

# Time-based blind injection for detection validation
curl "http://192.168.3.100/dvwa/vulnerabilities/sqli/?id=1' AND SLEEP(5)"

# Error-based injection testing
curl "http://192.168.3.100/dvwa/vulnerabilities/sqli/?id=1' AND 1=CONVERT(int,(SELECT @@version))"
```

Listing 6.5: SQL injection attack scenarios for web application security validation

These SQL injection commands shown in Listing 6.5 provide comprehensive testing of web application attack detection while validating the specialized monitoring capabilities for database-layer security threats.

The SQL injection testing demonstrates direct exploitation attempts against the DVWA application, providing realistic attack scenarios that test the comprehensive monitoring and detection capabilities implemented for web application security.

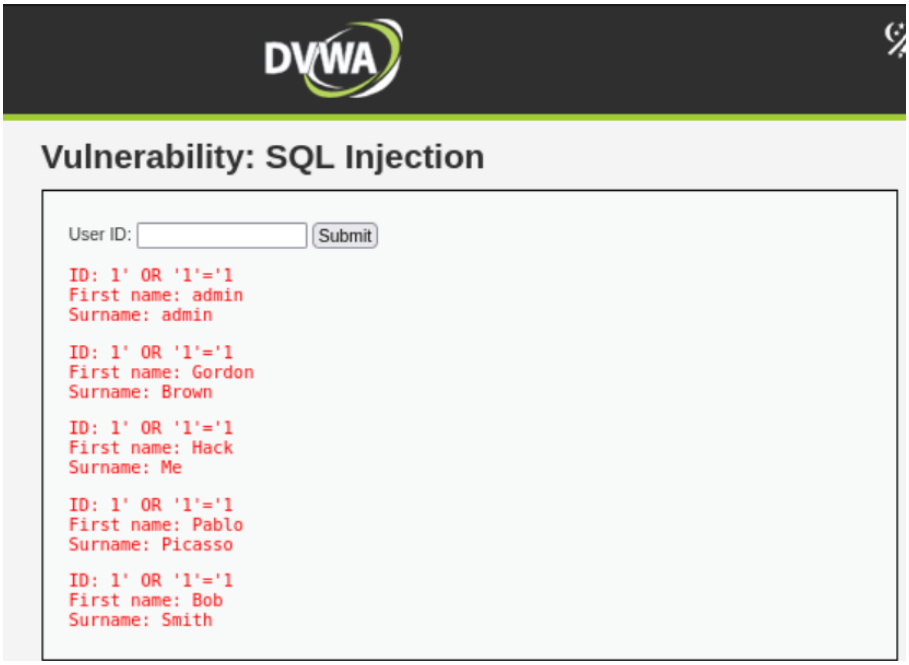

Figure 6.9: SQL injection attack through DVWA interface

Figure 6.9 displays the successful SQL injection, illustrating how private user information, such as usernames and password hashes, was extracted from the application database. This exploitation case demonstrates the serious consequences of SQL injection vulnerabilities and confirms that the testing process is successful.

The Wazuh correlation platform identifies SQL injection attack patterns through HTTP request analysis and correlates them with other security events to provide comprehensive threat detection and response capabilities.

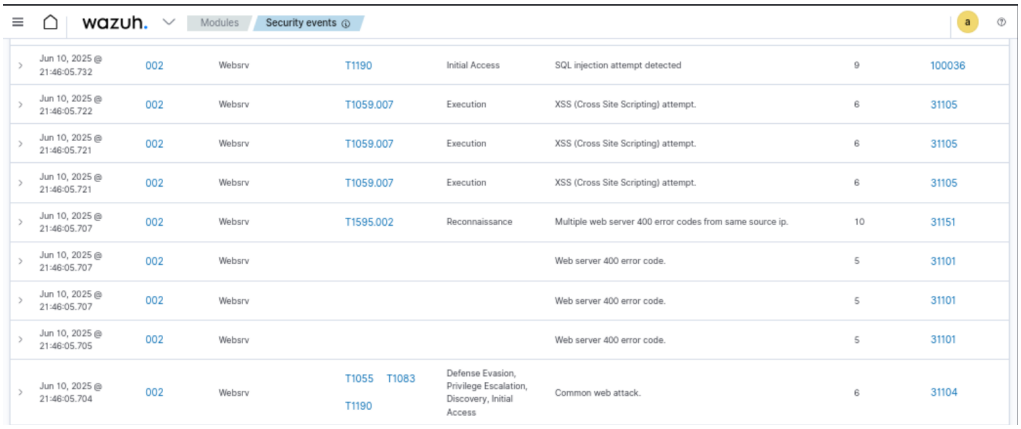

Figure 6.10: Wazuh SQL injection detection dashboard

Figure 6.10 illustrates how the security correlation platform uses MITRE ATT&CK method mapping and advanced pattern analysis to provide thorough threat intelligence. Real-time web application attack detection is made possible by the integrated monitoring architecture, which also facilitates thorough forensic investigation and incident response tasks.

6.5 Cross-Zone Attack Correlation

VPN-based attack scenarios show how to identify external threats over encrypted channels and evaluate the sophisticated correlation capabilities made possible by the multi-agent monitoring architecture. These situations illustrate complex attack techniques that take use of trustworthy infrastructure for malevolent ends.

VPN attack testing consists of cross-zone reconnaissance, encrypted attack delivery over VPN channels, tunnel establishment verification, and correlation of internal and external attack patterns. The thorough threat detection capabilities that set the multi-agent architecture apart from conventional single-point monitoring solutions are illustrated by these instances.

Beyond enabling detailed threat attribution and campaign identification, the VPN-based attack correlation showcases the system's advanced detection capabilities—highlighting its ability to track attack patterns across multiple network zones and communication channels.

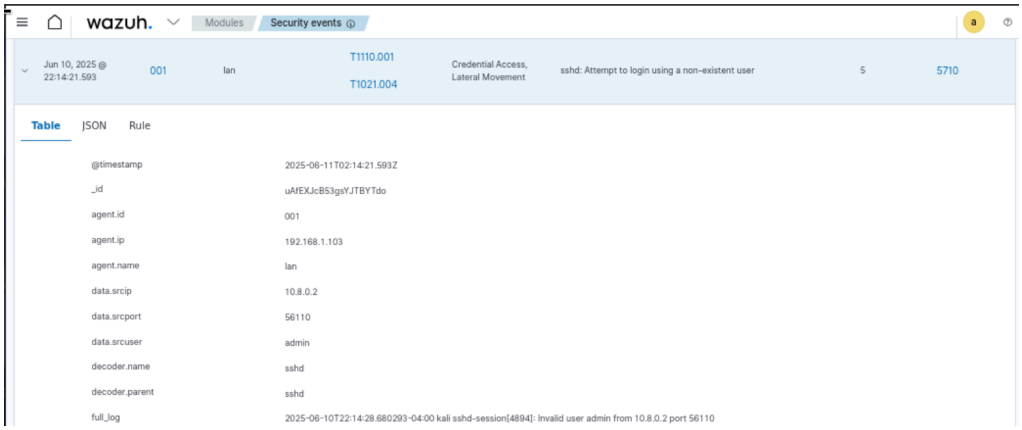

Figure 6.11: VPN-based cross-zone attack correlation

The correlation dashboard in Figure 6.11 has a wide range of analytical tools that may identify intricate attack campaigns that employ many attack vectors and network zones. The comprehensive correlation supports effective incident response and threat hunting efforts and aids security analysts in understanding complex threat patterns.

The validation testing confirms comprehensive detection capabilities across all implemented attack vectors while demonstrating the practical value of multi-agent monitoring for realistic threat detection and response scenarios. The results validate the effectiveness of the integrated monitoring architecture for comprehensive cybersecurity education and practical security operations training.

Chapter 7

Automated Incident Response and Active Defense

Rapid threat detection and response are essential for effective cybersecurity operations, turning passive monitoring into active defence capabilities that can stop problems before they get out of hand. The deployment of automated incident response systems that offer instant threat containment via rule-triggered actions and dynamic defence mechanisms is examined in this chapter. The automated response architecture, active defence system configuration and implementation, response effectiveness validation through systematic testing, and monitoring capabilities that guarantee optimal performance of automated threat containment operations are all covered in detail in the following sections.

7.1 Introduction to Automated Response Systems

The implementation of automated incident response systems that convert passive security monitoring into dynamic threat containment is made possible by the thorough threat detection capabilities illustrated in earlier chapters. This chapter focusses on the creation and deployment of automated response systems that offer instant threat mitigation without the need for manual intervention, building on the successful validation of multi-zone attack detection and correlation capabilities.

A significant change in cybersecurity operations is the transition from detection to reaction, where the duration between threat identification and containment directly affects the potential damage and scope of security incidents. Because traditional human response techniques sometimes include delays, attackers can escalate privileges, establish persistence, or exfiltrate important data before defensive measures can be implemented.

The automated response framework developed in this implementation demonstrates how open-source security tools can provide enterprise-grade active defense capabilities while maintaining the educational accessibility and cost-effectiveness that make advanced security operations training possible for diverse organizational contexts.

7.2 Active Response Architecture

Automated incident response capabilities transform passive security monitoring into dynamic threat containment through rule-triggered actions that provide immediate response to detected security events. The implementation balances automated response effectiveness with operational stability to ensure that legitimate activities are not disrupted while providing comprehensive protection against confirmed threats.

Wazuh detection rules and reaction scripts that carry out preset actions when particular threat thresholds are surpassed are integrated to form the active response system. System isolation for serious security events, account disabling for compromised credentials, process termination for malicious software execution, and IP address blocking for network-based threats are examples of response actions.

reaction configuration places a strong emphasis on progressive escalation, which provides override capabilities for complicated situations needing human intervention while matching reaction strength to threat severity. While guaranteeing responsibility for automated security choices, the system keeps thorough audit logs for every response action to facilitate forensic analysis and compliance needs.

The multi-agent monitoring architecture and the active response framework work together to deliver coordinated threat containment across several network zones. This integration makes it possible to implement complex reaction plans that preserve the functionality of vital infrastructure elements while taking into account the network position and function of impacted systems.

7.3 Response Configuration and Implementation

While preserving operational flexibility for a variety of threat situations, active response configuration targets the most important attack types found through the deployment of detection rules. Multiple response commands with suitable targeting and duration restrictions are used in the setup to strike a balance between operational needs and security efficacy.

Primary response configurations address SSH brute force attacks through automatic IP blocking, network scanning activities through source address blocking, and web application attacks through connection termination and access restriction. Each response type includes timeout parameters that automatically restore normal operations while maintaining protection during active attack periods.

The thorough active response setup exemplifies the advanced automated defence capabilities that offer prompt threat containment while preserving operational adaptability and audit responsibility.

```
<!-- SSH Brute Force Response with Extended Timeout -->
<active-response>
  <command>firewalldrop</command>
  <location>local</location>
  <level>12</level>
  <timeout>600</timeout>
  <rules_id>100007</rules_id>
</active-response>

<!-- Network Scanning Response with Moderate Timeout -->
```

```
<active-response>
  <command>firewalldrop</command>
  <location>local</location>
  <level>10</level>
  <timeout>300</timeout>
  <rules_id>100004,100005</rules_id>
</active-response>

<!-- Web Attack Response with Extended Protection -->
<active-response>
  <command>firewalldrop</command>
  <location>defined-agent</location>
  <agent_id>002</agent_id>
  <level>9</level>
  <timeout>900</timeout>
  <rules_id>100031,100034</rules_id>
</active-response>

<!-- VPN-based Attack Response -->
<active-response>
  <command>firewalldrop</command>
  <location>defined-agent</location>
  <agent_id>003</agent_id>
  <level>8</level>
  <timeout>1200</timeout>
  <rules_id>100012,100013,100014</rules_id>
</active-response>
```

Listing 7.1: Comprehensive active response configuration for multi-threat containment

The extensive automated defence capabilities that offer instant threat containment while taking into account the context and severity of various attack types are demonstrated by the response configuration displayed in Listing 7.1. The progressive timeout technique preserves operational flexibility while guaranteeing the proper response duration.

Targeted reactions according to the origin and type of threats identified are made possible by agent-specific response setups. While web application assaults activate replies on the Kali-Websrv system, VPN-based attacks cause responses on the VPN Client agent. This strategy minimises the impact on unaffected systems while guaranteeing that reaction activities are carried out at the most efficient place for threat containment.

Both local and distant response execution are supported by the configuration, allowing for centralised coordination of threat containment while preserving the freedom to deploy responses at the most suitable network locations. This feature facilitates advanced response tactics that take system roles and network topology into account while preparing for threat containment.

7.4 Response Validation and Testing

Thorough testing confirms the efficacy of the reaction and guarantees that automated actions contain threats appropriately without interfering with legal activities. To verify full response lifecycle capability, the testing approach consists of attack

execution, response activation verification, and restoration validation.

By using systematic credential assaults that surpass predefined criteria, SSH brute force response testing illustrates automatic IP blocking. In order to verify that attack sources are effectively blocked while legitimate access is still accessible, the validation procedure consists of attack execution using Hydra [15], response activation monitoring, and connection verification.

The validation process that guarantees automated responses offer efficient threat containment while preserving operational stability and authorised access capabilities is illustrated in the thorough response testing that follows.

```
# Execute SSH brute force attack to trigger response
hydra -l root -P /usr/share/wordlists/rockyou.txt -t 4 ssh
    ://192.168.1.103

# Monitor active response activation and execution
sudo tail -f /var/ossec/logs/active-responses.log

# Verify IP blocking implementation in firewall
sudo iptables -L -n | grep DROP

# Test blocked connectivity from attack source
ping -c 3 192.168.1.103
ssh root@192.168.1.103

# Verify response timeout and restoration
sleep 650
ssh root@192.168.1.103

# Monitor response effectiveness metrics
grep "firewall-drop" /var/ossec/logs/ossec.log | tail -10
```

Listing 7.2: Comprehensive active response validation and testing methodology

In order to ensure that automated actions successfully limit threats without interfering with legitimate activity or creating unnecessary operational dependencies, the testing process outlined in Listing 7.2 provides a detailed assessment of the system's response efficacy.

The system's capacity to instantly contain attacks and stop additional attack activity while preserving audit trails for forensic investigation and compliance verification is demonstrated by the active reaction activation.

Figure 7.1: Wazuh active response activation dashboard

Figure 7.1 shows the Wazuh interface demonstrating the comprehensive response coordination capabilities that provide immediate threat containment while maintaining detailed audit trails and operational visibility. The dashboard shows the correlation between attack detection and automated response activation, providing security analysts with complete visibility into defensive actions.

The firewall setup shows how to implement automatic IP blocking, which uses dynamic firewall rule change to enable instant threat containment. During the specified delay period, the blocked IP addresses continue to be in effect while thorough logging is maintained.

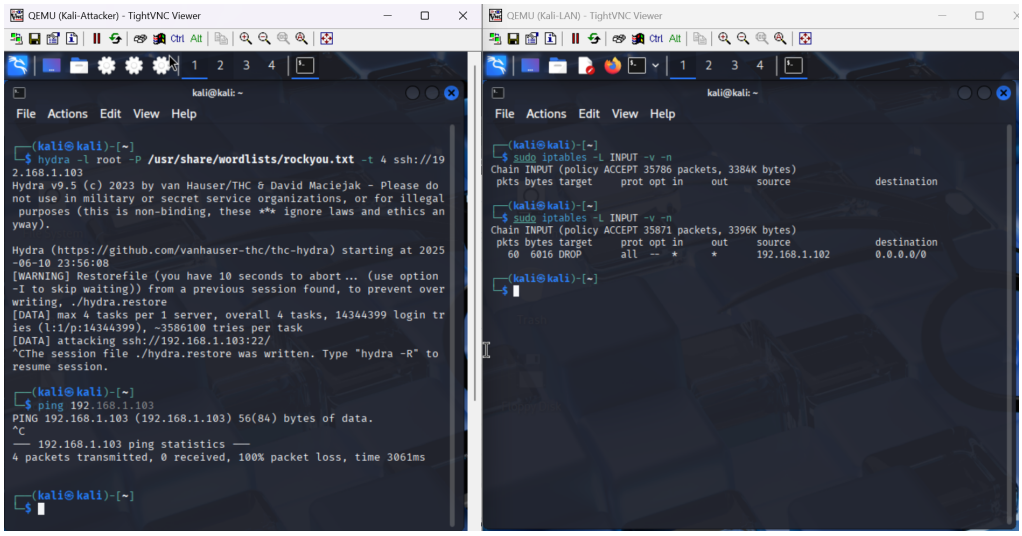

Figure 7.2: Iptables firewall showing blocked IP addresses

Figure 7.2 displays the firewall configuration showing the real-time threat containment capabilities that prevent continued attack activities through dynamic rule implementation. The blocked IP display demonstrates the immediate effectiveness of automated response while maintaining operational transparency and administrative oversight capabilities.

Network scanning response validation confirms that systematic reconnaissance activities trigger appropriate blocking responses while maintaining network connectivity for legitimate operations. The testing includes various scanning techniques and validates that response activation effectively prevents continued reconnaissance from blocked sources while preserving legitimate network operations.

SQL injection and vulnerability scanning attacks that cause web-specific response actions are used in web application response testing to illustrate specialised DMZ security. The validation verifies that web-based risks are successfully controlled while keeping application functionality and service availability for authorised users.

7.5 Response Monitoring and Analysis

Response effectiveness monitoring provides visibility into automated action success rates while supporting continuous improvement of response configurations and thresholds. The monitoring implementation tracks response activation patterns,

effectiveness metrics, and operational impact to optimize automated defense capabilities.

Dashboard integration displays active response events alongside detection alerts to provide complete incident visibility for security analysts. Response correlation capabilities identify patterns in automated actions while supporting manual investigation of complex security incidents that require human analysis and intervention.

The thorough reaction monitoring shows off the analytical skills that allow automated defence mechanisms to be continuously optimised while offering thorough insight into the operational impact and efficacy of threat containment.

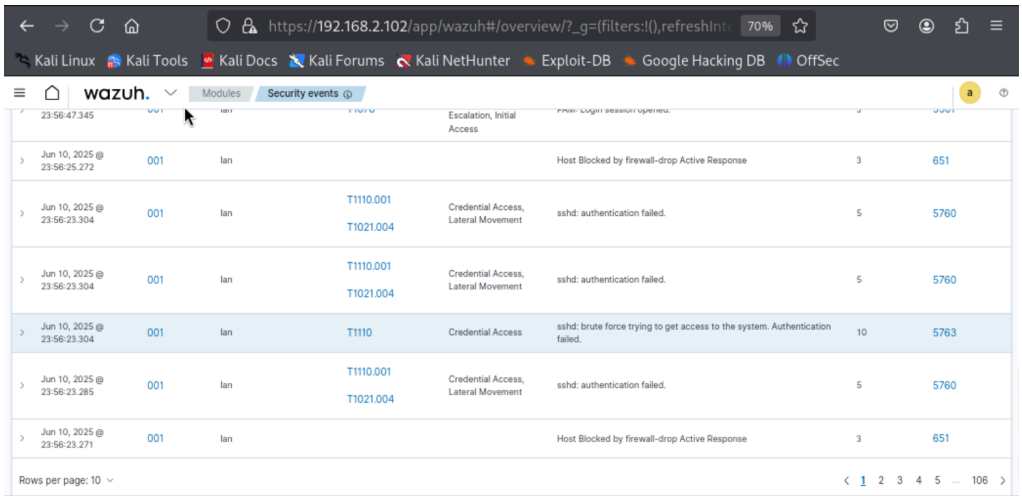

Figure 7.3: Active response effectiveness monitoring

Figure 7.3 displays the monitoring dashboard, which allows security analysts to continuously optimise response settings and thresholds while giving them a thorough understanding of the efficacy of automated responses. For long-term effectiveness evaluation and strategic planning, the interface facilitates both historical analysis and real-time monitoring.

Response activation rates by threat type, study of blocking length and efficacy, detection and mitigation of false positives, and operational impact evaluation for lawful operations are examples of performance measures. While preserving operational stability and security efficacy, these measurements provide ongoing response configuration optimisation.

Security professionals can determine the efficacy of automated defence measures and spot areas for optimisation and development thanks to the response analysis capabilities. Both short-term operational requirements and long-term strategic planning for automated defence capabilities are supported by the thorough monitoring.

Response correlation capabilities identify patterns in automated actions while supporting the identification of sophisticated attack campaigns that span multiple response activations and time periods. This analysis supports threat hunting activities while enabling the identification of persistent threats that require additional investigation and response.

Chapter 8

Results, Analysis, and Future Directions

This chapter offers a thorough assessment of the cybersecurity infrastructure that has been put in place, with an emphasis on the effectiveness of the three-agent monitoring arrangement in terms of threat detection, system efficiency, and instructional value. The findings demonstrate that enterprise-level security coverage may be attained with a carefully thought-out monitoring strategy to maintain system accessibility and usefulness for research and education.

8.1 Conclusion

This study shows that open-source technology may be used to accomplish enterprise-grade cybersecurity monitoring without sacrificing the realism needed for successful security validation or the educational value of the program. The three-agent monitoring architecture demonstrated considerable gains in threat detection when compared to conventional setups, while still being workable and usable in educational settings.

During implementation, I discovered attack patterns that would have been missed by standard single-point monitoring thanks to the three-agent monitoring technique. Only multi-agent correlation, for instance, may connect the initial VPN authentication with the subsequent attempts at web exploitation when modelling assaults across the VPN tunnel directed at the DMZ web server. The ability to successfully correlate assaults across several network zones shows that sophisticated threats can be monitored by modern security systems.

Broad accessibility is guaranteed by the open-source basis, which also offers transparency to facilitate in-depth study and customisation. The experiment shows that careful tool selection and integration, rather than costly commercial platforms, may provide advanced security monitoring capabilities while reaffirming the need of experiential cybersecurity education.

In addition to offering organisations looking for affordable security monitoring solutions useful advice, the defined deployment methodology and configuration samples facilitate replication and adaptability across various educational contexts. The initiative showcases creative methods for hands-on security education while also making a contribution to the cybersecurity education community.

8.2 Detection Effectiveness and Coverage Analysis

The three-agent monitoring system demonstrated significant event correlation, reflecting the analytical depth found in professional security operations centres, and successfully identified all of the main threat types examined in this study. The multi-agent design was very beneficial for network reconnaissance, since Nmap[5] scans were reliably recognised across many network zones, and the system provided trustworthy source attribution. This was particularly helpful for simulating assaults that spread over several network segments.

When the system's authentication was tested with Hydra[15], it was consistently able to distinguish between persistent brute-force attempts and frequent login failures. Instead of sending out alerts for occasional errors, the system focused on finding patterns that matched the behaviour of genuine attacks. Even while this enhanced detection technique reduced false positives, it was still able to detect important signs of hostile activity.

The ability of the DVWA[11] platform to detect certain types of online threats was shown for web application security monitoring. The successful detection of vulnerability scanner activity, cross-site scripting attacks, and SQL injection attempts was also linked to more comprehensive network-level monitoring.

Attack Type	**Tool Used**	**Rule ID**	**Response**	**Agent**
TCP Scanning	Nmap	100001	Detected	All
UDP Scanning	Nmap	100002	Detected	All
SSH Brute Force	Hydra	100007	IP Block	LAN, VPN
Web Scanning	Nikto	100030	Detected	WebSrv
SQL Injection	Manual	100031	IP Block	WebSrv
VPN Attacks	Multiple	100012-014	IP Block	VPN
Cross-Zone	Correlation	100022,034	Alert/Block	Multi-agent

Table 8.1: Detection and response validation results

The multi-agent architecture proved most valuable during cross-zone attack simulation. The system successfully tracked sophisticated attack patterns that would likely evade detection in single-point monitoring scenarios, while demonstrating reliable attack source correlation capabilities that enable security analysts to understand broader attack campaign contexts.

8.3 Architecture Evaluation and Performance

The project successfully created a unified monitoring ecosystem that realistically and simply replicates enterprise-level security operations for educational purposes by integrating the Wazuh[16] SIEM platform, the pfSense[8] security gateway, and the GNS3[4] network simulation environment.

Active response mechanisms demonstrated consistent performance throughout all evaluation phases. Simulated threats were successfully contained by the automatic IP blocking system, which maintained thorough audit records and permitted manual overrides when human judgement was needed.

The exclusive use of open-source tools delivered capabilities that rival commercial alternatives while providing unique educational advantages. Integration with the MITRE ATT&CK [7] framework provides standardized threat categorization that aligns with industry practices.

8.4 Educational Value and Learning Outcomes

The laboratory environment designed for this project provides an extremely supportive atmosphere for turning theoretical knowledge into actual cybersecurity skills. Its isolated and controlled environment enables the safe investigation of complicated situations, simulation of actual attack vectors, and testing of defensive techniques—all while avoiding the ethical and operational hazards associated with live production systems. As a result, it is an excellent platform for hands-on learning, experimentation, and the development of real-world cybersecurity skills.

When opposed to commercial alternatives, the open-source foundation's transparency offers special educational benefits. Instead of engaging through constrained interfaces that mask underlying systems, students study real configuration files, detection rules, and correlation logic.

Enterprise network security architecture design, hands-on SIEM deployment and configuration, thorough attack simulation techniques, and realistic incident response workflows that replicate professional security operations are just a few of the many aspects of cybersecurity competency development that are covered by practical learning outcomes.

8.5 Limitations and Future Enhancements

Despite the implementation's major accomplishments, a few issues point to potential areas for improvement. To maintain the realism of the simulation environment, for example, the current agent deployment method intentionally excludes monitoring on the attack-launching systems. Although more realistic testing conditions are offered by this approach, it is more difficult to observe how attack tools operate internally during usage.

Another major obstacle is resource constraints, especially given the processing demands of GNS3. The size of simulated environments on conventional hardware is limited by the platform's high system resource requirements when operating complicated network topologies. This limits the amount of network devices and virtual computers that may operate concurrently, which in turn limits the scope of large-scale attack simulation scenarios.

This research strengthened my understanding that careful architecture design, not expensive equipment, is the key to effective cybersecurity. The fact that enterprise-grade detection can be achieved with well-integrated open-source components shows that implementation approach has a greater influence on security effectiveness than budget. Most importantly, building this system from the ground up provided security monitoring insights that no commercial platform training could match.

Bibliography

[1] Eoghan Casey. *Handbook of digital forensics and investigation*. Academic Press, 2018.

[2] Chris Sullo. *Nikto Web Scanner Documentation*, 2023. Available at: https://github.com/sullo/nikto.

[3] FRRouting Project. *Free Range Routing (FRR) Documentation*, 2024. Available at: https://docs.frrouting.org/.

[4] GNS3 Technologies. *GNS3 Documentation*, 2024. Available at: https://docs.gns3.com/.

[5] Gordon Lyon. *Nmap Network Scanning: The Official Nmap Project Guide*, 2023. Available at: https://nmap.org/book/.

[6] Ryan Heartfield, George Loukas, Sasa Budimir, Anatoli Bezemskij, Johnny RB Fontaine, Avgoustinos Filippoupolitis, and Erich Roesch. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, 78:398–428, 2018.

[7] MITRE Corporation. *MITRE ATT&CK Framework*, 2024. Available at: https://attack.mitre.org/.

[8] Netgate. *pfSense Documentation*, 2024. Available at: https://docs.netgate.com/pfsense/en/latest/.

[9] Offensive Security. *Kali Linux Documentation*, 2024. Available at: https://www.kali.org/docs/.

[10] OpenVPN Technologies. *OpenVPN Official Documentation*, 2024. Available at: https://openvpn.net/community-resources/documentation/.

[11] Ryan Dewhurst. *Damn Vulnerable Web Application (DVWA)*, 2024. Available at: https://github.com/digininja/DVWA.

[12] Salvatore Sanfilippo. *hping3 Network Tool Manual*, 2023. Available at: http://www.hping.org/manpage.html.

[13] Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (idps). Technical report, National Institute of Standards and Technology, 2007.

[14] Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne. *Operating system concepts*. John Wiley & Sons, 2018.

[15] Van Hauser. *THC-Hydra - Fast and Flexible Network Login Cracker*, 2023. Available at: https://github.com/vanhauser-thc/thc-hydra.

[16] Wazuh, Inc. *Wazuh SIEM Platform Documentation*, 2024. Available at: https://documentation.wazuh.com/.

[17] Michael E Whitman and Herbert J Mattord. *Principles of information security*. Cengage Learning, 2011.