Blue Ants: Mini Security Operations Center (SOC) Project

System Analysis:

1. High-Level System Overview

The project implements a segmented virtualized Security Operations Center (SOC) environment with three dedicated subnets managed through a central pfSense firewall. This architecture enables controlled security monitoring with isolated network segments for comprehensive threat detection and analysis across subnets.

- **Primary Inputs:** Security events from Victims VMs (Windows, Linux), Network Telemetry from pfSense firewall with Snort IDS, and Attack Traffic from Kali Linux VM

- **Core Processing:** Centralized aggregation, normalization, correlation, and alerting performed by Wazuh SEIM

- **Primary Outputs:** Security alerts, incident reports, cross-subnet attack analysis, MITRE ATT&CK mappings, and operational KPIs

2. Stakeholder Analysis

Stakeholders

- **SOC Analyst**: Monitors cross-subnet attacks through Wazuh dashboard, investigates incidents, generates security reports

- **Penetration Tester**: Operates Kali Linux VM from attacker subnet, simulates attacks, validates detection capabilities

- **Infrastructure Admin:** Manages hypervisor, subnet routing, VM deployments across segmented network architecture

3. Functional Requirements

FR1: **Segmented Network Log Ingestion Pipeline**

- Install and configure Wazuh on Ubuntu Server in monitoring subnet

- Install and register Wazuh agents on Windows VM and Linux VM in victim’s subnet

- Configure pfSense VM with Snort IDS for gateway duties and cross-subnet monitoring

- Configure syslog forwarding from all subnets through pfSense to Wazuh server

- Deploy Kali Linux VM in attacker DMZ subnet for controlled security testing

***FR2:* <u>Cross-Subnet Attack Detection & Correlation</u>**

- Implement and tune Wazuh's built-in decoders and rules for cross-subnet attack detection

- Develop and activate custom correlation rules for Kali VM attack scenarios across subnets:

  - Brute Force Attack (detecting hydra attacks crossing subnets)

  - Network Reconnaissance (detecting Nmap scans between segments)

***FR3:* <u>Cross-Subnet Attack Triage & Analysis</u>**

- Use Wazuh dashboard to investigate alerts triggered by cross-subnet Kali VM activities

- Map multi-subnet attack sequences to MITRE ATT&CK framework

- Document TTPs (Tactics, Techniques, Procedures) and IOCs from cross-subnet attacker activities

***FR4:* <u>Segmented Environment Reporting & Validation</u>**

- Generate cross-subnet attack analysis reports covering Kali VM activities

- Extract detection efficacy KPIs against known multi-subnet attack sequences

- Perform Root Cause Analysis for successful cross-subnet attack simulations

4. Non-Functional Requirements

- **Performance:** The Wazuh Ubuntu server must process cross-subnet attack traffic and logs from Kali VM activities while maintaining real-time detection capabilities

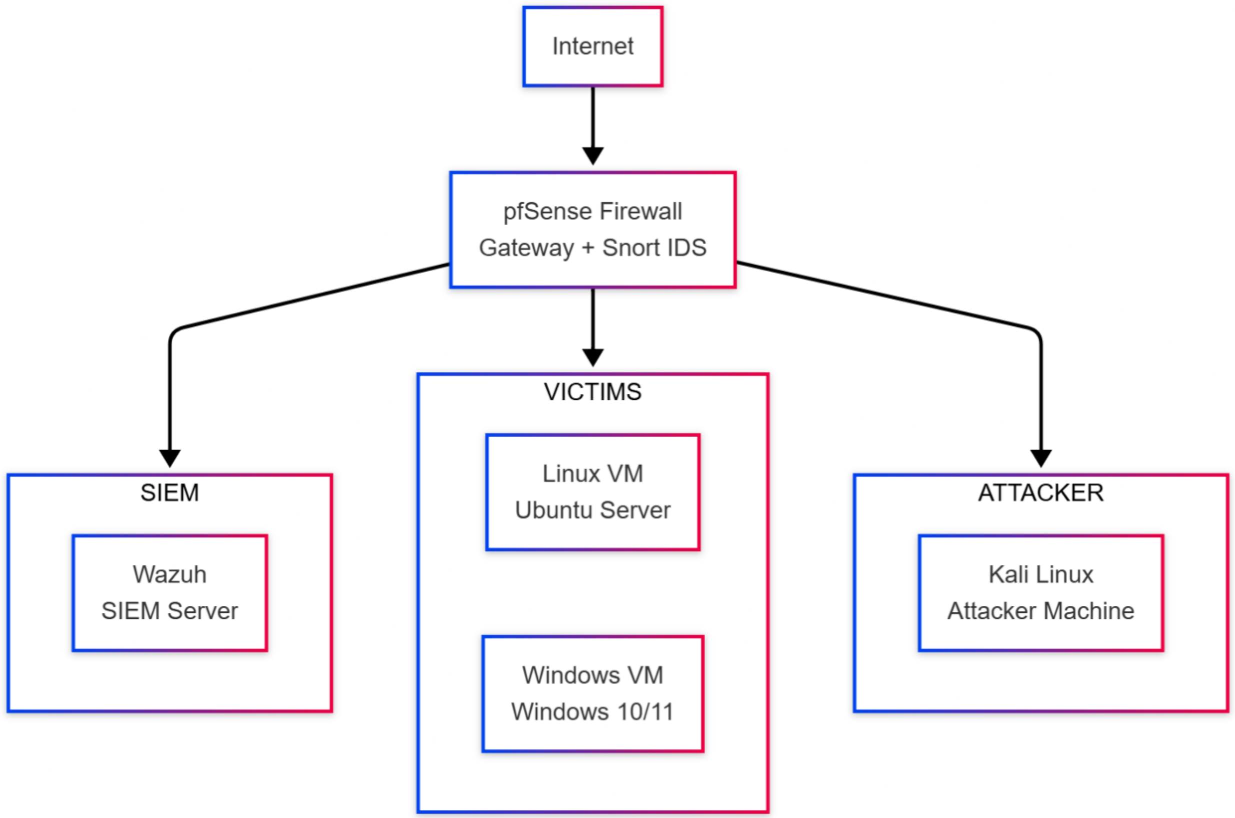
- **Segmented Network Management:** Ensure proper subnet routing and firewall rules while maintaining comprehensive security monitoring coverage

- **Attack Isolation:** Implement controlled attack scenarios between subnets to prevent accidental VM compromise while maintaining realistic testing

- **Forensic Capability:** Maintain sufficient logging and evidence collection from all subnets to support cross-subnet attack chain reconstruction

5. System Architecture & Technology Stack

Segmented Network Virtual Infrastructure Architecture



Technology Stack Analysis

- **1) SIEM & Core Platform:** Wazuh on Ubuntu Server

- **Role:** Central correlation and analysis platform detecting and documenting cross-subnet Kali VM attack activities from monitoring subnet

- **2) Firewall & IDS:** pfSense VM with Snort

- **Role***:* Network gateway with Snort IDS providing segmentation, filtering, and cross-subnet traffic monitoring and logging

- **3) Victims Endpoints:** Windows VM & Linux VM

- **Role:** Target systems in victims' subnet for Kali VM attacks, running Wazuh agents for endpoint detection and response

- **4) Attacker Platform:** Kali Linux VM

- **Role:** Dedicated attack machine in DMZ subnet running penetration testing tools (Nmap, Metasploit, burp suite, hydra, etc.)

Segmented Network Implementation:

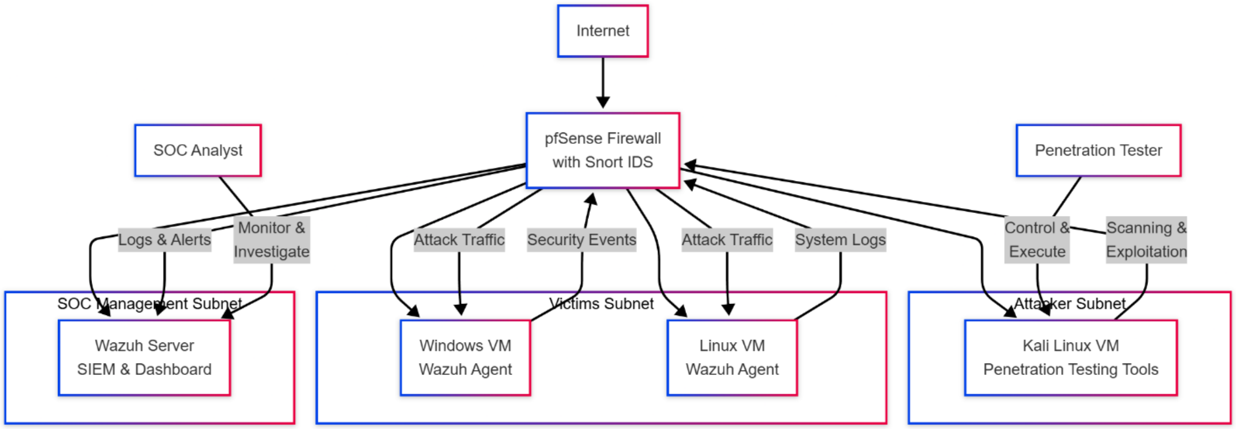
- **Network Architecture:** Three isolated subnets (Management, Victims, Attacker) with controlled routing through pfSense

- **Subnet Routing:** Controlled communication between subnets via pfSense firewall rules with Snort inspection

- **Service Discovery:** Managed access between subnets for comprehensive security testing and monitoring

- **Attack Surface:** Controlled exposure between segments for detection validation and security control testing

6.Traffic Flow Analysis



1. Cross-Subnet Attack Execution

- Kali Linux VM executes reconnaissance, exploitation, and post-exploitation attacks from attacke subnet

- Attacks traverse subnet boundaries through pfSense to target victims VMs

- Snort IDS detects cross-subnet network attacks and generates alerts

- pfSense firewall logs all inter-subnet attack traffic and connection attempts

2. Multi-Subnet Endpoint Detection

- Wazuh agents on Windows and Linux VMs in victim’s subnet detect attack artifacts:

  - Cross-subnet authentication attempts and failures

  - Suspicious process creation from external subnets

  - File modifications and integrity changes from network attacks

  - Registry and system configuration changes from remote exploitation

3. Cross-Subnet Centralized Correlation

- Wazuh on Ubuntu Server in monitoring subnet correlates attacks across multiple subnets:
  - Snort IDS alerts + cross-subnet authentication failures = brute force detection
  - Inter-subnet network scans + subsequent exploitation attempts = attack progression

4. Segmented Environment Incident Response

- SOC analyst investigates correlated alerts from cross-subnet Kali VM activities through Wazuh dashboard
- Multi-subnet attack timeline reconstruction using logs from all segments through pfSense
- MITRE ATT&CK mapping of complete cross-subnet attack kill chain
- Documentation of TTPs and IOCs from cross-subnet attacker activities

---

7. Risk Analysis & Mitigation Strategies

Network Connectivity Risks

- **1) Subnet Routing Complexity:** Multiple subnets with centralized pfSense routing
  - **Fix:** Test and document routing between all subnets, verify firewall rules for monitoring traffic
- **2) Cross-Subnet Monitoring Challenges:** Wazuh requires visibility across network segments
  - **Fix:** Ensure Wazuh Ubuntu server in monitoring subnet can communicate with all other subnets through pfSense
- **3) Firewall Rule Management:** Complex pfSense rules managing inter-subnet traffic
  - **Fix:** Document and test firewall rules, implement allow rules for essential monitoring traffic

Computational Power Requirements

- **4) CPU Resources:** Multiple VMs across segmented network architecture with routing overhead
  - **Fix:** 2+ core for Wazuh Ubuntu server, 1 core for other VMs, prioritize resource allocation
- **5) Memory Overload:** Segmented architecture increases memory overhead
  - **Fix:** Wazuh Ubuntu (8GB), Kali (4GB), pfSense (2GB), Windows (4GB), Linux (4GB) = 22GB minimum
- **6) Storage I/O Contention:** Multiple VMs across subnets competing for disk access
  - **Fix:** Use SSD storage, separate VMDK files, implement storage prioritization

Infrastructure Requirements

- **7) Host System:** 8 cores, 32GB RAM, 250GB SSD minimum for segmented environment

  - **Fix:** Close background applications, implement resource monitoring, strategic VM allocation

- **8) Network Bandwidth:** Inter-subnet communication requires stable virtual switching through pfSense

  - **Fix:** Use bridged networking, ensure host NIC capacity for cross-subnet traffic

---

8. Success Metrics (KPIs)

Cross-Subnet Attack Detection KPIs

- **Detection Coverage:** Percentage of cross-subnet Kali VM attack techniques successfully detected

- **Time to Detection:** MTTD for various cross-subnet attack stages (reconnaissance, exploitation, persistence)

- **False Positive Rate**: Ratio of false alerts to true cross-subnet attacks from Kali VM activities

Segmented SOC Performance Metrics

- **Cross-Subnet Attack Reconstruction:** Ability to document complete attack sequence across multiple subnets

- **MITRE ATT&CK Coverage:** Number of techniques detected from Kali VM toolset in cross-subnet attacks

- **Incident Response Time:** Time from cross-subnet attack detection to completed analysis and reporting

Segmented Security Control Effectiveness

- **Prevention Rate:** Percentage of cross-subnet attacks blocked by security controls

- **Detection Rate:** Percentage of cross-subnet attacks detected by monitoring systems

- **Analysis Quality:** Completeness and accuracy of cross-subnet attack reports and documentation

---

9. Conclusion

The Blue Ants Mini-SOC project creates a practical learning environment for understanding security operations in segmented networks. The three-subnet architecture with SIEM, Victims, and Attackers segments provides a clear separation of functions while maintaining essential monitoring capabilities.

The Wazuh installation on Ubuntu Server serves as the central monitoring platform, offering comprehensive security visibility across all network segments. Combined with pfSense firewall and Snort IDS, this setup demonstrates fundamental security monitoring principles in a controlled virtual environment.

This implementation focuses on building practical skills in security tool configuration, log analysis, and basic incident investigation. The segmented network approach helps understand how security controls operate in different network zones and how to monitor traffic between them.

The project provides a solid foundation for learning enterprise security concepts while maintaining simplicity for educational purposes. It offers hands-on experience with essential security tools and workflows, preparing participants for further exploration in cybersecurity operations.