BazTech SOC Project Report

Executive Summary

This report presents the execution of the BazTech SOC Project, which simulated a Security Operations Center (SOC) within a segmented network to detect, analyze, and respond to cyber threats. The project utilized pfSense for network segmentation, Wazuh for centralized log monitoring, and Kali Linux to simulate attack scenarios.

Key outcomes included the detection of SSH brute-force attacks, log correlation across Linux and Windows systems, and identification of potential lateral movement risks. The project demonstrated the importance of network segmentation, centralized monitoring, and proactive detection measures.

Recommendations focus on strengthening firewall rules, implementing stricter authentication policies, and establishing standard operating procedures for incident response. This project validates that a properly configured SOC can significantly improve organizational security posture.

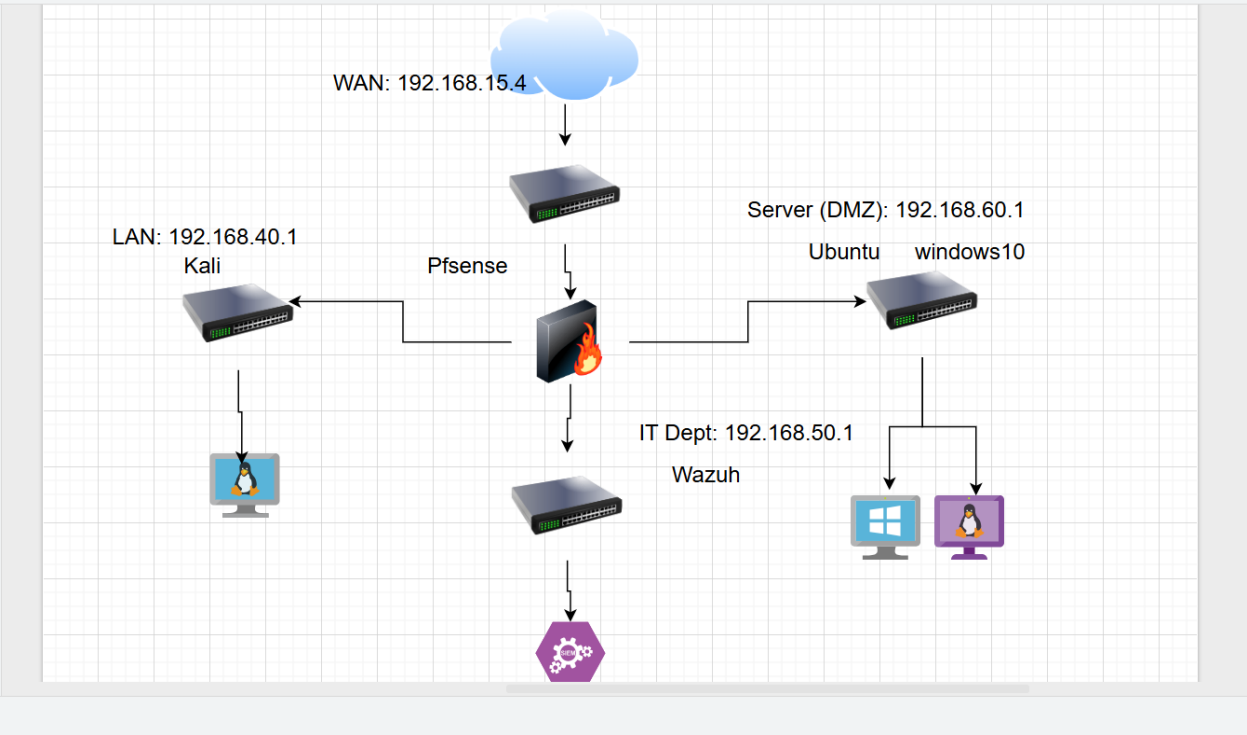
1. Introduction

This project simulated a Security Operations Center (SOC) for BazTech Inc., a startup aiming to secure its segmented infrastructure. Using pfSense for network segmentation, Wazuh for monitoring, and Kali Linux for attack simulation, the project demonstrated detection, analysis, and reporting of cyber threats.

2. Project Setup

- **Network Segmentation (pfSense):**
  - WAN: `192.168.15.4`
  - LAN: `192.168.40.1` (Kali Attacker)
  - IT Dept: `192.168.50.1` (Wazuh Manager)
  - DMZ: `192.168.60.1` (Ubuntu + Windows 10 Servers)
- **Tools Deployed:**
  - pfSense – Network firewall & routing.
  - Wazuh Manager – SOC monitoring tool.
  - Wazuh Agents – Installed on Ubuntu & Windows 10.
  - Kali Linux – Attack simulation (SSH brute-force).

See below pfSense Network Diagram:

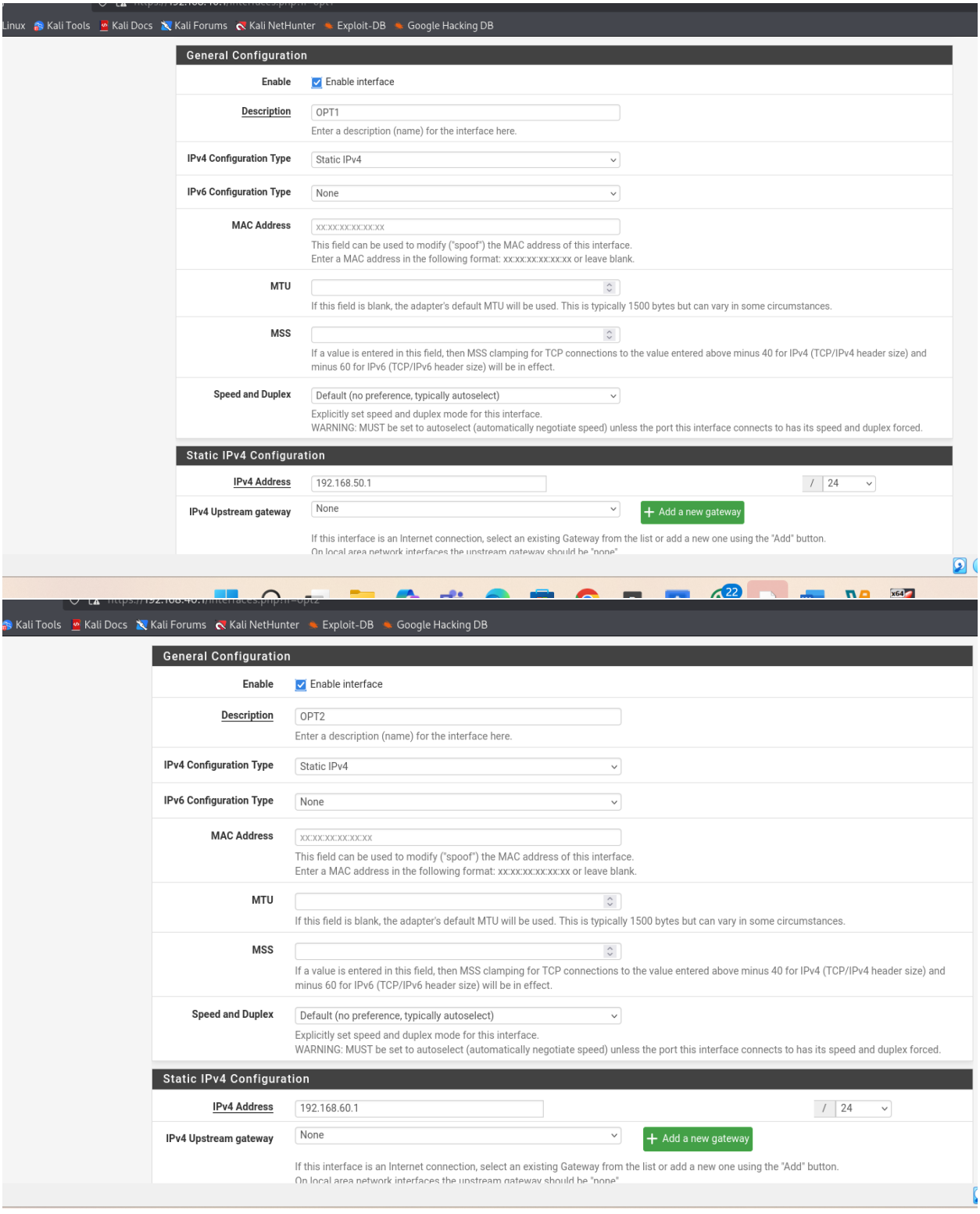


3. Execution & Evidence (Screenshots)

The following key activities were documented with screenshots:

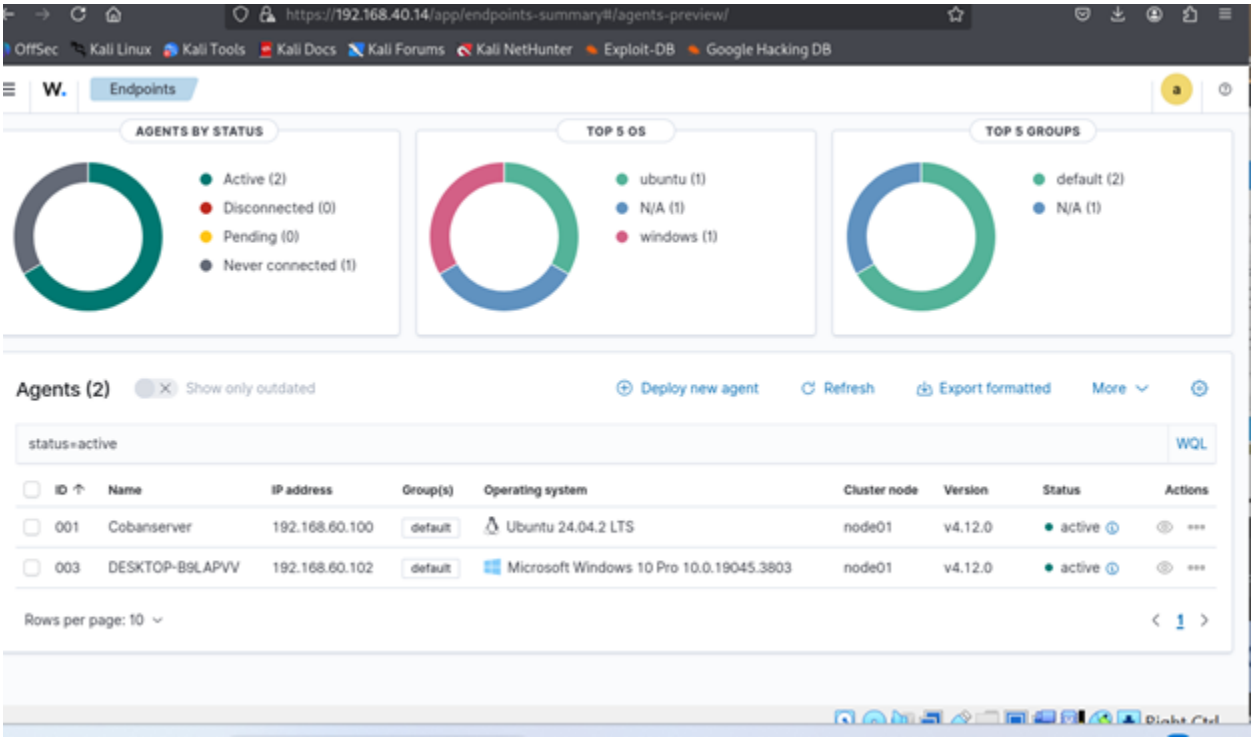
1. **pfSense Configuration:** Static IP assignments and firewall rules.

   See below screenshots of static Ip assign



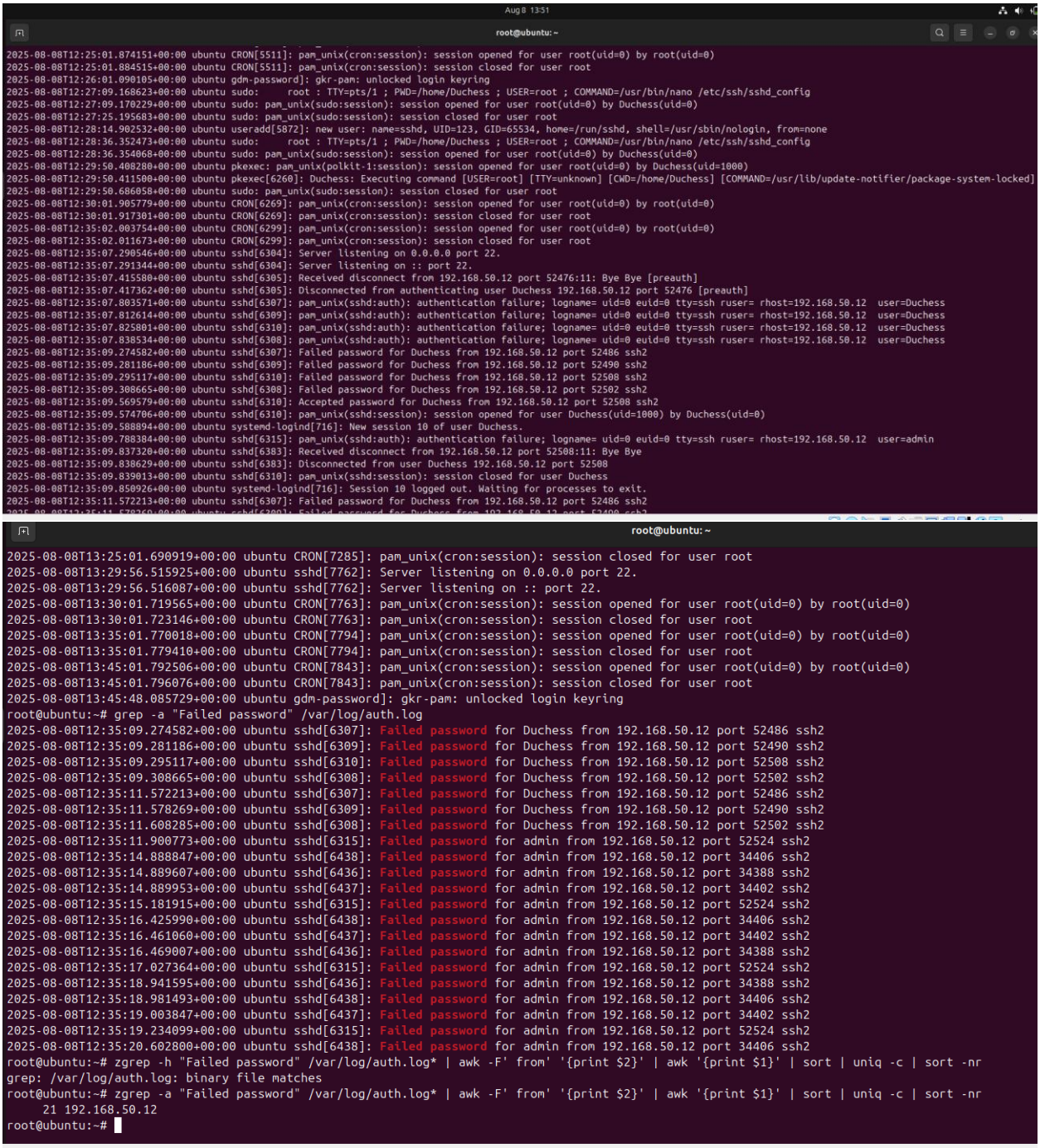
2. **Wazuh Deployment:** Manager installed; agents on Ubuntu & Windows connected successfully.

See below screenshot of wazuh dashboard with ubuntu and windows server active



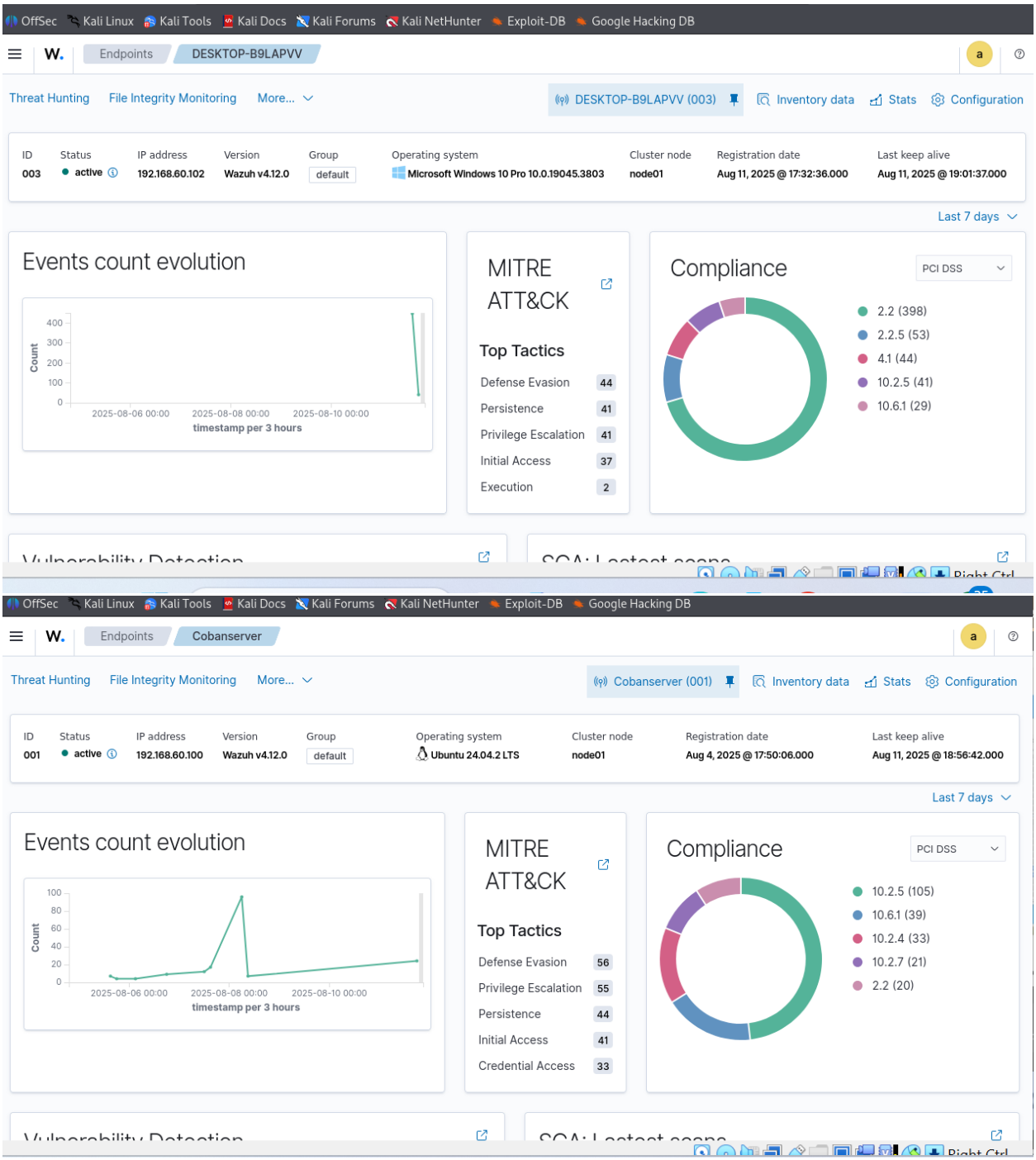
3. **Attack Simulation (Kali):** SSH brute-force attempts against Ubuntu DMZ server.

   See below screenshots of logs from SSH attack from kali

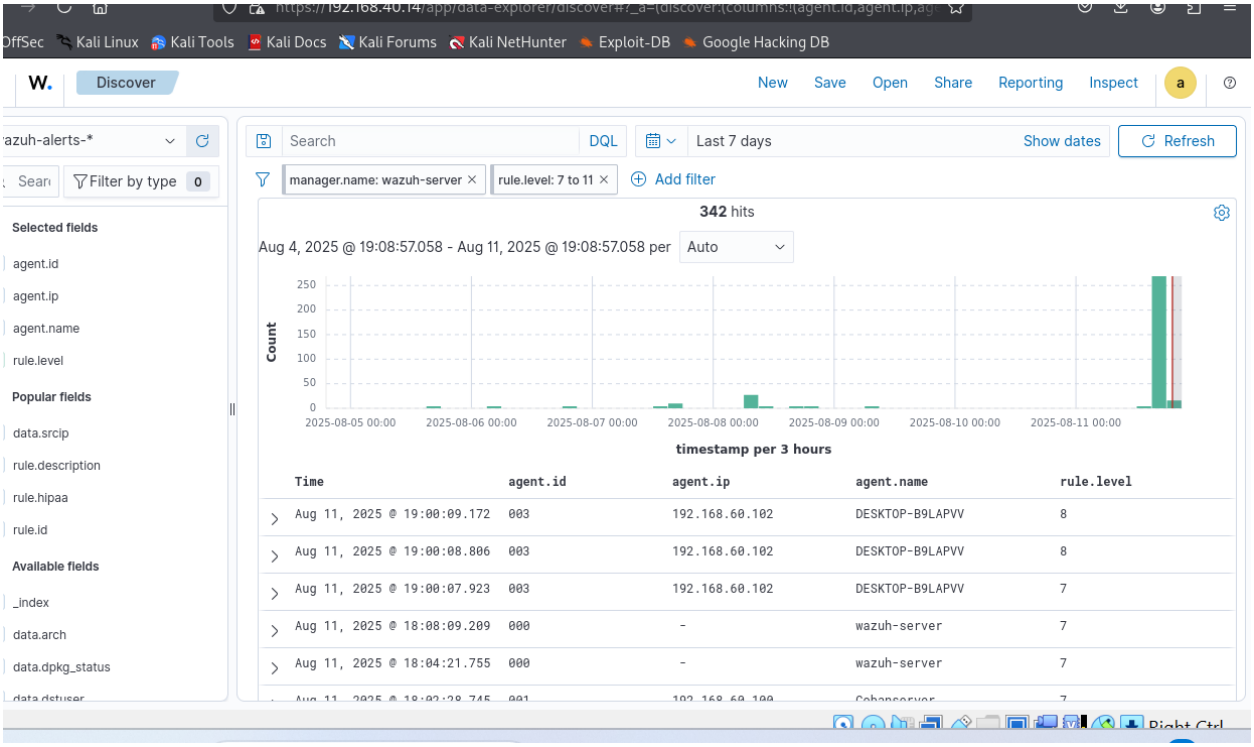


4. **Log Collection & Correlation:** Logs collected from Linux and Windows, correlated in Wazuh.

   See below screenshots of auth.log



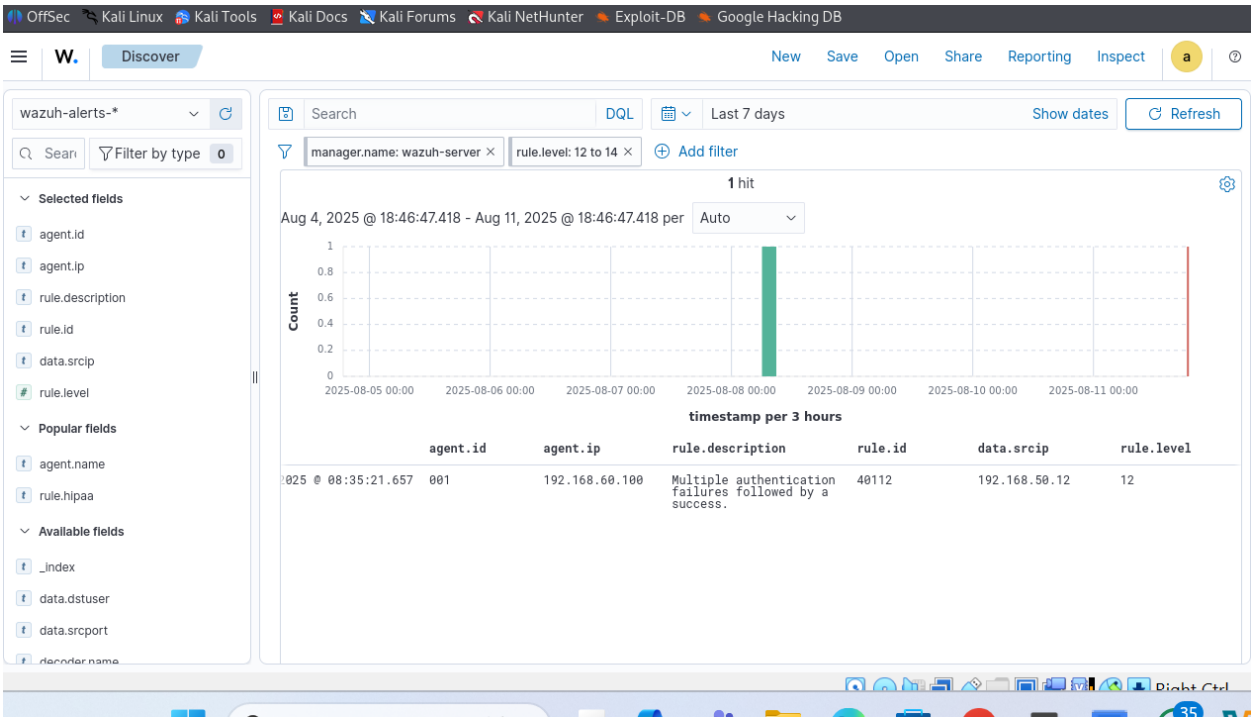
5. **Detection & Alerts:** Wazuh dashboard showed brute-force alerts with attacker IP, host, and attack type.
   See screenshot of wazuh alert dashboard below



4. Findings

- **Unauthorized Access Attempts:** Detected brute-force attempts from Kali to Ubuntu.
- **Log Correlation:** Wazuh correlated logs across Linux and Windows.
- **Lateral Movement Risk:** Evidence of potential LAN-to-DMZ attack path.

See screenshot of suspicious activity captured by wazuh below



5. Lessons Learned

1. Centralized Log Monitoring is critical.
2. Segmentation limits attack surface.
3. Simulated attacks improve SOC readiness.
4. Multi-source log correlation is essential for attack pattern detection.

6. Conclusion

The project successfully demonstrated how a SOC setup with pfSense and Wazuh can detect and analyze cyber threats in a segmented environment. Attack simulations validated the monitoring system's ability to detect brute-force attempts and highlight risks of lateral movement.

7. Recommendations

- Enhance Firewall Rules: Restrict LAN-to-DMZ access.
- Implement Account Lockout Policies: Mitigate brute-force attempts.
- Strengthen Authentication: Enforce MFA for remote logins.
- Continuous Monitoring: Keep Wazuh tuned with updated rules.
- Documentation SOP: Standardize incident reporting for quicker responses.