SIEM Use Case — Incident Report

Incident Report: Brute-force SSH Attempts

Project: SIEM Use Case Implementation (Wazuh)
Author: Hassan Zannoon
Date: 2025-12-09

Summary
Detected multiple failed SSH authentication attempts against host 192.168.56.10. Wazuh rule triggered after 7 failures within 10 minutes, indicating a likely brute-force attempt from external IP 203.0.113.55.

Timeline
- 2025-12-08 02:12 IST — First failed attempt observed.
- 2025-12-08 02:15 IST — Additional failed attempts; rule threshold reached.
- 2025-12-08 02:20 IST — Alert generated and exported to alerts/alert-bruteforce.json.

Detection
- Rule ID: 100900
- Description: Multiple failed SSH authentications within a short timeframe.
- Evidence: alerts/alert-bruteforce.json, dashboards/logins.png, rawlogs/auth.log snippet

Investigation Steps
1. Confirm alert details in Wazuh dashboard and retrieve alert JSON.
2. Correlate source IP across logs (auth.log, firewall logs).
3. Check for successful logins from the same IP or user accounts.
4. Examine process list and scheduled tasks on target host for persistence indicators.
5. Collect PCAP for the timeframe if network capture enabled.

Findings
- Source IP: 203.0.113.55 (external)
- No successful logins observed.
- No unusual processes found during initial triage.
- Multiple username guesses attempted; common usernames targeted (admin, root).

Impact Assessment
- No confirmed compromise; possible reconnaissance and credential-stuffing attempts.
- Potential risk if weak passwords or exposed services present.

Containment & Remediation
- Block IP 203.0.113.55 at the firewall (temporary).
- Enforce account lockout policy and MFA for administrative accounts.
- Rotate credentials for exposed accounts and review SSH access controls.
- Ensure failures are logged and monitoring thresholds are tuned to reduce noise.

Recommendations
- Implement IP block and review authentication logs for other source IPs.
- Harden SSH (disable password auth, use keys, change default port if needed).
- Add threat intel enrichment to block listed malicious IPs automatically.

Evidence Files
- alerts/alert-bruteforce.json
- dashboards/logins.png
- rawlogs/auth.log (snippet)
- incident-report.md (this file)