Incident Report

Report Date: November 15, 2025

Incident Tracking Number: IR-LAB-001

Table of Contents

1. *Executive Summary* 3
2. *Incident Identification and Declaration* 4
3. *Triage and Initial Analysis* 5
4. *Incident Categorization and Prioritization* 6
5. *Detailed Investigation and Impact Analysis* 7
6. *Containment, Eradication, and Mitigation* 9
7. *Recovery and Restoration* 10
8. *Communication and Reporting* 11
9. *Lessons Learned and Recommendations* 12
10. *Evidence and Documentation Appendix* 14

1. Executive Summary

Content:

Between November 13 and 14, 2025, the Security Operations Center (SOC) lab detected a multi-vector cyber attack originating from the Kali Linux system (192.168.0.200). The attack consisted of a sustained SSH brute force attempt against the Ubuntu target (192.168.0.11) and repeated network reconnaissance against the Windows target (192.168.0.40). The incident was successfully detected through correlated alerts from the Wazuh SIEM and Suricata IDS. The pre-established security architecture, including the Windows Firewall and SSH authentication controls, provided automatic containment, preventing any breach or system compromise. The incident concluded on November 14, 2025, demonstrating the effectiveness of the lab's defensive monitoring but also highlighting opportunities for enhancing automated response capabilities.

2. Incident Identification and Declaration

Content:

- **Initial Detection:** The incident was initially detected on November 13, 2025 at 23:24:52 UTC by Wazuh Alert Rule 5710 on the Ubuntu target.
- **Event Description:**
    - **Ubuntu Target:** Multiple Wazuh Alert Rule 5710 - "sshd: brute force trying to get access to the system. Authentication failed." from source IP 192.168.0.200 between 23:24:52 and 23:26:52 on November 13, 2025.
    - **Windows Target:** Multiple Wazuh Alert Rule 4151 - "Multiple Firewall drop events from same source" between 23:34:55 and 23:54:29 on November 14, 2025.
- **Incident Declaration:** The events were declared a confirmed cybersecurity incident exercise on November 14, 2025 as they represented a clear, multi-pronged attack pattern across two days.
- **Declaration Criteria:** The event met the defined incident criteria per the lab's incident response policy as it involved active attempts to gain unauthorized access and perform network reconnaissance.

---

3. Triage and Initial Analysis

Content:

- **Preliminary Review:** Initial triage confirmed the alerts were true positives originating from a controlled attack simulation. The correlation of alerts across both days and systems confirmed a sustained attack campaign.
- **Initial Severity Estimation:** Based on the sustained nature of the attacks (brute force over 2 minutes and reconnaissance over 20 minutes) and the criticality of the targeted systems, the initial severity was estimated as **Medium** within the lab context.
- **Urgency of Response:** Immediate response was not required as automated security controls had already contained the threats. The focus shifted to analysis and documentation.

---

4. Incident Categorization and Prioritization

Content:

- **Incident Type:** Unauthorized Access Attempt & Network Reconnaissance.
- **Priority Level: P2 - Medium.** This incident was prioritized for analysis and process refinement, as the immediate threat was neutralized by automated controls. Resources were allocated to fully document the attack sequence and defensive effectiveness.

---

5. Detailed Investigation and Impact Analysis

Content:

- **Timeline of Events:**
    - **November 13, 2025, 23:24:52 - 23:26:52:** Sustained SSH brute force attacks from 192.168.0.200 against Ubuntu target (192.168.0.11). Three authentication failure alerts recorded over 2-minute period. ○ **November 14, 2025, 23:34:55 - 23:54:29:** Network reconnaissance (port scans) from 192.168.0.200 against Windows target (192.168.0.40). Four firewall drop alerts recorded over 20-minute period.
    - **Throughout:** Wazuh and Suricata generated immediate alerts, correlating the multi-day attack pattern.
    - **Throughout:** Windows Firewall dropped reconnaissance packets; Ubuntu SSH service rejected authentication attempts.
- **Assets and Data Impacted:**
    - **Targeted Systems:** Ubuntu Server (192.168.0.11), Windows Target (192.168.0.40).
    - **Attack Source:** Kali Linux (192.168.0.200).
    - **Data Impacted:** None. No systems were breached; no data was accessed or exfiltrated.
- **Root Cause Analysis:** The root cause was a planned simulation to test the lab's detection and response capabilities. From a defensive perspective, the attack was successful due to:
    - **Preparation (GV, ID, PR):** The comprehensive security architecture established during the **Preparation**

phase, including the 4-VM environment, Wazuh SIEM, Suricata IDS, and host firewalls.

- **Threat Actor and TTPs:**
  - **Actor:** Simulated attacker (Kali Linux).
  - **Tactics, Techniques, and Procedures (TTPs):**
    - T1110 - Brute Force (against SSH)
    - T1046 - Network Service Scanning (against SMB ports 135, 139, 445)
- **Estimated Magnitude:** The incident's magnitude is assessed as **Low**. It was a controlled simulation with no operational impact, no data loss, and successful automated containment.

---

6. Containment, Eradication, and Mitigation

Content:

- **Containment (RS.MI-01):**
  - **Short-term Containment:** Achieved automatically by pre-existing security controls.
    - **Windows Target:** Firewall automatically dropped all reconnaissance packets at 23:34:55, 23:45:48, 23:50:06, and 23:54:29 on November 14, 2025, preventing service enumeration.
    - **Ubuntu Target:** SSH service rejected brute force attempts through authentication controls at 23:24:52, 23:25:52, and 23:26:52 on November 13, 2025.
- **Eradication (RS.MI-02):**
  - The attack ceased when the simulation ended. No malicious persistence was established, so no eradication actions were needed.

---

7. Recovery and Restoration

Content:

- **Recovery Actions:** Not applicable. All systems remained fully operational throughout the incident. No restoration was required.
- **Integrity Verification:** System integrity was continuously verified through Wazuh agent checks. No deviations from the baseline were found.
- **End of Recovery:** The incident concluded with the end of the simulation on November 14, 2025. Normal operations were uninterrupted.

---

8. Communication and Reporting

Content:

- **Internal:**
  - **SOC Team:** All alerts and findings were documented in the Wazuh dashboard and project documentation (`/docs/attack-simulation.md`).
  - **Lab Management:** Findings were reported as part of the standard project review process.

---

9. Lessons Learned and Recommendations

Content:

- **Key Findings:**
  - The layered defense strategy was effective. Hostbased (Wazuh) and network-based (Suricata) detection provided complementary visibility across a multi-day attack. ○ Automated preventative controls (firewall, SSH authentication) successfully contained sustained attacks without manual intervention. ○ Alert correlation across systems provided comprehensive attack context, revealing a coordinated campaign against multiple targets.
- **Recommended Improvements (R):**
  - **R1:** Implement Active Response: Configure Wazuh active response to automatically block attacker IP addresses after 3 failed SSH authentication attempts within 2 minutes. *(Owner: SOC, Due: December 15, 2025)*
  - ○ **R2:** Enhance Monitoring: Expand Suricata rules to better detect and alert on SSH brute force patterns at the network level, providing earlier detection. *(Owner: SOC, Due: December 15, 2025)*
  - **R3:** Process Refinement: Develop and document formal playbooks for automated response to common attack patterns like brute force and reconnaissance. *(Owner: SOC, Due: December 30, 2025)*
  - **R4:** Training: Conduct regular attack simulations to maintain and improve SOC analyst proficiency in correlating multi-vector attacks. *(Owner: SOC*

Management, Due: Recurring Quarterly)

---

10. Evidence and Documentation Appendix

- **Contents:**
    - Project Issues #1-4 (Preparation Phase)
    - `/docs/wazuh-setup.md` (SIEM Configuration)
    - `/docs/suricata-setup.md` (IDS Configuration)
    - `/docs/attack-simulation.md` (Attack Timeline and Details)
    - Wazuh dashboard alerts (Rules 5710, 4151)
    - Suricata logs (`/logs/alerts.json`)

Prepared by: Jibraan Islam