Incedent Response Report

1. Executive Summary

On 12 December 2025, Wazuh detected repeated failed SSH login attempts targeting host 10.0.2.16 from source IP 10.0.2.19. The behavior matched a typical Brute-Force SSH Attempt. The attempts did not succeed and no compromise was identified. The incident was monitored, validated as low malicious probability, and mitigation recommendations were recorded for future prevention.

2. Timeline

Time	Event
2025-12-12 09:02:00	Wazuh triggers Alert ID 5503 for multiple failed SSH authentications.
2025-12-11 09:05:00	Security analyst reviews the alert and confirms pattern consistent with brute-force activity.
2025-12-11 09:15:00	Source IP reputation checked — no malicious history found.
2025-12-11 09:20:00	Verification started to determine if the source IP is internal/admin testing.
2025-12-11 09:30:00	Monitoring rule applied to track further SSH attempts. No successful logins observed.
Ongoing	Continued monitoring with conditional actions prepared (block or isolate if attempts increase).

Table 1: Timeline

3. Impact Analysis

The brute-force attempts were unsuccessful, resulting in no system compromise. However, if successful, the attack could have led to:

- Unauthorized system access
- Privilege escalation
- Data theft or modification

- Lateral movement across the internal network

Impact Rating: Medium

The system remained stable, and normal operations were not disrupted.

4. Remediation Steps

Completed / Ongoing Actions

- Continued monitoring of SSH authentication logs.
- Validation of source IP as potential internal activity.

Recommended Enhancements

- Implement Fail2Ban or similar rate-limiting to block repeated SSH failures.
- Enforce strong password policies and enable MFA for SSH access.
- Apply network segmentation or firewall rules to restrict unnecessary SSH exposure.
- Block or isolate the source IP if attempts persist or escalate.

5. Lessons Learned

- Early detection via Wazuh allowed quick identification of brute-force activity.
- Monitoring and correlation with threat-intelligence sources helped confirm low malicious probability.
- SSH services remain a common attack vector; proactive hardening and MFA can significantly reduce risk.
- Clear triage workflows ensure consistent evaluation and faster decision-making during similar incidents.

6. Summary

The alert shows repeated failed SSH login attempts from 10.0.2.19 indicating a potential brute-force attack. No successful access occurred and the system remains uncompromised. Monitoring is ongoing with recommendations to apply MFA and stronger password controls to prevent future attempts and reduce overall risk.