**Incident Response Report**

**Incident Title:** Unauthorized SSH Access Attempt  
**Date of Incident:** 13/09/2025  
**Prepared by:** Samuel Oduro Acheampong  
**Role:** Incident Responder (IR Simulation)

**1. Executive Summary**

On 13/09/2025, unusual authentication activity was detected on a Linux server within the lab environment. Multiple failed SSH login attempts were followed by a successful login from an unauthorized IP address. The incident was simulated as part of a controlled exercise to demonstrate incident detection, containment, and response procedures.

The simulated attack was successfully contained, eradicated, and lessons were documented to improve detection and response readiness.

**2. Incident Description**

* **System Affected:** Linux server (Ubuntu 20.04)
* **Type of Incident:** Unauthorized access attempt / brute force attack
* **Detection Source:** ELK SIEM (Kibana dashboards + detection rule)
* **Initial Indicator:** More than 50 failed SSH login attempts in 5 minutes, followed by a successful root login from foreign IP.

**3. Timeline of Events**

| **Time (UTC)** | **Event** | **Details** |
| --- | --- | --- |
| 10:01 | Detection | SIEM flagged excessive failed SSH attempts |
| 10:02 | Analysis | Analyst confirmed unusual source IP (not on allowlist) |
| 10:04 | Escalation | Successful root login detected |
| 10:05 | Containment | Affected server isolated from lab network |
| 10:10 | Remediation | Root account disabled, credentials rotated |
| 10:20 | Recovery | Clean server image restored, hardening applied |

**4. Root Cause Analysis**

The root cause of the incident was a weak root credential that was vulnerable to brute-force attempts. The lack of SSH hardening allowed repeated login attempts without triggering sufficient protections.

**5. Containment, Eradication, and Recovery Actions**

* **Containment:** Isolated server from the lab network, blocked malicious IP via firewall.
* **Eradication:** Disabled compromised account, wiped affected system.
* **Recovery:** Restored server from clean snapshot, enforced SSH key-based authentication, disabled root login, applied latest security patches.

**6. Impact Assessment**

* **Data Exposure:** None (controlled lab environment, no sensitive data).
* **System Downtime:** ~15 minutes (lab only).
* **Business Impact:** None (educational simulation).

**7. Lessons Learned**

* Implement account lockout policies to limit brute force attempts.
* Enable MFA for privileged accounts.
* Improve monitoring: correlation rules should detect *failed logins + successful login* from the same source within short time.
* Maintain pre-built IR playbooks to ensure faster triage and containment.

**8. Recommendations**

1. Enforce SSH hardening (disable root login, use key-based auth, limit sources).
2. Enable MFA for administrative access.
3. Develop automated alerting rules in SIEM for brute force patterns.
4. Regularly review logs for abnormal login behaviour.
5. Conduct recurring IR tabletop exercises to strengthen readiness.

**9. Supporting Evidence**

* **SIEM Screenshots:** Kibana dashboard showing login attempts and triggered alert.
* **Detection Rule:** Correlation rule JSON (included in repo).
* **Log Extracts:** Sanitized SSH log snippets showing failed/successful login patterns.

**10. Conclusion**

The exercise successfully simulated a realistic intrusion attempt and validated the incident response process. The incident was promptly detected, contained, and eradicated. Preventive measures have been identified to reduce the likelihood of recurrence.

**Disclaimer:** This report is based on a simulated incident conducted in a controlled lab environment for training and demonstration purposes. No real-world systems or data were compromised.