Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 16

Incident Response Report

1. Executive Summary

On **February 13, 2026**, a simulated security incident involving a **brute-force attack** followed by **unauthorized access** to a local user account (*victim_user*) was detected and addressed.

The incident was classified as **High Severity** because user credentials were successfully compromised, creating potential risk for further system impact.

Immediate containment actions included locking the compromised account and terminating active sessions. Remediation involved removing the affected account from the system.

2. Incident Details

- **Date & Time of Detection:** February 13, 2026 – 06:15:01 (GMT+5:30)
- **Incident Type:** Brute-Force Attack / Unauthorized Access
- **Affected Account:** *victim_user* (Linux sandbox environment)
- **Attack Vector:** Repeated failed login attempts using the su mechanism, eventually leading to successful unauthorized access

3. Incident Classification

Category	**Details**
Incident Type	Brute-Force Attack / Unauthorized Access
Attack Vector	Local Privilege Escalation / Credential Guessing via su
Severity	High
Impact	Unauthorized access to user account; potential for data exfiltration or lateral movement
Status	Closed

Justification

System logs showed multiple failed login attempts followed by a successful authentication session for *victim_user*. Since account integrity was compromised, the incident warranted a **High Severity** classification.

---

4. Incident Response Actions

The response followed a structured incident handling lifecycle:

4.1 Detection and Analysis

- Suspicious activity identified through system log analysis
- Multiple failed authentication attempts detected
- Successful unauthorized access confirmed

4.2 Containment

- The compromised account was immediately locked
- All active sessions associated with the account were terminated

4.3 Eradication

- The compromised account and associated home directory were removed
- A review of system files was conducted
- No malicious artifacts were identified beyond the simulated activity

4.4 Recovery

- The system was verified for any remaining suspicious processes
- No additional threats were detected
- System operations continued without disruption

---

5. Incident Timeline

Refer to the attached **Incident Timeline Document** for a detailed chronological record of events.

---

6. Recommendations for Preventive Security Improvements

1. **Implement Account Lockout Policies**
   Automatically lock accounts after 3–5 failed login attempts within a defined timeframe.
2. **Strengthen Password Policies**
   Enforce strong password complexity requirements and periodic password changes.
3. **Multi-Factor Authentication (MFA)**
   Add an additional authentication factor beyond passwords for critical accounts.
4. **Deploy IDS/IPS Solutions**
   Monitor and block suspicious login behavior in real time.
5. **Centralized Log Monitoring and SIEM Integration**
   Aggregate and analyze logs with real-time alerting for abnormal login patterns.
6. **Regular Security Audits and Penetration Testing**
   Identify vulnerabilities proactively before exploitation.
7. **User Awareness Training**
   Educate users about password hygiene and reporting suspicious activity.
8. **Principle of Least Privilege**
   Ensure users operate with only the permissions necessary for their roles.

---

7. Conclusion

The simulated brute-force attack and unauthorized access incident was successfully detected, contained, and eradicated. The structured incident response process proved effective in minimizing risk and maintaining system integrity.

Implementing the recommended preventive controls will significantly strengthen protection against similar credential-based attacks in the future.