**Incident Documentation Report**

**1. Incident Overview**

* **Incident Name:** [Short, descriptive title]
* **Date & Time Detected:** [MM/DD/YYYY - HH:MM AM/PM]
* **Reporter Name:** [Your Name]
* **Team Member(s) Involved:** [Names of those who worked on it]
* **Incident Category:** [Exploitation, Malware, Unauthorized Access, DoS, etc.]

**2. Incident Details**

* **Description of Incident:**  
  [Briefly describe what happened, e.g., "Unauthorized SSH login attempt detected from IP 192.168.1.10."]
* **Systems Affected:**
  + Hostname(s): [e.g., WebServer01, DBServer02]
  + IP Address(es): [e.g., 10.0.0.5, 192.168.1.20]
  + Service(s) Impacted: [e.g., Email, Web, Database]
* **Indicators of Compromise (IoCs):**
  + [List suspicious logs, file changes, unexpected processes, etc.]
  + [E.g., "Multiple failed login attempts on SSH from external IP."]

**3. Response Actions Taken**

* **Detection Method:** [e.g., SIEM alert, log review, IDS/IPS]
* **Mitigation Steps:**
  + [Step 1: E.g., "Blocked malicious IP on firewall."]
  + [Step 2: E.g., "Reset compromised user credentials."]
  + [Step 3: E.g., "Patched vulnerability in Apache Web Server."]

**4. Impact Assessment**

* **Data Compromised?** [Yes/No, details if Yes]
* **System Downtime?** [Yes/No, duration if Yes]
* **Business Impact Summary:**  
  [E.g., "Website was offline for 15 minutes, potential loss of customer transactions."]

**5. Lessons Learned & Future Recommendations**

* **Root Cause Analysis:** [Explain how the attack happened]
* **Preventative Measures:**
  + [E.g., "Implement stricter firewall rules."]
  + [E.g., "Enforce 2FA for SSH logins."]
  + [E.g., "Increase log monitoring frequency."]

**6. Supporting Evidence**

* **Log Excerpts:** [Paste relevant log entries]
* **Screenshots:** [Attach if applicable]
* **Additional Notes:** [Anything else worth mentioning]

**Report Completed By:** [Your Name]  
**Date/Time Submitted:** [MM/DD/YYYY - HH:MM AM/PM]