**Incident Report Analysis**

**1. Summary of the Security Event**

* **Event:** A Distributed Denial of Service (DDoS) attack disrupted the organization's internal network for two hours.
* **Cause:** The attack was caused by a flood of ICMP packets sent by a malicious actor through an unconfigured firewall.
* **Impact:** Internal network services were unavailable for two hours, affecting normal business operations. No internal network traffic could access resources during the attack.
* **Response:** The incident management team blocked incoming ICMP packets, stopped non-critical network services, and successfully restored critical services.

**2. Identify**

* **Type of Attack:** Distributed Denial of Service (DDoS) attack using ICMP flood.
* **Impacted Systems:** The entire internal network was compromised, specifically due to a vulnerability in the firewall configuration that allowed the ICMP flood to overwhelm the network.

**3. Protect**

* **Protection Plan:**
  + **Update Firewall Rules:** Implement a new firewall rule to limit the rate of incoming ICMP packets, preventing future ICMP flood attacks.
  + **Source IP Verification:** Configure the firewall to verify the source IP addresses of incoming packets, reducing the risk of IP spoofing.
  + **Staff Training:** Conduct regular training for the IT staff on cybersecurity best practices, including firewall configuration and maintenance.
  + **Regular Audits:** Schedule regular security audits of the network infrastructure to identify and rectify potential vulnerabilities, such as misconfigured firewalls or outdated security protocols.

**4. Detect**

* **Detection Methods:**
  + **Network Monitoring:** Deploy network monitoring software to continuously monitor traffic patterns and detect anomalies, such as unusual ICMP traffic, in real-time.
  + **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** Implement IDS/IPS solutions to filter out suspicious ICMP traffic and respond automatically to detected threats.
  + **Regular Log Reviews:** Establish a routine for reviewing network logs to identify any unusual activity, such as repeated attempts to flood the network with ICMP packets.

**5. Respond**

* **Response Plan:**
  + **Incident Containment:** Immediately block incoming ICMP traffic at the firewall when an attack is detected to contain the threat and prevent further disruption.
  + **Neutralization Procedures:** Temporarily shut down non-essential services to minimize network load and focus resources on maintaining critical services.
  + **Incident Analysis:** After neutralizing the threat, analyze logs and other data to understand the attack vector, identify the attacker, and document lessons learned.
  + **Communication Protocol:** Establish a clear communication protocol for notifying stakeholders about the incident, including its impact and the measures taken to resolve it.

**6. Recover**

* **Recovery Plan:**
  + **System Restoration:** Restore all network services to normal operation and verify that the firewall and other network devices are properly configured.
  + **Data Integrity Verification:** Ensure that no data was compromised during the attack and that all critical information is intact.
  + **Post-Incident Review:** Conduct a thorough post-incident review to assess the effectiveness of the response and recovery efforts, identifying any gaps that need to be addressed.
  + **Process Improvements:** Update the organization's incident response and recovery procedures based on insights gained from handling this incident to better prepare for future events.