**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | **Security Event:** A Distributed Denial of Service (DDoS) attack occurred, targeting the company’s network by flooding it with ICMP packets, which caused the network services to become unresponsive for two hours.  **Cause:** The attack exploited a vulnerability in an unconfigured firewall, allowing an overwhelming amount of ICMP traffic into the network.  **Impact:** The internal network was down for two hours, disrupting business operations, potentially leading to loss of revenue and customer trust.  **Response:** The incident management team mitigated the attack by blocking incoming ICMP packets, shutting down non-critical services, and restoring critical network functions. | | |
| --- | --- | --- | --- |
| Identify | **Type of Attack:** The attack was a Distributed Denial of Service (DDoS) attack specifically targeting the network with ICMP packet flooding.  **Affected Systems:** Internal network systems, including web servers, application servers, and potentially any services relying on network connectivity were affected by the attack. | | |
| Protect | **Firewall Configuration:** Ensure all firewalls are properly configured to handle ICMP traffic and other types of network traffic.  Rate Limiting: Implement rate limiting on all incoming ICMP packets to prevent future DDoS attacks.  **Access Controls:** Review and update access controls to ensure only authorized personnel can modify network settings.  Training: Conduct regular security training for IT staff on DDoS prevention and response strategies. | | |
| Detect | **Monitoring and Analysis:**   * **Network Monitoring:** Use network monitoring software to detect unusual traffic patterns, such as a sudden increase in ICMP packets. * **Intrusion Detection/Prevention Systems (IDS/IPS):** Deploy IDS/IPS to filter out malicious traffic based on known attack signatures and patterns. * **Traffic Analysis:** Regularly analyze network traffic logs to identify any signs of probing or other suspicious activities. * **User Activity Monitoring:** Implement monitoring tools to track user activity and detect unauthorized access or abnormal behaviors. | | |
| Respond | **Response Plan:**   * **Incident Containment:** Immediately isolate affected systems to prevent the spread of an attack. For DDoS attacks, block or throttle incoming traffic from suspicious sources. * **Neutralization:** Use the IDS/IPS and firewall rules to stop the attack in real-time. * **Analysis:** Collect and analyze logs, network traffic, and other data to understand the nature of the attack and identify the source. * **Communication:** Notify relevant stakeholders, including management and potentially affected customers, about the incident and the steps being taken to address it. | | |
| Recover | **Recovery Steps:**   * **Data Restoration:** Ensure that all critical data is backed up regularly and that backup systems are functioning correctly to allow quick recovery. * **System Restoration:** Restore affected systems from clean backups or images to ensure no malicious code remains. * **Service Resumption:** Gradually bring systems back online, starting with the most critical services. * **Post-Incident Review:** Conduct a post-incident review to assess the effectiveness of the response and identify areas for improvement in the recovery process. | | |

### **Summary of Recommendations**

Based on the analysis, here are the key recommendations:

* **Enhance Firewall Security:** Implement stricter firewall rules and regularly audit configurations.
* **Improve Monitoring:** Invest in advanced network monitoring tools and regularly update IDS/IPS signatures.
* **Develop a Comprehensive Incident Response Plan:** Ensure all team members are trained and the plan is tested regularly.
* **Regular Backups and Disaster Recovery Testing:** Regularly back up data and test disaster recovery processes to ensure they work effectively.

| Reflections/Notes: |
| --- |