**Incident report analysis**

|  |  |
| --- | --- |
| Summary | Summary  A DDoS attack targeting the company’s network flooded it with ICMP packets, causing a two-hour disruption. The attack exploited an unconfigured firewall, allowing malicious traffic to enter. After mitigation efforts, the team implemented firewall rules, source IP verification, network monitoring tools, and an IDS/IPS system to prevent future occurrences. |
| Identify | Security Risks Identified:   * Unconfigured firewall allowed ICMP traffic from unverified sources. * Lack of ICMP rate-limiting exposed the network to packet floods. * Absence of effective monitoring to detect abnormal traffic early.   Action Steps:   * Conduct regular firewall audits. * Perform vulnerability scans across internal network assets. * Review access privileges and network segmentation. |
| Protect | Mitigation Techniques:   * Implement firewall rules to rate-limit ICMP packets. * Enable source IP verification to block spoofed traffic. * Train staff to identify early symptoms of DDoS attacks.   Policies/Procedures:   * Update and enforce firewall configuration standards. * Maintain a documented incident response protocol. |
| Detect | Improvements Made:   * Installed network monitoring tools to flag traffic anomalies. * Deployed IDS/IPS systems to analyze and block suspicious ICMP packets.   Ongoing Actions:   * Set up alert thresholds for DDoS-like traffic. * Log and analyze incoming traffic patterns continuously. |
| Respond | Response to Incident:   * Blocked all incoming ICMP packets. * Shut down non-critical services to preserve bandwidth. * Restored critical services once the threat was contained.   Process Improvements:   * Review and revise the incident response plan. * Conduct post-incident briefings to improve future coordination. |
| Recover | Recovery Actions:   * Restored affected services to normal operation. * Verified system integrity and no residual threats. * Maintained communication with stakeholders during recovery.   Future Planning:   * Schedule DDoS simulation drills. * Maintain backup configurations for rapid system restore. |

|  |
| --- |
| Reflections/Notes: This event emphasized the need for proactive firewall configuration and continuous network monitoring. Future incidents can be reduced by strengthening the detection phase and ensuring misconfigurations are caught during audits. Aligning with the NIST CSF offers a clear, phased approach to both response and long-term improvement. |