Incident report analysis

Summary	DDoS using ICMP Flooding
Identify	External malicious actor exploiting an unconfigured firewall.
Protect	**Immediate Action Plan:** **1. Firewall Configuration:** ○ **Implement rate-limiting rules for ICMP traffic to prevent flooding.** ○ **Enable source IP address verification to detect and block spoofed IP addresses.**
Detect	**Monitoring and Detection Improvements:** 1. **Network Monitoring Software:** ○ Deploy advanced network monitoring tools to detect abnormal traffic patterns in real-time. 2. **Intrusion Detection and Prevention Systems (IDS/IPS):** ○ Use IDS/IPS to filter out suspicious ICMP traffic and other malicious activity. 3. **Log Analysis:** ○ Implement a Security Information and Event Management (SIEM) system to analyze network logs and identify potential threats. 4. **User Activity Monitoring:** ○ Track authorized and unauthorized user activity to detect

	unusual behavior.
Respond	1. **Containment:** ○ Immediately isolate affected systems to prevent the spread of the attack. ○ Block malicious traffic at the firewall level. 2. **Neutralization:** ○ Disable non-critical services to restore critical operations. ○ Use IDS/IPS to filter out malicious traffic. 3. **Analysis:** ○ Collect and analyze network logs, firewall logs, and IDS/IPS alerts to understand the attack vector and impact. ○ Document the incident for future reference and improvement. 4. **Improvement:** ○ Update incident response procedures based on lessons learned. ○ Conduct post-incident reviews to identify gaps in the response process.
Recover	**covery Steps:** 1. **System Restoration:** ○ Restore affected systems to normal operation using backups and redundancy measures. 2. **Data Recovery:** ○ Ensure all critical data is recovered and verified for integrity. 3. **Process Improvement:** ○ Update recovery processes to reduce downtime in future incidents.

	○ Implement automated backup and recovery solutions. 4. **Communication:** ○ Notify stakeholders of the incident and the steps taken to resolve it. ○ Provide regular updates on recovery progress.

Reflections/Notes:**Reflections/Notes:**

- The incident highlighted the importance of proper firewall configuration and network monitoring.
- Implementing rate-limiting rules and IP address verification significantly reduced the risk of similar attacks.
- Regular security audits and employee training are essential to maintaining a strong security posture.
- The organization should invest in advanced monitoring tools and automated response systems to improve detection and recovery times.