Incident report analysis

Summary	1. The company has experienced Distributed Denial of Service attack. Significant amount of ICMP pings have been sent, which resulted in making the network services unresponsive for two hours. 2. The root cause of the attack was the firewall that haven't been configured, and didn't filter, or restrict the overflooding traffic. 3. The attack affected the users' and employee access, and the service availability. 4. The incident was resolved by setting a limit for the rate of ICMP packets, checking for spoofed IP addresses on the incoming ICMP packages, implementing software to detect abnormal traffic, and IDS/IPS system to filter the suspicious traffic.
Identify	1. Type of attack – DDoS – ICMP flood attack 2. Impacted systems: Internal network, web servers, network services, firewall 3. Processes impacted – the whole system – the internal network services, the customer facing apps, critical servers were unresponsive due the attack.
Protect	1. Update firewall rules to limit and filter ICMP traffic 2. Schedule regular firewall audits and pen testing. 3. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets 4. A new firewall rule to limit the rate of incoming ICMP packets 5. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics 6. Conduct regular training to the IT and security teams on identifying DDoS vulnerabilities.

Detect	1. Deploy software to monitor the network and detect malicious patterns in the traffic. 2. Implement SIEM tools to generate warnings for potential DDoS attempts. 3. Set up IDS/IPS system to alert abnormal traffic. 4. Implement log monitoring to flag unusual ICMP traffic.
Respond	1. Establish and document a formal DDoS incident response plan. 2. Define team roles and escalation paths for responding to DDoS events. 3. Utilize firewall controls and network segmentation to isolate and mitigate attacks in progress. 4. Perform a post-incident analysis after every major event to identify root causes and adjust defenses. 5. Communicate incident details and action steps to stakeholders, including leadership and affected employees.
Recover	1. Restore full network functionality after verifying firewall rules and service health. 2. Check system integrity to ensure no configuration or data corruption occurred during the attack. 3. Document the full timeline of the incident, including detection, response, and recovery actions. 4. Update the organization's business continuity and disaster recovery plans based on lessons learned. 5. Schedule a post-recovery review meeting with all involved teams to share findings and improvements.

Reflections/Notes: The DDoS incident shows critical gaps in the organization's network security, especially in the firewall configuration and the effective traffic monitoring. The incident shows that even small gaps in the configuration can lead to serious system disruptions due to malicious attacks.
Implementing different software, IDS/IPS system, reconfiguring the firewall, conducting regular audits

strengthens the security posture, but additional measures should be taken to protect the system. Regular training and updates should be done, port filtering can be applied to lower the attack surface, regular log check-ups to check for different threats and weak spots of the system, that should be resolved.
The organization should prioritize a culture of security awareness, regular testing (such as simulated attacks or penetration tests), and transparent communication between teams and leadership during incidents.