Incident report analysis

Summary	For two hours, the company experiences a DDoS to their internal network. This caused the company's network services to go down and rendered usable until resolved. The attack was a flood of ICMP packets that used up all of the network's resources. The incident management team started by blocking all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. After the cybersecurity team investigated the event, they found that the malicious actor overwhelmed the network by sending a flood of ICMP pings through an unconfigured firewall. The network security team then implemented these security hardening methods. ● A new firewall rule to limit the rate of incoming ICMP packets ● Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets ● Network monitoring software to detect abnormal traffic patterns ● An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Identify	After the security/network team audited the network and systems, they found that the vulnerabilities in the firewall were taken advantage of by a malicious actor to send a flood of ICMP pings through an unconfigured firewall. They also audited the systems that were affected and recovered, checking for integrity and confidentiality.
Protect	Concerning this issue, there should be regular maintenance and configuration to the network's firewall and security devices, hubs, switches, routers,etc. The company's resolution time is also quite an issue, two hours of the company's operational time to be down and possibly costing the company revenue. Regular IT training for the staff, employees and especially the security teams,

	no use of playbooks seemed to be used.
Detect	To detect further firewall intrusion, IP spoofing and similar attacks, an Intrusion Detection System can be used to detect and alert security teams. An Intrusion Prevention System can also be used to take action against intrusive and suspicious activity and stop the activity. To monitor and detect log data a Security Information and Event Management tool (SIEM) can be used so the network team can closely monitor suspicious activity.
Respond	An action plan for the DFIR team could be to log this event into a playbook, include ways to improve and how others should respond when under similar attacks. Superiors and company stakeholders should be first made aware of the attack and the current procedures being made to mitigate/stop the attack. When the attack was first made aware, teams made sure to stop the ICMP pings, suspend affected network services, then recover them after resolution.
Recover	The team recovered affected services by temporarily suspending them offline, then resuming operation after resolution of the incident.