Incident report analysis

Summary	The organization experienced a DDoS attack, specifically an ICMP flood attack compromising internal networks for two hours until it was resolved. During the attack, the organization's network services suddenly stopped responding due to an incoming flood of ICMP packets, hindering normal internal network traffic's access to any and all resources.
Identify	The cybersecurity team's investigation found that a malicious actor has sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	To address this security event, the network security team implemented: ● 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
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool, network monitoring software and IDS to monitor all incoming traffic from the internet.
Respond	The team configured its firewalls and adopted various other network hardening measures to safeguards its network

Recover	The team ensured that all systems are clean and brought back online. The attack was documented and gave a key on how to respond, secure and maintain its network. The team also adopted continuous monitoring to improve future incident detection and response.

Reflections/Notes: