Incident report analysis

Summary	The organization's internal network was compromised for two hours due an DDoS attack. The network services suddenly stopped responding due an incoming flood of ICMP packets and normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The cybersecurity team investigated the event and found out that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. The entire network was affected. All critical network resources needed to be secured and restored to a functioning state.
Protect	To address the occurred event the company's cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and a IDS/IPS to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns.
Respond	For future security events the cybersecurity team will isolate the affected areas to control it and prevent other areas from being disrupted. They will attempt to restore any system and services that were disrupted by the event. Then, the team will analyze the network logs looking for suspicious and abnormal activity

	and report all the found incidents to a superior management, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored and back to a normal functioning state. To prevent future external ICMP flood attacks it can be blocked by a Firewall. Then, all non-critical network services should be temporarily stopped to reduce internal network traffic since critical network services should be prioritized and restored. Once the ICMP packets have diminished, all remaining non-critical network systems and services can be brought back online to ensure full operational recovery.

Reflections/Notes: Continuous monitoring and security updates should be implemented to prevent future attacks.