Incident report analysis

Summary	DDoS attack compromised internal network causing it to stop suddenly. The attack was caused by an incoming flood of ICMP packets through an unconfigured firewall, causing normal internal network traffic to be unable to be accessed by any network resources. Incident response team stopped all non-critical network services offline and blocked incoming ICMP packets.
Identify	ICMP flood attack through attacking incorrectly configured firewall causing the entire internal network to go down. All critical network resources needed to be secured and restored.
Protect	Stopping all non-critical network services offline by blocking incoming ICMP packets resolved the issue. This was done by implementing a new firewall rule to limit the rate of incoming ICMP packets. Additionally, IDS/IPS system can be implemented to filter ICMP traffic.
Detect	Team configured source IP address verification on the firewall, checking for spoofed IP addresses. Also, IDS/IPS were implemented to detect these problems in the future
Respond	In the future, the team will isolate affected systems and restore any critical systems and services as well as analyzing network logs to check for abnormal activity.
Recover	Access to network services need to be restored following a DDoS attack. External ICMP flood attacks can be blocked at the firewall. Afterwards, non-critical network services should be stopped to reduce network traffic and critical network services should be restored. Once ICMP packets that are flooding in have timed out, all non-critical network systems and services can be brought online again.