Incident report analysis

Summary	A flood of ICMP packets came into the network through an unconfigured firewall, overwhelming the network. The ICMP packets stopped normal internal network traffic from accessing network resources for 2 hours. The team blocked the attack, stopped all non-critical services and restored critical services.
Identify	The attack was a distributed denial of service (DDoS) attack that prohibited those with access to the network from utilizing network resources and critical network services.
Protect	The team has configured the firewall with rules that limit the rate of incoming ICMP packets and that verify the source IP of all incoming ICMP packets to check for spoofed IP addresses. Furthermore, an IDS/IPS system has been implemented to filter out suspicious ICMP traffic.
Detect	To detect and monitor incoming ICMP packets in the future, the team has implemented a source IP verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	Access to the network must be restored to normal functionality and all non-critical network services will need to be stopped to reduce internal network traffic. Those network services which are critical to operations will need to be restored first and then once the ICMP packets have timed out, non-critical functions can be restored again.