Incident report analysis

Summary	The company recently faced a disruptive DDoS attack. The incident, lasting two hours, was triggered by a flood of ICMP pings exploiting an unconfigured firewall. The incident management team responded promptly by blocking ICMP packets, taking non-critical services offline and restoring critical services. Subsequent investigation revealed the need for improvements in network security.
Identify	A malicious actor or actors specifically targeted the company with an ICMP flood attack, impacting the entire internal network. The focus was on securing and restoring all critical network resources to normal functionality.
Protect	To enhance protection measures, the cybersecurity team introduced a new firewall rule limiting the rate of incoming ICMP packets. Additionally, an IDS/IPS system was implemented to filter out specific ICMP traffic based on suspicious characteristics.
Detect	Implementing source IP address verification on the firewall for incoming ICMP packets became a critical detection enhancement. Network monitoring software was also deployed to identify abnormal traffic patterns.
Respond	In preparation for future security events, the cybersecurity team outlined a proactive response plan. This involves isolating affected systems to prevent further network disruption, restoring disrupted critical systems and services, analyzing network logs for suspicious activity and promptly reporting incidents to upper management and legal authorities if necessary.
Recover	To recover from a DDoS attack involving ICMP flooding, the company will restore access to network services to a normal functioning state. Future

	external ICMP flood attacks will be blocked at the firewall, followed by the temporary idling of non-critical network services to reduce internal traffic. Critical network services will be prioritized for restoration, and once the ICMP packet flood subsides, non-critical network systems and services can be brought back online.

Reflections/Notes: