Incident Report Analysis

Summary	The company faced a security incident where all network services abruptly became unresponsive. Upon investigation, the cybersecurity team determined that a distributed denial of service (DDoS) attack was the cause, initiated by a flood of incoming ICMP packets. To mitigate the attack, the team promptly blocked the malicious traffic and temporarily halted non-essential network services, allowing them to restore critical network operations.
Identify	The company was deliberately targeted by one or more malicious actors using an ICMP flood attack, which disrupted the entire internal network. It was crucial to secure and restore all critical network resources to ensure normal operations could resume.
Protect	The cybersecurity team introduced a new firewall rule to control the number of incoming ICMP packets and deployed an IDS/IPS system to analyze and block certain ICMP traffic that exhibited suspicious attributes.
Detect	The cybersecurity team set up source IP address verification on the firewall to detect spoofed IP addresses in incoming ICMP packets. They also installed network monitoring software to identify any unusual traffic patterns.
Respond	In future security incidents, the cybersecurity team plans to isolate affected systems to contain any further disruption to the network. They will prioritize restoring critical systems and services that were impacted. Following this, the team will review network logs to identify any signs of unusual or suspicious activity. Additionally, they will ensure that all incidents are promptly reported to senior management and, if necessary, relevant legal authorities.

Recover	To recover from an ICMP flooding DDoS attack, it's essential to restore normal operation of network services. In the future, external ICMP flood attacks can be prevented by blocking them at the firewall. To manage internal network traffic during an attack, non-critical network services should be temporarily halted. Critical network services should then be prioritized for restoration. Once the flood of ICMP packets subsides, non-critical systems and services can be safely restored.

Reflections/Notes: